EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

Which functions of an SDN architecture require southbound APIs to enable communication?

A. SDN controller and the network elements

B. management console and the SDN controller

C. management console and the cloud

D. SDN controller and the cloud

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

Thusi26 Highly Voted 4 years, 8 months ago
Software-defined southbound application program interfaces (SDN southbound APIs) are used to communicate between the SDN Controller and the switches and routers of the network.
upvoted 16 times

sull3y Highly Voted 3 years, 7 months ago
A Southbound APIs are used to enable communication between the SDN controller and the network elements (such as switches, routers, etc.) in the network. The SDN controller uses these APIs to send commands and configuration instructions to the network elements, and to receive status and other information from them. This allows the SDN controller to centrally control and manage the network elements, and to dynamically adjust the network's behavior in response to changing conditions.
upvoted 6 times

Inoraset Most Recent 1 year, 8 months ago
Southbound APIs that relay information between the controller and the individual network devices (such as switches, access points, routers, and firewalls)
upvoted 2 times

Marshpillowz 2 years, 5 months ago
Answer is 'A' as per the other responses.
upvoted 2 times

Naderelmansi 3 years, 9 months ago
southbound APIs are used to communicate between the SDN controller and the switches and routers within the infrastructure. Chapter 3. Software-Defined Networking Security and Network Programmability Official Cert Guide
upvoted 3 times

sheki2005 4 years, 3 months ago
A is correct
upvoted 3 times

Question #2 *Topic 1*

Which two request methods of REST API are valid on the Cisco ASA Platform? (Choose two.)

A. put

B. options

C. get

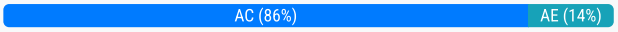
D. push

E. connect

Suggested Answer: *A, C*

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

Community vote distribution



sajoz123 Highly Voted 4 years, 1 month ago

ans is correct. Available request methods are:

GET – Retrieves data from the specified object. PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist. POST – Creates the object with the supplied information. DELETE – Deletes the specified object. PATCH – Applies partial modifications to the specified object.

upvoted 13 times

sajoz123 Highly Voted 4 years, 1 month ago

ans is correct. Available request methods are: GET – Retrieves data from the specified object. PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist. POST – Creates the object with the supplied information. DELETE – Deletes the specified object. PATCH – Applies partial modifications to the specified object.reference : https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

upvoted 13 times

abdulmalik_mail 4 years ago

reference : https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

upvoted 4 times

AkosiRomeo Most Recent 1 year, 1 month ago

A C is the correct answer

upvoted 1 times

CyberGhost666 1 year, 1 month ago

GET and PUT are the correct and valid REST API methods for Cisco ASA.

upvoted 1 times

Marshpillowz 1 year, 11 months ago

A and C are correct answers. Request Structure Available request methods are: GET – Retrieves data from the specified object. PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist. POST – Creates the object with the supplied information. DELETE – Deletes the specified object. PATCH – Applies partial modifications to the specified object.

upvoted 1 times

Anonymous983475 3 years ago

Definitely A and C sajoz123 described exactly why.

upvoted 2 times

sull3y 3 years ago

AC GET and PUT are valid request methods of REST API that can be used on the Cisco ASA Platform. GET is used to retrieve information from the server, while PUT is used to update or replace existing information on the server. The other options are not valid request methods of REST API on the Cisco ASA Platform.

upvoted 2 times

ross123 3 years, 1 month ago

Correct answer as per https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

upvoted 1 times

Naderelmansi 3 years, 3 months ago

Selected Answer: AE

The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology. All API requests are sent over HTTPS to the ASA, and a response is returned. This section provides an overview of how requests are structured, and the expected responses,

Request Structure Available request methods are:

GET – Retrieves data from the specified object. PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist. POST – Creates the object with the supplied information. DELETE – Deletes the specified object. PATCH – Applies partial modifications to the specified object.

upvoted 1 times

Naderelmansi 3 years, 3 months ago

The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology. All API requests are sent over HTTPS to the ASA, and a response is returned. This section provides an overview of how requests are structured, and the expected responses, Request Structure Available request methods are: GET – Retrieves data from the specified object. PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist. POST – Creates the object with the supplied information. DELETE – Deletes the specified object. PATCH – Applies partial modifications to the specified object.I guess you meant to write AC

upvoted 1 times

cyberwhizzy0 2 years, 8 months ago

I guess you meant to write AC

upvoted 2 times

sheki2005 3 years, 9 months ago

yes correct answers

upvoted 1 times

Question #3 *Topic 1*

The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

A. SDN controller and the cloud

B. management console and the SDN controller

C. management console and the cloud

D. SDN controller and the management solution

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

Alee86 Highly Voted 4 years, 4 months ago
Correct answer is D: SDN Controller and the management solution How Do Northbound APIs Work? Northbound APIs are the link between the applications and the SDN controller. The applications can tell the network what they need (data, storage, bandwidth, and so on) and the network can deliver those resources, or communicate what it has.
upvoted 19 times

nomanlands 3 years, 7 months ago
Selected Answer: D
D The management solution is the applications that are supporting and managing control over the network. "The Cloud" could be correct if some of those applications live in the cloud but isn't a complete answer. Applications and SDN Controller should really be an answer here because this is pretty vague and poor.

A should really be incorrect due to virtual switches and routers could live in "the cloud" but be a Southbound API so this is why I would completely remove A as an answer.
upvoted 6 times

nomanlands Highly Voted 3 years, 7 months ago
D The management solution is the applications that are supporting and managing control over the network. "The Cloud" could be correct if some of those applications live in the cloud but isn't a complete answer. Applications and SDN Controller should really be an answer here because this is pretty vague and poor. A should really be incorrect due to virtual switches and routers could live in "the cloud" but be a Southbound API so this is why I would completely remove A as an answer.In technicals term might me I am wrong we call management console when discussing for SDN network is not the correct answer should be c?
upvoted 7 times

uditpatel1 Most Recent 1 month ago
In technicals term might me I am wrong we call management console when discussing for SDN network is not the correct answer should be c?
upvoted 1 times

Marshpillowz 1 year, 11 months ago
Answer is D. Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network.
upvoted 1 times

jCho 3 years, 8 months ago
Northbound interfaces define the way the SDN controller should interact with the application plane. Applications and services are things like load-balancers, firewalls, security services and cloud resources. The idea is to abstract the inner-workings of the network, so that application developers can 'hook' into the network and make changes to accommodate the needs of the application without having to understand exactly what that means for the network. https://www.econfigs.com/ccna-7-7-c-northbound-and-southbound-apis/ A
upvoted 1 times

bassfunk 4 years, 2 months ago
The answer should be B https://www.sdxcentral.com/networking/sdn/definitions/north-bound-interfaces-api/
upvoted 1 times

LippaCippa 3 years, 10 months ago

Correct answer is D: From the official study Guide "Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the applications and the SDN controller. "

upvoted 3 times

bassfunk 4 years, 2 months ago

The answer should be B https://www.sdxcentral.com/networking/sdn/definitions/north-bound-interfaces-api/According to your website the answer should be A. Examples of the types of network applications that can be optimized via the northbound interface include load balancers, firewalls, or other software-defined security services, or orchestration applications across cloud resources.

upvoted 1 times

heamgu 4 years, 3 months ago

Answer should be A: SCOR Reference Book: Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the applications and the SDN controller. In modern environments, applications can tell the network devices (physical or virtual) what type of resources they need and, in turn, the SDN solution can provide the necessary resources to the application.

upvoted 2 times

Cock 4 years, 2 months ago

According to your website the answer should be A. Examples of the types of network applications that can be optimized via the northbound interface include load balancers, firewalls, or other software-defined security services, or orchestration applications across cloud resources.

upvoted 1 times

heamgu 4 years, 3 months ago

Answer should be A: SCOR Reference Book: Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the applications and the SDN controller. In modern environments, applications can tell the network devices (physical or virtual) what type of resources they need and, in turn, the SDN solution can provide the necessary resources to the application.Answer should be D : SDN controller and management solution as cloud is to specific and the management solution can be on prem or a cisco cloud solution. Your actually stating it in your reference: In short, northbound APIs are basically the link between the applications and the SDN controller. In modern environments, applications can tell the network devices (physical or virtual) what type of resources they need and, in turn, the SDN solution can provide the necessary resources to the application.

upvoted 2 times

NWguy 3 years, 10 months ago

Answer should be D : SDN controller and management solution as cloud is to specific and the management solution can be on prem or a cisco cloud solution. Your actually stating it in your reference: In short, northbound APIs are basically the link between the applications and the SDN controller. In modern environments, applications can tell the network devices (physical or virtual) what type of resources they need and, in turn, the SDN solution can provide the necessary resources to the application.

upvoted 1 times

beeker98106 4 years, 3 months ago

I'll go with A too. NB is basically everything but the infra components, not just the mgmt solution

upvoted 1 times

Amedeou 4 years, 5 months ago

answer should A

upvoted 2 times

Question #4 *Topic 1*

What is a feature of the open platform capabilities of Cisco DNA Center?

A. application adapters

B. domain integration

C. intent-based APIs

D. automation adapters

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

Cisco DNA Center uses Intent-Based APIs as part of its open platform capabilities.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

Intent APIs: The Intent APIs are northbound REST APIs that expose specific capabilities of Cisco DNA Center platform. The Intent APIs provide policy-based abstraction of business intent, allowing you to focus on an outcome to achieve instead of struggling with the mechanisms that implement that outcome. The APIs conform to the REST API architectural style. The APIs are simple, extensible, secure to use, and support the standard REST methods, which include the GET, POST, PUT, and DELETE operations through HTTPS.

upvoted 2 times

MPoels 1 year, 11 months ago

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-platform/2-3-7/user-guide/b-dnac-platform-ug-2-3-7/b-dnac-platform-ug-2-3-7-chapter-01.html#id_76824

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/DEVNET-2087.pdf

upvoted 1 times

samtestking 2 years, 1 month ago

Really C?

upvoted 1 times

Question #5 *Topic 1*

Refer to the exhibit. What does the API do when connected to a Cisco security appliance?

```
import requests

client_id = 'a1b2c3d4e5'

api_key = 'a1b2c3d4-e5f6-g7h8'

url = 'https://api.amp.cisco.com/v1/computers'

response = requests.get(url, auth=(client_id, api_key))

response_json = response.json()

for computer in response_json['data']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)
```

A. create an SNMP pull mechanism for managing AMP

B. gather network telemetry information from AMP for endpoints

C. get the process and PID information from the computers in the network

D. gather the network interface information about the computers AMP sees

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

uditpatel1 Most Recent 1 month ago

Based on the request URL seems Cisco AMP(Advnace Malware Protection) which is now I guess Cisco Secure Endpoint. and based on the python 'for' 'loop' gethering all endpoint's interface infromation like IPv4, IPv6 and MAC address.

upvoted 1 times

CyberGhost666 1 year, 1 month ago

The code connects to Cisco AMP using REST API and it retrieves network interface information. Correct Option is D

upvoted 3 times

00a4c44 1 year, 3 months ago

D is the answer

upvoted 1 times

corelan 1 year, 11 months ago

My choose is D

upvoted 2 times

Question #6 *Topic 1*

Which form of attack is launched using botnets?

A. TCP flood

B. DDOS

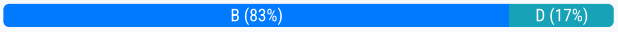
C. DOS

D. virus

Suggested Answer: *B*

Official Answer: B

Community vote distribution



pohqinan Highly Voted 4 years, 7 months ago

https://en.wikipedia.org/wiki/Botnet Correct answer DDOS

upvoted 9 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct Option is B

upvoted 1 times

sull3y 1 year, 10 months ago

B. DDOS A Distributed Denial of Service (DDOS) attack is a type of cyber attack in which multiple systems, often compromised through malware and controlled remotely by attackers, known as "botnets", flood the target website or network with a huge amount of traffic in order to overload the system and make it unavailable for legitimate users. The large number of systems participating in the attack amplifies the volume of traffic, making it very difficult for the targeted website or network to handle, resulting in a denial of service. Botnets are commonly used to launch DDoS attacks as they allow attackers to launch a much larger attack than they would be able to accomplish with a single system.

upvoted 3 times

zamkljo 1 year, 10 months ago

Botnets – Short for “robot network,” these are networks of infected computers under the control of single attacking parties using command-and-control servers. Botnets are highly versatile and adaptable, able to maintain resilience through redundant servers and by using infected computers to relay traffic. Botnets are often the armies behind today's distributed denial-of-service (DDoS) attacks. A botnet (short for “robot network”) is a network of computers infected by malware that are under the control of a single attacking party

upvoted 2 times

Marshpillowz 2 years, 4 months ago

Answer is distributed denial of service (DDOS)

upvoted 1 times

MPoels 2 years, 5 months ago

A botnet is a collection of compromised machines that the attacker can manipulate from a command-and-control (often referred to as a C2 or CnC) system to participate in a DDoS, send spam emails, and perform other illicit activities.

upvoted 1 times

royallyre20 3 years, 11 months ago

There is no TCP Flood attack.there is TCP sync flood attack which is one of DDOS attack. So answers is D

upvoted 1 times

Question #7 *Topic 1*

In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

A. smurf

B. distributed denial of service

C. cross-site scripting

D. rootkit exploit

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

Alee86 Highly Voted 4 years, 10 months ago
Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. For example the code below is written in hex: Click Here is equivalent to: Click Here Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form
upvoted 10 times

Alee86 Highly Voted 4 years, 10 months ago
Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. For example the code below is written in hex: Click Here is equivalent to: Click Here Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form
upvoted 10 times

sull3y 1 year, 10 months ago
C. cross-site scripting Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications, that allows an attacker to inject malicious code into a web page viewed by other users. One of the methods attackers use to evade detection and make the injected code more difficult to detect is by using alternate encoding, such as hexadecimal representation. This makes the code harder to read and understand, making it more difficult to detect and remove. This technique is often used in XSS attacks as it allows attackers to hide the malicious code and evade detection by security software and systems.
upvoted 5 times

CyberGhost666 Most Recent 1 year, 1 month ago
Cross-Site Scripting (XSS) is the attack where alternate encoding, such as hexadecimal or URL encoding, is most commonly observed.
upvoted 1 times

heamgu 4 years, 6 months ago
Ans: C
upvoted 2 times

abdulmalik_mail 4 years, 6 months ago
It's C
upvoted 3 times

ic0deem 4 years, 11 months ago
It could be C but why not D?
upvoted 1 times

Raajaa 5 years, 1 month ago
not sure about the correct answer for this Q
upvoted 1 times

Max95 5 years, 2 months ago

There are some common characters sets that are used in Web applications attacks. For example, Path Traversal attacks use ../ (dot-dot-slash) , while XSS attacks use characters. These characters give a hexadecimal representation that differs from normal data. https://owasp.org/www-community/Double_Encoding

upvoted 3 times

deathfrom 5 years, 2 months ago

Would somebody be able to explain why the answer is Cross Side Scripting please?A and B are wrong as related to ICMP or related network attacks

upvoted 1 times

deathfrom 5 years, 2 months ago

Would somebody be able to explain why the answer is Cross Side Scripting please?

upvoted 1 times

Seawanderer 5 years, 1 month ago

A and B are wrong as related to ICMP or related network attacks

upvoted 1 times

Question #8 *Topic 1*

Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

A. user input validation in a web page or web application

B. Linux and Windows operating systems

C. database

D. web page images

Suggested Answer: *A*

Reference: https://tools.cisco.com/security/center/resources/sql_injection

Community vote distribution

A (100%)

kudlaaaaty Highly Voted 6 years, 2 months ago

should be A

upvoted 19 times

eazy99 Highly Voted 4 years, 11 months ago

This is a tricky question, and I believe the provided answer is correct and here is why. They ask what is the flaw that caused the attacker to exploit this vulnerability? I agree that the attacker uses the web application or the user input to exploit the vulnerability, and give commands to connect to the database and get everything needed about the database. But what where is the actual flaw? Was it A. the web application and the user input? No, it's not, or it would be XSS vulnerability. The attacker leveraged a flaw in the Database, using the web application or the user input as a way to communicate with the Database and extract all the info about the database. With that being said, I believe that the provided answer is correct, and I will go with C.The database exploitation is the end result, it's not the flawThe flaw is in the web application/user input as it did not have input validation. The database.

upvoted 9 times

eazy99 4 years, 11 months ago

This is a tricky question, and I believe the provided answer is correct and here is why. They ask what is the flaw that caused the attacker to exploit this vulnerability? I agree that the attacker uses the web application or the user input to exploit the vulnerability, and give commands to connect to the database and get everything needed about the database. But what where is the actual flaw? Was it A. the web application and the user input? No, it's not, or it would be XSS vulnerability. The attacker leveraged a flaw in the Database, using the web application or the user input as a way to communicate with the Database and extract all the info about the database. With that being said, I believe that the provided answer is correct, and I will go with C.

upvoted 9 times

Dorr20 3 years, 4 months ago

The database exploitation is the end result, it's not the flaw

upvoted 4 times

otzu1 4 years, 3 months ago

The flaw is in the web application/user input as it did not have input validation. The database.

upvoted 2 times

Rockbo47 Most Recent 1 year, 10 months ago

As others have highlighted already, the "flaw" would refer to the vulnerability which in this example would be the user input validation (or lack of). https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-dcnm-sql-inj-OAQOObP.html This is also verified in the above link... "CVE-2021-1248: Cisco DCNM SQL Injection Vulnerability A vulnerability in a REST API endpoint of Cisco DCNM could allow an authenticated, remote attacker with administrative privileges to execute arbitrary SQL commands on an affected device. This vulnerability is due to insufficient validation of user-supplied input to the API. An attacker with administrative privileges could exploit this vulnerability by sending a crafted request to the API"

upvoted 3 times

itsklk 3 years, 3 months ago

Which "flaw" does. So its cause in my understanding

upvoted 1 times

nomanlands 4 years, 1 month ago

Exploiting input validation at the source and destination. It isn't a flaw within the database itself.

upvoted 3 times

tom_1991 4 years, 2 months ago

I believe the answer is C. The Database is unable to sanitize the data sent to it through the web page/application as it relies heavily on the web page/application to sanitize the code. That is the databases flaw. The attacker is leveraging the fact that the database can't do anything to prevent the attacker from sending the code. Very tricky question...

upvoted 2 times

TesterDude 4 years, 3 months ago

Exploiting no data validation

upvoted 1 times

sheki2005 4 years, 3 months ago

for me the answer is C, because you can have systems which is using web to connect into database, so all the queries are coming from web to database, the user wont exploit web but database through web, so for me I will go with Database instead of web.

upvoted 1 times

brownbear505 4 years, 5 months ago

To prevent SQL injection one means of preventing is input validation.

upvoted 1 times

elast1c 4 years, 6 months ago

definitely A

upvoted 1 times

urathod 4 years, 7 months ago

should be A

upvoted 1 times

efongvan 4 years, 7 months ago

Answer is definitely A.

upvoted 2 times

PrinM 4 years, 8 months ago

should be A

upvoted 2 times

bassfunk 4 years, 8 months ago

Answer is definitely A. Input validation is the vulnerability, not the database.

upvoted 2 times

jaciro11 4 years, 8 months ago

The answer is A

upvoted 2 times

ExamP 4 years, 11 months ago

A https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-dcnm-sql-inj-OAQOObP.html

upvoted 2 times

Raajaa 5 years, 1 month ago

I go with A

upvoted 2 times

Question #9 *Topic 1*

What is the difference between deceptive phishing and spear phishing?

A. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.

B. A spear phishing campaign is aimed at a specific person versus a group of people.

C. Spear phishing is when the attack is aimed at the C-level executives of an organization.

D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

fabio3wz Highly Voted 5 years, 6 months ago
Nope, the answer should be B. You can easily google it, and you can find that Spear phishing relates to attacks targeted to individuals. Spear phishing always focuses on one victim
upvoted 24 times

sull3y 3 years ago
B. A spear phishing campaign is aimed at a specific person versus a group of people. Deceptive Phishing is a general term used to describe any type of phishing attack that uses deception to trick the victim into providing personal information or login credentials. It can be targeted at a large group of people, indiscriminately. Spear Phishing is a targeted type of phishing attack that is aimed at a specific individual or group of people within an organization. It is more sophisticated than a general phishing attack and often uses personal information about the target to make the email or message appear legitimate. Spear phishing is also known to target specific roles or positions, such as C-level executives within an organization. Deceptive Phishing does not hijack and manipulate the DNS server of the victim and redirect the user to a false webpage, this kind of attack is called "pharming" attack.
upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago
Answer is B - spear phishing targets a specific victim (normally high-level or authoritative figure).
upvoted 1 times

royallyre20 3 years, 4 months ago
ansswer: B
upvoted 1 times

Wang87 4 years ago
Spear Phishing is targeted at one particular person who generally is C-Level but not necessarily. So correct answer is B
upvoted 2 times

efongvan 4 years, 1 month ago
Correct answer is B. https://terranovasecurity.com/spear-phishing-vs-phishing/
upvoted 1 times

eazy99 4 years, 5 months ago
The provided answer is correct B.
upvoted 2 times

myccnptest 5 years, 2 months ago
https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/ So B
upvoted 3 times

tester90 5 years, 6 months ago
Correct is C.Wrong, that is Whaling
upvoted 1 times

tester90 5 years, 6 months ago
Correct is C.
upvoted 1 times

5tuple Highly Voted 5 years, 1 month ago

Wrong, that is Whaling

upvoted 8 times

Question #10 *Topic 1*

Which two behavioral patterns characterize a ping of death attack? (Choose two.)

A. The attack is fragmented into groups of 16 octets before transmission.

B. The attack is fragmented into groups of 8 octets before transmission.

C. Short synchronized bursts of traffic are used to disrupt TCP connections.

D. Malformed packets are used to crash systems.

E. Publicly accessible DNS servers are typically used to execute the attack.

Suggested Answer: *B, D*

Reference: https://en.wikipedia.org/wiki/Ping_of_death

Community vote distribution

BD (100%)

aalnman Highly Voted 5 years, 1 month ago

B and D is correct. If you google either or both B and D you'll land on a Wikipedia page that confirms the information: https://en.wikipedia.org/wiki/Ping_of_death#:~:text=Like%20other%20large%20but%20well,the%20injection%20of%20malicious%20code.

upvoted 9 times

sull3y Highly Voted 3 years, 6 months ago

D. Malformed packets are used to crash systems. B. The attack is fragmented into groups of 8 octets before transmission. A Ping of death attack is a type of denial-of-service attack that sends malformed or oversized ping packets to a target network. The packets are typically fragmented into groups of 8 octets before transmission and when the target system reassembles the packets it can cause the system to crash or become unstable.

upvoted 6 times

MerlinTheWizard Most Recent 1 year ago

Answers are not entirely correct. The packets are not malformed - they have a valid header and valid data (8-octet long). The problem would be reassembly at the target machine - which has a vulnerability in the protocol/system/etc., but the packets themselves, despite being fragmented, are entirely valid.

upvoted 1 times

CyberGhost666 1 year, 1 month ago

These fragments are typically broken into 8-octet (8-byte) segments — because IP fragmentation offsets are measured in 8-byte units And malformed packets are used on these attacks.

upvoted 1 times

Cock 1 year, 9 months ago

The typical fragmentation size related to this attack is around 8 octets.

upvoted 1 times

testingacc 1 year, 10 months ago

B,D The "ping of death" is a network attack that sends oversized or malformed ICMP packets to crash or disrupt a target system. While it was more common in the past, most modern systems have defenses against it. This attack underscores the need for regular system updates and the use of firewalls to protect against malicious traffic.

upvoted 1 times

Marshpillowz 2 years, 4 months ago

Answers are B and D as per other responses

upvoted 1 times

c3qu1 2 years, 5 months ago

B and D is correct

upvoted 1 times

samtestking 2 years, 7 months ago

Why Choose only two?

upvoted 1 times

DarexTech100 2 years, 8 months ago

I'll th

upvoted 1 times

Question #11 *Topic 1*

Which two mechanisms are used to control phishing attacks? (Choose two.)

A. Enable browser alerts for fraudulent websites.

B. Define security group memberships.

C. Revoke expired CRL of the websites.

D. Use antispyware software.

E. Implement email filtering techniques.

Suggested Answer: *A, E*

Official Answer: AE

Community vote distribution

AE (100%)

heamgu Highly Voted 4 years ago

Answer is A and E. Reference: https://www.ncsc.gov.uk/guidance/phishing#downloads

upvoted 5 times

CyberGhost666 Most Recent 1 year, 1 month ago

A and E are the correct answers

upvoted 1 times

Marshpillowz 1 year, 10 months ago

A and E are the correct answers

upvoted 1 times

sull3y 3 years ago

A. Enable browser alerts for fraudulent websites. E. Implement email filtering techniques. Phishing attacks are attempts to trick individuals into providing sensitive information such as passwords or credit card numbers by disguising as a trustworthy entity. Two common mechanisms used to control phishing attacks are: Enable browser alerts for fraudulent websites: Some web browsers have built-in phishing filters that can detect and warn users when they visit a potentially fraudulent website. Implement email filtering techniques: Email filters can help to identify and block phishing emails from reaching the inbox by using techniques such as keyword filtering, bayesian filtering, and sender reputation analysis.

upvoted 4 times

eazy99 4 years, 5 months ago

From the options provided, the best answer is AE, we would tru to protect the employee from accessing any fraudulent websites used in the phishing emails, and try to filter emails to prevent such emails.

upvoted 3 times

Fazy 4 years, 5 months ago

AE are correct

upvoted 4 times

Sarbi 4 years, 6 months ago

B and D

upvoted 1 times

Question #12 *Topic 1*

Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting

B. water holing

C. DDoS

D. buffer overflow

Suggested Answer: *D*

Reference: https://en.wikipedia.org/wiki/Buffer_overflow

Community vote distribution

D (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

Buffer overflow is the attack most commonly associated with C and C++ due to their low-level memory management and lack of automatic safety checks.

upvoted 2 times

Marshpillowz 1 year, 10 months ago

D - buffer overflow is correct

upvoted 1 times

ama6 3 years ago

d IS cORRECT

upvoted 4 times

sull3y 3 years ago

D A buffer overflow is a type of security vulnerability that occurs when a program tries to store more data in a buffer (a temporary storage area in memory) than it can hold. This can cause the extra data to overflow into adjacent memory areas, potentially corrupting or overwriting important data or instructions. In some cases, an attacker can use a buffer overflow to execute arbitrary code or take control of a program or system. C and C++ programming languages, due to their low-level manipulation of memory, are particularly susceptible to buffer overflow attacks.

upvoted 4 times

Question #13 *Topic 1*

Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two.)

A. Check integer, float, or Boolean string parameters to ensure accurate values.

B. Use prepared statements and parameterized queries.

C. Secure the connection between the web and the app tier.

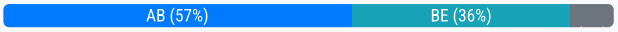
D. Write SQL code instead of using object-relational mapping libraries.

E. Block SQL code execution in the web application database login.

Suggested Answer: *A, B*

Reference: https://en.wikipedia.org/wiki/SQL_injection

Community vote distribution



sull3y Highly Voted 3 years, 6 months ago

BE Checking integer, float, or Boolean string parameters to ensure accurate values (Option A) can help prevent certain types of injection attacks, such as those that rely on unexpected input. However, it is not a comprehensive solution and can still be bypassed by a determined attacker. Using prepared statements and parameterized queries (Option B) is a more robust method of preventing SQL injection attacks. These techniques separate the data and the SQL command, preventing attackers from injecting malicious code into the SQL command. Blocking SQL code execution in the web application database login (Option E) is another robust method to mitigate SQL injection attacks. This technique ensures that no malicious SQL statements can be executed in the database. Therefore, B and E are correct answers as they are more robust methods of preventing SQL injection attacks.Option C, Securing the connection between the web and the app tier, is important for overall security, but it is not directly related to preventing SQL injection attacks. Having a secure connection ensures that the data being transmitted between the web and app tier is protected, but it does not prevent attackers from injecting malicious code into the SQL command. Option D, Writing SQL code instead of using object-relational mapping libraries, can help prevent SQL injection attacks by giving you more control over the SQL commands being executed, but it is not a guarantee. It is still possible to make mistakes in the SQL code that can lead to SQL injection vulnerabilities. Prepared statements and parameterized queries (Option B) is a more robust method of preventing SQL injection attacks, regardless of whether you are using an ORM library or writing raw SQL code. In summary, B and E are the best options for preventing SQL injection attacks. While C and D may improve overall security, they do not directly address SQL injection vulnerabilities.

upvoted 11 times

sull3y Highly Voted 3 years, 6 months ago

BE Checking integer, float, or Boolean string parameters to ensure accurate values (Option A) can help prevent certain types of injection attacks, such as those that rely on unexpected input. However, it is not a comprehensive solution and can still be bypassed by a determined attacker.

Using prepared statements and parameterized queries (Option B) is a more robust method of preventing SQL injection attacks. These techniques separate the data and the SQL command, preventing attackers from injecting malicious code into the SQL command.

Blocking SQL code execution in the web application database login (Option E) is another robust method to mitigate SQL injection attacks. This technique ensures that no malicious SQL statements can be executed in the database.

Therefore, B and E are correct answers as they are more robust methods of preventing SQL injection attacks.

upvoted 11 times

sull3y 3 years, 6 months ago

Option C, Securing the connection between the web and the app tier, is important for overall security, but it is not directly related to preventing SQL injection attacks. Having a secure connection ensures that the data being transmitted between the web and app tier is protected, but it does not prevent attackers from injecting malicious code into the SQL command. Option D, Writing SQL code instead of using object-relational mapping libraries, can help prevent SQL injection attacks by giving you more control over the SQL commands being executed, but it is not a guarantee. It is still possible to make mistakes in the SQL code that can lead to SQL injection vulnerabilities. Prepared statements and parameterized queries (Option B) is a more robust method of preventing SQL injection attacks, regardless of whether you are using an ORM library or writing raw SQL code. In summary, B and E are the best options for preventing SQL injection attacks. While C and D may improve overall security, they do not directly address SQL injection vulnerabilities.

upvoted 2 times

MerlinTheWizard Most Recent 1 year ago

Again, misleading answers. A is correct-ish, since that is basically input validation but it's not sufficient to validate these 3 types. B is text-book solution, but the parameterized queries are misleading - having a parameterized query is what is actually allowing sql injection to happen, the prevention happens at the input validation that is required by the parameterized queries. E is also correcty.

upvoted 3 times

CyberGhost666 1 year, 1 month ago

Correct choices are A and B

upvoted 2 times

Cock 1 year, 9 months ago

Not only dealing with web application

upvoted 2 times

certtaker202 1 year, 10 months ago

A. Input sanitization is a must to mitigate SQL injection B. By using prepared statements and parameterized queries, you don't execute SQL statements introduced in the SQLi vulnerable form

upvoted 1 times

davedavedave 1 year, 10 months ago

B AND E SQL Injection is best prevented through the use of parameterized queries. FROM: https://cheatsheetseries.owasp.org/cheatsheets/Query_Parameterization_Cheat_Sheet.html

upvoted 3 times

Cokamaniako 1 year, 10 months ago

Answer A and B Parameterized statements Main article: Prepared statement With most development platforms, parameterized statements that work with parameters can be used (sometimes called placeholders or bind variables) instead of embedding user input in the statement. A placeholder can only store a value of the given type and not an arbitrary SQL fragment. Hence the SQL injection would simply be treated as a strange (and probably invalid) parameter value. In many cases, the SQL statement is fixed, and each parameter is a scalar, not a table. The user input is then assigned (bound) to a parameter Pattern check Integer, float or boolean, string parameters can be checked if their value is valid representation for the given type. Strings that must follow some strict pattern (date, UUID, alphanumeric only, etc.) can be checked if they match this pattern.

upvoted 2 times

Marshpillowz 2 years, 4 months ago

B and E are correct as per sull3y's response

upvoted 1 times

nep1019 3 years ago

According to Cisco's documentation: https://tools.cisco.com/security/center/resources/sql_injection.html B and C are correct: Parameterized queries in ASP.NET, prepared statements in Java, or similar techniques in other languages should be used comprehensively in addition to strict input validation. Application layer protocol inspection performs deep packet inspection of traffic that transits the firewall. Using application layer protocol inspection on Cisco firewalls to mitigate SQL attacks against web servers is discussed in Cisco TAC Security Podcast Episode #16. Only way to do the second, imo, is to secure the connection between the web and app tier (Application layer protocol inspection)Changing back to A and B based on this statement that comes at the beginning of the section on mitigating these attacks: The primary approaches include validation of user-supplied data, in the form of whitelisting or blacklisting, and the construction of SQL statements such that user-supplied data cannot influence the logic of the statement. Last sentence is all about the statements and A and B are directly about that so must be those two.

upvoted 1 times

nep1019 3 years ago

According to Cisco's documentation: https://tools.cisco.com/security/center/resources/sql_injection.html B and C are correct: Parameterized queries in ASP.NET, prepared statements in Java, or similar techniques in other languages should be used comprehensively in addition to strict input validation.

Application layer protocol inspection performs deep packet inspection of traffic that transits the firewall. Using application layer protocol inspection on Cisco firewalls to mitigate SQL attacks against web servers is discussed in Cisco TAC Security Podcast Episode #16.

Only way to do the second, imo, is to secure the connection between the web and app tier (Application layer protocol inspection)

upvoted 1 times

nep1019 3 years ago

Changing back to A and B based on this statement that comes at the beginning of the section on mitigating these attacks: The primary approaches include validation of user-supplied data, in the form of whitelisting or blacklisting, and the construction of SQL statements such that user-supplied data cannot influence the logic of the statement. Last sentence is all about the statements and A and B are directly about that so must be those two.

upvoted 1 times

Brain_Power 3 years, 2 months ago

correct answer B & E

upvoted 1 times

maddyr 3 years, 2 months ago

B and E for me https://en.wikipedia.org/wiki/SQL_injection#MitigationIT is B and D according to the URL provided. Parameterized statements Main article: Prepared statement With most development platforms, parameterized statements that work with parameters can be used (sometimes called placeholders or bind variables) instead of embedding user input in the statement. A placeholder can only store a value of the given type and not an arbitrary SQL fragment. Hence the SQL injection would simply be treated as a strange (and probably invalid) parameter value. In many cases, the SQL statement is fixed, and each parameter is a scalar, not a table. The user input is then assigned (bound) to a parameter.[24] Enforcement at the coding level Using object-relational mapping libraries avoids the need to write SQL code. The ORM library in effect will generate parameterized SQL statements from object-oriented code.

upvoted 2 times

maddyr 3 years, 2 months ago

B and E for me

https://en.wikipedia.org/wiki/SQL_injection#Mitigation

upvoted 2 times

Przemol 3 years, 1 month ago

IT is B and D according to the URL provided. Parameterized statements Main article: Prepared statement With most development platforms, parameterized statements that work with parameters can be used (sometimes called placeholders or bind variables) instead of embedding user input in the statement. A placeholder can only store a value of the given type and not an arbitrary SQL fragment. Hence the SQL injection would simply be treated as a strange (and probably invalid) parameter value. In many cases, the SQL statement is fixed, and each parameter is a scalar, not a table. The user input is then assigned (bound) to a parameter.[24] Enforcement at the coding level Using object-relational mapping libraries avoids the need to write SQL code. The ORM library in effect will generate parameterized SQL statements from object-oriented code.

upvoted 1 times

cyberwhizzy0 3 years, 2 months ago

A and B is correct

upvoted 2 times

achille5 3 years, 5 months ago

B. Prepared statements and parameterized queries are a way of separating the SQL code from the data that is being passed into the query. By doing this, the SQL injection attack is prevented because the attacker cannot inject any SQL code into the prepared statement or parameterized query. C. Securing the connection between the web and the app tier is also an important prevention technique to mitigate SQL injection attacks. This is because an attacker can intercept network traffic and view the data that is being passed between the web and the app tier. By using SSL or TLS encryption, the data that is being passed between the two tiers is encrypted, making it much harder for an attacker to view or manipulate.After further reading i changed to A, B. https://en.wikipedia.org/wiki/SQL_injection

upvoted 1 times

achille5 3 years, 5 months ago

After further reading i changed to A, B. https://en.wikipedia.org/wiki/SQL_injection

upvoted 3 times

jienBoq 3 years, 8 months ago

to me it's B and C as per this Cisco article: https://tools.cisco.com/security/center/resources/sql_injection.html "A SQL injection attack can be detected and potentially blocked at two locations in an application traffic flow: in the application and in the network." "Parameterized queries in ASP.NET, prepared statements in Java, or similar techniques in other languages should be used comprehensively in addition to strict input validation." A's wording doesn't necessary imply input validation D doesn't make sense E is not a solution which I've seen suggested anywhere.B. Prepared statements and parameterized queries are a way of separating the SQL code from the data that is being passed into the query. By doing this, the SQL injection attack is prevented because the attacker cannot inject any SQL code into the prepared statement or parameterized query. C. Securing the connection between the web and the app tier is also an important prevention technique to mitigate SQL injection attacks. This is because an attacker can intercept network traffic and view the data that is being passed between the web and the app tier. By using SSL or TLS encryption, the data that is being passed between the two tiers is encrypted, making it much harder for an attacker to view or manipulate.

upvoted 2 times

jienBoq 3 years, 8 months ago

to me it's B and C as per this Cisco article: https://tools.cisco.com/security/center/resources/sql_injection.html

"A SQL injection attack can be detected and potentially blocked at two locations in an application traffic flow: in the application and in the network."

"Parameterized queries in ASP.NET, prepared statements in Java, or similar techniques in other languages should be used comprehensively in addition to strict input validation."

A's wording doesn't necessary imply input validation D doesn't make sense E is not a solution which I've seen suggested anywhere.

upvoted 2 times

achille5 3 years, 5 months ago

B. Prepared statements and parameterized queries are a way of separating the SQL code from the data that is being passed into the query. By doing this, the SQL injection attack is prevented because the attacker cannot inject any SQL code into the prepared statement or parameterized query. C. Securing the connection between the web and the app tier is also an important prevention technique to mitigate SQL injection attacks. This is because an attacker can intercept network traffic and view the data that is being passed between the web and the app tier. By using SSL or TLS encryption, the data that is being passed between the two tiers is encrypted, making it much harder for an attacker to view or manipulate.

upvoted 2 times

JavierAcuna 3 years, 9 months ago

Answer found in: https://tools.cisco.com/security/center/resources/sql_injection.html

upvoted 1 times

NikoNiko 4 years, 1 month ago

Correct are A, B. Countermeasure against SQLi: ..you should most definitely use ORM (Object-Relational Mappings) and prepared statements. = option B. They take away the vast majority of SQL Injection risk, and are generally good software practices. However, you shouldn't think that using these packages makes you completely immune. Instead, you should also use input validation. This will keep malicious input out of your system to begin with, which is a great way to reduce risk. = option A https://snyk.io/blog/sql-injection-orm-vulnerabilities/

upvoted 3 times

HilaM 4 years, 1 month ago

A,B correct Answer found in: https://tools.cisco.com/security/center/resources/sql_injection.html

upvoted 2 times

HilaM 4 years, 1 month ago

A,B correct Answer found in: https://tools.cisco.com/security/center/resources/sql_injection.htmlThis is from this link: Parameterized queries in ASP.NET, prepared statements in Java, or similar techniques in other languages should be used comprehensively in addition to strict input validation. Each of these techniques performs all required escaping of dangerous characters before the SQL statement is passed to the underlying database system.

upvoted 2 times

davezz 3 years, 9 months ago

This is from this link: Parameterized queries in ASP.NET, prepared statements in Java, or similar techniques in other languages should be used comprehensively in addition to strict input validation. Each of these techniques performs all required escaping of dangerous characters before the SQL statement is passed to the underlying database system.

upvoted 1 times

Question #14 *Topic 1*

Which two kinds of attacks are prevented by multifactor authentication? (Choose two.)

A. phishing

B. brute force

C. man-in-the-middle

D. DDOS

E. tear drop

Suggested Answer: *A, B*

Official Answer: AB

Community vote distribution

AB (100%)

crh23 Highly Voted 5 years, 7 months ago

Its A and B cisco document https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-mfa-password-security-infographic.pdf

upvoted 30 times

Benkelly18 Highly Voted 5 years, 6 months ago

mfa does not prevent phishing. I've seen phishing attacks where people managed to get them to send the code from the mfa device.

Basically one way is they send a marketing with a reply to unsubscribe, having already obtained the password, when someones texts stop or whatever they log in, and say please tell us the six digit code just messaged to your phone in order to unsubscribe.

It helps prevent as the above is quite uncommon but it doesn't prevent it.

upvoted 11 times

Benkelly18 5 years, 6 months ago

mfa does not prevent phishing. I've seen phishing attacks where people managed to get them to send the code from the mfa device. Basically one way is they send a marketing with a reply to unsubscribe, having already obtained the password, when someones texts stop or whatever they log in, and say please tell us the six digit code just messaged to your phone in order to unsubscribe. It helps prevent as the above is quite uncommon but it doesn't prevent it.I'd classify that as a MitM attack (the bad actor is relaying between Authentication Service and the victim) where a general Phishing attack would be used to gather the password in the first place (cast a line with bait and see who bites). In this context, the MFA would prevent the phishing attack from being successful, user pops in the username/password, but without the OTP, bad actor can't log in. It doesn't stop them from further social engineering to get the OTP as you describe, but it does prevent a credential harvesting attack from being successful.A, B and C are correct, but it matters what Cisco wants. From Cisco website (about Trust Center): MFA protects against phishing, social engineering and password brute- force attacks and secures your logins from attackers exploiting weak or stolen credentials. So it's simple for me, correct is A & B.

upvoted 11 times

bigdadzzz 5 years, 1 month ago

I'd classify that as a MitM attack (the bad actor is relaying between Authentication Service and the victim) where a general Phishing attack would be used to gather the password in the first place (cast a line with bait and see who bites). In this context, the MFA would prevent the phishing attack from being successful, user pops in the username/password, but without the OTP, bad actor can't log in. It doesn't stop them from further social engineering to get the OTP as you describe, but it does prevent a credential harvesting attack from being successful.

upvoted 5 times

klu16 4 years, 5 months ago

A, B and C are correct, but it matters what Cisco wants. From Cisco website (about Trust Center): MFA protects against phishing, social engineering and password brute- force attacks and secures your logins from attackers exploiting weak or stolen credentials. So it's simple for me, correct is A & B.

upvoted 9 times

Marshpillowz Most Recent 1 year, 10 months ago

A and B are correct

upvoted 1 times

Rododendron2 1 year, 10 months ago

How can ever C be wrong ?

upvoted 1 times

sull3y 3 years ago

A. Phishing B. Brute force

upvoted 2 times

sis_net_sec 3 years, 7 months ago

AB is correct

upvoted 1 times

nomanlands 3 years, 7 months ago

Cisco answer is AB. Real life, mainly B and could help with A or C.

upvoted 1 times

Cyril_the_Squirl 3 years, 7 months ago

B & C are Correct. https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack

upvoted 2 times

philip8787 3 years, 8 months ago

https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa 2FA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials. so A and B

upvoted 2 times

Iron21 3 years, 9 months ago

Its A and B

upvoted 1 times

brownbear505 3 years, 12 months ago

MFA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials. A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

upvoted 2 times

Wang87 4 years ago

Phishing is correct because here it means that even if someone phished your password MFA won't allow threat actors to exploit your passwords as 2nd step of authentication will prevent login.

upvoted 3 times

jaciro11 4 years, 2 months ago

Its A and B there is in CISCO documents

upvoted 2 times

pfunkylol 4 years, 2 months ago

Phishing attempts to get logon credentials just a brute force attempts to use credentials; multi-factor authentication means you need an additional factor (biometric / RSA token, etc.) to log in. Man-in-the-middle attacks can see the extra factor so it will not be mitigated by MFA (multi factor authentication). DDoS and Tear Drop are denial of services, again not affected by MFA.

upvoted 1 times

heamgu 4 years, 3 months ago

So if you are not sure what is the answer check this PDF from Cisco. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-top-10-cyber-tips.pdf Answer is A and B.

upvoted 6 times

Hormore 4 years, 4 months ago

It's definitely A&B, MITM is getting the info inbetween the packet conversation… not when user are just trying to authenticate.

upvoted 2 times

SirFrates24 4 years, 7 months ago

MFA protects against phishing, social engineering and password bruteforce attacks and secures your logins from attackers exploiting weak or stolen credentials.

upvoted 3 times

Question #15 *Topic 1*

What are two rootkit types? (Choose two.)

A. registry

B. buffer mode

C. user mode

D. bootloader

E. virtual

Suggested Answer: *C, D*

Official Answer: CD

Community vote distribution



Iarn Highly Voted 3 years, 9 months ago

1. Kernel rootkit 2. Hardware or firmware rootkit 3. Hyper-V rootkits 4. Bootloader rootkit or bootkit 5. Memory rootkit 6. User-mode or application rootkit

upvoted 12 times

Cock Highly Voted 4 years, 2 months ago

C&D. https://heimdalsecurity.com/blog/rootkit/

upvoted 6 times

Marshpillowz Most Recent 1 year, 10 months ago

User mode and bootloader - C and D

upvoted 1 times

sull3y 3 years ago

C. User mode D. Bootloader A rootkit is a type of malicious software that is designed to hide itself and its activities from the system and its users. There are several types of rootkits, but the two most common are user-mode and bootloader rootkits. A user-mode rootkit runs at the same privilege level as a normal application and is able to intercept and modify system calls made by other processes. It can also hide its presence by modifying the output of system commands such as "ps" or "netstat" A bootloader rootkit infects the system's bootloader, which is the first piece of software that runs when a computer starts up. By infecting the bootloader, a rootkit can ensure that it is loaded before the operating system, making it difficult for the system to detect and remove it. Additionally, it can also hide its presence by modifying the output of system commands such as "ps" or "netstat" Option A, registry, is a database in Windows operating systems that stores configuration settings and options for the operating system, applications, and users. Registry is not a type of rootkit.

upvoted 6 times

DeepaBP 4 years, 3 months ago

Please ignore the first comment C & D is the correct answer, Kernel, user, bootloader and Memory are the 4 types of rootkits,

upvoted 5 times

DeepaBP 4 years, 3 months ago

B &C is the correct answer kernel Rootkit, User Mode Rootkits, Buffer Mode Rootkit and Memory Rootkits are the four

upvoted 1 times

jonsmackface 4 years, 3 months ago

https://en.wikipedia.org/wiki/Rootkit#Types User mode (C) Bootkits (D)

upvoted 2 times

jairusster 4 years, 4 months ago

User-mode or application rootkit - User-mode rootkits are simpler and easier to detect than kernel or boot record rootkits. This is because they hide within an application itself, and not system-critical files. In other words, they operate at the level of standard programs such as Paint, Word, PC games and so on. This means a good antivirus or anti-rootkit program will probably find the malware and then remove it.

upvoted 1 times

Sarbi 4 years, 5 months ago

The correct answer is Bootloader and Virtual toll kit.There is no user-mode tool kit. Hypervisor (Virtualized) Level Rootkits: Hypervisor (Virtualized) Level Rootkits are created by exploiting hardware features such as Intel VT or AMD-V (Hardware assisted virtualization technologies). Hypervisor

level rootkits hosts the target operating system as a virtual machine and therefore they can intercept all hardware calls made by the target operating system. Boot loader Level (Bootkit) Rootkits: Boot loader Level (Bootkit) Rootkits replaces or modifies the legitimate boot loader with another one thus enabling the Boot loader Level (Bootkit) to be activated even before the operating system is started. Boot loader Level (Bootkit) Rootkits are serious threat to security because they can be used to hack the encryption keys and passwords.https://resources.infosecinstitute.com/topic/rootkits-user-mode-kernel-mode-part-1/

upvoted 3 times

Sarbi 4 years, 5 months ago

The correct answer is Bootloader and Virtual toll kit.There is no user-mode tool kit. Hypervisor (Virtualized) Level Rootkits: Hypervisor (Virtualized) Level Rootkits are created by exploiting hardware features such as Intel VT or AMD-V (Hardware assisted virtualization technologies). Hypervisor level rootkits hosts the target operating system as a virtual machine and therefore they can intercept all hardware calls made by the target operating system.

Boot loader Level (Bootkit) Rootkits: Boot loader Level (Bootkit) Rootkits replaces or modifies the legitimate boot loader with another one thus enabling the Boot loader Level (Bootkit) to be activated even before the operating system is started. Boot loader Level (Bootkit) Rootkits are serious threat to security because they can be used to hack the encryption keys and passwords.

upvoted 3 times

capwapap555 4 years, 5 months ago

https://resources.infosecinstitute.com/topic/rootkits-user-mode-kernel-mode-part-1/

upvoted 1 times

Question #16 *Topic 1*

How is DNS tunneling used to exfiltrate data out of a corporate network?

A. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers

B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data

C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network

D. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (86%) C (14%)

Jetnor Highly Voted 1 year, 10 months ago
I would go with B, based on the question . because we are asked how is DNS tunneling used, and the attacker encodes text information in base64 to then send it to the malicious DNS server which is mentioned at the end of the question (DNS server rebuilds the exfiltrated data) "C" does not explain how the information is encoded.
upvoted 9 times

sull3y Highly Voted 3 years, 6 months ago
B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data

DNS Tunneling is a technique used to exfiltrate data out of a corporate network by encoding the payload with random characters that are broken into short strings and then sending these strings as DNS queries. These queries are sent to a domain controlled by the attacker, which then rebuilds the exfiltrated data. This technique takes advantage of the fact that many corporate networks allow outgoing DNS queries, while other types of traffic may be blocked.

Option A, It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers, is not exactly the way DNS Tunneling works, it's more about encoding data into DNS queries and exfiltrating it through this channel.
upvoted 5 times

sull3y 3 years, 6 months ago
B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data DNS Tunneling is a technique used to exfiltrate data out of a corporate network by encoding the payload with random characters that are broken into short strings and then sending these strings as DNS queries. These queries are sent to a domain controlled by the attacker, which then rebuilds the exfiltrated data. This technique takes advantage of the fact that many corporate networks allow outgoing DNS queries, while other types of traffic may be blocked. Option A, It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers, is not exactly the way DNS Tunneling works, it's more about encoding data into DNS queries and exfiltrating it through this channel.Option C, It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network, is not exactly how DNS Tunneling works. This technique is more about exfiltrating data, not stealing credentials. Option D, It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks, is not exactly how DNS Tunneling works. DNS Tunneling is more about exfiltrating data, not corrupting DNS servers.
upvoted 5 times

sull3y 3 years, 6 months ago
Option C, It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network, is not exactly how DNS Tunneling works. This technique is more about exfiltrating data, not stealing credentials. Option D, It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks, is not exactly how DNS Tunneling works. DNS Tunneling is more about exfiltrating data, not corrupting DNS servers.
upvoted 1 times

Rockbo47 Most Recent 1 year ago
From Cisco's official 350-701 course:- "Most commonly, the data being tunneled out over DNS will be encoded by the attacker to avoid detection. Two of the common encoding methods include Base32 and Base64 encoding"
upvoted 2 times

CyberGhost666 1 year, 1 month ago

Correct Answer is B

upvoted 1 times

chikatchy 1 year, 10 months ago

The answer is B.

upvoted 1 times

gamingoddess 1 year, 10 months ago

Attackers can use outbound DNS requests to send encoded exfiltrated data to their infrastructure. The DNS tunneling client malware on the infected machine reads the data to be exfiltrated line by line, slices the data into small chunks and performs base64 encoding on each line. So, option B is the closest to describing how DNS tunneling is used to exfiltrate data out of a corporate network.

upvoted 1 times

Premium_Pils 1 year, 10 months ago

Maybe it is just me, but I can't see how "redirection" would fit in. "attackers use the DNS protocol to embed data within packets in DNS queries", and get the data shipped out to the attackers DNS server. (not redirecting, just directing it to the malicious server) The data needs to be split into smaller chunks (to be protocol conform), and is often encoded with base64. https://www.akamai.com/glossary/what-is-dns-data-exfiltration https://bluegoatcyber.com/blog/dns-exfiltration-with-base64-encoding-a-stealthy-data-theft-technique/ I vote for B.

upvoted 1 times

Marshpillowz 2 years, 4 months ago

B is correct

upvoted 1 times

klu16 2 years, 5 months ago

Well, for me it all depends if these answers are really worded like this. If so, then B cannot be correct, because DNS servers do not rebuild information (DNS server's role is to handle DNS queries and responses). Option C seems to be the most logical, since the data is encoded, then the encoded payload is inserted into DNS queries and manipulated DNS packets are sent to a malicious DNS server controlled by the attacker. I think I will go with answer C because of that.

upvoted 1 times

Cokamaniako 3 years, 1 month ago

The DNS server can not rebuild information.

upvoted 1 times

littlewilly 3 years, 2 months ago

This is C

upvoted 2 times

stalkr3 3 years, 4 months ago

B is false imo - "It encodes the payload with RANDOM characters..." - What is the point of exfiltrating random characters?

upvoted 2 times

pioo1979 3 years, 5 months ago

I think the correct answer is C. B - "It encodes the payload with RANDOM characters..." There is no sense to exfiltrate random data..

upvoted 1 times

Anonymous983475 3 years, 7 months ago

C should be the correct answer. for more inforwation watch this short vid https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunnelingActually jaciro11 is right, C is correct, but the keyword "redirrect" makes it incorrect as the information is exfiltrated by being encoded in base64

upvoted 1 times

Anonymous983475 3 years, 7 months ago

Selected Answer: C

C should be the correct answer. for more inforwation watch this short vid https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

upvoted 1 times

Anonymous983475 3 years, 7 months ago

Actually jaciro11 is right, C is correct, but the keyword "redirrect" makes it incorrect as the information is exfiltrated by being encoded in base64

upvoted 1 times

jaciro11 4 years, 5 months ago

Once the desired data is obtained, the payload encodes the data as a series of 32 characters broken into short strings... The problem with answer C, is that this not only to get credentials

upvoted 2 times

brownb 4 years, 9 months ago

Im leaning more toward C in this case. Is the point of the DNS attack not to redirect the victim to a server to then attempt to steal data?me too

upvoted 2 times

brownb 4 years, 9 months ago

Im leaning more toward C in this case. Is the point of the DNS attack not to redirect the victim to a server to then attempt to steal data?

upvoted 2 times

nomad 4 years, 8 months ago

me too

upvoted 1 times

Question #17 *Topic 1*

Which type of attack is social engineering?

A. trojan

B. MITM

C. phishing

D. malware

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

luismg Most Recent 1 year, 11 months ago
C is clear.
upvoted 1 times

Marshpillowz 2 years, 4 months ago
Selected Answer: C
C is correct
upvoted 1 times

sull3y 3 years, 6 months ago
C. Phishing

Social engineering is a type of attack that relies on manipulating people to gain access to sensitive information or resources. Social engineering attacks can take many forms, but the most common is phishing.

Phishing is a form of social engineering that uses email or other electronic communication methods to trick people into providing sensitive information or performing an action, such as clicking on a link that downloads malware. Phishing can take many forms, but the goal is always to trick people into giving up their personal information or taking actions that can compromise the security of their computer or network.

Option A, Trojan, is a type of malware that disguises itself as legitimate software in order to gain access to a system. It can be delivered via social engineering but it is not the same thing as social engineering.
upvoted 4 times

sull3y 3 years, 6 months ago
Option B, MITM (Man in the Middle) is a type of attack where an attacker intercepts communication between two parties to steal information. MITM can be performed via social engineering but it is not the same thing as social engineering.

Option D, Malware, is a software that is specifically designed to damage or disrupt computer systems. Malware can be delivered via social engineering but it is not the same thing as social engineering.
upvoted 1 times

idto 4 years, 8 months ago
Agreed. Definitely phishing.
upvoted 3 times

Thusi26 4 years, 8 months ago
Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization.

https://us-cert.cisa.gov/ncas/tips/ST04-014
upvoted 2 times

Question #18 *Topic 1*

What are two DDoS attack categories? (Choose two.)

A. protocol

B. source-based

C. database

D. sequential

E. volume-based

Suggested Answer: *A, E*

Official Answer: AE

Community vote distribution

AE (100%)

SirFrates24 Highly Voted 4 years, 7 months ago

Volume Based Attacks. Includes UDP floods, ICMP floods, and other spoofed-packet floods. ... Protocol Attacks. Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. ... Application Layer Attacks.

upvoted 12 times

sull3y Highly Voted 3 years ago

A. protocol E. volume-based DDoS (Distributed Denial of Service) attacks are a type of cyberattack that aims to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic. There are several categories of DDoS attacks, including: A. Protocol: This type of DDoS attack targets the underlying communication protocols used by the targeted server or network, such as TCP, UDP, or ICMP. E. Volume-based: This type of DDoS attack floods the targeted server or network with a large volume of traffic, such as a flood of packets, in order to overload and disrupt its normal functioning.

upvoted 5 times

cd1c33b Most Recent 3 months, 1 week ago

A. protocol: This category of DDoS attacks exploits vulnerabilities in network layer protocols (Layers 3 and 4 of the OSI model). They target the connection tables of network infrastructure components like routers, firewalls, and load balancers to exhaust system resources. Common examples include SYN floods and Ping of Death. E. volume-based: Also known as volumetric attacks, this category aims to saturate the target network's overall bandwidth capacity. Attackers flood the system with massive amounts of spoofed data packets or amplification traffic to completely block legitimate users. Common examples include UDP floods and ICMP floods.

upvoted 1 times

CyberGhost666 1 year, 1 month ago

Correct Answers are A and E

upvoted 1 times

Marshpillowz 1 year, 10 months ago

A and E correct

upvoted 1 times

sheki2005 3 years, 9 months ago

A,E are correct answers

upvoted 2 times

heamgu 4 years, 3 months ago

Answer A and E. There are three different general categories of DDoS attacks: Volume-based DDoS attacks Application DDoS attacks Low-rate DoS (LDoS) attacks https://tools.cisco.com/security/center/resources/guide_ddos_defense.html

upvoted 4 times

Question #19 *Topic 1*

In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?

A. man-in-the-middle

B. LDAP injection

C. insecure API

D. cross-site scripting

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

chikatchy Most Recent 1 year, 10 months ago

The answer is A

upvoted 1 times

Marshpillowz 2 years, 4 months ago

A - MITM

upvoted 1 times

IETF1 2 years, 8 months ago

A. man-in-the-middle

upvoted 1 times

Abdelmoneim656 2 years, 9 months ago

NNNNNNNNNNNNNNNNNNNNNNNN

upvoted 1 times

Question #20 *Topic 1*

How does Cisco Advanced Phishing Protection protect users?

A. It utilizes sensors that send messages securely.

B. It uses machine learning and real-time behavior analytics.

C. It validates the sender by using DKIM.

D. It determines which identities are perceived by the sender.

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

SirFrates24 Highly Voted 5 years, 3 months ago
Cisco® Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advance machine learning techniques, real time behavior analytics, relationship modeling and telemetry to protect against identity deception–based threats.

answer should be B
upvoted 29 times

SirFrates24 Highly Voted 5 years, 3 months ago
Cisco® Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advance machine learning techniques, real time behavior analytics, relationship modeling and telemetry to protect against identity deception–based threats. answer should be Bcorrect . B
upvoted 29 times

samismayilov 5 years, 3 months ago
correct . B
upvoted 3 times

ChrisElkin Most Recent 1 year, 10 months ago
Answer D is a red herring. It references identities perceived by the sender, but the Cisco docs point to "identities the recipient perceives". The correct answer is B. Again Cisco docs reference three areas of machine learning: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf
upvoted 1 times

Wang87 1 year, 10 months ago
Phishing Defense provides sender authentication and BEC detection capabilities. It uses advance machine learning techniques, real time behavior analytics, relationship modeling and telemetry to protect against identity deception–based threats. This intelligence continuously adapts to drive a real-time understanding of senders, prevent breaches and provide enhanced protection
upvoted 2 times

brownbear505 1 year, 10 months ago
Cisco Advanced Phishing Protection provides Business Email Compromise (BEC) and phishing detection capabilities. It detects identity deception-based threats by performing reputation checks on sender address by using advanced machine learning techniques and added intelligence. This intelligence continuously adapts to drive a real-time understanding of senders and provides enhanced protection.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html
upvoted 1 times

surforlife 1 year, 10 months ago
You can configure mail policies to enable forwarding of message metadata to the Cisco Advanced Phishing Protection cloud service. When you enable the Cisco AdvancedPhishingProtection cloud service on your email gateway, the following message headers are shared with the Cisco Advanced Phishing Protection Cloud service : • dkim_selector • last_hop_ip_address • helo_domain • dkim_result • dkim_domain • dmarc_result • dkim_signatures • to_header • header_subject • header_from • message_id • spf_result • rcpt_to • full_header_from • mail_from • Received-SPF • Received-Header • Authentication-Results • reply_to • original_sender • received-timestamps • Authentication-Results-original • X-originating-ip
upvoted 1 times

Marshpillowz 2 years, 4 months ago
Answer is B

upvoted 1 times

sull3y 3 years, 6 months ago

B. It uses machine learning and real-time behavior analytics. Cisco Advanced Phishing Protection uses machine learning to identify and analyze patterns in email and other online communication, and can detect and block phishing attempts in real-time. It also uses behavior analytics to identify anomalies and suspicious activity, helping to protect users from phishing attacks. The solution also integrates threat intelligence and machine learning to detect new types of malicious emails, and it also uses a combination of techniques, including URL and attachment scanning, to detect and block phishing attacks.

upvoted 3 times

Thumbzy_Thumbzy 4 years, 4 months ago

Funny enough, as much as B sounds correct but the flaw with that answer is that Cisco Advanced Phishing Protection doesn't provide "real-time behavior analytics" it actually bases it's data according to historic email data sent to organization. Check out below statement from the cisco webpage

The Advanced Phishing Protection engine on the email gateway checks the unique behavior of all legitimate senders, based on the historic email traffic to your organization. The cloud service interface of the Cisco Advanced Phishing Protection provides risk analysis to distinguish good messages from potentially malicious messages.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html

upvoted 2 times

Thumbzy_Thumbzy 4 years, 4 months ago

Funny enough, as much as B sounds correct but the flaw with that answer is that Cisco Advanced Phishing Protection doesn't provide "real-time behavior analytics" it actually bases it's data according to historic email data sent to organization. Check out below statement from the cisco webpage The Advanced Phishing Protection engine on the email gateway checks the unique behavior of all legitimate senders, based on the historic email traffic to your organization. The cloud service interface of the Cisco Advanced Phishing Protection provides risk analysis to distinguish good messages from potentially malicious messages. https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.htmlD would be correct if it was "It determines which identities are perceived by the RECEIVER." but it's not so that leaves B as the most correct answer.Sorry, one more time. On the same link, it also says this in the section of "Benefits of Cisco Advanced Phishing Protection": Gain a real-time understanding of senders, learn, and authenticate email identities and behavioral relationships to protect against BEC attacksOn the same link, it also says in the section of "Benefits of Cisco Advanced Phishing Protection": this Gain a real-time understanding of senders, learn, and authenticate email identities and behavioral relationships to protect against BEC attacks

upvoted 2 times

migueli 4 years, 1 month ago

D would be correct if it was "It determines which identities are perceived by the RECEIVER." but it's not so that leaves B as the most correct answer.

upvoted 1 times

davezz 3 years, 9 months ago

Sorry, one more time. On the same link, it also says this in the section of "Benefits of Cisco Advanced Phishing Protection": Gain a real-time understanding of senders, learn, and authenticate email identities and behavioral relationships to protect against BEC attacks

upvoted 1 times

davezz 3 years, 9 months ago

On the same link, it also says in the section of "Benefits of Cisco Advanced Phishing Protection": this Gain a real-time understanding of senders, learn, and authenticate email identities and behavioral relationships to protect against BEC attacks

upvoted 1 times

urathod 4 years, 7 months ago

Correct answer should be B

upvoted 2 times

jfuentesf 4 years, 8 months ago

Advanced Phishing Protection uses advance machine learning techniques. Answer B

upvoted 3 times

san111 4 years, 9 months ago

It should be B

upvoted 2 times

u777 4 years, 11 months ago

Answer is B It detects identity deception-based threats by performing reputation checks on sender address by using advanced machine learning techniques and added intelligence. This intelligence continuously adapts to drive a real-time understanding of senders and provides enhanced

protection. https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html

upvoted 1 times

shahed4062 4 years, 11 months ago

Answer is B Machine Learning

upvoted 4 times

Sarbi 4 years, 12 months ago

It should be B.

upvoted 1 times

kakakayayaya 5 years, 3 months ago

https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf "Determines which identities the recipient perceives is sending the message" - differ from this answer,Phishing Defense leverages three areas of machine learning modeling. • Determines which identities the recipient perceives is sending the message • Analyzes the expected sending behavior for anomalies relative to that identity

upvoted 2 times

kakakayayaya 5 years, 3 months ago

https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf

"Determines which identities the recipient perceives is sending the message" - differ from this answer,

upvoted 2 times

nospampls 5 years ago

Phishing Defense leverages three areas of machine learning modeling. • Determines which identities the recipient perceives is sending the message • Analyzes the expected sending behavior for anomalies relative to that identity

upvoted 1 times

kakakayayaya 5 years, 3 months ago

Wrong answer. It's all about machine learning.

upvoted 4 times

Question #21 *Topic 1*

How does DNS Tunneling exfiltrate data?

A. An attacker registers a domain that a client connects to based on DNS records and sends malware through that connection.

B. An attacker opens a reverse DNS shell to get into the client's system and install malware on it.

C. An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a malicious domain.

D. An attacker uses a non-standard DNS port to gain access to the organization's DNS servers in order to poison the resolutions.

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (75%) B (25%)

Alee86 Highly Voted 4 years, 4 months ago
Correct Answer A

The attacker registers a domain, such as badsite.com. The domain's name server points to the attacker's server, where a tunneling malware program is installed. The attacker infects a computer, which often sits behind a company's firewall, with malware. Because DNS requests are always allowed to move in and out of the firewall, the infected computer is allowed to send a query to the DNS resolver. The DNS resolver is a server that relays requests for IP addresses to root and top-level domain servers. The DNS resolver routes the query to the attacker's command-and-control server, where the tunneling program is installed. A connection is now established between the victim and the attacker through the DNS resolver. This tunnel can be used to exfiltrate data or for other malicious purposes. Because there is no direct connection between the attacker and victim, it is more difficult to trace the attacker's computer.
upvoted 18 times

Alee86 Highly Voted 4 years, 4 months ago
Correct Answer A The attacker registers a domain, such as badsite.com. The domain's name server points to the attacker's server, where a tunneling malware program is installed. The attacker infects a computer, which often sits behind a company's firewall, with malware. Because DNS requests are always allowed to move in and out of the firewall, the infected computer is allowed to send a query to the DNS resolver. The DNS resolver is a server that relays requests for IP addresses to root and top-level domain servers. The DNS resolver routes the query to the attacker's command-and-control server, where the tunneling program is installed. A connection is now established between the victim and the attacker through the DNS resolver. This tunnel can be used to exfiltrate data or for other malicious purposes. Because there is no direct connection between the attacker and victim, it is more difficult to trace the attacker's computer.https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling
upvoted 18 times

davezz 3 years, 7 months ago
https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling
upvoted 4 times

ic0deem 4 years, 5 months ago
None of the answers address the actual question.
upvoted 15 times

Marshpillowz Most Recent 1 year, 10 months ago
Answer is A
upvoted 1 times

klu16 1 year, 12 months ago
I would also go with answer A.
upvoted 1 times

Cokamaniako 2 years, 7 months ago
The attacker registers a domain, such as badsite.com. The domain's name server points to the attacker's server, where a tunneling malware program is installed. The attacker infects a computer, which often sits behind a company's firewall, with malware. Because DNS requests are always allowed to move in and out of the firewall, the infected computer is allowed to send a query to the DNS resolver. The DNS resolver is a server that relays requests for IP addresses to root and top-level domain servers.
upvoted 1 times

Brain_Power 2 years, 8 months ago

I think B is the correct

upvoted 1 times

sull3y 2 years, 10 months ago

DNS tunneling is a technique used by attackers to exfiltrate data by encoding the data into DNS queries or responses. The attacker creates a covert communication channel between the victim's computer and a server controlled by the attacker. This technique uses the DNS protocol to bypass firewalls and other network security measures. The correct answer is A. An attacker registers a domain that a client connects to based on DNS records and sends malware through that connection. The attacker creates a DNS tunnel by encoding the data in the DNS queries or responses that are sent to the server controlled by the attacker. The server then extracts the data from the queries or responses and sends it to the attacker.

upvoted 5 times

Smileebloke 3 years, 10 months ago

Dont think any of the answers are correct, DNS exfil wont deliver malware. Malware will use DNS tunneling to exfil data.Perfect, I agree with you

upvoted 9 times

Smileebloke 3 years, 10 months ago

Dont think any of the answers are correct, DNS exfil wont deliver malware. Malware will use DNS tunneling to exfil data.

upvoted 9 times

ffsilveira10 2 years, 4 months ago

Perfect, I agree with you

upvoted 1 times

whiteherondance 4 years, 2 months ago

Does anyone else think this questions answers have been mixed up with Question 16?

upvoted 4 times

Question #22 *Topic 1*

An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system's applications. Which vulnerability allows the attacker to see the passwords being transmitted in clear text?

A. unencrypted links for traffic

B. weak passwords for authentication

C. improper file security

D. software bugs on applications

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Marshpillowz Most Recent 1 year, 10 months ago

A is correct

upvoted 1 times

Alizade 2 years, 4 months ago

A. Unencrypted links for traffic

upvoted 1 times

sull3y 3 years ago

A Reconnaissance in this context refers to the process of gathering information about a target system in order to identify vulnerabilities that can be exploited. The attacker needs to know what weaknesses the system has, so they can plan their attack accordingly. Answer A is correct because if the VPN links are not encrypted, then any data transmitted over those links, including passwords, can be intercepted and read by an attacker. This allows the attacker to see the passwords being transmitted in clear text and potentially use them to gain access to the system.

upvoted 2 times

Question #23 *Topic 1*

A user has a device in the network that is receiving too many connection requests from multiple machines. Which type of attack is the device undergoing?

A. SYN flood

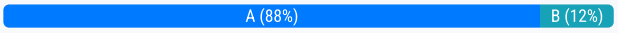
B. slowloris

C. phishing

D. pharming

Suggested Answer: *A*
Official Answer: A

Community vote distribution



pohqinan Highly Voted 4 years, 1 month ago
Answer is A Slowloris use a single machine to hold as many connections, The question is asking multi machine
https://en.wikipedia.org/wiki/Slowloris_(computer_security)
upvoted 7 times

G0909 Most Recent 1 month, 2 weeks ago
A SYN flood attack is a type of Denial-of-Service (DoS) attack where an attacker overwhelms a target with a large number of TCP connection requests (SYN packets). Also in question it says multiple machine
upvoted 1 times

CyberGhost666 1 year, 1 month ago
Correct answer is A.
upvoted 1 times

Marshpillowz 1 year, 10 months ago
A is correct
upvoted 1 times

jienBoq 3 years ago
Slowloris attack originates from one machine. The question mentions multiple machines.
upvoted 1 times

sis_net_sec 3 years, 4 months ago
Selected Answer: B
Slowloris is an application layer DDoS attack which uses partial HTTP requests to open connections between a single computer and a targeted Web server, then keeping those connections open for as long as possible, thus overwhelming and slowing down the target.
upvoted 1 times

GatPat 3 years, 1 month ago
A SYN flood is a type of denial of service (DoS) attack that is designed to overwhelm a target device or network resource by flooding it with connection requests. In a SYN flood attack, the attacker sends a large number of SYN packets (a type of packet used to initiate a TCP connection) to the target device with spoofed source addresses.
upvoted 3 times

sis_net_sec 3 years, 4 months ago
Slowloris is an application layer DDoS attack which uses partial HTTP requests to open connections between a single computer and a targeted Web server, then keeping those connections open for as long as possible, thus overwhelming and slowing down the target.Question is asking " from multiple machines" Slowloris attacks are initiated from single machine.
upvoted 1 times

PrinM 4 years, 2 months ago
I think answer is B.
upvoted 1 times

Taibu 2 years, 11 months ago
Question is asking " from multiple machines" Slowloris attacks are initiated from single machine.

upvoted 2 times

PrinM 4 years, 2 months ago

I think answer is B.It is A . Slowloris is a type of denial of service attack tool which allows a single machine to take down another machine's web server with minimal bandwidth.

upvoted 1 times

PrinM 4 years, 2 months ago

It is A . Slowloris is a type of denial of service attack tool which allows a single machine to take down another machine's web server with minimal bandwidth.

upvoted 2 times

Question #24 *Topic 1*

Which two preventive measures are used to control cross-site scripting? (Choose two.)

A. Enable client-side scripts on a per-domain basis.

B. Incorporate contextual output encoding/escaping.

C. Disable cookie inspection in the HTML inspection engine.

D. Run untrusted HTML input through an HTML sanitization engine.

E. SameSite cookie attribute should not be used.

Suggested Answer: *B, D*

Official Answer: BD

Community vote distribution

BD (100%)

dashiawia Highly Voted 5 years ago

Should be BD

upvoted 9 times

sull3y Highly Voted 3 years ago

B. Incorporate contextual output encoding/escaping D. Run untrusted HTML input through an HTML sanitization engine.

Cross-site scripting (XSS) is a type of security vulnerability that allows an attacker to inject malicious code into a web page viewed by other users. To prevent XSS attacks, it's important to properly handle user input and output on the server-side.

Incorporating contextual output encoding/escaping is an important preventive measure because it ensures that any user input that is included in the output of a web page is properly encoded and cannot be executed as code. This makes it difficult for an attacker to inject malicious code into the web page.

Running untrusted HTML input through an HTML sanitization engine is another important preventive measure because it ensures that any malicious code is removed from the input before it is processed by the server. This also makes it difficult for an attacker to inject malicious code into the web page.

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: BD

Correct Answers are B and D

upvoted 1 times

Marshpillowz 1 year, 10 months ago

Selected Answer: BD

B and D are correct

upvoted 1 times

nomanlands 3 years, 7 months ago

The cisco training material really only refers to input validation and scripts being executed. They don't really review running HTML through sanitation which seems more likely... I think A and B is what Cisco will look for but who knows

upvoted 1 times

jaciro11 3 years, 11 months ago

Selected Answer: BD

It is B & D

upvoted 4 times

jaciro11 3 years, 11 months ago

Selected Answer: BD

BD are correct

upvoted 3 times

mic9 4 years ago

A and B are correct because the question is asking how to prevent before cross scripting happens D its after it happens

upvoted 5 times

jfuentesf 4 years, 2 months ago

Selected Answer: BD

https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input B and D

upvoted 5 times

Dinges 4 years, 7 months ago

ABD are all valid options. They request only two, so if we need to pick only the better options, we should choose BD: While disabling scripts in general and enabling them on a per-doman basis, it does have some drawbacks for functionality. Users would be forced to enable scripting to have the site fully functional, which would make the user vulnerable to XXS attack again. Selectively disabling scripts is a good alternative, but is not in the question list of answers. That makes BD the better answer. From https://en.wikipedia.org/wiki/Cross-site_scripting: -The most significant problem with blocking all scripts on all websites by default is substantial reduction in functionality andresponsiveness . Another problem with script blocking is that many users do not understand it, and do not know how to properly secure their browsers. Yet another drawback is that many sites do not work without client-side scripting, forcing users to disable protection for that site and opening their systems to vulnerabilities.

upvoted 4 times

Jayde 4 years, 8 months ago

Unfortunately, A, B, D are all correct answers https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

upvoted 2 times

samismayilov 4 years, 9 months ago

BD are correct

upvoted 3 times

juanlecho 4 years, 11 months ago

I found this at the end of this article. https://spanning.com/blog/cross-site-scripting-web-based-application-security-part-3/

acording to that is BD

upvoted 4 times

bobby14 5 years ago

Very sade question, because A, B and D are correct answers. https://www.techknowlogy.in/security/cross-site-scripting-xss/

upvoted 1 times

Question #25 *Topic 1*

Which threat involves software being used to gain unauthorized access to a computer system?

A. ping of death

B. HTTP flood

C. NTP amplification

D. virus

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Marshpillowz Most Recent 1 year, 10 months ago

D - Virus

upvoted 1 times

mm_cisco_2022 3 years, 1 month ago

https://www.techtarget.com/searchsecurity/definition/RAT-remote-access-Trojan

upvoted 2 times

mm_cisco_2022 3 years, 1 month ago

A RAT (remote access Trojan) is malware an attacker uses to gain full administrative privileges and remote control of a target computer. Therefore virus is used to gain access for the target! select Virus is a correct option

upvoted 2 times

ureis 3 years, 5 months ago

D is correct

upvoted 1 times

chawiz 3 years, 8 months ago

D is the answer

upvoted 1 times

Question #26 *Topic 1*

Which two capabilities does TAXII support? (Choose two.)

A. exchange

B. pull messaging

C. binding

D. correlation

E. mitigating

Suggested Answer: *A, B*

Official Answer: AB

Community vote distribution

AB (100%)

statikd Highly Voted 4 years, 8 months ago

https://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part1-overview.html "There are three Capabilities that the current version of TAXII supports: push messaging, pull messaging, and discovery." "Discovery does, however, allow for the automated exchange of information..." The correct answer is A and B

upvoted 12 times

karmaomar Highly Voted 4 years, 8 months ago

Correct answer is A& B .. Binding is not supported by TAXII

upvoted 7 times

Marshpillowz Most Recent 1 year, 10 months ago

A and B correct

upvoted 1 times

SegaMasterSystemAdmin 2 years, 11 months ago

This is a questions that shouldn't even be on this exam. The official guide points to a link for more info so this is BS

upvoted 2 times

sull3y 3 years ago

A. exchange refers to the ability of TAXII to exchange Cyber Threat Intelligence (CTI) information between different systems and organizations in a secure and standardized way. This enables different CTI providers to share and consume information in a consistent and interoperable manner. B. pull messaging refers to the ability of TAXII to use a pull-based messaging model, which allows a client to request specific CTI information from a server, rather than receiving unsolicited CTI information. This allows clients to only receive the CTI information that is relevant to them.

upvoted 2 times

ColonelSRW 3 years, 6 months ago

Not understanding how so many folks vote for A when the TAXII specifications on github repeatedly refer to the binding attributes in very obvious language. Not to mention that answer B is an exchange, so choosing A is redundant. Note that the Official Cert Guide provides a link to the github project as well.

upvoted 2 times

brownbear505 3 years, 12 months ago

Cisco ScanCenter allows you to pull information on incidents detected by CTA down to your client for further correlation analysis and archival. The service supports MITRE's Trusted Automated eXchange of Indicator Information (TAXII) standard for integration with your Security Information and Event Management (SIEM) system. The TAXII standard specifies transport mechanisms used to share cyber threat information between systems.

upvoted 2 times

elast1c 4 years ago

Binding is not part of it: "TAXII is bound to neither a particular network protocol nor to a particular message binding"

upvoted 1 times

jfuentesf 4 years, 2 months ago

TAXII is an exchange utility using Pull Messaging, Push Messaging, Discovery, and Query

upvoted 4 times

pfunkylol 4 years, 3 months ago

TAXII - Trusted Automated eXchange of Indicator Information. TAXII is an exchange utility using Pull Messaging, Push Messaging, Discovery, and Query.

upvoted 2 times

Alee86 4 years, 4 months ago

Correct Answer B, C

TAXII implementers have a great deal of flexibility in choosing which TAXII Capabilities they support. As noted earlier, TAXII is bound to neither a particular network protocol nor to a particular message binding. In order to facilitate automated communication, TAXII includes the ability to discover the specific TAXII Services a TAXII user (or group of TAXII users) fields, as well as their network address and supported bindings. This does not remove the need for human involvement in the establishment of sharing agreements - sharing agreement negotiation is outside the scope of TAXII. Discovery does, however, allow for the automated exchange of information about which TAXII Capabilities a Producer might support and the technical mechanisms they employ in doing so.

upvoted 3 times

Alee86 4 years, 4 months ago

Correct Answer B, C TAXII implementers have a great deal of flexibility in choosing which TAXII Capabilities they support. As noted earlier, TAXII is bound to neither a particular network protocol nor to a particular message binding. In order to facilitate automated communication, TAXII includes the ability to discover the specific TAXII Services a TAXII user (or group of TAXII users) fields, as well as their network address and supported bindings. This does not remove the need for human involvement in the establishment of sharing agreements - sharing agreement negotiation is outside the scope of TAXII. Discovery does, however, allow for the automated exchange of information about which TAXII Capabilities a Producer might support and the technical mechanisms they employ in doing so.I meant A and B are correct

upvoted 3 times

Alee86 4 years, 4 months ago

I meant A and B are correct

upvoted 3 times

Sarbi 4 years, 5 months ago

The Correct answer is A and B.Tax11 supports pull, push, and discovery. So discovery means exchange.https://www.forumstandaardisatie.nl/open-standaarden/stix-en-taxii

upvoted 1 times

Dinges 4 years, 7 months ago

B and C are correct TAXII does not offer the exchange of the information as a service, enables the exchange, through its services that standardize information. The Standardization is accomplished through bindings, which TAXII defines: Message Binding Specification, Protocol Binding Specification, Content Binding Reference. http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part2-services.html The Discovery Service provides a requester with a list of TAXII Services and how these Services can be invoked (i.e., the address of the TAXII Daemon that implements that service and the bindings that Daemon supports). https://taxiiproject.github.io/releases/1.1/TAXII_Overview.pdf Trusted Automated eXchange of Indicator Information (TAXII ™) defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not an information sharing initiative...

upvoted 2 times

Dinges 4 years, 7 months ago

B and C are correct TAXII does not offer the exchange of the information as a service, enables the exchange, through its services that standardize information. The Standardization is accomplished through bindings, which TAXII defines: Message Binding Specification, Protocol Binding Specification, Content Binding Reference. http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part2-services.html The Discovery Service provides a requester with a list of TAXII Services and how these Services can be invoked (i.e., the address of the TAXII Daemon that implements that service and the bindings that Daemon supports). https://taxiiproject.github.io/releases/1.1/TAXII_Overview.pdf Trusted Automated eXchange of Indicator Information (TAXII ™) defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not an information sharing initiative...I gained new insight: STIX is structured languages to standardise threat information. Taxii is a protocol for automated exchange of this information. https://www.forumstandaardisatie.nl/open-standaarden/stix-en-taxii its AB

upvoted 2 times

Dinges 4 years, 7 months ago

I gained new insight: STIX is structured languages to standardise threat information. Taxii is a protocol for automated exchange of this information. https://www.forumstandaardisatie.nl/open-standaarden/stix-en-taxii its AB

upvoted 3 times

samismayilov 4 years, 9 months ago

A & B

upvoted 1 times

bobby14 5 years ago

There are three Capabilities that the current version of TAXII supports: push messaging, pull messaging, and discoveryAnd so the right answer is ????

upvoted 2 times

bobby14 5 years ago

There are three Capabilities that the current version of TAXII supports: push messaging, pull messaging, and discovery

upvoted 2 times

N0PT4U 5 years ago

And so the right answer is ????

upvoted 2 times

CISCO_CCNP 5 years, 3 months ago

Correct B and C

upvoted 3 times

thegreek1 5 years, 4 months ago

With the definition listed below: How does C, D, and E communicate that information?

STIX is the critical threat information. TAXII is the protocol to communicate it.

Trusted Automated Exchange of Intelligence Information (TAXII) is an application layer protocol specially designed to enable the exchange of STIX objects for facilitating cyber threat intel sharing and communication.

TAXII runs over HTTPS which also makes it secure and suitable for building online services that can consume and process STIX objects. It provides the developers an ability to build TAXII servers and TAXII clients which can communicate with each other in a request/response manner.

upvoted 2 times

thegreek1 5 years, 4 months ago

With the definition listed below: How does C, D, and E communicate that information? STIX is the critical threat information. TAXII is the protocol to communicate it. Trusted Automated Exchange of Intelligence Information (TAXII) is an application layer protocol specially designed to enable the exchange of STIX objects for facilitating cyber threat intel sharing and communication. TAXII runs over HTTPS which also makes it secure and suitable for building online services that can consume and process STIX objects. It provides the developers an ability to build TAXII servers and TAXII clients which can communicate with each other in a request/response manner.And so for you is A&B?

upvoted 2 times

N0PT4U 5 years ago

And so for you is A&B?

upvoted 2 times

Question #27 *Topic 1*

Which two conditions are prerequisites for stateful failover for IPsec? (Choose two.)

A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically.

B. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.

C. The IPsec configuration that is set up on the active device must be duplicated on the standby device.

D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.

E. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device.

Suggested Answer: *C, E*

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html

Community vote distribution

CE (100%)

mlu Highly Voted 5 years, 7 months ago

CE https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html#:~:text=Stateful%20failover%20for%20IPsec%20requires,accelerator%20or%20identical%20encryption%20accelerators. Restrictions for Stateful Failover for IPsec When configuring redundancy for a VPN, the following restrictions apply: Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via a hub or switch.

upvoted 20 times

DJO_2020 Highly Voted 5 years, 3 months ago

C and E Restrictions for Stateful Failover for IPsec When configuring redundancy for a VPN, the following restrictions apply: Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via a hub or switch.

upvoted 7 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct Answers are C and E

upvoted 1 times

Marshpillowz 1 year, 10 months ago

C and E are correct

upvoted 1 times

sull3y 3 years ago

CE Stateful failover for IPsec is a feature that allows for a standby device to take over the responsibilities of an active device in the event of a failure. In order for this to happen, certain conditions must be met: -The IPsec configuration that is set up on the active device must be duplicated on the standby device. This includes the IPsec policies, access control lists, and other settings that are required for the IPsec connections to function. -The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device. This is necessary to ensure that the standby device is capable of handling the same IPsec connections as the active device and that any issues can be resolved with the same software version.

upvoted 2 times

surforlife 3 years, 6 months ago

Device Requirements Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators. Restrictions for Stateful Failover for IPsec When configuring redundancy for a VPN, the following restrictions apply: Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via a hub or switch. "C and E"

upvoted 1 times

nomanlands 3 years, 7 months ago

CE because even if sometimes B may work, it's definitely not best practice and you shouldn't be doing it.

upvoted 1 times

breezer 3 years, 10 months ago

Technically B and C are correct.. When the FW HA is upgraded, for a time being both the units are running different OS versions. Still the failover is statefulAlso the doc does not mention that they need to be on same version: Device Requirements Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html#GUID-484562B6-A113-4901-A630-37869F8494D8

upvoted 1 times

breezer 3 years, 10 months ago

Technically B and C are correct.. When the FW HA is upgraded, for a time being both the units are running different OS versions. Still the failover is stateful

upvoted 1 times

breezer 3 years, 10 months ago

Also the doc does not mention that they need to be on same version: Device Requirements Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html#GUID-484562B6-A113-4901-A630-37869F8494D8

upvoted 1 times

brownbear505 3 years, 12 months ago

Prerequisites for Stateful Failover for IPsec Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via a hub or switch.

upvoted 2 times

CipherTrumpet 4 years, 1 month ago

Review the prerequisites

upvoted 2 times

urathod 4 years, 1 month ago

Should be C & E

upvoted 3 times

shaanthom 4 years, 1 month ago

C,E Prerequisites for Stateful Failover for IPsec Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices This document assumes that you have a complete IKE and IPsec configuration. The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device. That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPsec profiles, IPsec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on crypto map sets, all AAA configurations used for crypto, client configuration groups, IP local pools used for crypto, and ISAKMP profiles.

upvoted 2 times

pfunkylol 4 years, 3 months ago

The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device. Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via hub or switch. Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device.

upvoted 2 times

djreymix 4 years, 4 months ago

CE absolutely

upvoted 1 times

Raajaa 4 years, 7 months ago

C and E for sure

upvoted 2 times

aalnman 4 years, 7 months ago

C & E are the correct answer. I deploy Cisco firewalls for a living and C & E are absolutely the correct answers.

upvoted 1 times

Zoli6 4 years, 8 months ago

C and E are correct. Device Requirements Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators. Restrictions for Stateful Failover for IPsec When configuring redundancy for a VPN, the following restrictions apply: Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via a hub or switch.

upvoted 3 times

Question #28 *Topic 1*

Which algorithm provides encryption and authentication for data plane communication?

A. AES-GCM

B. SHA-96

C. AES-256

D. SHA-384

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Kris92 Highly Voted 4 years, 11 months ago

It is A, AES-GCM can do encryption like all other AES and has an authentication tag, rest of the options can be used for encryption or authentication, but not both. In cryptography, Galois/Counter Mode (GCM) is a mode of operation for symmetric-key cryptographic block ciphers which is widely adopted for its performance. GCM throughput rates for state-of-the-art, high-speed communication channels can be achieved with inexpensive hardware resources.[1] The operation is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality. https://en.wikipedia.org/wiki/Galois/Counter_Mode

upvoted 13 times

Vic25H Highly Voted 5 years, 6 months ago

It's A because of the GCM, this mode of block ciphers provide confidentiality and integrity. AES-256 refers to the CBC mode beacuse its the default mode in Cisco. https://en.wikipedia.org/wiki/Galois/Counter_Mode https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Answer is A, AES-GMC

upvoted 1 times

Marshpillowz 1 year, 10 months ago

Answer is A - AES GCM

upvoted 1 times

sull3y 3 years ago

A. AES-GCM (Advanced Encryption Standard-Galios/Counter Mode) is the correct answer because it provides both encryption and authentication for data plane communication. It uses the Advanced Encryption Standard (AES) algorithm for encryption and the Galios/Counter Mode (GCM) for authentication. GCM is a block cipher mode of operation that provides both confidentiality and integrity for data. It uses a unique initialization vector (IV) for each message and also a unique authentication tag for each message. GCM is considered to be a very secure algorithm that is resistant to tampering and replay attacks.

upvoted 2 times

sull3y 3 years ago

A. AES-GCM (Advanced Encryption Standard-Galios/Counter Mode) is the correct answer because it provides both encryption and authentication for data plane communication. It uses the Advanced Encryption Standard (AES) algorithm for encryption and the Galios/Counter Mode (GCM) for authentication. GCM is a block cipher mode of operation that provides both confidentiality and integrity for data. It uses a unique initialization vector (IV) for each message and also a unique authentication tag for each message. GCM is considered to be a very secure algorithm that is resistant to tampering and replay attacks.AES-256 provides encryption for the data, but it does not provide authentication for the data. Authentication is a process of proving the integrity and origin of the data. It ensures that the data has not been tampered with and that it came from a trusted source. To provide both encryption and authentication for data, AES-256 can be combined with a separate authentication algorithm such as GCM (Galois/Counter Mode) or HMAC (Hash-based Message Authentication Code).

upvoted 2 times

sull3y 3 years ago

AES-256 provides encryption for the data, but it does not provide authentication for the data. Authentication is a process of proving the integrity and origin of the data. It ensures that the data has not been tampered with and that it came from a trusted source. To provide both encryption and

authentication for data, AES-256 can be combined with a separate authentication algorithm such as GCM (Galois/Counter Mode) or HMAC (Hash-based Message Authentication Code).

upvoted 1 times

johnsonwale 4 years, 4 months ago

It's A.

upvoted 3 times

naddaf 5 years, 7 months ago

In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetric-key algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. These packets contain information that the vSmart controller uses to determine the network topology, including the router's TLOC (a tuple of the system IP address and traffic color) and AES key. The vSmart controller then places these OMP route packets into reachability advertisements that it sends to the other routers in the network. In this way, the AES keys for all the routers are distributed across the network. Even though the key exchange is symmetric, the routers use it in an asymmetric fashion. The result is a simple and scalable key exchange process that uses the Cisco vSmart Controller.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html#id_112385

upvoted 2 times

Gurak 5 years, 7 months ago

Could someone tell me if I'm wrong? I see AES-256 https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.1/05Security/01Security_Overview/Data_Plane_Security_Overview#:~:text=duplicates%20encrypted%20packets.-,Data%20Plane%20Authentication%20and%20Encryption,each%20other%20over%20this%20connection.AES-256 should be refer to control plane

upvoted 1 times

Gurak 5 years, 7 months ago

Could someone tell me if I'm wrong? I see AES-256 https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.1/05Security/01Security_Overview/Data_Plane_Security_Overview#:~:text=duplicates%20encrypted%20packets.-,Data%20Plane%20Authentication%20and%20Encryption,each%20other%20over%20this%20connection.

upvoted 1 times

Max95 4 years, 8 months ago

AES-256 should be refer to control plane

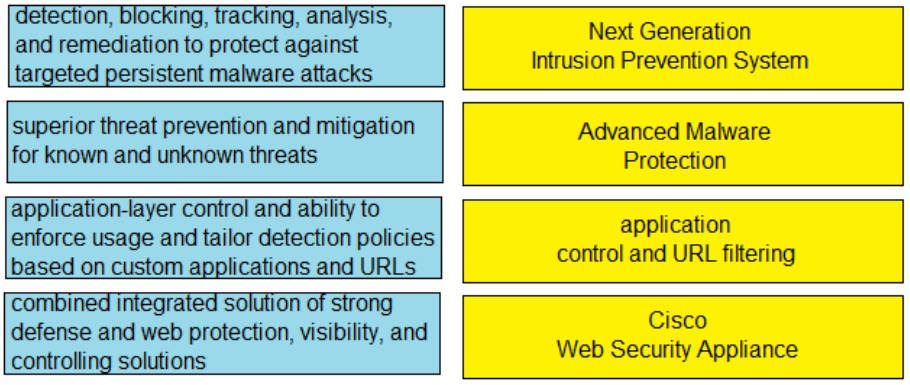
upvoted 1 times

Question #29 *Topic 1*

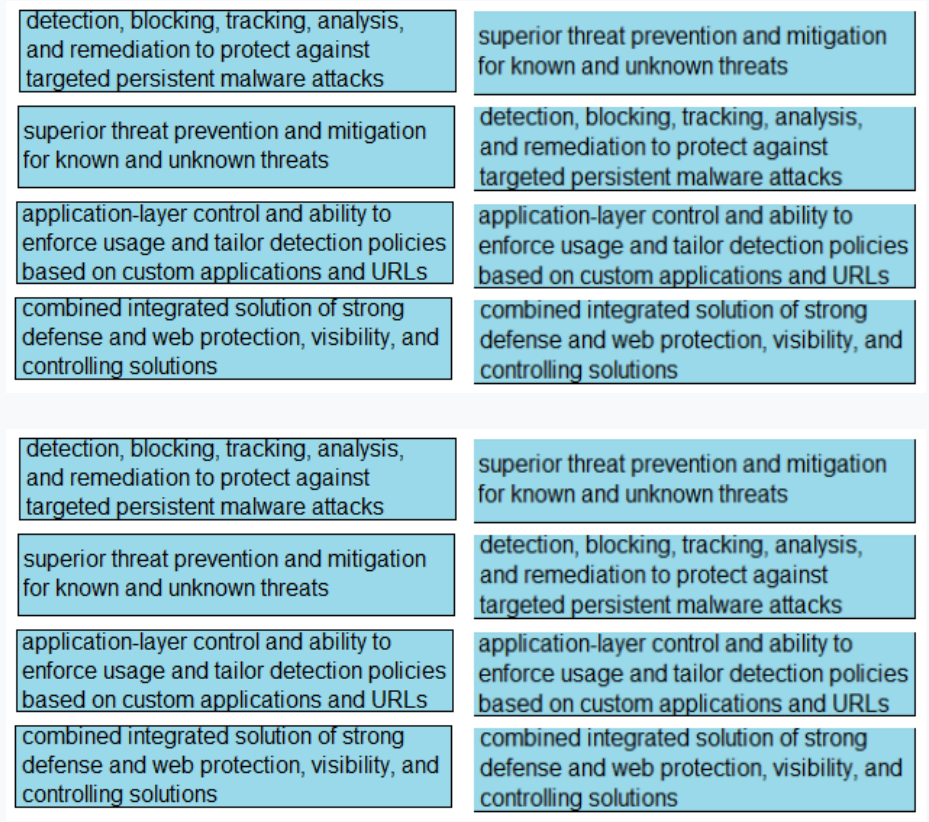
DRAG DROP -

Drag and drop the capabilities from the left onto the correct technologies on the right.

Select and Place:



Suggested Answer:



pohqinan Highly Voted 1 year, 11 months ago

Key word: prevention = Next generation intrusion prevention system Protect = Advanced Malware Protection Application Layer = Application control and URL filtering Combined integrated = Cisco web security Appliance

upvoted 15 times

Question #30 *Topic 1*

Which two key and block sizes are valid for AES? (Choose two.)

A. 64-bit block size, 112-bit key length

B. 64-bit block size, 168-bit key length

C. 128-bit block size, 192-bit key length

D. 128-bit block size, 256-bit key length

E. 192-bit block size, 256-bit key length

Suggested Answer: *C, D*

Reference: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Community vote distribution



CyberGhost666 Most Recent 1 year, 1 month ago

C and D are the correct Answers. AES always uses a fixed block size of 128 bits (16 bytes). This is true for all AES variants (AES-128, AES-192, AES-256).

upvoted 1 times

Marshpillowz 1 year, 10 months ago

C and D are correct

upvoted 1 times

sull3y 3 years ago

C. 128-bit block size, 192-bit key length D. 128-bit block size, 256-bit key length AES (Advanced Encryption Standard) is a symmetric-key encryption algorithm that supports several key and block sizes. The most commonly used key sizes for AES are 128-bit, 192-bit, and 256-bit. The block size is always fixed at 128-bit. AES-128 uses a 128-bit key length and 128-bit block size AES-192 uses a 192-bit key length and 128-bit block size AES-256 uses a 256-bit key length and 128-bit block size Option A and B are not correct because AES does not support 64-bit block size. Option E is not correct because AES does not support 192-bit block size AES-128, AES-192, and AES-256 are the valid key sizes for AES. The block size is always fixed at 128-bit.

upvoted 4 times

nomanlands 3 years, 7 months ago

128 block size is defined in the AES standard

upvoted 1 times

abdulmalik_mail 4 years ago

correct, It's CD

upvoted 3 times

Question #31 *Topic 1*

Which two descriptions of AES encryption are true? (Choose two.)

A. AES is less secure than 3DES.

B. AES is more secure than 3DES.

C. AES can use a 168-bit key for encryption.

D. AES can use a 256-bit key for encryption.

E. AES encrypts and decrypts a key three times in sequence.

Suggested Answer: *B, D*

Reference: https://gpdb.docs.pivotal.io/43190/admin_guide/topics/ipsec.html

Community vote distribution

BD (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

Correct Answers are B and D. AES is more secure than 3DES and AES can use a 256-bit key for encryption.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

B and D are correct

upvoted 1 times

sull3y 3 years ago

B. AES is more secure than 3DES. D. AES can use a 256-bit key for encryption. AES (Advanced Encryption Standard) is a widely used symmetric-key encryption algorithm that is considered to be more secure than its predecessor, 3DES (Triple Data Encryption Standard). AES uses a fixed block size of 128 bits and support key sizes of 128,192, and 256 bits. AES is considered to be more secure than 3DES because it uses a larger block size and key size, which makes it more resistant to brute-force attacks. AES uses a complex substitution-permutation network (SPN) structure which is more secure than the Feistel network of 3DES. Option A is not correct because AES is more secure than 3DES. Option C is not correct because AES does not support a 168-bit key size. Option E is not correct because AES uses only one round of encryption and decryption, not three times. AES-128, AES-192, and AES-256 are the valid key sizes for AES. The block size is always fixed at 128-bit.

upvoted 2 times

abdulmalik_mail 4 years ago

Correct, It's BD Reference : https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

upvoted 3 times

Question #32 *Topic 1*

What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

A. STIX

B. XMPP

C. pxGrid

D. SMTP

Suggested Answer: *A*

Reference:
https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_0100011.pdf

Community vote distribution

A (100%)

sull3y Highly Voted 3 years ago

A. STIX (Structured Threat Information eXpression) is a language format designed to exchange threat intelligence that can be transported over the TAXII (Trusted Automated eXchange of Indicator Information) protocol. STIX enables organizations to share cyber threat intelligence, such as information about malware, vulnerabilities, and indicators of compromise, in a structured and machine-readable format. It allows for the exchange of information about the cyber threats, including details on the threat actors, their tools, and tactics, techniques and procedures (TTPs).

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

A) STIX is the language format designed to exchange threat intelligence, and it is commonly transported over the TAXII protocol.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

A - STIX

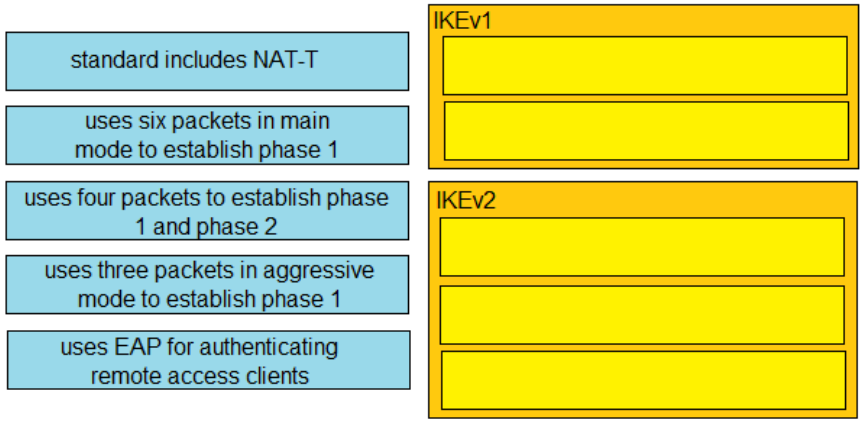
upvoted 1 times

Question #33 *Topic 1*

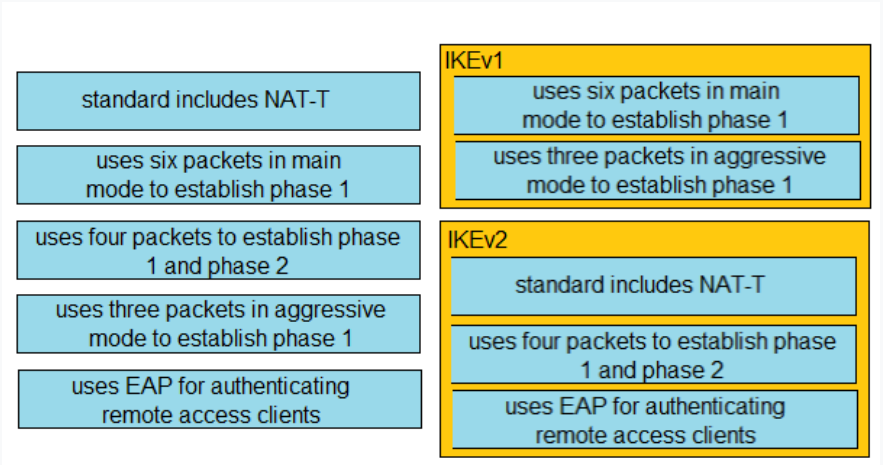
DRAG DROP -

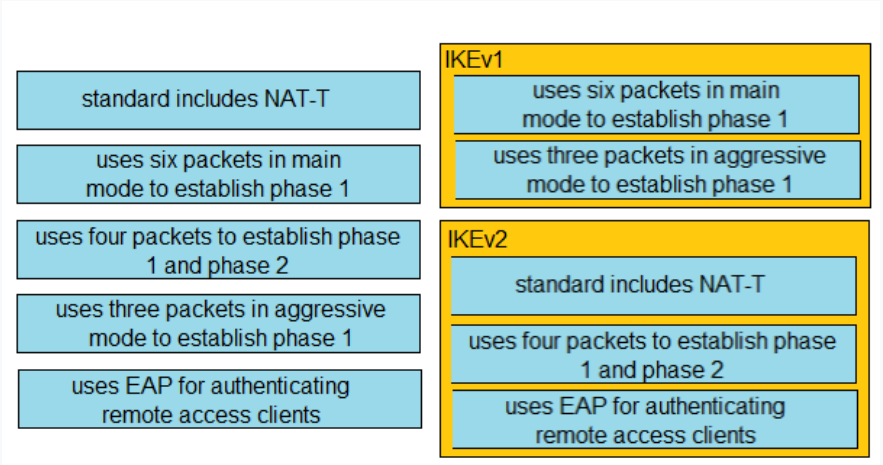
Drag and drop the descriptions from the left onto the correct protocol versions on the right.

Select and Place:



Suggested Answer:





pfunkylol Highly Voted 4 years, 3 months ago

correct.

upvoted 6 times

Marshpillowz Most Recent 1 year, 10 months ago

Correct!

upvoted 2 times

Question #34 *Topic 1*

Which VPN technology can support a multivendor environment and secure traffic between sites?

A. SSL VPN

B. GET VPN

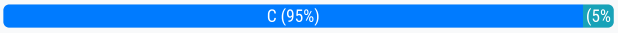
C. FlexVPN

D. DMVPN

Suggested Answer: *C*

Reference: https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

Community vote distribution



nomanlands Highly Voted 3 years, 7 months ago

SSL VPN is a remote access VPN, not a S2S vpn. The question is specifically looking to connect sites. The below comes from the link that is supplied with the answer as well which should've made this very obvious. "Third-party compatibility: As the IT world transitions to cloud- and mobile-based computing, more and more VPN routers and VPN endpoints from different vendors are required. The Cisco IOS FlexVPN solution provides compatibility with any IKEv2-based third-party VPN vendors, including native VPN clients from Apple iOS and Android devices."

upvoted 11 times

ITPro21 Most Recent 1 year, 4 months ago

"Third-party compatibility: As the IT world transitions to cloud- and mobile-based computing, more and more VPN routers and VPN endpoints from different vendors are required. The Cisco IOS FlexVPN solution provides compatibility with any IKEv2-based third-party VPN vendors, including native VPN clients from Apple iOS and Android devices."

upvoted 1 times

Marshpillowz 1 year, 10 months ago

C - FlexVPN

upvoted 1 times

Cokamaniako 2 years, 7 months ago

● Third-party compatibility: As the IT world transitions to cloud- and mobile-based computing, more and more VPN routers and VPN endpoints from different vendors are required. The Cisco IOS FlexVPN solution provides compatibility with any IKEv2-based third-party VPN vendors, including native VPN clients from Apple iOS and Android devices.

upvoted 1 times

sull3y 3 years ago

C. FlexVPN is a VPN technology that can support a multivendor environment and secure traffic between sites. FlexVPN is a Cisco's IOS-based VPN solution that simplifies the configuration and deployment of VPNs. It provides a unified configuration model that simplifies the process of configuring VPNs across multiple vendors, making it a good choice for multivendor environments. FlexVPN can support various types of VPNs such as site-to-site, remote access, and Easy VPN remote connections. It also supports various protocols such as IKEv2, SSL, and IPsec. FlexVPN uses a simplified and unified configuration model, which reduces the complexity of the VPN deployment and allows for easy troubleshooting and maintenance. It also includes advanced features such as IPsec IKEv2, FlexVPN-Cisco Easy VPN, which is a simplified VPN solution for branch offices and teleworkers. In summary, FlexVPN is a Cisco's VPN technology that simplifies the configuration and deployment of VPNs across multiple vendors and provide a secure traffic between sites, it's a great choice for multivendor environments.

upvoted 4 times

smartcarter 3 years, 6 months ago

"FlexVPN relies on open-standards-based IKEv2 as a security technology and provides on top of it many Cisco® specific enhancements to provide high levels of security, added value, and competitive differentiations". https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html FlexVpn supports open source standard - Ikev2 which is also supported by other vendors. C is in order.

upvoted 2 times

nemeses667 3 years, 6 months ago

Can't be A, that is RA - C ● Third-party compatibility: As the IT world transitions to cloud- and mobile-based computing, more and more VPN routers and VPN endpoints from different vendors are required. The Cisco IOS FlexVPN solution provides compatibility with any IKEv2-based third-party VPN vendors, including native VPN clients from Apple iOS and Android devices.

upvoted 1 times

cbadea 3 years, 7 months ago

A is correct

upvoted 1 times

Kevbo02 3 years, 10 months ago

"FlexVPN is a framework to configure IPSec VPNs on CISCO IOS devices". Since it is a multi-vendor environment the answer is A.

upvoted 2 times

Kevbo02 3 years, 10 months ago

"FlexVPN is a framework to configure IPSec VPNs on CISCO IOS devices". Since it is a multi-vendor environment the answer is A.In question there is an information about multivendor environment so I understand that Palo Alto, Fortinet and Cisco must support it. B, C and D are Cisco property so only answer A left.question ask about between sites, ssl vpn is use for remote .So answer is C .

upvoted 2 times

asdasd123123iu 3 years, 8 months ago

In question there is an information about multivendor environment so I understand that Palo Alto, Fortinet and Cisco must support it. B, C and D are Cisco property so only answer A left.

upvoted 2 times

asdasd123123iu 3 years, 8 months ago

In question there is an information about multivendor environment so I understand that Palo Alto, Fortinet and Cisco must support it. B, C and D are Cisco property so only answer A left.question ask about between sites, ssl vpn is use for remote .So answer is C .

upvoted 2 times

royallyre20 3 years, 4 months ago

question ask about between sites, ssl vpn is use for remote .So answer is C .

upvoted 1 times

e_mwas 3 years, 10 months ago

I change my answer to C

upvoted 3 times

mecacig953 3 years, 11 months ago

FlexVPN was created to simplify the deployment of VPNs, to address the complexity of multiple solutions, and as a unified ecosystem to cover all types of VPN: remote access, teleworker, site to site, mobility, managed security services, and others.https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

upvoted 1 times

e_mwas 3 years, 11 months ago

I would go with A, the rest seems like cisco proprietaryssl vpn is for remote access not site to sitePlease keep in mind this is a Cisco Exam ;-)

upvoted 1 times

e_mwas 3 years, 11 months ago

I would go with A, the rest seems like cisco proprietary

upvoted 1 times

haiderzaid 2 years, 10 months ago

ssl vpn is for remote access not site to site

upvoted 1 times

mmenen 3 years, 10 months ago

Please keep in mind this is a Cisco Exam ;-)

upvoted 3 times

Question #35 *Topic 1*

Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

A. DMVPN

B. FlexVPN

C. IPsec DVTI

D. GET VPN

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

Raajaa Highly Voted 4 years, 7 months ago
D is the answer
upvoted 9 times

Kris92 Highly Voted 4 years, 11 months ago
you can use DMVPN with private IPs also GET VPN is more scalable and needs less resources, but can't be used on internet because IP preservation I think they expect GET VPN here
upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago
Selected Answer: D
GETVPN is the correct Cisco technology for secure, scalable, any-to-any VPN connectivity over a private IP cloud.
upvoted 1 times

Marshpillowz 1 year, 10 months ago
Selected Answer: D
D - GetVPN
upvoted 1 times

aal 3 years, 9 months ago
Why not FlexVPN, it can also be used in private networks?
upvoted 1 times

NikoNiko 3 years, 7 months ago
Also DMVPN can be used but GET VPN is better solution.
upvoted 1 times

roolmereyes 2 years, 6 months ago
Because FlexVPN does not support Full Mesh Topology
upvoted 1 times

otzu1 3 years, 10 months ago
Cisco's Group Encrypted Transport VPN (GETVPN) provides a collection of features and capabilities to protect IP multicast group traffic or unicast traffic over a private WAN.

Note "Private"

From the OCG
upvoted 4 times

neta1o 4 years, 1 month ago
This seems to confirm D https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html
upvoted 2 times

thefiresays 4 years, 11 months ago

Over a private line is what they want you to associate GET with.

upvoted 3 times

Javimc 5 years ago

Why not DMVPN?

upvoted 1 times

bobby14 5 years ago

because over a private IP cloud, not public IP like internet.

upvoted 6 times

Question #36 *Topic 1*

What is a commonality between DMVPN and FlexVPN technologies?

A. FlexVPN and DMVPN use the new key management protocol, IKEv2

B. FlexVPN and DMVPN use IS-IS routing protocol to communicate with spokes

C. IOS routers run the same NHRP code for DMVPN and FlexVPN

D. FlexVPN and DMVPN use the same hashing algorithms

Suggested Answer: *C*

Reference: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/#:~:text=In%20its%20essence%2C%20FlexVPN%20is,both%20are%20Cisco's% 20proprietary%20technologies .

Community vote distribution



thefiresays Highly Voted 4 years, 10 months ago

I'm thinking this question should be: what is NOT a commonality? IS-IS routing is not a commonality. Both FlexVPN and DMVPN are compatible with IKEv2, both use NHRP, and they can use the same hashing algorithms.

upvoted 7 times

thefiresays Highly Voted 4 years, 10 months ago

I'm thinking this question should be: what is NOT a commonality? IS-IS routing is not a commonality. Both FlexVPN and DMVPN are compatible with IKEv2, both use NHRP, and they can use the same hashing algorithms.The key is necessity. Both are compatible with IKEv2, but flexVPN supports ONLY IKEv2, where dmvpn also supports IKEv1. So they dont necessarily have the IKE version in communality. Same with Hashing. While they both support the same pool of algorithms, that doesnt necesserily mean that they use the same algorithm in a particular setup.

upvoted 7 times

Dinges 4 years, 7 months ago

The key is necessity. Both are compatible with IKEv2, but flexVPN supports ONLY IKEv2, where dmvpn also supports IKEv1. So they dont necessarily have the IKE version in communality. Same with Hashing. While they both support the same pool of algorithms, that doesnt necesserily mean that they use the same algorithm in a particular setup.

upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago

C appears to be most accurate

upvoted 1 times

otzu1 3 years, 10 months ago

FlexVPN uses NHRP for name resolution I believe. If you pay close attention to the option, it's saying it's the IOS is running the same NHRP being used, which is accurate as it's the build on the IOS. FlexVPN NHRP is primarily used to establish spoke to spoke communication.

upvoted 1 times

abdulmalik_mail 4 years ago

correct, it's C, FlexVPN is based on these same fundamental technologies with DMVPN using IPSEC, GRE and NHRP Reference : https://community.cisco.com/t5/network-security/what-is-the-difference-between-dmvpn-and-flexvpn/td-p/3438913

upvoted 4 times

Steve122 4 years, 3 months ago

Closest answer is C, both use NHRP

upvoted 1 times

Raajaa 4 years, 7 months ago

not clear with the Q

upvoted 1 times

Question #37 *Topic 1*

Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?

A. DTLSv1

B. TLSv1

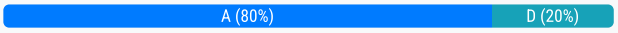
C. TLSv1.1

D. TLSv1.2

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/215331-anyconnect-implementation-and-performanc.html

Community vote distribution



Husein2024 Most Recent 1 year, 8 months ago

DTLS is UDP based which allows it to outperform TLS (TCP based)

upvoted 4 times

Marshpillowz 1 year, 10 months ago

A - DTLS

upvoted 1 times

ch1be2les3 2 years, 1 month ago

The ciphers available are TLS 1.2, DTLS 1.2 and IKEv2. A,B and C are not available on the system. If A was DTLSv1.2 then I think A would be the best choice.

upvoted 1 times

sull3y 3 years ago

A. DTLSv1 (Datagram Transport Layer Security version 1) provides the strongest throughput performance when using Cisco AnyConnect VPN. According to the Cisco document, DTLS (Datagram Transport Layer Security) is the default protocol used by the Cisco AnyConnect VPN Client for SSL connections, it can provide a better throughput performance compared to TLS (Transport Layer Security). DTLS uses UDP as the transport protocol, and it is designed for use in situations where the underlying transport protocol is unreliable, this allows DTLS to be more efficient than TCP-based TLS, especially in situations where network conditions are less than ideal. DTLS is a variation of the TLS protocol that is optimized for use over unreliable networks and is implemented on top of the User Datagram Protocol (UDP) to provide a more efficient and faster data transfer. It provides similar security to TLS and it is used by Cisco AnyConnect VPN client to secure communications between the VPN client and the VPN server.

upvoted 4 times

mecacig953 3 years, 11 months ago

A is correct By default, group policies on ASAs are configured to attempt establishing a DTLS tunnel. If UDP 443 traffic is blocked between the VPN headend and the AnyConnect client, it will automatically fallback to TLS. It is recommended to use DTLS or IKEv2 to increase maximum VPN throughput performance. DTLS offers better performance than TLS due to less protocol overhead. IKEv2 also offers better throughput than TLS. Additionally, using AES-GCM ciphers may slightly improve performance. These ciphers are available in TLS 1.2, DTLS 1.2 and IKEv2.

upvoted 3 times

Question #38 *Topic 1*

Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?

A. Talos

B. PSIRT

C. SCIRT

D. DEVNET

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

sull3y Highly Voted 3 years ago
A. Talos is a group within Cisco that writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats. Talos is a Cisco's threat intelligence team that focuses on identifying and analyzing cyber threats, vulnerabilities, and incidents. They publish a weekly newsletter called the Talos Threat Intelligence Report, which provides information on the latest threats, vulnerabilities, and trends in the cyber security industry. The report also includes technical details and recommendations for mitigating the identified threats. The Talos Threat Intelligence Report is widely read by cybersecurity professionals and organizations worldwide, as it provides valuable information on the latest threats and vulnerabilities, which helps them to better protect their networks and systems.
upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago
A - Cisco Talos
upvoted 1 times

Alizade 2 years, 4 months ago
A. Talos
upvoted 1 times

mm_cisco_2022 3 years, 1 month ago
Sign Up for Weekly Intelligence Updates from the Talos Security Intelligence and Research Group
https://engage2demand.cisco.com/subscribetalosthreatsource
upvoted 2 times

Raajaa 4 years, 7 months ago
A is the answer
upvoted 4 times

Question #39 *Topic 1*

When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?

A. Common Vulnerabilities, Exploits and Threats

B. Common Vulnerabilities and Exposures

C. Common Exploits and Vulnerabilities

D. Common Security Exploits

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

Raajaa Highly Voted 4 years, 7 months ago

B is the answer

upvoted 5 times

johnsonwale Highly Voted 4 years, 4 months ago

It's B. https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

upvoted 5 times

Diegosuarezb Most Recent 1 year, 4 months ago

CVE its B

upvoted 1 times

Marshpillowz 1 year, 10 months ago

B is correct

upvoted 1 times

mhd96far 1 year, 11 months ago

The Common Vulnerabilities and Exposures (CVE) system is a widely adopted standard for identifying and naming security vulnerabilities. It provides a unique identifier (CVE ID) for each known vulnerability, along with additional information about the vulnerability, such as its severity, affected software versions, and potential impact. This standardized approach allows organizations to reference and communicate about vulnerabilities consistently across different platforms and vendors.

upvoted 1 times

sull3y 2 years, 10 months ago

B:When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, the name used is B. Common Vulnerabilities and Exposures (CVE). CVE is a standardized naming convention used to identify and track publicly disclosed cybersecurity vulnerabilities and exposures. It provides a unique identifier for each vulnerability and is used by organizations to reference and communicate about specific vulnerabilities.

upvoted 3 times

Question #40 *Topic 1*

Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two.)

A. accounting

B. assurance

C. automation

D. authentication

E. encryption

Suggested Answer: *B, C*

Reference: https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html

Community vote distribution

BC (100%)

Raajaa Highly Voted 4 years, 7 months ago

B and C

upvoted 7 times

thefiresays Highly Voted 4 years, 11 months ago

Design Automation Provision Assurance

upvoted 7 times

Marshpillowz Most Recent 1 year, 10 months ago

B and C are correct

upvoted 1 times

sull3y 3 years ago

C. automation B. assurance Cisco DNA Center is a network management platform that provides a centralized, programmable, and automated approach to managing and automating the network. The two features that are used in a Software Defined Network solution are Automation and Assurance. Automation: Cisco DNA Center allows for the automation of network configuration and management, which can improve the speed and efficiency of managing the network. Automating repetitive tasks and reducing manual configuration errors can lead to increased network uptime, improved security, and better network performance. Assurance: Cisco DNA Center provides real-time monitoring and analytics for the network, which can be used to proactively identify and resolve issues. This feature allows for the assurance of network performance, security and compliance. With the network's real-time telemetry and historical data, it can identify issues, troubleshoot and resolve them quickly, which ensures a smooth network operation.

upvoted 7 times

Question #41 *Topic 1*

What provides the ability to program and monitor networks from somewhere other than the DNAC GUI?

A. ASDM

B. NetFlow

C. API

D. desktop client

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

Raajaa Highly Voted 4 years, 7 months ago

API...C is the answer

upvoted 7 times

Marshpillowz Most Recent 1 year, 10 months ago

Selected Answer: C

C - API

upvoted 1 times

Question #42 *Topic 1*

What is a function of 3DES in reference to cryptography?

A. It encrypts traffic.

B. It creates one-time use passwords.

C. It hashes files.

D. It generates private keys.

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Raajaa Highly Voted 4 years, 7 months ago

A is the answer

upvoted 6 times

Marshpillowz Most Recent 1 year, 10 months ago

A - encryption

upvoted 1 times

sull3y 3 years ago

A. It encrypts traffic. 3DES (Triple Data Encryption Standard) is a symmetric-key block cipher algorithm that is used to encrypt data. It uses the same key for encrypting and decrypting data, and it is considered to be more secure than its predecessor, the Data Encryption Standard (DES), as it applies the DES algorithm three times in succession to the data, which makes it more resistant to cryptographic attacks. 3DES is widely used in various applications such as virtual private networks (VPNs), electronic commerce (e-commerce), and other secure communications systems, to encrypt and protect data in transit. It is important to note that 3DES is considered less secure than AES (Advanced Encryption Standard) which is now widely recommended.

upvoted 4 times

Question #43 *Topic 1*

Which two activities can be done using Cisco DNA Center? (Choose two.)

A. DHCP

B. design

C. accounting

D. DNS

E. provision

Suggested Answer: *B, E*

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-1/user_guide/ b_dnac_ug_1_2_1/b_dnac_ug_1_2_chapter_00.pdf

Community vote distribution

BE (100%)

Cock Highly Voted 4 years, 2 months ago

Design Automation Provision Assurance

upvoted 10 times

sull3y Highly Voted 3 years ago

B. design E. provision Cisco DNA Center is a network management platform that provides a centralized, programmable, and automated approach to managing and automating the network. The two activities that can be done using Cisco DNA Center are design and provision. Design: Cisco DNA Center provides an intuitive and visual interface for designing, modeling, and simulating the network. It allows network administrators to create and test network configurations before deploying them to the production network. This feature can help to improve the speed and efficiency of managing the network. Provision: Cisco DNA Center provides an automated approach to provisioning and configuring network devices. It allows network administrators to automate repetitive tasks such as configuring network devices, and reducing manual configuration errors can lead to increased network uptime, improved security, and better network performance.

upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago

B and E are correct

upvoted 1 times

Wang87 4 years ago

DNAC can be used for Design and Provision B & E are Correct answers

upvoted 5 times

Question #44 *Topic 1*

Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

A. terminal

B. selfsigned

C. url

D. profile

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

Stardec Highly Voted 4 years, 3 months ago
D. Certificate Enrollment Profiles Certificate enrollment profiles allow users to specify certificate authentication, enrollment, and reenrollment parameters when prompted. The values for these parameters are referenced by two templates that make up the profile. One template contains parameters for the HTTP request that is sent to the CA server to obtain the certificate of the CA (also known as certificate authentication); the other template contains parameters for the HTTP request that is sent to the CA for certificate enrollment.
upvoted 10 times

CyberGhost666 Most Recent 1 year, 1 month ago
D. profile — because it allows separation of authentication and enrollment, and supports HTTP/TFTP-based file retrieval from the server.
upvoted 1 times

Marshpillowz 1 year, 10 months ago
D - profile
upvoted 1 times

Raajaa 4 years, 7 months ago
D is the correct answer
upvoted 2 times

cwolff 4 years, 8 months ago
D seems correct https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-cert-enroll-pki.html#GUID-CF1092E8-D696-491E-A1E2-302CAF9FBB64
upvoted 4 times

Question #45 *Topic 1*

Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat?

A. southbound API

B. westbound API

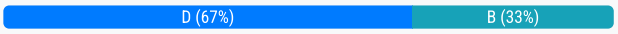
C. eastbound API

D. northbound API

Suggested Answer: *D*

Official Answer: D

Community vote distribution



eazy99 Highly Voted 4 years, 11 months ago

Don't over think it guys, the provided answer is correct. The security application which is the (northbound) is the one who is notifying, (sending the notification to the southbound)

upvoted 12 times

Premium_Pils 2 years ago

Selected Answer: B

I go with B. For me Northbound would be to control policies and simplify the management actions. Westbound is to integrate the controller with other devices, and use inputs received from other devices.

upvoted 2 times

cd1c33b Most Recent 2 months, 4 weeks ago

In SDN architecture: * Applications ↔ Controller = Northbound API * Controller ↔ Network devices = Southbound API So if a security application notifies the controller about a threat, that communication is occurring through a northbound API. That means the more Cisco-aligned exam answer is actually: □ D. northbound API

upvoted 1 times

Premium_Pils 2 years ago

I go with B. For me Northbound would be to control policies and simplify the management actions. Westbound is to integrate the controller with other devices, and use inputs received from other devices.https://learningnetwork.cisco.com/s/question/0D53i00000Kt419CAB/what-is-the-difference-between-northbound-and-southbound-interfaces I reviewed the topic. It should be northbound based on the above article. (Application is sending notification.)

upvoted 2 times

Premium_Pils 1 year, 1 month ago

https://learningnetwork.cisco.com/s/question/0D53i00000Kt419CAB/what-is-the-difference-between-northbound-and-southbound-interfaces I reviewed the topic. It should be northbound based on the above article. (Application is sending notification.)

upvoted 4 times

ffsilveira10 2 years, 4 months ago

I would go with B.

upvoted 2 times

Marshpillowz 2 years, 4 months ago

Answer is D

upvoted 1 times

eriksm 2 years, 10 months ago

Northbound API: Intent-based API Southbound API: controllers -> devices

upvoted 1 times

jku2cya 3 years, 1 month ago

D - application is north of the controller

upvoted 3 times

Carlis 3 years, 4 months ago

Intent (Northbound) APIs - used to enforce the configurations and settings - creating and managing sites - retrieving network health information - policy creation - Rest APIs - Common in web services - Use HTTP requests for data transfer - GET, PUT, POST and DELETE requests

Integration (Westbound) APIs: - Integrate controller with other platforms - Communicate with third-party IT service management solutions - Ticket and request automation - Publish the network data, events and notifications to the external systems Multivendor Support (Southbound) APIs: - Multivendor Software Development Kit (SDK) - SDKs can include multiple APIs - SDKs allow for management of non-Cisco devices

Events and Notifications (Eastbound) APIs: - Allow external systems to take action against notifications - Especially useful for security compliance
upvoted 2 times

appfw 3 years, 4 months ago
Answer is D: Northbound APIs --> communication between Applications and the SDN Controller Southbound APIs --> communication between Network Devices and the SDN Controller
upvoted 3 times

Carlis 3 years, 4 months ago
Intent (Northbound) APIs - used to enforce the configurations and settings - creating and managing sites - retrieving network health information - policy creation - Rest APIs - Common in web services - Use HTTP requests for data transfer - GET, PUT, POST and DELETE requests Integration (Westbound) APIs: - Integrate controller with other platforms - Communicate with third-party IT service management solutions - Ticket and request automation - Publish the network data, events and notifications to the external systems Multivendor Support (Southbound) APIs: - Multivendor Software Development Kit (SDK) - SDKs can include multiple APIs - SDKs allow for management of non-Cisco devices Events and Notifications (Eastbound) APIs: - Allow external systems to take action against notifications - Especially useful for security compliancel would go for Westbound
upvoted 2 times

ddev3737 3 years, 6 months ago
Sorry meant Northbound APIs are typically used to communicate between the SDN controller and the services and applications running over the network. However, in the context of the question provided, a security application is notifying the controller about a specific security threat, which would be accomplished through a Southbound API. Northbound APIs are generally used for different purposes such as automation and orchestration of the network components, whereas Southbound APIs are used for communication between the controller and the underlying network devices.
upvoted 1 times

Carlis 3 years, 4 months ago
I would go for Westbound
upvoted 2 times

ddev3737 3 years, 6 months ago
How about this info? Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the APPLICATIONS and the SDN controller.
upvoted 1 times

ddev3737_111 3 years, 6 months ago
Sorry meant Northbound APIs are typically used to communicate between the SDN controller and the services and applications running over the network. However, in the context of the question provided, a security application is notifying the controller about a specific security threat, which would be accomplished through a Southbound API. Northbound APIs are generally used for different purposes such as automation and orchestration of the network components, whereas Southbound APIs are used for communication between the controller and the underlying network devices.
upvoted 1 times

ddev3737_111 3 years, 6 months ago
How about this info? Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the APPLICATIONS and the SDN controller.
upvoted 1 times

GatPat 3 years, 7 months ago
NorthBound API for sure
upvoted 2 times

SulSulEi 3 years, 11 months ago
Answer is D, check quick video below, https://youtu.be/BUuNgQn3uNc
upvoted 3 times

getafix 4 years, 1 month ago

Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the applications and the SDN controller. In modern environments, applications can tell the network devices (physical or virtual) what type of resources they need and, in turn, the SDN solution can provide the necessary resources to the application. From the Cisco OCG. Answer is D since the question talks about a security application

upvoted 2 times

TesterDude 4 years, 3 months ago

It's D. Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the APPLICATIONS and the SDN controller. Santos, Omar. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide (p. 118). Pearson Education. Kindle Edition.

upvoted 3 times

awsnoob1 4 years, 3 months ago

Answer should be B , the difference between Northbound and Westbound API interfaces is very clear from the bellow link : https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitive-advantage

upvoted 1 times

ospf858 4 years, 4 months ago

Answer should B. https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitive-advantage

upvoted 1 times

Sattm1 4 years, 3 months ago

Westbound should be right: Northbound - intent-based management user to controller Southbound - Controller to network elements Eastbound - Controller to other Applications Westbound - Other software to Controller https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/intent-api-northbound

upvoted 1 times

Question #46 *Topic 1*

An organization has two machines hosting web applications. Machine 1 is vulnerable to SQL injection while machine 2 is vulnerable to buffer overflows. What action would allow the attacker to gain access to machine 1 but not machine 2?

A. sniffing the packets between the two hosts

B. sending continuous pings

C. overflowing the buffer's memory

D. inserting malicious commands into the database

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Raajaa Highly Voted 4 years, 7 months ago

D is the answer

upvoted 10 times

sull3y Highly Voted 3 years ago

D. inserting malicious commands into the database. SQL injection is a type of security vulnerability that allows an attacker to insert malicious code into an SQL statement, allowing them to gain unauthorized access to a database or manipulate its data. This can be done by exploiting vulnerabilities in the way that user input is handled by a web application. So by inserting malicious commands into the database hosted on Machine 1, an attacker can gain access to the database and potentially steal or manipulate data. On the other hand, a buffer overflow is a type of security vulnerability that occurs when more data is written to a buffer than it can hold. This can cause the program to crash or execute arbitrary code, allowing an attacker to gain control of the affected machine. However, in this scenario, Machine 2 is vulnerable to buffer overflows, so overflowing the buffer's memory on Machine 2 would allow the attacker to gain access to Machine 2 but not to Machine 1.

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct answer is D

upvoted 1 times

Marshpillowz 1 year, 10 months ago

D is right

upvoted 1 times

eriksm 2 years, 4 months ago

D is the right answer

upvoted 1 times

Alizade 2 years, 4 months ago

D. inserting malicious commands into the database

upvoted 1 times

eazy99 4 years, 5 months ago

Yup, D it is

upvoted 5 times

Question #47 *Topic 1*

What is the function of SDN southbound API protocols?

A. to allow for the static configuration of control plane applications

B. to enable the controller to use REST

C. to enable the controller to make changes

D. to allow for the dynamic configuration of control plane applications

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

statikd Highly Voted 4 years, 8 months ago
Official Cert Guide: "Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs." But... the Northbound APIs communicates with the control plane applications, not the Southbound APIs. So technically C is still correct, even though Southbound APIs make dynamic changes it still makes changes, hence does not have to say it makes the changes dynamically. This is one of them questions to catch you off guard. The key is the control plane applications. Northbound also uses the REST.
upvoted 7 times

Marshpillowz Most Recent 1 year, 10 months ago
C appears most accurate here
upvoted 1 times

jku2cya 2 years, 7 months ago
C is the best amongst a bunch of really bad alternatives. Don't think its B as there is mention of REST but not REST API. Don't think its either A or D because SDN controllers either control north (application) or south (network/switch)
upvoted 1 times

sull3y 3 years ago
C. to enable the controller to make changes. The southbound API protocol of a Software-Defined Network (SDN) enables communication between the SDN controller and the networking devices, such as switches and routers, in the network. This allows the controller to make changes and manage the network's configuration.
upvoted 4 times

getafix 3 years, 8 months ago
In an SDN architecture, southbound APIs are used to communicate between the SDN controller and the switches and routers within the infrastructure. These APIs can be open or proprietary.Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs. OpenFlow and Cisco OpFlex provide southbound API capabilities. Above is an extract from the OCG (Official Cert Guide for the exam).
upvoted 3 times

TesterDude 3 years, 9 months ago
C Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs. OpenFlow and Cisco OpFlex provide southbound API capabilities. Santos, Omar. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide (p. 118). Pearson Education. Kindle Edition.
upvoted 2 times

Thusi26 4 years, 5 months ago
C How Do SDN Southbound APIs Work? Southbound APIs facilitate control over the network and enable the SDN Controller to dynamically make changes according to real-time demands and needs. OpenFlow, which was developed by the Open Networking Foundation (ONF), is the first and probably most well-known southbound interface. OpenFlow defines the way the SDN Controller should interact with the forwarding plane to make adjustments to the network, so it can better adapt to changing business requirements. With OpenFlow, entries can be added and removed to the internal flow-table of switches and routers to make the network more responsive to real-time traffic demands.
upvoted 4 times

Raajaa 4 years, 7 months ago
I go with C as only Northbound APIs deals with control plane

upvoted 4 times

bazinga31 4 years, 8 months ago

C? But it allows the controller to [dynamically] make changes. Doesn't mention about the control plane?

upvoted 1 times

SirFrates24 4 years, 8 months ago

Southbound APIs facilitate control over the network and enable the SDN Controller to dynamically make changes according to real-time demands and needs. D is the correct answer

upvoted 2 times

SirFrates24 4 years, 8 months ago

Southbound APIs facilitate control over the network and enable the SDN Controller to dynamically make changes according to real-time demands and needs. D is the correct answeri stand corrected. C is the answer

upvoted 2 times

SirFrates24 4 years, 7 months ago

i stand corrected. C is the answer

upvoted 1 times

rad9899 4 years, 9 months ago

D. to allow for the dynamic configuration of control plane applications its correct

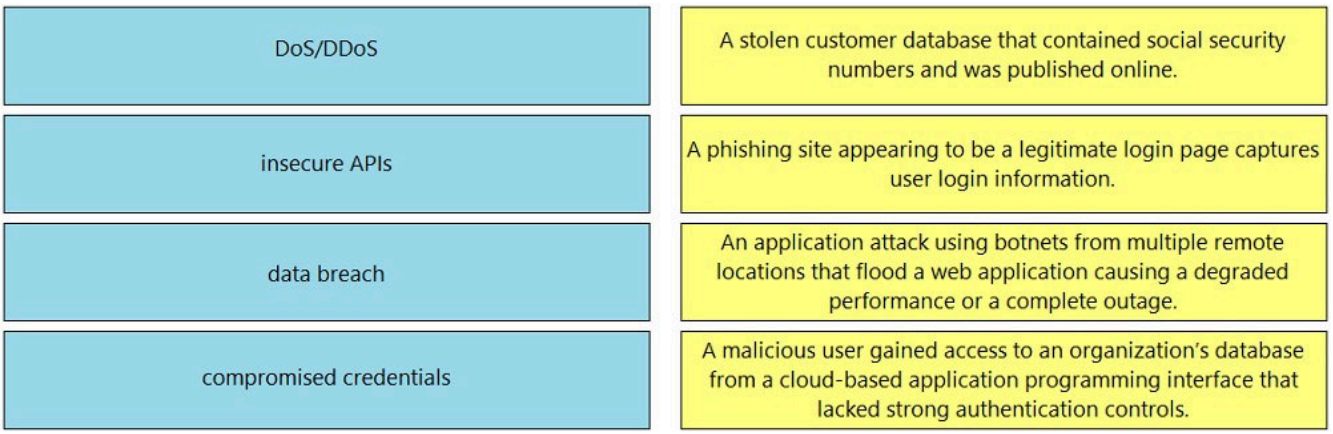
upvoted 3 times

Question #48 *Topic 1*

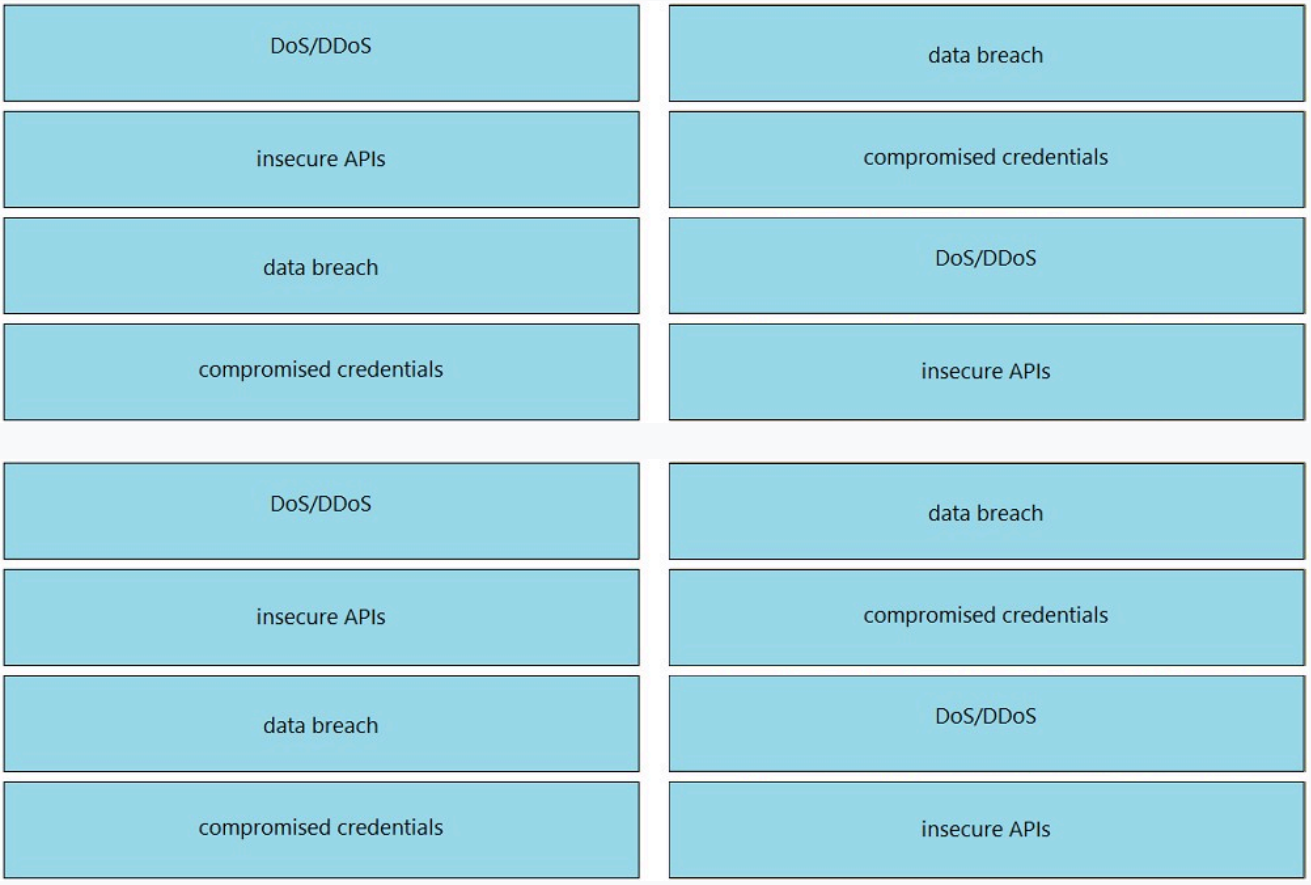
DRAG DROP -

Drag and drop the threats from the left onto examples of that threat on the right.

Select and Place:



Suggested Answer:



Marshpillowz Most Recent 1 year, 10 months ago

Answer is correct

upvoted 2 times

mm_cisco_2022 3 years, 1 month ago

1 - 3 2 - 4 3 - 1 4 - 2

upvoted 2 times

sis_net_sec 3 years, 4 months ago

1-3 2-4 3-1 4-2

upvoted 2 times

Kyle1776 3 years, 11 months ago

1-3 2-4 3-1 4-2

upvoted 3 times

Question #49 *Topic 1*

What is the difference between Cross-site Scripting and SQL Injection attacks?

A. Cross-site Scripting is when executives in a corporation are attacked, whereas SQL Injection is when a database is manipulated.

B. Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.

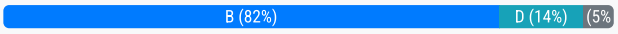
C. Cross-site Scripting is a brute force attack targeting remote sites, whereas SQL Injection is a social engineering attack.

D. Cross-site Scripting is an attack where code is injected into a database, whereas SQL Injection is an attack where code is injected into a browser.

Suggested Answer: *B*

Official Answer: B

Community vote distribution



jaciro11 Highly Voted 3 years, 11 months ago

Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.

upvoted 9 times

sull3y Highly Voted 3 years ago

The correct answer is: B. Cross-site Scripting is an attack where code is executed from the client side, whereas SQL Injection is an attack where code is executed from the server side. In Cross-site scripting (XSS) the attacker injects malicious code into a web page viewed by other users, the code is executed by the client's browser. SQL Injection is a server-side attack, where the attacker manipulates an SQL statement by injecting malicious code into the query. The malicious code is executed on the server, often with the goal of accessing or modifying sensitive data in the database

upvoted 5 times

SomKeat Most Recent 2 months, 3 weeks ago

Answer is A Cross-site Scripting is an attack where malicious code is executed on the client side (browser). SQL Injection is an attack where malicious code is executed on the server side (database)

upvoted 1 times

Husein2024 1 year, 8 months ago

The answer is B

upvoted 1 times

Marshpillowz 1 year, 10 months ago

B is correct

upvoted 1 times

squirrelzzz 1 year, 11 months ago

SQL is injected in browser and runs on server. XSS is injected in browser and loaded into server database then executes on clients browser

upvoted 1 times

ddev3737 3 years ago

Option A is the closest to being correct, as executives in a corporation can be considered targeted users of a website, and XSS is a client-side vulnerability that targets other users of the application.

So, to summarize:

XSS is a client-side vulnerability where malicious code is injected into a website and targets other users of the application, including executives in a corporation. SQLi is a server-side vulnerability where an attacker can manipulate the database of a website by injecting malicious SQL commands.

upvoted 2 times

jku2cya 2 years, 7 months ago

Can't be A because XSS is not whaling. Can't be D because XSS because code is injected into the web app and not database: https://owasp.org/www-community/attacks/xss/ ; and SQL Injection is more about browser input rather than injecting code into a browser: https://owasp.org/www-community/attacks/SQL_Injection

upvoted 2 times

ddev3737_111 3 years ago

Option A is the closest to being correct, as executives in a corporation can be considered targeted users of a website, and XSS is a client-side vulnerability that targets other users of the application. So, to summarize: XSS is a client-side vulnerability where malicious code is injected into a website and targets other users of the application, including executives in a corporation. SQLi is a server-side vulnerability where an attacker can manipulate the database of a website by injecting malicious SQL commands.

upvoted 2 times

psuoh 3 years, 1 month ago

Answer B appears to be the Cisco's choice as correct. Key Concepts of XSS XSS is a web-based attack performed on vulnerable web applications. In XSS attacks, the victim is the user and not the application. In XSS attacks, malicious content is delivered to users using JavaScript.

upvoted 2 times

tom_1991 3 years, 8 months ago

I would say D is most accurate. For XSS malicious links can be inserted into databases, If webpages store and pull links to append to their HTML (instead of manually typing each one in their code click me) so when an unsuspecting user download the page and pulls the links from the database, they unknowingly pull those malicious links as well. The reason why it isn't B is because XSS isn't executed on the server, it is executed on the clients browser when the user initially downloads the HTML page and all associated scripts (.js .css etc). SQL code is sent from the user using HTML form (POST) submission and executed on the server when the server opens a connection to the database and executes the SQL commands. The answer could equally be A as well however, XSS isn't just targeted at executives, It could be targeted at anyone providing there is a vulnerability to exploit.

upvoted 3 times

Metgatz 3 years, 9 months ago

D Explination: Therefore only answer D is left. In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST parameters. Note: The main difference between a SQL and XSS injection attack is that SQL injection attacks are used to steal information from databases whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

upvoted 3 times

brownbear505 3 years, 12 months ago

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

upvoted 2 times

Wang87 4 years ago

Answer is B as XSS happens when Client is exploited and used to run code on another site. 2nd part where SQL injection happens from client end and run on server. Notice the wording it says FROM client which is correct.

upvoted 4 times

bassfunk 4 years, 2 months ago

B is correct. The key word there is "from". They are talking about the origin of the code not where it's being executed.

upvoted 5 times

Brumik 4 years ago

If anything definitely A. XSS is a client side side attack, the code is executed from the clients browser. SQL injection is a server side attack, code is executed on the server side. B is wrong. C+D are completely wrong.

upvoted 2 times

bassfunk 4 years, 2 months ago

B is correct. The key word there is "from". They are talking about the origin of the code not where it's being executed.Yes indeed, it should be BAgreed. Focusing on the keyword reverses the meaning, hence server-side attack (SQL injection) is originated from the client (browser), while client-side attack (XSS) originated from the web server, which is the location the victim queried.

upvoted 5 times

rbrain 4 years, 1 month ago

Yes indeed, it should be B

upvoted 2 times

MerlinTheWizard 1 year ago

Agreed. Focusing on the keyword reverses the meaning, hence server-side attack (SQL injection) is originated from the client (browser), while client-side attack (XSS) originated from the web server, which is the location the victim queried.

upvoted 1 times

duck_hat 4 years, 3 months ago

I think maybe can mean stored XSS and SQL inject A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. https://owasp.org/www-community/attacks/SQL_Injection

upvoted 1 times

eazy99 4 years, 5 months ago

This question is so bad, but I would go with A and here is why. First, all other options is messed up and obviously wrong without questioning. Now, if we look at A, the second part is perfect description for SQL “ SQL Injection is when a database is manipulated” So what about XSS? I would say that because all other options are wrong that leaves us to the fact that when XSS are performed on the corporation internal website, executives and everyone else is attacked. I’m assuming this is why they chose A, the rest of options is so bad.

upvoted 3 times

jaciro11 4 years, 3 months ago

Its B The only problem with A is @Cross-site Scripting is when executives in a corporation are attacked@

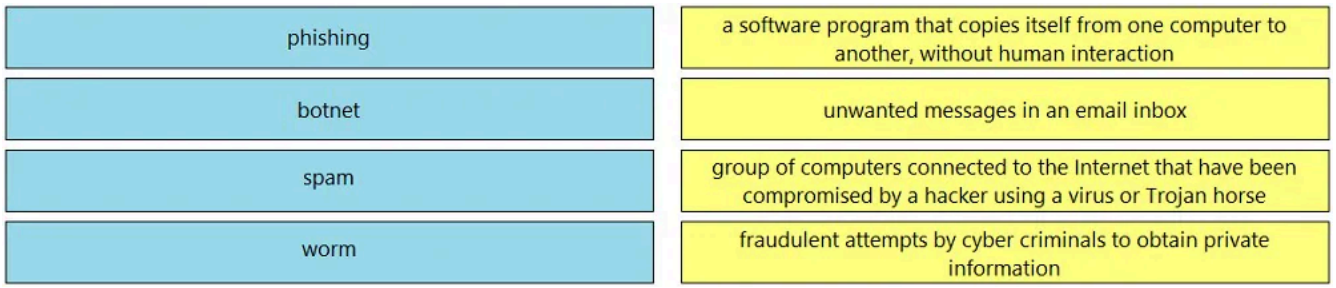
upvoted 3 times

Question #50 *Topic 1*

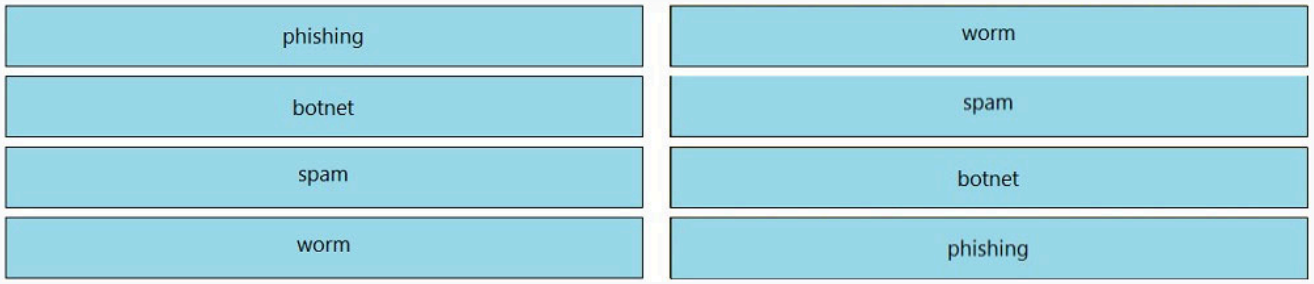
DRAG DROP -

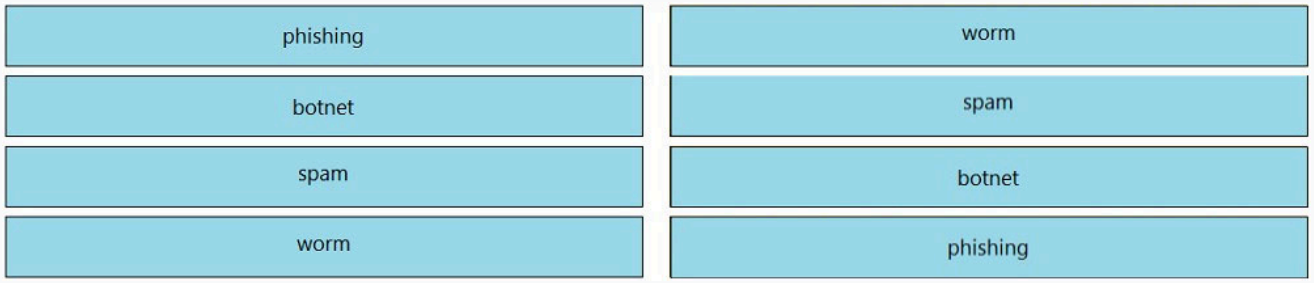
Drag and drop the common security threats from the left onto the definitions on the right.

Select and Place:



Suggested Answer:





flash007 Most Recent 1 year, 10 months ago

Worm copies to other devices

upvoted 2 times

Marshpillowz 1 year, 10 months ago

Answer is correct

upvoted 2 times

mbaviskar01 3 years ago

1 –> 4 2 –> 3 3 –> 2 4 –> 1

upvoted 2 times

Question #51 *Topic 1*

Which type of dashboard does Cisco DNA Center provide for complete control of the network?

A. distributed management

B. service management

C. application management

D. centralized management

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

sull3y Highly Voted 3 years ago

D. centralized management. Cisco DNA Center provides a centralized management dashboard that allows network administrators to have complete control over the network. The dashboard provides a single point of access to manage and monitor all aspects of the network, including devices, users, applications, and services. It allows administrators to easily configure, troubleshoot, and optimize their network, ensuring that it is running at peak performance.

upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago

D - centralized

upvoted 1 times

Question #52 *Topic 1*

Refer to the exhibit. What will happen when this Python script is run?

```
import requests
url = https://api.amp.cisco.com/v1/computers
headers = {
    'accept': 'application/json',
    'Content-type': 'application/json',
    'authorization': "Basic <API Credentials",
    'cache-control': "no-cache",
    }
response = requests.request("GET", url, headers=headers)
print(response.text)
```

A. The list of computers, policies, and connector statuses will be received from Cisco AMP.

B. The list of computers and their current vulnerabilities will be received from Cisco AMP.

C. The compromised computers and malware trajectories will be received from Cisco AMP.

D. The compromised computers and what compromised them will be received from Cisco AMP.

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

CyberGhost666 Most Recent 1 year, 1 month ago
Option A is accurate.
upvoted 1 times

iluvmicrosoft 1 year, 10 months ago
im struggling with this one, all the other json scripts that print multiple records have a for loop: for computer in response_json['data']: hostname = computer['hostname'] print(hostname) how is it printing more than 1 line?Because it is doing an API call without any filter, so in that case it will return all computers.
upvoted 1 times

iluvmicrosoft 1 year, 10 months ago
im struggling with this one, all the other json scripts that print multiple records have a for loop:

for computer in response_json['data']: hostname = computer['hostname'] print(hostname)

how is it printing more than 1 line?
upvoted 1 times

ffsilveira10 1 year, 10 months ago
Because it is doing an API call without any filter, so in that case it will return all computers.
upvoted 2 times

Marshpillowz 1 year, 10 months ago
A is correct
upvoted 1 times

otzu1 3 years, 10 months ago
A https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.amp.cisco.com&api_resource=Computer&api_version=v1
upvoted 4 times

Question #53 *Topic 1*

Refer to the exhibit. What will happen when the Python script is executed?

```
import requests
clinet_id = '<Client ID>'
api_key = '<API Key>'
url = 'https://api.amp.cisco.com/v1/computers'
response = requests.get(url, auth=(client_id, api_key))
response_json = response.json()
for computer in response_json['data']:
    hostname = computer['hostname']
    print(hostname)
```

A. The hostname will be printed for the client in the client ID field.

B. The hostname will be translated to an IP address and printed.

C. The script will pull all computer hostnames and print them.

D. The script will translate the IP address to FQDN and print it.

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

Correct Answer is C

upvoted 1 times

Marshpillowz 1 year, 10 months ago

C is correct

upvoted 1 times

red_sparrow_Gr 2 years, 2 months ago

I believe that the correct answer is A. The for response is for a specific client_ID.....

upvoted 2 times

red_sparrow_Gr 2 years, 2 months ago

I believe that the correct answer is A. The for response is for a specific client_ID.....Answer C is right. The answer to the question of what a client ID is: API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a username and password, and should be treated as such. https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/201121-Overview-of-the-Cisco-AMP-for-Endpoints.html

upvoted 2 times

MPoels 1 year, 11 months ago

Answer C is right. The answer to the question of what a client ID is: API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a username and password, and should be treated as such. https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/201121-Overview-of-the-Cisco-AMP-for-Endpoints.html

upvoted 1 times

Question #54 *Topic 1*

With which components does a southbound API within a software-defined network architecture communicate?

A. applications

B. controllers within the network

C. appliances

D. devices such as routers and switches

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Raajaa Highly Voted 4 years, 7 months ago

D is the answer

upvoted 10 times

flash007 Most Recent 1 year, 10 months ago

Southbound is when it goes to the network devices

upvoted 1 times

Marshpillowz 1 year, 10 months ago

Selected Answer: D

D is correct

upvoted 1 times

alexyozgat24 2 years, 9 months ago

D is correct since SBI(southboundinterface) mainly deals with data plane(network device)

https://www.ciscopress.com/articles/article.asp?p=2995354&seqNum=2

https://ptgmedia.pearsoncmg.com/images/chap16_9781587147135/elementLinks/16fig05_alt.jpg

upvoted 1 times

achille5 2 years, 11 months ago

Selected Answer: D

A southbound API within a software-defined network architecture typically communicates with devices such as routers and switches

upvoted 2 times

dr4gn00t 4 years ago

I think D is the right answer but C is correct also since the question is SDN in general, not just Cisco solutions.

upvoted 1 times

flejd 4 years, 1 month ago

B. Controller to network devices.

upvoted 2 times

asdasd123123iu 3 years, 8 months ago

No, answer B is 'controllers within the network'. Correct is D

upvoted 3 times

Question #55 *Topic 1*

Which method is used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources?

A. BYOD onboarding

B. MAC authentication bypass

C. client provisioning

D. Simple Certificate Enrollment Protocol

Suggested Answer: *D*
Official Answer: D

Community vote distribution
A (44%) C (38%) D (18%)

karmaomar Highly Voted 5 years, 2 months ago
correct answer is A. BYOD onboarding
upvoted 24 times

Tuxzinator 3 years, 6 months ago
Selected Answer: C
C.

The method used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources is C) client provisioning.

Client provisioning is a process of deploying network settings, certificates, and other configuration information to mobile devices to enable them to securely connect to a network. This process involves configuring the supplicant, which is the client software that communicates with the network, to use the appropriate authentication methods and credentials required to access network resources.

BYOD onboarding is a process that enables personal devices to connect to a corporate network, and it may include client provisioning as one of its steps. MAC authentication bypass is a method of granting network access based on the device's MAC address, without requiring any authentication credentials. Simple Certificate Enrollment Protocol (SCEP) is a protocol used for certificate management, but it is not specifically related to configuring the supplicant or deploying network settings to mobile devices.
upvoted 11 times

Tuxzinator Highly Voted 3 years, 6 months ago
C. The method used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources is C) client provisioning. Client provisioning is a process of deploying network settings, certificates, and other configuration information to mobile devices to enable them to securely connect to a network. This process involves configuring the supplicant, which is the client software that communicates with the network, to use the appropriate authentication methods and credentials required to access network resources. BYOD onboarding is a process that enables personal devices to connect to a corporate network, and it may include client provisioning as one of its steps. MAC authentication bypass is a method of granting network access based on the device's MAC address, without requiring any authentication credentials. Simple Certificate Enrollment Protocol (SCEP) is a protocol used for certificate management, but it is not specifically related to configuring the supplicant or deploying network settings to mobile devices.Thank you, ChatGPT?do not trust chat gpt on questions like that, especially for Cisco exams, it makes a lot of mistakesC. Client provisioning (Partially correct but not the best) Client provisioning is a sub-process of BYOD onboarding that can push certificates and configure supplicants. However, in Cisco Identity Services Engine (ISE), client provisioning is more commonly associated with AnyConnect VPN clients and posture assessments, not full BYOD onboarding. It does not necessarily handle all aspects of certificate enrollment like SCEP does within the BYOD process.
upvoted 13 times

nseguy 3 years, 3 months ago
Thank you, ChatGPT?do not trust chat gpt on questions like that, especially for Cisco exams, it makes a lot of mistakes
upvoted 3 times

nseguy 3 years, 3 months ago
Thank you, ChatGPT?
upvoted 3 times

mhd96far 2 years, 5 months ago

do not trust chat gpt on questions like that, especially for Cisco exams, it makes a lot of mistakes

upvoted 2 times

Pierre_Bouvier 1 year, 6 months ago

C. Client provisioning (Partially correct but not the best) Client provisioning is a sub-process of BYOD onboarding that can push certificates and configure supplicants. However, in Cisco Identity Services Engine (ISE), client provisioning is more commonly associated with AnyConnect VPN clients and posture assessments, not full BYOD onboarding. It does not necessarily handle all aspects of certificate enrollment like SCEP does within the BYOD process.

upvoted 2 times

G0909 Most Recent 1 month, 2 weeks ago

In BYOD certificate is deployed automatically for secure cert based authentication.

upvoted 1 times

josmen85 3 months, 2 weeks ago

Explicación técnica (nivel Cisco ISE / Enterprise) En entornos de Cisco Identity Services Engine, el proceso de client provisioning es el mecanismo utilizado para: Instalar automáticamente el supplicant 802.1X Desplegar certificados digitales en el endpoint Configurar perfiles de red (EAP-TLS, PEAP, etc.) Preparar el dispositivo para autenticación segura Esto es exactamente lo que la pregunta describe: configurar supplicant + desplegar certificados en dispositivos (especialmente móviles)

upvoted 1 times

ExamTopicsuser23 5 months, 1 week ago

C is the way

upvoted 1 times

gaurav4101 7 months, 2 weeks ago

If a device supports native supplicant installation BYOD portal can be used while in other case Client provisioning portal is used.

upvoted 1 times

diverjim64 11 months, 3 weeks ago

ISE Cert Guide, p. 487. "BYOD onboarding: this includes registering a device with ISE, provisioning the certificate to the device, and configuring the device's supplicant."

upvoted 1 times

CyberGhost666 1 year, 1 month ago

I'll go with A. Option A is the entire process of securely bringing a personal (non-corporate) device onto the network and includes: • Authenticating the user • Installing a certificate • Configuring the supplicant (like 802.1X or EAP-TLS) • Applying network access policies • It uses client provisioning as one step in the process.

upvoted 1 times

Vroomp 1 year, 6 months ago

Client Provisioning is the process of enabling devices to connect to the network. BYOD is more of allowing personal devices to connect. Client provisioning is the most suitable response, given the options available.

upvoted 1 times

Inoraset 1 year, 8 months ago

BYOD (Bring Your Own Device) onboarding refers to the process of securely enrolling personal mobile devices (e.g., smartphones, tablets) into a network. During onboarding, the following actions typically occur: • Certificates are deployed to the device for secure authentication. • The supplicant (software responsible for 802.1X authentication) is configured to connect to the network. • Security policies are applied to ensure proper access control and compliance. This method is widely used in environments where employees or users bring their own devices and need secure access to enterprise network resources

upvoted 4 times

kloug 1 year, 9 months ago

Answer a

upvoted 1 times

Premium_Pils 1 year, 10 months ago

Jessie and sully seems to have done a good research on the topic

upvoted 1 times

ffsilveira10 2 years, 4 months ago

I would go with D. a) the question don't say nothing if the device is corporate owned or not. So BYOD it doesn't make sense. b) authentication bypass certainly is not a method to deploy certificates. c) client provisioning is not related to certificates deployment.

upvoted 4 times

Marshpillowz 2 years, 4 months ago

I think A - BYOD

upvoted 1 times

4pelos 2 years, 5 months ago

Correct answer A: When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network. Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal. Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod.html

upvoted 3 times

kylesam2017 2 years, 11 months ago

'D' is perhaps the right answer, after all. Simple Certificate Enrollment Protocol (SCEP): SCEP is a protocol that allows mobile devices to request and obtain digital certificates from a certificate authority (CA). The certificates can then be used for authentication and secure network access.

upvoted 1 times

petestudies 2 years, 8 months ago

D for sure. I have done this.

upvoted 1 times

ums008 3 years, 1 month ago

Selected Answer: C

I will go with C:

based on Tuxzinator's response

BYOD encompasses a broader set of activities including client provisioning.

This makes Client Provisioning the more specific answer

upvoted 2 times

KnackerTopf1 2 years, 8 months ago

It is not byod, since it's not explicitly stating that it's about employees own devices, but its rather just client provisioning

upvoted 1 times

Question #56 *Topic 1*

What are two characteristics of Cisco DNA Center APIs? (Choose two.)

A. They are Cisco proprietary.

B. They do not support Python scripts.

C. They view the overall health of the network.

D. They quickly provision new devices.

E. Postman is required to utilize Cisco DNA Center API calls.

Suggested Answer: *C, D*

Official Answer: CD

Community vote distribution

CD (100%)

Dinges Highly Voted 4 years, 7 months ago

C and D are correct -Use the Know Your Network REST methods to GET information about clients, sites, topology, devices, and issues: Retrieve network health information and site and network physical, Layer 2, Layer 3, and VLAN information. -Configuration Templates with the Template Programmer/Editior is a centralized CLI-management tool that facilitates design and provisioning of workflows in Cisco DNA Center. https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/intent-api-northbound Postman is not required: Python, SDK and postman can be used. https://robertcsapo.medium.com/3-simple-ways-to-use-cisco-dna-center-platform-apis-7eee49b76287 These APIs can be open or proprietary. https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2

upvoted 17 times

kornman Highly Voted 4 years, 7 months ago

I believe C & D are correct

upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago

C and D are correct

upvoted 1 times

Naderelmansi 2 years, 11 months ago

It is C and D

upvoted 2 times

mecacig953 3 years, 11 months ago

Postman is not required

upvoted 4 times

brownbear505 3 years, 12 months ago

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/LTRNMS-2500-LG.pdf

upvoted 3 times

Wang87 4 years ago

C & D are correct

upvoted 3 times

efongvan 4 years, 1 month ago

c and d are correct.No doubt.

upvoted 2 times

eazy99 4 years, 5 months ago

I believe C and D

upvoted 2 times

Sarbi 4 years, 5 months ago

c and d are correct.No doubt

upvoted 2 times

Sarbi 4 years, 5 months ago

C and D are Correct

upvoted 2 times

aalnman 4 years, 7 months ago

C and D

upvoted 4 times

itisfakemaillol 4 years, 7 months ago

Vote for C and D

upvoted 4 times

Question #57 *Topic 1*

A company discovered an attack propagating through their network via a file. A custom file detection policy was created in order to track this in the future and ensure no other endpoints execute to infected file. In addition, it was discovered during testing that the scans are not detecting the file as an indicator of compromise. What must be done in order to ensure that the policy created is functioning as it should?

A. Create an IP block list for the website from which the file was downloaded.

B. Block the application that the file was using to open.

C. Upload the hash for the file into the policy.

D. Send the file to Cisco Threat Grid for dynamic analysis.

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

zeroC00L Highly Voted 4 years, 5 months ago

i would go with C here because it looks like they are refering to the "custom detection list" from FMC(Firepower) which is part of the File Policy. With this you can do the following:

Override File Disposition Using Custom Lists If a file has a disposition in the AMP cloud that you know to be incorrect, you can add the file's SHA-256 value to a file list that overrides the disposition from the cloud:

To treat a file as if the AMP cloud assigned a clean disposition, add the file to the clean list.

To treat a file as if the AMP cloud assigned a malware disposition, add the file to the custom detection list.

On subsequent detection, the device either allows or blocks the file without reevaluating the file's disposition. You can use the clean list or custom detection list per file policy.

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_policies_and_advanced_malware_protection.html

upvoted 7 times

sull3y Highly Voted 3 years ago

C. Upload the hash for the file into the policy.

When a custom file detection policy is created in order to track a specific file, it is necessary to ensure that the file is being properly detected by the security scans. One way to do this is by uploading the hash of the file into the policy. The hash, also known as a digital fingerprint, is a unique identification code that is specific to a file. By including the hash of the infected file in the policy, the scans will be able to detect the file based on its unique characteristics, even if the file has been modified or renamed. This ensures that the policy is functioning as it should and that the infected file will be detected in the future.

Although options like blocking the application that the file was using to open, sending the file to Cisco Threat Grid for dynamic analysis or creating an IP block list for the website from which the file was downloaded are good options to prevent the attack but they are not related to the custom file detection policy functionality.

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: C

Correct option is C.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

Selected Answer: C

C is correct

upvoted 1 times

Naderelmansi 2 years, 10 months ago

Selected Answer: C

The correct answer is C. Upload the hash for the file into the policy.

Option A is not an appropriate response to ensure the policy is functioning, as it involves blocking an IP address rather than detecting the file.

Option B is also not an appropriate response, as blocking the application used to open the file may not prevent the file from being downloaded or executed on the endpoint.

Option D is a good practice for threat analysis, but it does not address the issue of the custom file detection policy not detecting the file as an indicator of compromise. Uploading the hash of the file into the policy is a more direct approach to ensuring the policy is functioning as it should.

upvoted 2 times

Emlia1 3 years, 2 months ago

It should be D

upvoted 1 times

sis_net_sec 3 years, 4 months ago

The correct answer is D

upvoted 2 times

otzu1 3 years, 10 months ago

C,

configuring the policy doesn't imply it was configured correctly, add the file hash using sha 256/

OCG:

Simple custom detection allows you to add file signatures, while the advanced custom detections are more like traditional antivirus signatures. Creating a simple custom detection is similar to adding new entries to a blacklist. You define one or more files that you are trying to quarantine by building a list of SHA-256 hashes. If you already have the SHA-256 hash of a file, you can paste that hash directly into the UI, or you can upload files directly and allow the cloud to create the SHA-256 hash for you. To create a simple custom detection, navigate to Outbreak Control > Custom Detections > Simple and the list of all existing simple custom detections appears, as shown in Figure 11-3. To add a new one, you must type it in the Name box and click Save, as shown in Figure 11-3.

upvoted 2 times

Wang87 4 years ago

Selected Answer: C

Answer is C because question is regarding making custom policy work. By adding hash of file the policy will start working as it should. What must be done in order to ensure that the policy created is functioning as it should?

upvoted 4 times

dr4gn00t 4 years ago

Exactly. I was first going with D, but after rereading the question C is best answer. You need to add hash for the custom policy to work. By uploading file to ThreatGrid, it would be detected dynamically but it wouldn't fix the custom detectetion policy, and this is what is been asked.

upvoted 1 times

Cock 4 years, 1 month ago

Selected Answer: C

I prefer C

upvoted 4 times

Jetnor 4 years, 2 months ago

I would vote for D Because these products are designed to work in automatic way so we have to send file to 'threat grid' , and threat grid will automatically update the hash value to AMP database where our device gets updates about threats.

upvoted 1 times

zheka 4 years, 2 months ago

For both AMP for endpoints and AMP under Firepower there's no way upload the hash for the file into the policy. This gives us an option of D - dynamic analysis with threat grid

upvoted 1 times

flejd 4 years, 1 month ago

You are wrong. Within Objects Tab you can find FILE LIST and in there a CUSTOM DETECTION LIST in which you can add/calculate a SH256 checksum.

upvoted 2 times

flejd 4 years, 1 month ago

but in the question they mention that the custom detection list is already prepared so its not C

upvoted 1 times

GatPat 3 years, 1 month ago

But then it also says - "What must be done in order to ensure that the policy created is functioning as it should?" So it would be C to make the policy work

upvoted 2 times

NullNull88 4 years, 2 months ago

Definitely no to A and B. Also not D because we are not sending every single file to threat-grid for analysis as this is not necessary. See documentation on Custom Detection Lists. Answer is C

upvoted 2 times

brownb 4 years, 2 months ago

Im thinking D. If the file is still considered unknown then the hash failed to get a positive ID through AMP so it needs dynamic analysis by sending it to threat grid for sandboxing.

upvoted 1 times

eazy99 4 years, 5 months ago

I believe the answer is C, they already created a custom file, and the scans can't discover it, so they need to upload the hash for the scans to detect it because the scans needs some help to identify the malicious file, and nothing better than the hash in this scenario.

upvoted 4 times

ic0deem 4 years, 5 months ago

I vote for D, since this is Cisco exam and traditional IoCs are not seemed effective

upvoted 1 times

Sarbi 4 years, 5 months ago

I think it is A

upvoted 1 times

Question #58 *Topic 1*

Refer to the exhibit. What does the Python script accomplish?

```
import http.client
import base64
import ssl
import sys

host = sys.argv[1]#"10.10.10.240"
user = sys.argv[2]#"ersad"
password = sys.argv[3]#"Password1"

conn = http.client.HTTPSConnection("{}:9060".format(host),
context=ssl.SSLContext(ssl.PROTOCOL_TLSv1_2))

creds = str.encode(':'.join((user, password)))
encodedAuth = bytes.decode(base64.b64encode(creds))

headers = {
   'accept': "application/json",
   'authorization': " ".join(("Basic",encodedAuth)),
   'cache-control': "no-cache",
   }

conn.request("GET", "/ers/config/internaluser/", headers=headers)

res = conn.getresponse()
data = res.read()

print("Status: {}".format(res.status))
print("Header:\n{}".format(res.header))
print("Body:\n{}".format(data.decode("utf-8")))
```

A. It authenticates to a Cisco ISE server using the username or ersad.

B. It lists the LDAP users from the external identity store configured on Cisco ISE.

C. It authenticates to a Cisco ISE with an SSH connection.

D. It allows authentication with TLSv1 SSL protocol.

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (47%) B (27%) D (20%)

zeroC00L Highly Voted 4 years, 4 months ago

i would go with "A" here because: - B cant be correct the GET is going after /ers/config/internaluser which is ISE own User DB - C cant be correct we we take a lookat the "context=" part we see the connection will be build by using the SSL Libary D cant be correct again if we look at the "context" part we see they take the TLSv1.2 from the ssl libary not TLSv1

upvoted 16 times

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: A

Correct answer is A

upvoted 1 times

4pelos 1 year, 11 months ago

Correct answer B

Note: The purpose of this Python script is used to get the guest users through ISE External RESTful Services (ERS) API. ERS is designed to allow external clients to perform CRUD (Create, Read, Update, Delete) operations on Cisco ISE resources.

upvoted 1 times

blacknblue8 2 years, 7 months ago

Selected Answer: A

Option A is the correct one, the answer has a typo .. as I check on other website the "or" should be "of"

upvoted 4 times

Odorka222 2 years, 9 months ago

Selected Answer: D

it is the same code from cisco web pages :-) https://developer.cisco.com/docs/identity-services-engine/latest/#!internal-users-get-user-by-id/execution

upvoted 1 times

HDragovich 2 years, 9 months ago

not the same look at "context"part its TLSv1_2 not TLSV1

upvoted 1 times

Jessie45785 2 years, 9 months ago

code is not the same, under your link you can clearly see that ssl.PROTOCOL_TLSv1 is listed as a context, in presented question you have ssl.PROTOCOL_TLSv1_2

... additionally it clearly tell you what this script is used for:

This script demonstrates how to use the ISE ERS internal users # # API by executing a Python script. # # # . . .

user = sys.argv[2] # "ersad"

os "A" is the correct answer

upvoted 3 times

iluvmicrosoft 1 year, 10 months ago

its eerily similar tho.. and more interesting when you read what the purpose of the script is - thank you!

upvoted 1 times

stalkr3 2 years, 10 months ago

I think D is the correct one. TLS is backwards-compatible. "After upgrading the default to 1.2, systems using 1.1 and 1.0 will continue to function, so if any of your processing requires 1.0 and 1.1, it will remain available."

upvoted 2 times

Jessie45785 2 years, 10 months ago

Selected Answer: A

I am sorry I have to correct myself A is correct - but the word "or" is probably a typo

upvoted 2 times

Jessie45785 2 years, 10 months ago

Selected Answer: D

Correct answers is D - A - make nonsense whatsoever - B - It is NOT external LDAP but internal DB - C - it is NOT SSH but restapi Call

D - is Correct TLSv1_2 are allowed!

upvoted 2 times

Jessie45785 2 years, 10 months ago

Selected Answer: C

see @GetPat - it is clearly C

upvoted 1 times

GatPat 3 years, 1 month ago

This code imports the http.client, base64, ssl, and sys modules. The http.client module is used to create an HTTP connection, the base64 module is used to encode the user credentials, and the ssl module is used to create an SSL context. The sys module is used to access command line arguments passed to the script.

The code sets the host, user, and password variables to the values of the first, second, and third command-line arguments respectively.

It creates an HTTPS connection to the specified host on port 9060 using the http.client.HTTPSConnection class, passing the hostname and port to the constructor and specifying that the connection should use the SSL/TLS protocol version 1.

The user credentials are then concatenated and encoded using the base64 module. The encoded credentials are saved in the encodedAuth variable.

In summary, this code creates an HTTPS connection to a specified host, using a specified username and password, encoded with base64, and using SSL/TLS protocol version 1.

upvoted 4 times

otzu1 3 years, 10 months ago

A "the" username "or" ersad. I think the sysarg function can prompt if i'm not mistaking

upvoted 2 times

stalkr3 2 years, 10 months ago

How does the function takes ersad from the comment?

upvoted 2 times

ilikevenice 3 years, 10 months ago

This is part of the get-all-internal-users.py script, to extract all internal users from ISE. https://developer.cisco.com/docs/identity-services-engine/v1/#!internal-users-get-all-users/get-all-internal-userspy-source-code

upvoted 3 times

jaciro11 3 years, 11 months ago

Selected Answer: B

A discarded C and D also

upvoted 4 times

jaciro11 3 years, 11 months ago

user ersad is a comment on the code, so A cannot be

upvoted 4 times

dr4gn00t 4 years ago

It is A. Only mistake is that user ersad is only a comment in the script. It will use what ever username is given as a second argument.

upvoted 4 times

gabbar 4 years, 4 months ago

Correct answer should be D

upvoted 1 times

jaciro11 4 years, 3 months ago

Man the AUTH is doing with TLSv1.2 WTF Answer is A

upvoted 4 times

asdasd123123iu 3 years, 8 months ago

A is incorrect because 'ersad' is commented. B is correct answer.

upvoted 2 times

alexyozgat24 2 years, 9 months ago

so i got the point why you are pointing for # comment out but - it is basically not comment out it's for reference sys.argv[1] is calling out ersad. after all other options I think A is make more sense. if the line was starting with #user=sys.argv[1] i would get your point.

upvoted 1 times

stalkr3 2 years, 10 months ago

TLS v1.2 is backwards compatible with v1.0

upvoted 1 times

Question #59 *Topic 1*

What is a difference between GETVPN and IPsec?

A. GETVPN is used to build a VPN network with multiple sites without having to statically configure all devices.

B. GETVPN is based on IKEv2 and does not support IKEv1.

C. GETVPN provides key management and security association management.

D. GETVPN reduces latency and provides encryption over MPLS without the use of a central hub.

Suggested Answer: *D*
Official Answer: D

Alee86 Highly Voted 4 years, 7 months ago

GETVPN Simplifies branch-to-branch instantaneous communications - Ensures low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub

Maximizes security - Provides encryption for MPLS networks while maintaining network intelligence such as full-mesh connectivity, natural routing path, and quality of service (QoS)

Complies with governmental regulation and privacy laws - Helps you meet security compliance and internal regulation by encrypting all WAN traffic

Offers management flexibility - Eliminates complex peer-to-peer key management with group encryption keys

upvoted 11 times

hdrnzienlaoroljol 3 years, 3 months ago

GETVPN Simplifies branch-to-branch instantaneous communications - Ensures low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub

Maximizes security - Provides encryption for MPLS networks while maintaining network intelligence such as full-mesh connectivity, natural routing path, and quality of service (QoS)

Complies with governmental regulation and privacy laws - Helps you meet security compliance and internal regulation by encrypting all WAN traffic

Offers management flexibility - Eliminates complex peer-to-peer key management with group encryption keys

upvoted 1 times

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: D

D. GETVPN reduces latency and provides encryption over MPLS without the use of a central hub.

upvoted 1 times

ITVI 1 year, 4 months ago

Selected Answer: D

D fits the bill based on everyones opnion, but since Cisco likes their marketing, this even fits better!

upvoted 2 times

Rododendron2 2 years, 2 months ago

Selected Answer: C

How can GETVPN reduce latency ? If I will not setup GETVPN, I will have to go via central hub ? No, so why the latency here. C is right answer , D is cisco marketing

upvoted 1 times

RemiK 2 years, 2 months ago

Selected Answer: A

I'll definitely answer A on this one. This looks like the fundamental difference between the two.

upvoted 1 times

XvidalX 2 years, 5 months ago

Selected Answer: D

D "Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub"
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html

upvoted 2 times

4pelos 2 years, 5 months ago

Answer correct D. Checked with securitytut

upvoted 1 times

Stevens0103 2 years, 7 months ago

Selected Answer: D

D. 100% correct.

"Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub"

"GET-based networks can be used in a variety of WAN environments, including IP and MPLS. MPLS VPNs that use this encryption technology are highly scalable, manageable, and cost-effective, and they meet government-mandated encryption requirements."

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html

upvoted 1 times

DaeIsBae 3 years, 6 months ago

Selected Answer: C

C is correct and D is wrong. GETVPN can reduce latency as it allows encrypted traffic to be transported over a pre-existing MPLS network. However, it does not necessarily eliminate the use of a central hub. In GETVPN, a group of routers called Key Servers act as a central hub for key management and security association management. So while GETVPN can provide encryption over MPLS, the use of a central hub is a key component of its design.

upvoted 4 times

Rododendron2 2 years, 2 months ago

key servers are for managment - not hub (= packets traverse via hub), nothing to do with data path and nothing to do with latency

upvoted 2 times

Net4dd 3 years, 7 months ago

This one is C

upvoted 1 times

GatPat 3 years, 7 months ago

Selected Answer: D

Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub

upvoted 1 times

Emlia1 3 years, 7 months ago

Selected Answer: D

I prefer D

upvoted 1 times

Jamesy 3 years, 10 months ago

C is the correct answer. Cheers

upvoted 1 times

surforlife 4 years, 1 month ago

'B" is correct answer. Question is regarding IPSEC differences. GET VPN currently supports only IKEv1.

upvoted 3 times

nemeses667 4 years ago

It does https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-16-6/sec-get-vpn-xe-16-6-book/sec-get-vpn-gikev2.html.xml

upvoted 2 times

psuoh 3 years, 7 months ago

Yep...."The GETVPN G-IKEv2 feature implements Internet Key Exchange version 2 (IKEv2) protocol on GETVPN thereby allowing GETVPN to derive the benefits of IKEv2.":

upvoted 1 times

Fragalot 4 years, 9 months ago

I believe it's C as it does use a central hub for key management and security association.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-16-11/sec-get-vpn-xe-16-11-book/sec-get-vpn.html
upvoted 2 times

Fragalot 4 years, 9 months ago
Must have been asleep when looking into this. It's D.
upvoted 3 times

psuoh 3 years, 7 months ago
Cisco wants you to choose D
upvoted 1 times

psuoh 3 years, 7 months ago
"..Cisco Group Encrypted Transport VPN provides the following benefits:

Provides data security and transport authentication, helping to meet security compliance and internal regulation by encrypting all WAN traffic

Enables high-scale network meshes and eliminates complex peer-to-peer key management with group encryption keys

For Multiprotocol Label Switching (MPLS) networks, maintains network intelligence such as full-mesh connectivity, natural routing path, and quality of service (QoS)

Grants easy membership control with a centralized key server

Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub

Reduces traffic loads on customer premises equipment (CPE) and provider-edge (PE) encryption devices by using the core network for replication of multicast traffic, avoiding packet replication at each individual peer site.."
upvoted 1 times

Question #60 *Topic 1*

Which algorithm provides asymmetric encryption?

A. 3DES

B. RC4

C. AES

D. RSA

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

D. RSA

upvoted 1 times

Marshpillowz 1 year, 10 months ago

D is correct

upvoted 1 times

Naderelmansi 2 years, 10 months ago

The most widely used asymmetric encryption algorithm is RSA (Rivest-Shamir-Adleman) algorithm.

upvoted 2 times

sull3y 3 years ago

D. RSA RSA is an algorithm that provides asymmetric encryption, which means that it uses a pair of keys, one for encryption and one for decryption. Data is encrypted with the public key and can only be decrypted with the corresponding private key. RSA is widely used in various applications, such as digital signatures, software protection, and secure communications. 3DES, RC4, and AES are symmetric encryption algorithms which means they use the same key for encryption and decryption. 3DES is a symmetric-key block cipher that applies the Data Encryption Standard (DES) algorithm three times to each data block. RC4 is a symmetric stream cipher, it's known for its simplicity and speed AES is a symmetric block cipher that supports key sizes of 128, 192, and 256 bits.

upvoted 4 times

migueli 3 years, 7 months ago

https://www.cisco.com/c/en/us/products/security/encryption-explained.html#~types-of-encryption RSA is asymmetric cryptography, so there is one public key and one private key.

upvoted 2 times

Question #61 *Topic 1*

What is a difference between an XSS attack and an SQL injection attack?

A. SQL injection is a hacking method used to attack SQL databases, whereas XSS attack can exist in many different types of applications.

B. XSS attacks are used to steal information from databases, whereas SQL injection attacks are used to redirect users to websites where attackers can steal data from them.

C. XSS is a hacking method used to attack SQL databases, whereas SQL injection attacks can exist in many different types of applications.

D. SQL injection attacks are used to steal information from databases, whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Marshpillowz Most Recent 1 year, 10 months ago

D is correct

upvoted 1 times

sull3y 3 years ago

D. SQL injection attacks are used to steal information from databases, whereas XSS attacks are used to redirect users to websites where attackers can steal data from them. Cross-site scripting (XSS) is a type of security vulnerability that allows attackers to inject malicious code into a website, which can be executed by unsuspecting users when they visit the website. The malicious code can be used to steal information from the user's browser, such as login credentials or personal information. XSS attacks can exist in many different types of applications, including web-based applications, mobile apps, and even PDFs. SQL injection is a type of attack that targets SQL databases. The attacker injects malicious SQL code into a web application's input fields, which can be executed by the database. This can allow the attacker to steal sensitive information from the database, such as login credentials, credit card numbers, and other sensitive data. SQL injection attacks can exist in many different types of applications that use SQL databases, including web-based applications, mobile apps, and even PDFs.According your comment, "XSS can exist in many different types of applications" This is true in A. So why is the answer not A?

upvoted 2 times

sull3y 3 years ago

D. SQL injection attacks are used to steal information from databases, whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

Cross-site scripting (XSS) is a type of security vulnerability that allows attackers to inject malicious code into a website, which can be executed by unsuspecting users when they visit the website. The malicious code can be used to steal information from the user's browser, such as login credentials or personal information. XSS attacks can exist in many different types of applications, including web-based applications, mobile apps, and even PDFs.

SQL injection is a type of attack that targets SQL databases. The attacker injects malicious SQL code into a web application's input fields, which can be executed by the database. This can allow the attacker to steal sensitive information from the database, such as login credentials, credit card numbers, and other sensitive data. SQL injection attacks can exist in many different types of applications that use SQL databases, including web-based applications, mobile apps, and even PDFs.

upvoted 2 times

networkhanim 2 years, 8 months ago

According your comment, "XSS can exist in many different types of applications" This is true in A. So why is the answer not A?

upvoted 2 times

GatPat 3 years, 1 month ago

Should be D

upvoted 2 times

NullNull88 4 years, 2 months ago

There can be no other answer,.. D

upvoted 4 times

kapplejacks 4 years, 4 months ago

Answer: D If it said for A "web applications" sure thats a good fit but applications are not subjected to XSS, only web applications are. A is invalid, answer D!

upvoted 3 times

eazy99 4 years, 5 months ago

A and D are correct, but D is better answer.

upvoted 2 times

Jayde 4 years, 5 months ago

I believe A is the answer

upvoted 4 times

Question #62 *Topic 1*

What is a difference between a DoS attack and DDos attack?

A. A DoS attack is where a computer is used to flood a server with TCP packets, whereas DDoS attack is where a computer is used to flood a server with UDP packets.

B. A DoS attack is where a computer is used to flood a server with UDP packets, whereas DDoS attack is where a computer is used to flood a server with TCP packets.

C. A DoS attack is where a computer is used to flood a server with TCP and UDP packets, whereas DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN.

D. A DoS attack is where a computer is used to flood a server with TCP and UDP packets, whereas DDoS attack is where multiple systems target a single system with a DoS attack.

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

sull3y Highly Voted 3 years ago
D. A DoS attack is where a computer is used to flood a server with TCP and UDP packets, whereas DDoS attack is where multiple systems target a single system with a DoS attack. A Denial of Service (DoS) attack is a type of cyber attack in which a single system floods a server with a large number of packets, overwhelming the server and causing it to become unavailable to legitimate users. The goal of a DoS attack is to prevent legitimate users from accessing the targeted server by consuming its resources or causing it to crash. A Distributed Denial of Service (DDoS) attack is a more sophisticated form of a DoS attack. In a DDoS attack, multiple systems, often compromised through malware, are used to flood a single server with packets, overwhelming it and making it unavailable to legitimate users. The goal of a DDoS attack is the same as a DoS attack, but the scale of the attack is much larger and the resources used to launch the attack are distributed across multiple systems. This makes DDoS attacks much harder to detect and mitigate.
upvoted 6 times

Marshpillowz Most Recent 1 year, 10 months ago
D is correct
upvoted 1 times

Naderelmansi 2 years, 10 months ago
The correct answer is D. A Denial of Service (DoS) attack and a Distributed Denial of Service (DDoS) attack are both types of attacks that aim to overwhelm a system or network, making it unavailable to users. However, the key difference between the two is the number of attacking systems involved. A DoS attack is typically launched from a single source, such as a single computer, and is intended to overwhelm a targeted system or network with traffic, making it unavailable to users. A DDoS attack, on the other hand, is launched from multiple systems, often a large number of compromised systems that form a botnet, and is intended to overwhelm the targeted system or network with a massive volume of traffic.
upvoted 3 times

Question #63 *Topic 1*

What are two advantages of using Cisco AnyConnect over DMVPN? (Choose two.)

A. It provides spoke-to-spoke communications without traversing the hub.

B. It enables VPN access for individual users from their machines.

C. It allows multiple sites to connect to the data center.

D. It allows different routing protocols to work over the tunnel.

E. It allows customization of access policies based on user identity.

Suggested Answer: *B, E*

Cisco Anyconnect is a Remote access VPN client based solution where users can install the client on their machines and can connect to the respective VPN devices (ASA/FTD/Router). In order to secure connectivity for Anyconnect Users, one can also create custom access policies to ensure proper conditions are met before access is granted to the VPN user.

Community vote distribution

BE (100%)

Marshpillowz Most Recent 1 year, 10 months ago

Selected Answer: BE

B and E are correct

upvoted 1 times

sull3y 2 years, 10 months ago

The two advantages of using Cisco AnyConnect over DMVPN are:

B. It enables VPN access for individual users from their machines. AnyConnect provides a client-based VPN solution that allows individual users to securely access the corporate network from their own machines or devices, whereas DMVPN is a site-to-site VPN solution that requires network devices to establish a secure tunnel between them.

E. It allows customization of access policies based on user identity. AnyConnect provides a robust identity-based access control solution, allowing network administrators to define different access policies for different users or groups of users. DMVPN does not provide such granular control over access policies.

upvoted 3 times

pioo1979 2 years, 11 months ago

Is there any situation when I have to choose between Anyconnect and DMVPN?

upvoted 3 times

Karitza 2 years, 1 month ago

No, because there are different types of vpn. Anyconnect application is used for remote access vpn to a concentrator la cisco ASA or cisco Secure Firewall and DVPN si a type of vpn that is applied in a hub and spoke topology (DMVPN only works for cisco).

upvoted 1 times

Question #64 *Topic 1*

What is the difference between a vulnerability and an exploit?

A. A vulnerability is a weakness that can be exploited by an attacker.

B. A vulnerability is a hypothetical event for an attacker to exploit.

C. An exploit is a hypothetical event that causes a vulnerability in the network.

D. An exploit is a weakness that can cause a vulnerability in the network.

Suggested Answer: *A*
Reference: https://debricked.com/blog/what-is-security-weakness/#:~:text=A%20vulnerability%20is%20a%20weakness,when%20it%20can%20be%20exploited.&text=This%20is%20a%20%E2%80%9Ccommunity%2Ddeveloped,of%20common%20software%20security%20weaknesses%E2%80%9D .

Community vote distribution

A (100%)

Naderelmansi Highly Voted 2 years, 10 months ago

The correct answer is A. A vulnerability is a weakness or flaw in a system, software, or network that can be exploited by an attacker to compromise the security or functionality of the system. A vulnerability can be caused by a variety of factors, including coding errors, misconfigurations, or design flaws. An exploit, on the other hand, is a tool or technique used by an attacker to take advantage of a vulnerability and gain unauthorized access or control over the target system. An exploit can be a piece of software, a script, or a command that leverages a vulnerability to execute malicious code or actions on the target system. Therefore, the difference between a vulnerability and an exploit is that a vulnerability is a weakness that can be exploited by an attacker, while an exploit is the means by which an attacker takes advantage of a vulnerability to compromise the system.

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct Answer is A.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

A is correct here

upvoted 1 times

Felice44 2 years, 11 months ago

No doubt, the vulnerability creates access to the exploit

upvoted 3 times

Question #65 *Topic 1*

What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?

A. threat intelligence

B. Indicators of Compromise

C. trusted automated exchange

D. The Exploit Database

Suggested Answer: *A*

Reference: https://en.wikipedia.org/wiki/Cyber_threat_intelligence

Community vote distribution

A (100%)

uditpatel1 Most Recent 1 month ago

A is right. Let's go down the question. What is the phrase for 'having knowledge' about threats and threat actors that 'helps minimise detrimental' occurrences that would otherwise 'compromise' networks or systems? This is what I am thinking: information, migration, and compromise.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

A is correct

upvoted 1 times

Naderelmansi 2 years, 10 months ago

The correct answer is A. The term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems is "threat intelligence." Threat intelligence refers to the knowledge and insights gained from analyzing and understanding potential threats and threat actors, including their tactics, techniques, and procedures (TTPs). By leveraging threat intelligence, organizations can better understand the risks they face and take proactive steps to prevent or mitigate potential attacks. Threat intelligence can come from a variety of sources, including open-source intelligence, commercial threat intelligence feeds, and internal security operations.

upvoted 3 times

Felice44 2 years, 11 months ago

Certainly A

upvoted 3 times

Question #66 *Topic 1*

Refer to the exhibit. An engineer is implementing a certificate based VPN. What is the result of the existing configuration?

```
crypto ikev2 name-mangler MANGLER
 dn organization-unit
```

A. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully.

B. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.

C. The OU of the IKEv2 peer certificate is set to MANGLER.

D. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER.

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

Smileebloke Highly Voted 3 years, 9 months ago

B: Configuring the IKEv2 Name Mangler Perform this task to specify the IKEv2 name mangler, which is used to derive a name for authorization requests and obtain AAA preshared keys. The name is derived from specified portions of different forms of remote IKE identities or the EAP identity.

enable configure terminal crypto ikev2 name-mangler mangler-name dn {common-name | country | domain | locality | organization | organization-unit | state} eap {all | dn {common-name | country | domain | locality | organization | organization-unit | state} | prefix | suffix {delimiter {. | @ | \}}} email {all | domain | username} fqdn {all | domain | hostname} end dn = Derives the name from any of the noted fields in the remote identity of type DN common-name country domain locality organization organization-unit state

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16-10/sec-flex-vpn-xe-16-10-book/sec-cfg-flex-serv.html=

upvoted 5 times

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: B

B. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

Selected Answer: B

B is correct

upvoted 1 times

Naderelmansi 2 years, 10 months ago

Selected Answer: B

The correct answer is B.

The "match identity certificate" command in the IKEv2 authorization policy is used to specify that the OU (Organizational Unit) attribute of the IKEv2 peer certificate should be used as the identity when matching the policy. The OU attribute is set to "MANGLER" in this case.

So, when an IKEv2 peer with a certificate that has an OU attribute of "MANGLER" attempts to establish an IKEv2 SA, the router will use the OU attribute as the identity when matching the authorization policy. If the policy is a match, the SA will be established successfully.

upvoted 4 times

Question #67 *Topic 1*

Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?

A. event

B. intent

C. integration

D. multivendor

Suggested Answer: *B*

Cisco is moving towards intent based networking and DNA center is a new addition to the solution offerings from Cisco.

Community vote distribution

B (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

B) Intent APIs allow administrators or external applications to express what they want the network to do (the “intent”), and DNA Center translates that into the actual configurations.across the infrastructure.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

B is correct

upvoted 1 times

Carlis 2 years, 10 months ago

event - eastbound intent - northbound integration - westbound multivendor - southbound

upvoted 4 times

Naderelmansi 2 years, 10 months ago

Therefore, the correct answer is B, Intent API. The API used with Cisco DNA Center to provision SSIDs, QoS policies, and update software versions on switches is the Cisco DNA Center Intent API. This API allows network administrators to automate network infrastructure tasks by expressing their intent through high-level policies rather than low-level device-specific configuration commands. The Cisco DNA Center Intent API uses RESTful APIs to provide a standardized interface for interacting with the network infrastructure. It allows network administrators to define their intent using JSON-based data models and use those models to provision, configure, and manage the network infrastructure.

upvoted 2 times

loser4fun 2 years, 11 months ago

B. Intent Intent API is a type of API that allows developers to program the desired intent for the network rather than the specific configuration details. Intent API simplifies the process of network automation by abstracting the complexity of device-specific configurations and providing a more natural and intuitive way to interact with the network. Cisco DNA Center uses Intent API to provide a simplified way to configure and manage network devices. With Intent API, administrators can specify the intent of the configuration, such as creating a new SSID or updating a QoS policy, and DNA Center takes care of the underlying device-specific configurations.

upvoted 1 times

sull3y 3 years ago

B. intent Cisco DNA Center uses Intent APIs to provision SSIDs, QoS policies, and update software versions on switches. Intent APIs allow the network administrator to define high-level policies, such as "this SSID should have these characteristics" or "this switch should run this version of software," and the Cisco DNA Center platform automatically translates those policies into the necessary low-level configurations on the network devices. This simplifies the management of the network and allows for a more automated and consistent provisioning process.

upvoted 3 times

Question #68 *Topic 1*

A network engineer needs to select a VPN type that provides the most stringent security, multiple security associations for the connections, and efficient VPN establishment with the least bandwidth consumption. Why should the engineer select either FlexVPN or DMVPN for this environment?

A. DMVPN because it uses multiple SAs and FlexVPN does not.

B. DMVPN because it supports IKEv2 and FlexVPN does not.

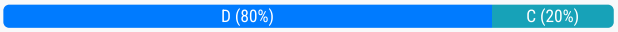
C. FlexVPN because it supports IKEv2 and DMVPN does not.

D. FlexVPN because it uses multiple SAs and DMVPN does not.

Suggested Answer: *D*

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16-12/sec-flex-vpn-xe-16-12-book/sec-cfg-flex-serv.html

Community vote distribution



Smileebloke Highly Voted 4 years, 3 months ago

IKEv2 Multi-SA The IKEv2 Multi-SA feature allows an IKEv2 Dynamic Virtual Tunnel Interface (DVTI) session on the IKEv2 responder to support multiple IPsec Security Associations (SA). The maximum number of IPsec SAs per DVTI session is either obtained from AAA authorization or configured on the IPsec profile. The value from AAA has a higher priority. Any change to the max-flow-limit argument in the IPsec profile is not applied to the current session but is applied to subsequent sessions. The IKEv2 Multi-SA feature makes the configuration of the IKEv2 profile in the IPsec profile optional. This optional configuration allows IPsec DVTI sessions using the same virtual template to have different IKEv2 profiles, thus saving the number of virtual template configurations.

Note The IKEv2 Multi-SA feature allows multiple IPsec SAs that have non-any-any proxies. However, when the IPsec SA proxies are any-any, a single IPsec SA is allowed.

For more information, see the “Multi-SA Support for Dynamic Virtual Tunnel Interfaces for IKEv2” module in the Security for VPNs with IPsec Configuration Guide.

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: D

Correct answer is D.

> DMVPN typically uses IKEv1 (though can be configured for IKEv2 in some cases).

upvoted 1 times

willroute 1 year, 9 months ago

Tricky question, as DMVPN can do it with sharing ipsec tunnel, so both can do it, but most logical is D....Cisco style question.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-share-ipsec-w-tun-protect.html#:~:text=Glossary%20Close-,Sharing%20IPsec%20with%20Tunnel%20Protection,results%20in%20network%20connectivity%20problems.&text=Security%20threats%20and%20the%20cryptographic,Encryption%20(NGE)%20white%20paper.

upvoted 2 times

Nonono2 2 years, 1 month ago

Selected Answer: C

The answer is C

upvoted 1 times

jku2cya 3 years, 1 month ago

Selected Answer: D

DMVPN can be configured with IKEv2, so answer is not C. I wasn't able to find Cisco documentation to back this up, but found this configuration example: https://journey2theccie.wordpress.com/2020/03/13/ikev1-ikev2-configuration-in-dmvpn/

upvoted 3 times

alexyozgat24 3 years, 3 months ago

Really like the comment on following link for this discussion, per say- it looks like Answer is C https://community.cisco.com/t5/network-security/what-is-the-difference-between-dmvpn-and-flexvpn/td-p/3438913

upvoted 1 times

psuoh 3 years, 7 months ago

What is the difference between FlexVPN and DMVPN? IPSec: One key difference between FlexVPN and default Dynamic Multipoint VPN (DMVPN) is the protocol used for negotiating IPsec Security Associations (SAs). While DMVPN defaults to using Internet Key Exchange version 1 (IKEv1), FlexVPN utilizes IKEv2.

upvoted 2 times

psuoh 3 years, 7 months ago

ANswer is C

upvoted 1 times

johnnybgud 3 years, 7 months ago

But DMVPN definitely support IKEv2, and Answer C says "...DMVPN does not". Therefore answer is likely D.

upvoted 4 times

Question #69 *Topic 1*

Refer to the exhibit. Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

Interface	MAC Address	Method	Domain	Status	Fg Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth	0A02198200000
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

A. show authentication registrations

B. show authentication method

C. show dot1x all

D. show authentication sessions

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

dzef13 Highly Voted 4 years, 8 months ago

D is correct answer

upvoted 5 times

yenp Highly Voted 4 years, 7 months ago

answer is D Displaying the Summary of All Auth Manager Sessions on the Switch Enter the following:

Switch# show authentication sessions Interface MAC Address Method Domain Status Session ID Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58 Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago

Selected Answer: D

D is correct

upvoted 1 times

Totosos1 2 years, 10 months ago

Selected Answer: D

Absolutely 'D' is the answer here:

https://www.ciscozine.com/basic-troubleshooting-dot1x-via-cli/?utm_content=cmp-true

upvoted 1 times

surforlife 3 years, 6 months ago

D=correct Usage Guidelines Use the show authentication sessions command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

Examples The following example shows how to display all authentication sessions on the switch:

Device# show authentication sessions

Interface MAC Address Method Domain Status Session ID Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58 Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

upvoted 2 times

nenotronix 3 years, 7 months ago

D is the correct answer "show authentication sessions"

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html

upvoted 2 times

Jardator 3 years, 9 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/50sg/configuration/guide/Wrapper-46SG/dot1x.html#wp1133930

upvoted 1 times

otzu1 3 years, 10 months ago

D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137

Ctrl F "show authentication sessions"

upvoted 2 times

brownbear505 3 years, 12 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137

upvoted 4 times

MoBreezy 4 years ago

Selected Answer: D

The only way to display the above output on a catalyst switch is to enter the show authentication sessions command and nothing else.

100% going with D

upvoted 3 times

Sun2sun 4 years ago

Selected Answer: D

D is correct

upvoted 3 times

NullNull88 4 years, 2 months ago

D is the correct answer

upvoted 3 times

pfunkylol 4 years, 3 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137

upvoted 4 times

Cisco_SecCol_111 4 years, 4 months ago

D is correct. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137

upvoted 3 times

Sarbi 4 years, 5 months ago

D is correct. The following example shows how to display all authentication sessions on the switch:

Device# show authentication sessions

Interface MAC Address Method Domain Status Session ID Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58 Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10

upvoted 3 times

Raajaa 4 years, 7 months ago

Answer is D

upvoted 4 times

samismayilov 4 years, 9 months ago

Question is generate this output and to show which ports are authenticating with dot1x or mab? And for this output u must use show authentication method , so answer is correct B!

upvoted 2 times

Question #70 *Topic 1*

Refer to the exhibit. What does the number 15 represent in this configuration?

```
snmp-server group SNMP v3 auth access 15
```

A. privilege level for an authorized user to this router

B. access list that identifies the SNMP devices that can access the router

C. interval in seconds between SNMPv3 authentication attempts

D. number of possible failed attempts until the SNMPv3 user is locked out

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

Cisco_SecCol_111 Highly Voted 4 years, 4 months ago

B is correct. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-16/snmp-xe-16-book/nm-snmp-cfg-snmp-support.html#GUID-10FB2FAD-39A6-41D8-AB14-0C4B6E20911F

upvoted 9 times

Marshpillowz Most Recent 1 year, 10 months ago

Selected Answer: B

B is correct

upvoted 2 times

Question #71 *Topic 1*

What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX

B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX

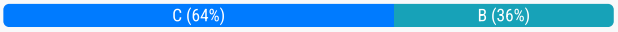
C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX

D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

Suggested Answer: *B*

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c4.html#wp6039879000

Community vote distribution



Ampersand Highly Voted 5 years, 5 months ago

B is correct. When you use “address” it is referring to the remote peer you share the key with. If you want to add more than 1 ip add, you will have to use group key.

upvoted 18 times

Ampersand Highly Voted 5 years, 5 months ago

B is correct. When you use “address” it is referring to the remote peer you share the key with. If you want to add more than 1 ip add, you will have to use group key.C is correct did this ins GNS3 R1(config)#crypto isakmp key 123123 address 172.16.0.0 R1(config)#end R1#show crypto isakmp key Keyring Hostname/Address Preshared Key default 172.16.0.0 [255.255.0.0] 123123 same as Seawanderer didYou are correct, I have verified in IOU. because the command "crypto isakmp key ciscXXXXXXXX address 172.16.0.0" did not specified the mask, the router will take is as /16, unless you specify the mask as "crypto isakmp key ciscXXXXXXXX address 172.16.0.0 255.255.255.0", the router will take it as /24.Man this is not true....

upvoted 18 times

nospampls 5 years ago

C is correct

did this ins GNS3

R1(config)#crypto isakmp key 123123 address 172.16.0.0 R1(config)#end R1#show crypto isakmp key Keyring Hostname/Address Preshared Key

default 172.16.0.0 [255.255.0.0] 123123

same as Seawanderer did

upvoted 16 times

nospampls 5 years ago

C is correct did this ins GNS3 R1(config)#crypto isakmp key 123123 address 172.16.0.0 R1(config)#end R1#show crypto isakmp key Keyring Hostname/Address Preshared Key default 172.16.0.0 [255.255.0.0] 123123 same as Seawanderer didYou are correct, I have verified in IOU. because the command "crypto isakmp key ciscXXXXXXXX address 172.16.0.0" did not specified the mask, the router will take is as /16, unless you specify the mask as "crypto isakmp key ciscXXXXXXXX address 172.16.0.0 255.255.255.0", the router will take it as /24.Man this is not true....

upvoted 16 times

kwong328 3 years, 5 months ago

You are correct, I have verified in IOU. because the command "crypto isakmp key ciscXXXXXXXX address 172.16.0.0" did not specified the mask, the router will take is as /16, unless you specify the mask as "crypto isakmp key ciscXXXXXXXX address 172.16.0.0 255.255.255.0", the router will take it as /24.

upvoted 4 times

jaciro11 4 years, 8 months ago

Man this is not true....

upvoted 4 times

thefiresays 5 years, 5 months ago

It's weird that they used a network address, but this command authenticates a single VPN peer. Leaving B correct.

upvoted 10 times

thefiresays 5 years, 5 months ago

It's weird that they used a network address, but this command authenticates a single VPN peer. Leaving B correct.This is not always a network address.... for example on this subnet 172.16.4.0/23, 172.16.5.0 is a valid IP address, and nothing to do with network address. It just looks weird because people tend to subnet on /24's mostly.

upvoted 10 times

loiphin 4 years, 7 months ago

This is not always a network address.... for example on this subnet 172.16.4.0/23, 172.16.5.0 is a valid IP address, and nothing to do with network address. It just looks weird because people tend to subnet on /24's mostly.

upvoted 4 times

babsoly Most Recent 1 year ago

The command contain "crypto isakmp" this is a command for IKEv1 so C is the correct answer.

upvoted 1 times

CyberGhost666 1 year, 1 month ago

Correct answer is C.

upvoted 1 times

willroute 1 year, 9 months ago

C is correct. https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios/218432-configure-a-site-to-site-ipsec-ikev1-tun.html....ikev1 is key....no pun intended....ikev2 diff, see below. https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118652-configure-asa-00.html

upvoted 1 times

luismg 1 year, 11 months ago

it is an IKE v1 command so the answer is C

upvoted 1 times

Rockbo47 2 years ago

isakmp command refers to IKEv1 and without specifying a mask it will use the default classful mask which in this case would be 255.255.0.0 for 172.16.0.0. So answer C is absolutely the correct answer. nospampls also demonstrates this with output.

upvoted 1 times

c3qu1 2 years, 5 months ago

C is correct, the command crypto isakmp key ciscXXXXXXXX address 172.16.0.0 0.0.255.255 authenticates IKEv1 peers in the 172.16.0.0/16 range by using the preshared key ciscXXXXXXXX.

upvoted 1 times

xziomal9 2 years, 9 months ago

Answer C

upvoted 2 times

squirrel49 2 years, 10 months ago

The command crypto isakmp key you provided is related to IKEv1, not IKEv2. IKEv1 (Internet Key Exchange version 1) is configured using crypto isakmp commands, whereas IKEv2 (Internet Key Exchange version 2) is configured using crypto ikev2 commands. If you want to configure a pre-shared key for IKEv1, the crypto isakmp key command is used as shown in your original question. If you want to configure a pre-shared key for IKEv2, you would use crypto ikev2 keyring and crypto ikev2 profile commands. The distinction is important because the two versions of IKE have different configurations and characteristics. So IMHO - C is the right answer!

upvoted 2 times

RafaelSTI 3 years ago

C is correct, o IOS assumes a /16 mask if you omit the mask, like when you put at the and 0.0.0.0 and the IOS assumes a /0 mask (any). I test in the lab: ... Router(config)# crypto isakmp key Mudar@123 address 172.16.0.0 Router(config)#do show crypto isakmp key Keyring Hostname/Address Preshared Key default 172.16.0.0 [255.255.0.0] Mudar@123 Router(config)#

upvoted 3 times

nep1019 3 years ago

Selected Answer: B

Some of you are overthinking this. Go here: https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfike.html#wp1017897

Search: crypto isakmp key and read. When you enter the peer using address, the mask is optional if you want to specify the subnet. If you specify no subnet then the address is to a single peer. In this case, 172.16.0.0/32 leaving B the only correct answer.

upvoted 1 times

nep1019 3 years ago

Some of you are overthinking this. Go here: https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfike.html#wp1017897 Search: crypto isakmp key and read. When you enter the peer using address, the mask is optional if you want to specify the subnet. If you specify no subnet then the address is to a single peer. In this case, 172.16.0.0/32 leaving B the only correct answer.Explanation from the source: mask (Optional) Specify the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)

upvoted 1 times

nep1019 3 years ago

Explanation from the source: mask (Optional) Specify the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)

upvoted 1 times

fdl543 3 years ago

B Is always correct. Using IKEv1 or IKEv2. C will fail if I use IKEv2...

upvoted 1 times

wizzlewazzle 3 years, 2 months ago

With the address keyword, you can also use the mask argument to indicate the remote peer ISAKMP identity will be established using the preshared key only. If the mask argument is used, preshared keys are no longer restricted between two users. Note If you specify mask, you must use a subnet address. (The subnet address 0.0.0.0 is not recommended because it encourages group preshared keys, which allow all peers to have the same group key, thereby reducing the security of your user authentication.)

upvoted 1 times

G33 3 years, 2 months ago

C is correct Apart from reasons already given by other C campaigners ikev2 uses a different format for keys crypto ikev2 keyring IKEv2-KEYRING peer 1.2.3.4 address 1.2.3.4 pre-shared-key cisco123 apart from that whe you actually run the command in a lab it results in 172.16.0.0 [255.255.0.0] It assumes a subnet for anything that ends in .0

upvoted 2 times

Kromwall 3 years, 2 months ago

B is correct

upvoted 1 times

gc999 3 years, 2 months ago

This question is tricky, it is testing the concept I believe. According to the CLI, it should be "peer". In Option B, it is 172.16.0.0/32 "peer", but in Option C, it is 172.16.0.0 "range". No matter then can be reachable, I will select the one with "peer".

upvoted 1 times

Question #72 *Topic 1*

Which command enables 802.1X globally on a Cisco switch?

A. dot1x system-auth-control

B. dot1x pae authenticator

C. authentication port-control auto

D. aaa new-model

Suggested Answer: *A*
Reference: https://www.cisco.com/c/en/us/td/docs/routers/nfvis/switch_command/b-nfvis-switch-command-reference/802_1x_commands.html

Community vote distribution
A (100%)

CyberGhost666 Most Recent 1 year, 1 month ago
Selected Answer: A
You have to use dot1x system-auth-control command in Global Configuration mode for this.
upvoted 1 times

Marshpillowz 1 year, 10 months ago
Selected Answer: A
A is correct
upvoted 1 times

bobie 2 years, 9 months ago
Selected Answer: A
The command to globally enable 802.1x authentication on the switch, use the dot1x system-auth-control command in Global Configuration mode.

https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5635-configure-global-802-1x-properties-on-a-switch-through-the-c.html
upvoted 3 times

Cnoteone 3 years, 3 months ago
To enable 802.1X globally, use the dot1x system-auth-control command in switch configuration mode. To restore the default configuration, use the no form of this command.

dot1x system-auth-control
upvoted 2 times

leowulf 3 years, 4 months ago
I will go with A

Step 3. To globally enable 802.1x authentication on the switch, use the dot1x system-auth-control command in Global Configuration mode.

https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5635-configure-global-802-1x-properties-on-a-switch-through-the-c.html
upvoted 3 times

SulSulEi 3 years, 5 months ago
Selected Answer: A
A is the answer, no doubt
upvoted 3 times

Odorka222 3 years, 5 months ago
B is answer, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

D - only enable AAA not 802.1x

upvoted 1 times

surforlife 3 years, 6 months ago

The following example shows how to enable IEEE 802.1X and AAA on Fast Ethernet port 2/1 and how to verify the configuration: Note In this example the Ethernet interface is configured as an access port by using the switchport mode access command in interface configuration mode. The Ethernet interface can also be configured as a trunk port using the switchport mode trunk command in interface configuration mode.

Device> enable Device# configure terminal Device(config)# dot1x system-auth-control Device(config)# aaa new-model Device(config)# aaa authentication dot1x default group radius Device(config)# interface fastethernet2/1 Device(config-if)# switchport mode access Device(config-if)# authentication port-control auto Device(config-if)# dot1x pae authenticator Device(config-if)# end

"A" looks like correct answer

upvoted 3 times

ureis 3 years, 4 months ago

this is not globally

upvoted 1 times

nenotronix 3 years, 7 months ago

correct answer is D "aaa new-model"

https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

upvoted 1 times

ureis 3 years, 4 months ago

Man this is for authentication not for dot1x

upvoted 3 times

Question #73 *Topic 1*

What is a characteristic of Dynamic ARP Inspection?

A. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database.

B. In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted.

C. DAI associates a trust state with each switch.

D. DAI intercepts all ARP requests and responses on trusted ports only.

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

Sarbi Highly Voted 4 years, 5 months ago
The correct answer is A. Dynamic ARP Inspection To prevent ARP poisoning attacks such as the one described in the previous section, a switch must ensure that only valid ARP requests and responses are relayed. DAI prevents these attacks by intercepting all ARP requests and responses. Each of these intercepted packets is verified for valid MAC address to IP address bindings before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped. DAI determines the validity of an ARP packet based on valid MAC address to IP address bindings stored in a trusted database. This database is built at runtime by DHCP snooping, provided that it is enabled on the VLANs and on the switch in question. In addition, DAI can also validate ARP packets against user-configured ARP ACLs in order to handle hosts that use statically configured IP addresses. DAI can also be configured to drop ARP packets when the IP addresses in the packet are invalid or when the MAC addresses in the body of the ARP packet do not match the addresses specified in the Ethernet header.
upvoted 7 times

Marshpillowz Most Recent 1 year, 10 months ago
A is correct
upvoted 1 times

Thusi26 3 years, 8 months ago
A is the correct answer
upvoted 2 times

otzu1 3 years, 10 months ago
OSG: Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks. DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. As described in the previous section, this database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid. A
upvoted 2 times

nickanme 4 years, 5 months ago
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_58_se/configuration/guide/3750xscg/swdynarp.html#wp1039773
upvoted 1 times

nickanme 4 years, 5 months ago
@ Amedeou n non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses. You define an ARP ACL by using the arp access-list acl-name global configuration command. For configuration information, see the “Configuring ARP ACLs for Non-DHCP Environments” section. The switch logs dropped packets. For more information about the log buffer, see the “Logging of Dropped Packets” section.
upvoted 1 times

Amedeou 4 years, 5 months ago
what happen if there is no DHCP involved ?
upvoted 1 times

Question #74 *Topic 1*

Which statement about IOS zone-based firewalls is true?

A. An unassigned interface can communicate with assigned interfaces

B. Only one interface can be assigned to a zone.

C. An interface can be assigned to multiple zones.

D. An interface can be assigned only to one zone.

Suggested Answer: *D*

Reference: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html

Community vote distribution

D (100%)

sull3y Highly Voted 3 years ago

D Rules For Zone-Based Policy Firewall Application Router network interface memberships in zones is subject to several rules that govern interface behavior, as is the traffic that moves between zone member interfaces:

A zone must be configured before interfaces can be assigned to the zone.

An interface can be assigned to only one security zone.

All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router.

Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone.

In order to permit traffic to and from a zone member interface, a policy that allows or inspects traffic must be configured between that zone and any other zone.

The self-zone is the only exception to the default deny all policy. All traffic to any router interface is allowed until traffic is explicitly denied.

upvoted 5 times

sull3y Highly Voted 3 years ago

D Rules For Zone-Based Policy Firewall Application Router network interface memberships in zones is subject to several rules that govern interface behavior, as is the traffic that moves between zone member interfaces: A zone must be configured before interfaces can be assigned to the zone. An interface can be assigned to only one security zone. All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router. Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone. In order to permit traffic to and from a zone member interface, a policy that allows or inspects traffic must be configured between that zone and any other zone. The self-zone is the only exception to the default deny all policy. All traffic to any router interface is allowed until traffic is explicitly denied.D correct!! https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html#anc11

upvoted 5 times

Here_comes_MrLamb 1 year, 10 months ago

D correct!! https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html#anc11

upvoted 1 times

Marshpillowz Most Recent 1 year, 10 months ago

D is correct

upvoted 1 times

Cnoteone 3 years, 3 months ago

D for me

upvoted 2 times

BloodyBronco 3 years, 11 months ago

D is correct

upvoted 4 times

Question #75 *Topic 1*

When wired 802.1X authentication is implemented, which two components are required? (Choose two.)

A. authentication server: Cisco Identity Service Engine

B. supplicant: Cisco AnyConnect ISE Posture module

C. authenticator: Cisco Catalyst switch

D. authenticator: Cisco Identity Services Engine

E. authentication server: Cisco Prime Infrastructure

Suggested Answer: *A, C*

Reference: https://www.lookingpoint.com/blog/ise-series-802.1x

Community vote distribution

AC (100%)

Rockbo47 Most Recent 2 years ago

Out of the provided options, A and C are the correct choices. B is there to catch you out because whilst a supplicant is required, the ISE Posture module is not

upvoted 1 times

Marshpillowz 2 years, 4 months ago

A and C are correct

upvoted 1 times

Question #76 *Topic 1*

Which SNMPv3 configuration must be used to support the strongest security possible?

A. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

B. asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

C. asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

D. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

sull3y Highly Voted 3 years ago

D. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy SNMPv3 offers three security levels: noAuthNoPriv, authNoPriv, and authPriv. The strongest security possible is achieved by using the authPriv security level. This level requires both an authentication and a privacy (encryption) protocol. Option D is using the authPriv security level, it uses the AES256 for encryption which is considered a stronger encryption algorithm than 3DES, and it uses the SHA for authentication which is considered a stronger authentication algorithm than MD5. It is important to note that the real configuration may vary depending on the device and the vendor.

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct answer is D.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

D is correct

upvoted 1 times

xziomal9 2 years, 3 months ago

A. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy B. asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy C. asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy D. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

upvoted 2 times

psuoh 3 years, 1 month ago

D is better Cisco answer AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES. Encryption is also much faster in AES vs. DES, making it ideal for applications, firmware and hardware that require low latency or high throughput. privacy in SNMP-server user (Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.

upvoted 2 times

Question #77 *Topic 1*

Under which two circumstances is a CoA issued? (Choose two.)

A. A new authentication rule was added to the policy on the Policy Service node.

B. An endpoint is deleted on the Identity Service Engine server.

C. A new Identity Source Sequence is created and referenced in the authentication policy.

D. An endpoint is profiled for the first time.

E. A new Identity Service Engine server is added to the deployment with the Administration persona.

Suggested Answer: *B, D*

Reference: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

Community vote distribution

BD (100%)

aadach Highly Voted 6 years ago

The profiler service implements the CoA in the following cases: •Static assignment of an endpoint •An exception action is configured •An endpoint is profiled for the first time •Endpoint deleted

upvoted 32 times

ozone1864 Highly Voted 6 years ago

Its B & D

upvoted 11 times

ITPro21 Most Recent 1 year, 4 months ago

An Endpoint is Profiled for the First Time The profiler service issues a CoA for an endpoint that is not statically assigned and profiled for the first time i.e. the profile changes from an unknown to a known profile. An Endpoint is Deleted The profiler service issues a CoA when an endpoint is deleted from the Endpoints page and the endpoint is most likely disconnected or removed from the network. For more information on CoA exemptions, see the "CoA Exemptions" section. For more information on CoA configuration details, see Table 17-2.

upvoted 1 times

Premium_Pils 2 years ago

Change of Authorization (CoA)

upvoted 1 times

Marshpillowz 2 years, 4 months ago

B and D correct

upvoted 1 times

Nizar_Makarem 4 years, 9 months ago

BD are correct

upvoted 3 times

Raajaa 5 years, 1 month ago

B and D is the answer

upvoted 3 times

thegreek1 5 years, 10 months ago

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html aadach 2 months, 1 week ago The profiler service implements the CoA in the following cases: •Static assignment of an endpoint •An exception action is configured •An endpoint is profiled for the first time •Endpoint deleted

upvoted 3 times

naddaf 6 years, 1 month ago

i think its A & C

upvoted 1 times

Question #78 *Topic 1*

Which ASA deployment mode can provide separation of management on a shared appliance?

A. DMZ multiple zone mode

B. transparent firewall mode

C. multiple context mode

D. routed mode

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

molinux Highly Voted 4 years, 2 months ago

Yes. Multicontext

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

I would choose D but because it make sense, but is it really a mode? I though you needed to by a license type to be able to use context, which make me thinks that is not necessarily a "mode" as transparent and routed which functions are off topic.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

C multi-context

upvoted 1 times

sull3y 3 years ago

C. multiple context mode The Cisco ASA firewall supports several deployment modes, one of them is multiple context mode also known as Security Contexts mode. This mode allows for the separation of management on a shared appliance by creating multiple virtual firewalls, each with its own security policies, interfaces, and administrators. This allows for a more granular control of network access and security, as well as logical separation of different security zones on the same physical appliance. This deployment mode is typically used in large enterprises or service providers to provide secure multitenancy, segregating different customers or departments on the same device while keeping their security policies separate.

upvoted 4 times

Question #79 *Topic 1*

Refer to the exhibit. Which command was used to display this output?

```
Sysauthcontrol              Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet1/0/12
-----------------------------------
PAE                 = AUTHENTICATOR
PortControl         = FORCE_AUTHORIZED
ControlDirection    = Both
HostMode            = SINGLE_HOST
QuietPeriod         = 60
ServerTimeout       = 0
SuppTimeout         = 30
ReAuthMax           = 2
MaxReq              = 2
TxPeriod            = 30
```

A. show dot1x all

B. show dot1x

C. show dot1x all summary

D. show dot1x interface gi1/0/12

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x- pba.html

Community vote distribution

A (100%)

CiscoTech Highly Voted 5 years, 7 months ago

It is. A The following example displays show dot1x all command output:

Device# show dot1x all

Sysauthcontrol Enabled Dot1x Protocol Version 2 Dot1x Info for FastEthernet1 ---------- PAE = AUTHENTICATOR PortControl = AUTO ControlDirection = Both HostMode = MULTI_HOST ReAuthentication = Disabled QuietPeriod = 60 ServerTimeout = 30 SuppTimeout = 30 ReAuthPeriod = 3600 (Locally configured) ReAuthMax = 2 MaxReq = 2 TxPeriod = 30 RateLimitPeriod = 0 Device-871# https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

upvoted 21 times

zheka Highly Voted 4 years, 2 months ago

I configured only one port on the real switch for dot1x together with the global dot1x authentication. Ran two commands to show the difference, see below and make a correct decision for the correct answer. 2960_SW3(config-if)#do sh dot1x all Sysauthcontrol Enabled Dot1x Protocol Version 3

Dot1x Info for GigabitEthernet1/0/45 ---------- PAE = AUTHENTICATOR QuietPeriod = 60 ServerTimeout = 0 SuppTimeout = 30 ReAuthMax = 2 MaxReq = 2 TxPeriod = 30

2960_SW3(config-if)#do sh dot1x int gig1/0/45 Dot1x Info for GigabitEthernet1/0/45 ---------- PAE = AUTHENTICATOR QuietPeriod = 60 ServerTimeout = 0 SuppTimeout = 30 ReAuthMax = 2 MaxReq = 2 TxPeriod = 30

upvoted 9 times

Marshpillowz Most Recent 1 year, 10 months ago

Selected Answer: A

A is correct

upvoted 1 times

Ferdaush 2 years, 2 months ago

It is: A

upvoted 1 times

Totosos1 2 years, 10 months ago

Selected Answer: A

Definitely 'A':

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

upvoted 1 times

Raajaa 4 years, 7 months ago

Answer is A

upvoted 4 times

juanlecho 4 years, 11 months ago

xxxxxx-xxxx-xxxx-sw1#$interface gigabitEthernet 1/0/1 Dot1x Info for GigabitEthernet1/0/1 ---------- PAE = AUTHENTICATOR QuietPeriod = 60 ServerTimeout = 0 SuppTimeout = 30 ReAuthMax = 2 MaxReq = 2 TxPeriod = 10 xxxxx-xxxx-xxxx-sw1# CCC

********** xxxx-xxxxx-xxxx-sw1#show dot1x all Sysauthcontrol Enabled Dot1x Protocol Version 3

Dot1x Info for GigabitEthernet1/0/1 ---------- PAE = AUTHENTICATOR QuietPeriod = 60 ServerTimeout = 0 SuppTimeout = 30 ReAuthMax = 2 MaxReq = 2 TxPeriod = 10

Dot1x Info for GigabitEthernet1/0/2 ---------- PAE = AUTHENTICATOR QuietPeriod = 60 ServerTimeout = 0 SuppTimeout = 30 ReAuthMax = 2 MaxReq = 2 TxPeriod = 10

!!!!!!!! ANSWER IS A !!!!!!

upvoted 2 times

Jeeves69 4 years, 11 months ago

A is the correct answer, because only the 'show dot1x all' command shows the 'Sysauthcontrol' status and Dot1x Protocol Version

upvoted 5 times

Kris92 4 years, 11 months ago

A should show all interfaces, D only for specific interface, so both are correct, would go with D if I have to choose To display the IEEE 802.1X administrative and operational status for the switch, use the show dot1x all [details | statistics | summary] command in privileged EXEC configuration mode. To display the IEEE 802.1X administrative and operational status for a specific port, use the show dot1x interface type number command in privileged EXEC configuration mode. For detailed information about the fields in these displays, see the command reference for this release. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

upvoted 1 times

Javimc 5 years ago

No, is A. With D ypu donat have sysauthcontrol info

upvoted 4 times

moiz_109 5 years, 7 months ago

No. It's A

upvoted 8 times

Vic25H 5 years, 8 months ago

Should be D

https://guides.co/g/cisco-trustsec-failed-authentications-and-authorizations/10982

upvoted 3 times

Question #80 *Topic 1*

What is a characteristic of Cisco ASA NetFlow v9 Secure Event Logging?

A. It tracks flow-create, flow-teardown, and flow-denied events.

B. It provides stateless IP flow tracking that exports all records of a specific flow.

C. It tracks the flow continuously and provides updates every 10 seconds.

D. Its events match all traffic classes in parallel.

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nsel.html

Community vote distribution

A (100%)

willroute Most Recent 1 year, 9 months ago

A is correct and also there is another question that what is specific to ASA NSEL, it is the capability to delay events, as it is noisy. both are in below .https://www.cisco.com/c/en/us/td/docs/security/asa/special/netflow/asa_netflow.html#delaysending

upvoted 1 times

Marshpillowz 2 years, 4 months ago

A is correct

upvoted 1 times

sull3y 3 years, 6 months ago

A. It tracks flow-create, flow-teardown, and flow-denied events. Cisco ASA NetFlow v9 Secure Event Logging is a feature that allows the ASA to export detailed information about network traffic flow and security events to a NetFlow collector for analysis. The exported information includes information about flow-create, flow-teardown and flow-denied events, which provide insight into the behavior of the traffic passing through the firewall. This feature also allows for the collection of detailed information about the traffic passing through the firewall which can be used for security incident investigations, capacity planning and troubleshooting. It does not provide stateless IP flow tracking that exports all records of a specific flow (B) or tracks the flow continuously and provides updates every 10 seconds (C) and also it does not match all traffic classes in parallel (D)

upvoted 3 times

surforlife 4 years, 1 month ago

A is correct. In stateful flow tracking, tracked flows go through a series of state changes. NSEL events are used to export data about flow status and are triggered by the event that caused the state change. The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs). In addition, the ASA and ASASM implementation of NSEL generates periodic NSEL events, flow-update events, to provide periodic byte counters over the duration of the flow. These events are usually time-driven, which makes them more in line with traditional NetFlow; however, they may also be triggered by state changes in the flow.

upvoted 3 times

Cyril_the_Squirl 4 years, 1 month ago

This is Correct

upvoted 1 times

Question #81 *Topic 1*

A network engineer has entered the snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0383320506 command and needs to send SNMP information to a host at 10.255.254.1. Which command achieves this goal?

A. snmp-server host inside 10.255.254.1 snmpv3 andy

B. snmp-server host inside 10.255.254.1 version 3 myv3

C. snmp-server host inside 10.255.254.1 snmpv3 myv3

D. snmp-server host inside 10.255.254.1 version 3 andy

Suggested Answer: *D*

Reference: https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/sm/snmp-server-host.html

Community vote distribution

D (100%)

Jeeves69 Highly Voted 5 years, 5 months ago

Correct answer is D See: https://www.networkstraining.com/how-to-configure-snmp-on-cisco-asa-5500-firewall/ And: https://www.cisco.com/c/en/us/td/docs/security/asa/snmp/snmpv3_tools/snmpv3_1.html

upvoted 23 times

willroute Most Recent 1 year, 9 months ago

https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/m_shox-sn.html#wp1203427780 D

upvoted 1 times

Marshpillowz 2 years, 4 months ago

D is correct

upvoted 1 times

Terry0987 3 years, 8 months ago

** CORRECT answer is D *** snmp-server host interface { hostname | ip_address } [trap | poll] [community community-string] [version { 1 | 2c | 3 username }] [udp-port port]

upvoted 3 times

hz033 4 years, 3 months ago

ASA(config)# snmp-server host inside 10.255.254.1 version 3 ? configure mode commands/options: Current available user name(s): ASA(config)# snmp-server host inside 10.255.254.1 version 3 andy require "Current available user name(s):" so D is correct

upvoted 3 times

rbrain 4 years, 7 months ago

D is correct

upvoted 4 times

zheka 4 years, 8 months ago

An attempt to add the SNMP server with the command on the ASA firewall: See what the firewall expect as the input fw(config)# snmp-server host inside 172.16.0.94 ver 3 ? configure mode commands/options: Current available user name(s): snmpuser

upvoted 1 times

Sarbi 4 years, 11 months ago

Anser D is correct. snmp-server enable traps ! ! …or insted select just some traps, for example: ! snmp-server enable traps envmon fan shutdown supply temperature status ospf cpu ! snmp-server group trapgroup v3 priv snmp-server user trapuser trapgroup v3 auth sha AuthPass priv 3des PrivPass snmp-server host 10.1.1.161 traps version 3 priv trapuser

upvoted 2 times

Sarbi 4 years, 11 months ago

The correct answer is D

upvoted 2 times

jshow 5 years, 1 month ago

100% D For community-string, when version 1 or version 2c is specified, enter the password-like community string sent with the notification operation. When version 3 is specified, enter the SNMPv3 username https://www.cisco.com/c/en/us/td/docs/routers/ir910/software/release/1_1/configuration/guide/ir910scg/swsnmp.html

upvoted 2 times

Zoli6 5 years, 2 months ago

Configuration Example of SNMP v3 Currently the most secure SNMP version is v3. To configure this version you need first to create an SNMP group, then an SNMP server and lastly a host (NMS) which will communicate with the firewall for management purposes. Let's configure SNMP v3 with the example below: ASA(config)# snmp-server enable ASA(config)# snmp-server group snmpgroup v3 auth <- create v3 group with authentication ASA(config)# snmp-server user administrator snmpgroup v3 auth sha strongpass <- create user "administrator" belonging to group "snmpgroup" ASA(config)#snmp-server host inside 10.1.1.1 version 3 administrator <- specify the NMS host Correct answer is D, administrator here is equal to andy

upvoted 3 times

deathfrom 5 years, 2 months ago

You associate the SNMP host config with a user not a group. D is the correct answer

upvoted 4 times

CyberG 5 years, 3 months ago

B is correct myv3 is the host, Andy is an user on host myv3myv3 is the snmp v3 group name. D is the correct answer

upvoted 1 times

CyberG 5 years, 3 months ago

B is correct myv3 is the host, Andy is an user on host myv3

upvoted 1 times

nemeses667 4 years ago

myv3 is the snmp v3 group name. D is the correct answer

upvoted 1 times

Question #82 *Topic 1*

An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?

A. flow exporter

B. ip flow-export destination 1.1.1.1 2055

C. flow-export destination inside 1.1.1.1 2055

D. ip flow monitor input

Suggested Answer: *C*

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/special/netflow/guide/asa_netflow.html

Community vote distribution

C (89%) D (11%)

Marshpillowz Most Recent 1 year, 10 months ago

C is correct

upvoted 2 times

yong08321 2 years, 9 months ago

The correct Cisco ASA command to generate NetFlow records on traffic traversing the device is "flow-export destination inside 1.1.1.1 2055". The "flow-export destination inside" command is used to specify the IP address and port number of the NetFlow collector that will receive the exported flow data. In this case, the collector is located on the inside interface of the ASA. The IP address "1.1.1.1" and port number "2055" are just examples and should be replaced with the actual IP address and port number of the collector. Option A, "flow exporter ", is used to configure the NetFlow exporter parameters, such as the version, transport protocol, and template options. Option B, "ip flow-export destination 1.1.1.1 2055", is a command used on Cisco routers to configure the NetFlow collector destination. Option D, "ip flow monitor input", is a command used on Cisco routers to enable NetFlow data export for the specified flow monitor. These commands are not used on the Cisco ASA.

upvoted 1 times

surforlife 3 years, 7 months ago

"C" should be the correct answer. Add an NSEL collector to which NetFlow packets may be sent. flow-export destination interface-name ipv4-address | hostname udp-port Example: ciscoasa(config)# flow-export destination inside 209.165.200.225 2002 The destination keyword indicates that a NSEL collector is being configured. The interface-name argument is the name of the ASA and ASA Services Module interface through which the collector is reached. The ipv4-address argument is the IP address of the machine running the collector application. The hostname argument is the destination IP address or name of the collector. The udp-port argument is the UDP port number to which NetFlow packets are sent. You can configure a maximum of five collectors. After a collector is configured, template records are automatically sent to all configured NSEL collectors.

upvoted 3 times

Pwned 3 years, 9 months ago

C is correct https://support.auvik.com/hc/en-us/articles/360025289112-How-to-configure-NetFlow-on-Cisco-ASA-firewalls

upvoted 3 times

jaciro11 3 years, 11 months ago

ASA do it like C

upvoted 3 times

Jetnor 4 years, 2 months ago

Selected Answer: D

Correct answer should be D, if we want to enable netflow to record traffic data we should apply monitor command on interface.

upvoted 1 times

Jetnor 4 years, 2 months ago

Correct answer should be D, if we want to enable netflow to record traffic data we should apply monitor command on interface.Nevermind, Answer is C since this is an ASA. on switches we use monitor

upvoted 1 times

Jetnor Highly Voted 4 years, 2 months ago

Nevermind, Answer is C since this is an ASA. on switches we use monitor

upvoted 6 times

Question #83 *Topic 1*

Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two.)

A. Define a NetFlow collector by using the flow-export command

B. Create a class map to match interesting traffic

C. Create an ACL to allow UDP traffic on port 9996

D. Enable NetFlow Version 9

E. Apply NetFlow Exporter to the outside interface in the inbound direction

Suggested Answer: *A, B*

Official Answer: AB

Community vote distribution

AB (100%)

Jeeves69 Highly Voted 4 years, 11 months ago

The Correct Answer is A and B. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/special/netflow/guide/asa_netflow.html#pgfId-1330480

upvoted 20 times

Raajaa Highly Voted 4 years, 7 months ago

A and B is the correct answer

upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago

A and B are correct

upvoted 1 times

yong08321 2 years, 9 months ago

The two tasks that are required to enable NetFlow on a Cisco ASA 5500 Series firewall are: B. Create a class map to match interesting traffic: A class map is used to identify the interesting traffic for which NetFlow data needs to be exported. It can be based on various parameters such as source and destination IP address, protocol, port numbers, etc. A. Define a NetFlow collector by using the flow-export command: This command is used to configure the NetFlow exporter parameters, such as the version, transport protocol, and template options. It also specifies the IP address and port number of the NetFlow collector that will receive the exported flow data.

upvoted 1 times

brownbear505 3 years, 12 months ago

The Correct Answer is A and B. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/special/netflow/guide/asa_netflow.html#pgfId-1330480

upvoted 5 times

coentror 4 years, 2 months ago

access-list global_mpc extended permit ip any any ! flow-export destination inside 192.168.1.13 2055 ! class-map global_class match access-list global_mpc

upvoted 1 times

Sarbi 4 years, 5 months ago

A and B is the correct answer

upvoted 4 times

jmosilva 4 years, 6 months ago

A and B "Flow-export actions are not supported in interface-based policies. You can configure flow-export actions in a class-map only with the match access-list, match any, or class-default commands. You can only apply flow-export actions in a global service policy. "

upvoted 5 times

Question #84 *Topic 1*

Refer to the exhibit. A network administrator configures command authorization for the admin5 user. What is the admin5 user able to do on HQ_Router after this configuration?

```
HQ_Router(config)# username admin5 privilege 5
HQ_Router(config)#privilege interface level 5 shutdown
HQ_Router(config)#privilege interface level 5 ip
HQ_Router(config)#privilege interface level 5 description
```

A. set the IP address of an interface

B. add subinterfaces

C. complete no configurations

D. complete all configurations

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

dansecu Highly Voted 4 years, 9 months ago
the answer is C because the below line is missing from privilege configuration and athe user will not be able to reache the interface config level:
privilege exec level 5 configure terminal
upvoted 21 times

Raajaa Highly Voted 4 years, 7 months ago
C is the answer
upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago
Selected Answer: C
C is correct
upvoted 1 times

sull3y 3 years ago
C. complete no configurations

Based on the given exhibit, the admin5 user has been given command authorization for only the "show" command. This means that the admin5 user is only able to view the current configurations and status of the router, but not make any changes or modifications. Therefore, the admin5 user would not be able to set the IP address of an interface, add subinterfaces, or complete any configurations other than "show" commands.
upvoted 4 times

psuoh 3 years, 1 month ago
Example So for example, consider the following set of privileges:

privilege interface level 5 shutdown

privilege interface level 5 ip address

privilege interface level 5 ip

privilege interface level 5 bandwidth

privilege configure level 5 interface

privilege exec level 5 show running-config

privilege exec level 5 show

The command show running-config will now display:

Current configuration : 425 bytes

!

boot-start-marker

boot-end-marker

!

!

!

!

!

interface Loopback0

ip address 10.255.255.1 255.255.255.255

!

interface FastEthernet0/0

no ip address

!

interface FastEthernet0/1

no ip address

shutdown

!

interface Serial1/0

bandwidth 512

ip address 10.0.0.1 255.255.255.0

!

interface Serial1/1

no ip address

shutdown

!

interface Serial1/2

no ip address

shutdown

!

interface Serial1/3

no ip address

shutdown

!

!

end

upvoted 3 times

BloodyBronco 3 years, 9 months ago

Selected Answer: C

definitely C!

upvoted 4 times

brownbear505 3 years, 12 months ago

Selected Answer: C

Needed: Privilege exec level 5 configure terminal Privilege configure level 5 interface

upvoted 2 times

Sun2sun 4 years ago

Selected Answer: C

C. complete no configurations

upvoted 3 times

Gaborimbo22 4 years, 10 months ago

letter C is the correct

upvoted 4 times

Question #85 *Topic 1*

A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0383320506 address 0.0.0.0 command on host A. The tunnel is not being established to host B. What action is needed to authenticate the VPN?

A. Change the password on host A to the default password

B. Enter the command with a different password on host B

C. Enter the same command on host B

D. Change isakmp to ikev2 in the command on host A

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

Marshpillowz Most Recent 1 year, 10 months ago
C is correct
upvoted 1 times

sull3y 3 years ago
C. Enter the same command on host B The crypto isakmp key command is used to set the shared secret key for Internet Security Association and Key Management Protocol (ISAKMP) on a router. In order for the VPN tunnel to be established between host A and host B, the same shared secret key must be configured on both hosts. In this case, the network engineer needs to enter the same crypto isakmp key command, with the same password, on host B as they did on host A. This will ensure that both hosts are using the same shared secret key for authentication and the tunnel will be established. The other options A, B and D are not correct.
upvoted 3 times

psuoh 3 years, 1 month ago
The question should say the crypto isakmp key cisc0383320506 address 0.0.0.0 0.0.0.0 Example Add dynamic pre-shared keys for all the remote VPN !--- routers and the hub router. crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
upvoted 1 times

Net4dd 3 years, 1 month ago
C. Is true https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/29240-dcmvpn.html
upvoted 2 times

dr4gn00t 4 years ago
C is correct answer according to DMVPN configuration examples in cert guide
upvoted 2 times

Laryoul 4 years, 1 month ago
For me the good answer is C. Enter 0.0.0.0 on a this command line could be done on Hub and Spoke. Hub configuration is done on ip nhrp.
https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfike.html#wp1017897
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html#GUID-BDBD63D7-C9FD-490F-B1AF-EFC38B6B497B
upvoted 2 times

loiphin 4 years, 1 month ago
I would say its A, because if you entered the same command on Host B, they would never establish a tunnel. crypto isakmp key xxx 0.0.0.0 is only ever used on hubs. If you use the same command on a spoke they will never connect to each other.How would spoke to spoke tunnels ever be encrypted then?
upvoted 1 times

loiphin 4 years, 1 month ago
I would say its A, because if you entered the same command on Host B, they would never establish a tunnel. crypto isakmp key xxx 0.0.0.0 is only ever used on hubs. If you use the same command on a spoke they will never connect to each other.
upvoted 1 times

DarkestHour 3 years, 7 months ago
How would spoke to spoke tunnels ever be encrypted then?

upvoted 1 times

nomad 4 years, 2 months ago

0.0.0.0 addres wth! threw me off :P

upvoted 1 times

Question #86 *Topic 1*

How many interfaces per bridge group does an ASA bridge group deployment support?

A. up to 16

B. up to 2

C. up to 4

D. up to 8

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

Moll Highly Voted 4 years, 3 months ago
C should be the only valid answer given the history of the SW versions..
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.html
upvoted 8 times

u777 Highly Voted 4 years, 5 months ago
C is the correct answer for Cisco ASA up to version 9.4 (up to 4 interfaces per bridge group)
https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/general/asa-94-general-config/interface-routed-tfw.html With Cisco ASA version 9.6 the correct answer is up to 64 interfaces per bridge group !!! No such number there !!!
https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general-config/interface-routed-tfw.html
upvoted 7 times

Marshpillowz Most Recent 1 year, 10 months ago
C is correct
upvoted 2 times

denverfly 3 years, 12 months ago
C is the correct answer for Cisco ASA up to version 9.4.....The bridge group maximum was increased from 8 to 250 bridge groups. You can configure up to 250 bridge groups in single mode or per context in multiple mode, with 4 interfaces maximum per bridge group.We modified the following commands: interface bvi, bridge-group.
upvoted 5 times

Raajaa 4 years, 7 months ago
C is the correct answer
upvoted 2 times

Barish 4 years, 9 months ago
C is the correct Answ - You can assign up to 4 interfaces to a bridge group. You cannot assign the same interface to more than one bridge group.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/general/asa-94-general-config/interface-routed-tfw.html
upvoted 2 times

kakakayayaya 4 years, 9 months ago
For Information: You can assign up to 64 interfaces to a bridge group. You cannot assign the same interface to more than one bridge group.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/interface-routed-tfw.html#concept_0545A38665F04B78B993BAC61725B26D ???The problem with evolving technologies is that the exams can't change at the same speed of the software. You are looking at ASA 9.7, but the 9.4 had different specs
upvoted 2 times

kakakayayaya 4 years, 9 months ago
For Information: You can assign up to 64 interfaces to a bridge group. You cannot assign the same interface to more than one bridge group.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/interface-routed-tfw.html#concept_0545A38665F04B78B993BAC61725B26D

???
upvoted 2 times

Seawanderer 4 years, 7 months ago

The problem with evolving technologies is that the exams can't change at the same speed of the software. You are looking at ASA 9.7, but the 9.4 had different specs

upvoted 4 times

Question #87 *Topic 1*

A network administrator configures Dynamic ARP Inspection on a switch. After Dynamic ARP Inspection is applied, all users on that switch are unable to communicate with any destination. The network administrator checks the Interface status of all interfaces, and there is no err-disabled interface. What is causing this problem?

A. DHCP snooping has not been enabled on all VLANs

B. Dynamic ARP inspection has not been enabled on all VLANs

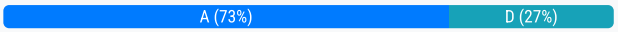
C. The ip arp inspection limit command is applied on all interfaces and is blocking the traffic of all users

D. The no ip arp inspection trust command is applied on all user host interfaces

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Jeeves69 Highly Voted 4 years, 5 months ago

The correct answer should be A. DHCP Snooping has not been enabled on all VLANs. DHCP Snooping is a prerequisite for Dynamic ARP Inspection (DAI). When DHCP Snooping is enabled the 'no ip arp inspection trust' command only ensures that DAI will do its job, blocking invalid traffic.

upvoted 22 times

brownbear505 Highly Voted 3 years, 5 months ago

Selected Answer: A

DAI requires DHCP Snooping

upvoted 7 times

xziomal9 Most Recent 1 year, 9 months ago

Answe D

upvoted 1 times

DWizard 2 years, 1 month ago

Selected Answer: D

The right answer is D. DAI can obtain its IP-MAC information from DHCP snooping or from ACLs statically configured by the admin, it could work without DHCP snooping, however, by default all the interfaces become untrusted, and you have to manually set the "no ip arp inspection trust" command on interfaces connecting to other switches, even if those switches do not support DAI, so the answer is D. You can read this, it's carefully explained:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html

upvoted 2 times

webwalker00 2 years, 3 months ago

Selected Answer: A

DHCP snooping is required for DAI.

upvoted 2 times

achille5 2 years, 5 months ago

Selected Answer: D

no err-disabled interfaces indicates that the problem may not be related to a physical or link-level issue, which could be the case with DHCP snooping misconfiguration. Likely option D as the cause of the problem.

upvoted 2 times

amtf8888 2 years, 7 months ago

Selected Answer: A

a is correct

upvoted 1 times

sis_net_sec 2 years, 10 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book/ipaddr- i1.html#wp2458863701

the command "no ip arp inspection trust" means the port is not trusted in DAI. This means that it will inspect packets from the port for appropriate entries in the DHCP Snooping table. This is the default state.
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multiboo
k/configuration_guide/b_consolidated_config_guide_3850_chapter_0110111.html err-disable on a port due to DAI comes from exceeding a rate limit.

upvoted 1 times

jaciro11 3 years, 9 months ago

In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted. With this configuration, all ARP packets entering the network from a given switch bypass the security check. It is unnecessary to perform a validation at any other place in the VLAN or in the network. You configure the trust setting by using the ip arp inspection trust interface configuration command.

Answer is D

upvoted 1 times

birdman6709 3 years, 11 months ago

I think the issue here is the wording, the question is looking for what is causing the problem. With 'no ip arp inspection trust' enabled on all user ports, the switch is intercepting the ARP request and responses, and if there is no valid IP-to-MAC binding, the traffic is dropped and logged. So I think the answer should be D based on that.

upvoted 1 times

birdman6709 3 years, 11 months ago

I take that back actually, the answer is A. Since all the ports are untrusted anyways, as soon as DAI is enabled without DHCP snooping, they would drop since there is no IP-to-MAC binding. Adding the DHCP snooing in this case would fix the issue.

upvoted 6 times

zap_pap 4 years ago

The answer is D. It is tricky "no ip apr inspection trust" -> Trust removed from all interfaces -> Interfaces disabled.

upvoted 1 times

jshow 4 years, 1 month ago

Its A Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses. When DHCP snooping is disabled or in non-DHCP environments, use ARP ACLs to permit or to deny packets.

upvoted 4 times

Dinges 4 years, 1 month ago

A NOT NECESSARILY TRUE: DHCP snooping is not REQUIRED, when ARP ACLs are configured. Also not enabling DHCP snooping only on some vlans would not cause ALL users, connected to the switch being unable to communicate. B NOT TRUE Not enabling DAI on a VLAN simply exempts the VLAN from DAI, it will not block traffic C TRUE: Rate-limit exceed can put the interface in err-disabled state. Even if its not configured by admin; it is set at 15 ARP pps by default, but admin could have configured it with even lower limit, or an actual DOS attack has occured. D NOT TRUE: No ip arp inspection trust command MUST be applied on all user HOST interfaces. Only ports leading to the DHCP server should be set as trusted (EXCEPT if the upstream switch does not have DAI enabled, then leave it as untrusted and apply ARP ACLs locally).
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html

upvoted 1 times

Dinges 4 years, 1 month ago

CORRECTION: The question explicitly mentions that no interface is in err-disabled state, so C cannot be the correct answer. D is not the cause: Packets arriving on trusted interfaces bypass all DAI validation checks, while those arriving on untrusted interfaces go through the DAI validation process. So, to me, that leaves on A as a possible answer. Im going with A

upvoted 6 times

FN21 4 years, 3 months ago

D is correct. DHCP snooping is not a prerequisite for Dynamic ARP. The question is tricky though. Since it doesn't mention about configuring DHCP snooping, issuing the "no ip apr inspection trust" command surely will kill all connections. All interfaces have become untrusted and Dynamic ARP doesn't have a DHCP snooping database to compare to.

upvoted 3 times

statikd 4 years, 1 month ago

Wrong. All switch ports connected to hosts should be untrusted. The only trusted ports should be ports connected to other switches. By default switch ports are untrusted. DHCP snooping works in conjunction with Dynamic ARP inspection. The answer is A

upvoted 3 times

dansecu 4 years, 3 months ago

Jeeves69 provided correct answer. it is A DHCP Snooping should be enable globaly and on VLANs. The IP-MAC pair is checed by DAI in DHCP database. Answer D is related to hosts interfaces and they should be always untrusted.

upvoted 3 times

thefiresays 4 years, 4 months ago

D is correct. By default all interfaces will be untrusted. You must have trusted interfaces facing other network devices. Interfaces connected to hosts are untrusted and will validate DHCP table bindings to decide whether to forward/drop.

What Jeeves wrote is true. But not enabling DHCP snooping would not break connectivity.

upvoted 2 times

Question #88 *Topic 1*

What is a difference between FlexVPN and DMVPN?

A. DMVPN uses only IKEv1. FlexVPN uses only IKEv2

B. FlexVPN uses IKEv2. DMVPN uses IKEv1 or IKEv2

C. DMVPN uses IKEv1 or IKEv2. FlexVPN only uses IKEv1

D. FlexVPN uses IKEv1 or IKEv2. DMVPN uses only IKEv2

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

sull3y Highly Voted 3 years ago
B. FlexVPN uses IKEv2. DMVPN uses IKEv1 or IKEv2

FlexVPN is a Cisco VPN solution that simplifies the deployment of VPNs using a centralized VPN management model. It uses IKEv2 as the default key exchange protocol to provide secure and flexible VPN connections. FlexVPN is supported on Cisco IOS XE and Cisco IOS software platforms.

DMVPN (Dynamic Multipoint Virtual Private Network) is a Cisco VPN solution that enables the creation of VPNs with dynamic spoke-to-spoke connections. It uses IKEv1 or IKEv2 as the key exchange protocol to provide secure VPN connections. DMVPN is supported on Cisco IOS, Cisco IOS XE and Cisco IOS XR software platforms.
upvoted 5 times

Raajaa Highly Voted 4 years, 7 months ago
B is the correct answer
upvoted 5 times

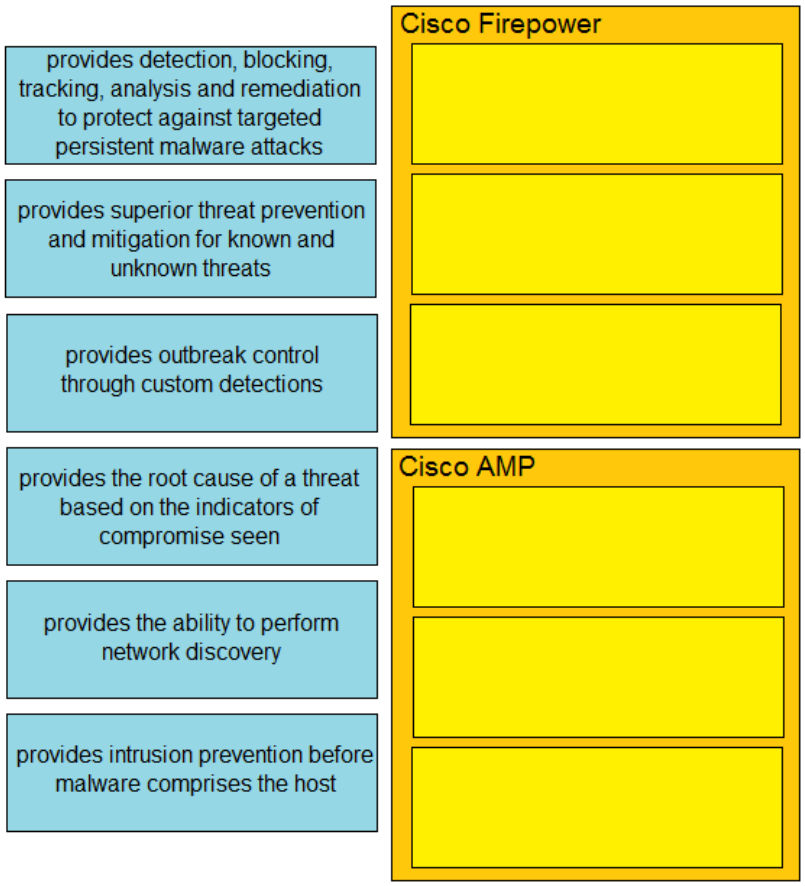
Marshpillowz Most Recent 1 year, 10 months ago
Selected Answer: B
B is correct
upvoted 1 times

Alizade 2 years, 4 months ago
Selected Answer: B
B. FlexVPN uses IKEv2. DMVPN uses IKEv1 or IKEv2.
upvoted 2 times

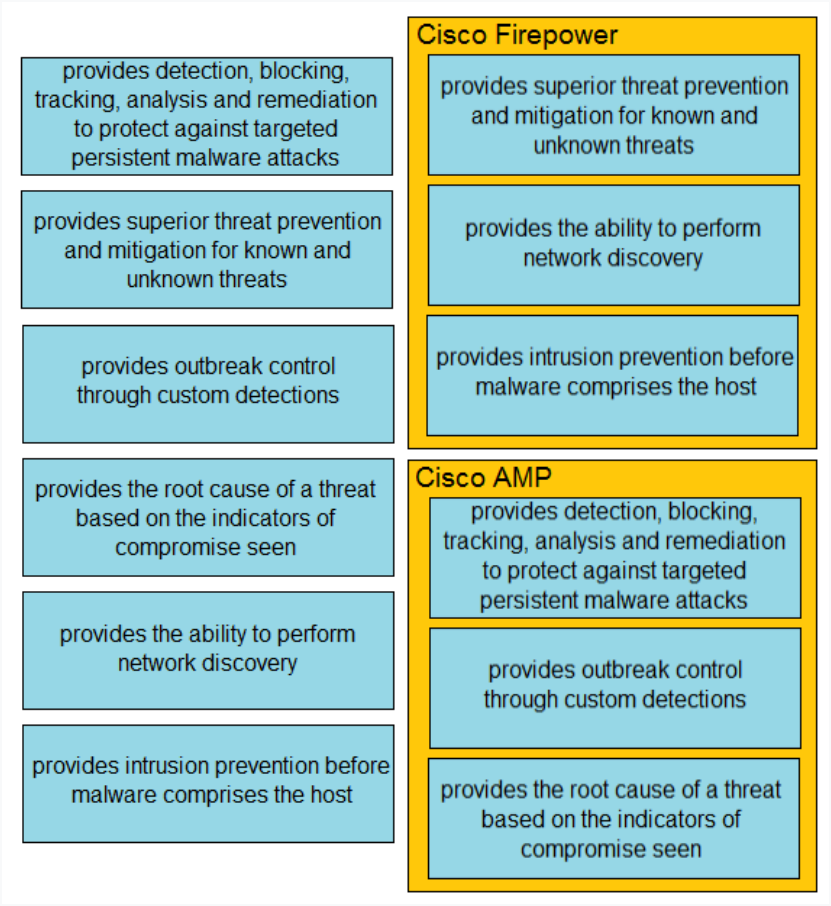
DRAG DROP -

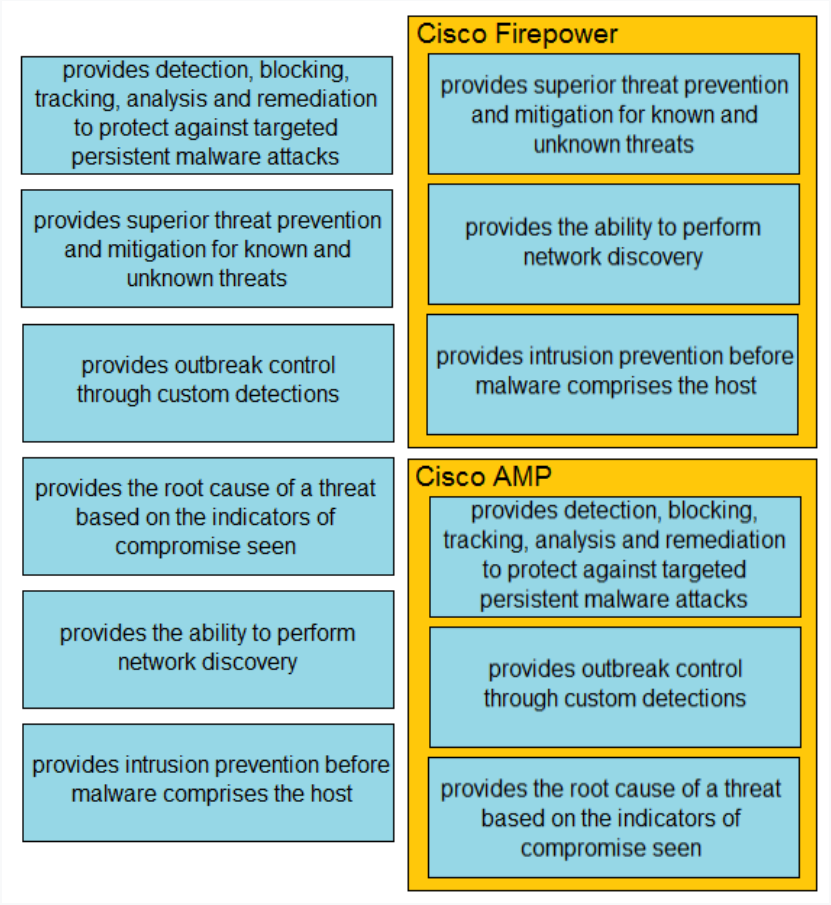
Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.

Select and Place:



Suggested Answer:





Cock 2 years, 1 month ago

AMP provides intrusion prevention before malware compromises the host The answer is wrong!!! https://essextec.com/wp-content/uploads/2018/03/Cisco-AMP-for-Endpoints-At-a-Glance.pdf

upvoted 1 times

Cock 2 years, 1 month ago

AMP provides intrusion prevention before malware compromises the host The answer is wrong!!! https://essextec.com/wp-content/uploads/2018/03/Cisco-AMP-for-Endpoints-At-a-Glance.pdfI am incorrect. The answer provided is correct

upvoted 1 times

Cock Highly Voted 2 years, 1 month ago

I am incorrect. The answer provided is correct

upvoted 8 times

Question #90 *Topic 1*

An engineer needs behavioral analysis to detect malicious activity on the hosts, and is configuring the organization's public cloud to send telemetry using the cloud provider's mechanisms to a security device. Which mechanism should the engineer configure to accomplish this goal?

A. sFlow

B. NetFlow

C. mirror port

D. VPC flow logs

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

acc2326 Highly Voted 5 years, 3 months ago
correct answer is D - VPC flow logs
upvoted 9 times

jaciro11 Highly Voted 4 years, 9 months ago
Its D I totally remember when I configure the first time the Stealthwatch Cloud
upvoted 9 times

Nonono2 Most Recent 2 years, 1 month ago
VPC flow logs
upvoted 1 times

Marshpillowz 2 years, 4 months ago
D is correct
upvoted 1 times

psuoh 3 years, 7 months ago
A, B, C are for data networks containing switches and routers VPC slow log is meant for cloud based network like AWS. Now, Secure Cloud Analytics (formerly Stealthwatch Cloud) can automatically retrieve VPC Flow Logs as a primary or supplementary data source for entity modeling. This means you can now monitor network activity in a cloud environment and increase your security.
upvoted 2 times

Rhoads 3 years, 7 months ago
Using the cloud provider..
upvoted 2 times

sis_net_sec 4 years ago
Stealthwatch Cloud can be deployed without software agents, relying on the native AWS Virtual Private Cloud (VPC) flow logs.
https://aws.amazon.com/marketplace/pp/prodview-woiawecmdlezq
upvoted 3 times

semi1750 4 years, 3 months ago
D - VPC flow logs is answer The question asks "public cloud" and cisco made the following explanation. Cisco Telemetry Broker The Cisco Telemetry Broker is capable of ingesting network telemetry from a variety of telemetry sources, transforming their data formats, and then forwarding that telemetry to one or multiple destinations. For example, it can ingest any of the following: ● On-premises network telemetry, including NetFlow, SYSLOG, and IPFIX ● Cloud-based telemetry sources, such as AWS VPC flow logs and Azure NSG flow logs And it can forward that telemetry to any or all of the following example destinations: ● Analytics platforms, such as Hadoop ● Network management and automation platforms, such as Cisco DNA Center ● Security Information and Event Management (SIEM) platforms ● Storage/smart capture, such as Cisco Security Analytics and Logging (On-premises) https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/datasheet-c78-739398.html
upvoted 3 times

brownbear505 4 years, 5 months ago
Specifically, AWS VPC Flow Logs contain the following information: ● Which IP entities are communicating inside and outside the VPC ● Which protocols (such as TCP and UDP) are being used ● How much traffic is sent and received by each entity ● Whether the flow was allowed or blocked by the security policyhttps://www.cisco.com/c/en/us/products/collateral/security/stealthwatch-cloud/at-a-glance-c45-739851.html

upvoted 3 times

brownbear505 4 years, 5 months ago

Selected Answer: D

Specifically, AWS VPC Flow Logs contain the following information: ● Which IP entities are communicating inside and outside the VPC ● Which protocols (such as TCP and UDP) are being used ● How much traffic is sent and received by each entity ● Whether the flow was allowed or blocked by the security policy

upvoted 3 times

psuoh 3 years, 7 months ago

https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch-cloud/at-a-glance-c45-739851.html

upvoted 1 times

Minion2021 4 years, 5 months ago

Correct answer is D

upvoted 2 times

dr4gn00t 4 years, 7 months ago

This is a tricky question. VPC is valid option only for AWS (Azure and Google uses different terms), and AWS doesn't send telemetry to Stealthwatch. Stealthwatch fetch logs from AWS via API. I think B is therefore most valid answer.

upvoted 4 times

neta1o 4 years, 7 months ago

Looks like this solution supports Azure and AWS. Based on the docs for Azure setup it doesn't look like they refer to the logs as VPC Flow Logs (AWS). So based on that I'd stick with B. https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html#pcm

upvoted 3 times

VI_Vershinin 5 years, 1 month ago

It's B From the book SCOR 350-701: Stealthwatch Cloud is a Software as a Service (SaaS) cloud solution. You can use Stealthwatch Cloud to monitor many different public cloud environments, such as Amazon's AWS, Google Cloud Platform, and Microsoft Azure. All of these cloud providers support their own implementation of NetFlow: ■■ In Amazon AWS, the equivalent of NetFlow is called VPC Flow Logs. You can obtain detailed information about VPC Flow Logs in AWS at https://docs.aws.amazon.com/ vpc/latest/userguide/flow-logs.html. ■■ Google Cloud Platform also supports VPC Flow Logs (or Google-branded GPC Flow Logs). You can obtain detailed information about VPC Flow Logs in Google Cloud Platform at https://cloud.google.com/vpc/docs/using-flow-logs. ■■ In Microsoft's Azure, traffic flows are collected in Network Security Group (NSG) flow logs. NSG flow logs are a feature of Network Watcher. You can obtain additional information about Azure's NSG flow logs and Network Watcher at https://docs.microsoft. com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview

upvoted 5 times

Dinges 5 years, 1 month ago

Its D https://aws.amazon.com/marketplace/pp/prodview-woiawecmdlezq

upvoted 3 times

SirFrates24 5 years, 1 month ago

Not seeing anything related to PUBLIC CLOUD and vpc

upvoted 1 times

SirFrates24 5 years, 1 month ago

Not seeing anything related to PUBLIC CLOUD and vpchttps://www.cisco.com/c/en/us/products/collateral/security/stealthwatch-cloud/at-a-glance-c45-739850.html

upvoted 1 times

Stardec 4 years, 9 months ago

https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch-cloud/at-a-glance-c45-739850.html

upvoted 1 times

yenp 5 years, 1 month ago

correct answer is b : In AWS environments, Cisco Stealthwatch Cloud can be deployed without software agents, relying on the native AWS Virtual Private Cloud (VPC) flow logs. Deployment can be accomplished in minutes by simply giving Cisco Stealthwatch Cloud read-only access to these VPC flow logs. In addition to VPC flows logs, other AWS telemetry data can also be used. GCP also uses VPC flow logs for rapid deployment and integration. Currently for Microsoft Azure environments, Cisco Stealthwatch Cloud relies first on a Linux-based software appliance, called the Observable Networks Appliance (ONA), and second on a third-party host-based NetFlow exporter such as Ziften or FlowTraq.

upvoted 2 times

yenp 5 years, 1 month ago

correct answer is b : In AWS environments, Cisco Stealthwatch Cloud can be deployed without software agents, relying on the native AWS Virtual Private Cloud (VPC) flow logs. Deployment can be accomplished in minutes by simply giving Cisco Stealthwatch Cloud read-only access to these VPC

flow logs. In addition to VPC flows logs, other AWS telemetry data can also be used. GCP also uses VPC flow logs for rapid deployment and integration. Currently for Microsoft Azure environments, Cisco Stealthwatch Cloud relies first on a Linux-based software appliance, called the Observable Networks Appliance (ONA), and second on a third-party host-based NetFlow exporter such as Ziften or FlowTraq.You mean Correct answer is D from your explanation

upvoted 2 times

Maleck 5 years, 1 month ago

You mean Correct answer is D from your explanation

upvoted 3 times

wfexco 5 years, 2 months ago

Answer is D - Stealthwatch Cloud can be deployed without software agents, relying on the native AWS Virtual Private Cloud (VPC) flow logs

upvoted 4 times

wfexco 5 years, 2 months ago

Answer is D - Stealthwatch Cloud can be deployed without software agents, relying on the native AWS Virtual Private Cloud (VPC) flow logsHow is it VPC flow logs when this question is an organization's public cloud, not a private cloud?VPC flow logs are the feature of the public clouds, like AWS

upvoted 4 times

statikd 5 years, 1 month ago

How is it VPC flow logs when this question is an organization's public cloud, not a private cloud?VPC flow logs are the feature of the public clouds, like AWS

upvoted 1 times

statikd 5 years, 1 month ago

How is it VPC flow logs when this question is an organization's public cloud, not a private cloud?

upvoted 1 times

itisfakemaillol 5 years, 1 month ago

VPC flow logs are the feature of the public clouds, like AWS

upvoted 2 times

Question #91 *Topic 1*

An engineer is trying to securely connect to a router and wants to prevent insecure algorithms from being used. However, the connection is failing. Which action should be taken to accomplish this goal?

A. Generate the RSA key using the crypto key generate rsa command.

B. Configure the port using the ip ssh port 22 command.

C. Enable the SSH server using the ip ssh server command.

D. Disable telnet using the no ip telnet command.

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Marshpillowz Most Recent 1 year, 10 months ago

A is correct

upvoted 1 times

OZ1 2 years, 7 months ago

Generate the RSA key using the crypto key generate rsa command.

upvoted 1 times

gondohwe 2 years, 9 months ago

scenario: enabling ssh,setting ssh version to 2 and configuring vty lines to support only ssh connections (config)#hostname FUNTECH-ROUTER #ip domain name FUNTECH.com #crypto key generate rsa (choose key length of your choice after entering this command) #ip ssh version 2 #line vty 0 4 #transport input ssh #password cisco #exit ....of all the provided answers A would make sense

upvoted 3 times

Question #92 *Topic 1*

Refer to the exhibit. Which type of authentication is in use?

```
Info: New SMTP ICID 30 interface Management (192.168.0.100)
     address 10.128.128.200 reverse dns host unknown verified no
Info: ICID 30 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS None
Info: ICID 30 TLS success protocol TLSv1 cipher
     DHE-RSA-AES256-SHA
Info: SMTP Auth: (ICID 30) succeeded for user: cisco using
     AUTH mechanism: LOGIN with profile: ldap_smtp
Info: MID 80 matched all recipients for per-recipient policy
     DEFAULT in the outbound table
```

A. POP3 authentication

B. SMTP relay server authentication

C. external user and relay mail authentication

D. LDAP authentication for Microsoft Outlook

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (44%) B (39%) C (17%)

jaciro11 Highly Voted 4 years, 9 months ago

Okay okay TEAM We will clarify the image: LDAP AUTH Its is true is the action committed for External user and relay mail auth.

And the question ask Told "Which Type of authentication is in use " D is the answer

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html This document describes how to configure LDAP SMTPAUTH to authenticate external users and relay mail. :)

upvoted 12 times

Silexis Most Recent 7 months, 1 week ago

The link is correct though it is not MS Outlook as it supports Outlook Express and Mozila Thunderbird. D can't be correct because is talking only about Microsoft Outlook and not specifying the external user condition

upvoted 1 times

naipoom Highly Voted 4 years, 4 months ago

C https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html

upvoted 7 times

Silexis 7 months, 1 week ago

Selected Answer: C

You can find the explanation with the same example of log snippet here https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html So the correct answer is C

upvoted 1 times

danielschmitz87 1 year ago

Selected Answer: D

It is definitely D

upvoted 1 times

DANT7 1 year, 3 months ago

Selected Answer: B

B. SMTP relay server authentication

Porque se está autenticando un usuario (cisco) usando LDAP como base de datos de autenticación en un servidor SMTP, lo cual es típico para relays que requieren validación antes de enviar correo.

upvoted 1 times

willroute 1 year, 9 months ago

It is C...SMTP and auth in log.... https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html

upvoted 2 times

Marshpillowz 2 years, 4 months ago

Selected Answer: D

I think D

upvoted 1 times

LTLnetworker 2 years, 7 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html

upvoted 2 times

Stevens0103 2 years, 7 months ago

Selected Answer: D

C is the object to be authenticated, not a type of authentication.

"Configure LDAP SMTPAUTH To Authenticate External Users and Relay Mail"

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html

upvoted 3 times

petestudies 2 years, 8 months ago

Selected Answer: C

C. external user and relay mail authentication https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html

--- Wed Sep 12 07:59:41 2007 Info: SMTP Auth: (ICID 36) succeeded for user: jsmith using AUTH mechanism: LOGIN with profile: ldap_smtp

upvoted 1 times

xziomal9 2 years, 9 months ago

Answer B

upvoted 1 times

fdl543 3 years ago

Selected Answer: B

B is correct. The problem with D is "for Microsoft Outlook" because LDAP does not restrict to Microsoft Outlook only...

upvoted 1 times

jku2cya 3 years, 1 month ago

Selected Answer: D

jaciro11 has the correct Troubleshooting Technote to reference link. It also has similar example logs, without the timestamps and it misses the " >>".

upvoted 1 times

littlewilly 3 years, 2 months ago

Selected Answer: C

Answer is C- this has nothing to do with outlook

upvoted 1 times

Carlis 3 years, 4 months ago

Selected Answer: B

SMTP Authentication using LDAP as Profile Type has been configured on Cisco ESA. Another tricky Cisco question, where the correct answer is what cisco wants to see. It authenticates External users and Relay Mail, using LDAP profile type as authentication mechanism for SMTP Authentication (as stated in the log).

Info: SMTP Auth: (ICID 30) succeeded for user: cisco using AUTH mechanism: LOGIN with profile: ldap_smtp

For me the correct answer is B.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html

upvoted 5 times

sull3y 3 years, 6 months ago

D. LDAP authentication for Microsoft Outlook

The exhibit refers to "AUTH Mechanism:LOGIN with profile: ldap_smtp", which indicates that the authentication mechanism in use is LDAP (Lightweight Directory Access Protocol) and the profile used is "ldap_smtp" . This means that users are being authenticated against an LDAP directory before they are allowed to send mail via SMTP, which is typically used for Microsoft Outlook.

upvoted 3 times

edu_web 3 years, 9 months ago

Why not B? https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118570-qa-esa-00.html

upvoted 2 times

Question #93 *Topic 1*

Refer to the exhibit. An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?

```
ip dhcp snooping
ip dhcp snooping vlan 41,44
!
interface GigabitEthernet1/0/1
 description Uplink_To_Distro_Switch_g1/0/11
 switchport trunk native vlan 999
 switchport trunk allowed vlan 40,41,44
 switchport mode trunk
```

A. ip dhcp snooping limit 41

B. ip dhcp snooping verify mac-address

C. ip dhcp snooping trust

D. ip dhcp snooping vlan 41

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

zheka Highly Voted 4 years, 2 months ago

Even though the correct answer is C the entire question and especially exhibit is stupid. We do not know where the DHCP server is. It could be on the same switch or the other switch reachable via the shown interface. If it is on the same switch then adding "ip dhcp snooping trust" on port 41 won't help because it needs added on the port where DHCP server is connected. An untrusted port is a port that does not accept DHCP server messages. In other words, if a device is connected to an untrusted port, it can obtain IP configuration from the DHCP server but it cannot offer an IP configuration. A trusted port is a port that accepts DHCP server messages. In other words, a DHCP server can provide IP configuration only if it is connected to a trusted port.

upvoted 16 times

asdasd123123iu 3 years, 8 months ago

I add that command from D is already visible in configuration and answer A i think is incorrect so B and C left. C work like zheka described so theoretically should resolve problem. B I'm not sure if it has any impact for clients, it's just security feature.

upvoted 1 times

psuoh 3 years, 1 month ago

perhaps it is using IP DHCP RELAY command...

upvoted 1 times

Wdgbill Highly Voted 3 years, 6 months ago

note here that the config is for the trunk port to a distribution switch and switch to switch ports need to be set to trusted. No detailed information but the possibility exists that the DHCP server is on another switch so without the trunk between switches being trusted no DHCP offers would transit the link

upvoted 6 times

Marshpillowz Most Recent 1 year, 10 months ago

Selected Answer: C

C is correct

upvoted 1 times

Question #94 *Topic 1*

Refer to the exhibit. Traffic is not passing through IPsec site-to-site VPN on the Firepower Threat Defense appliance. What is causing this issue?

```
> show crypto ipsec sa
interface: Outside
     Crypto map tag: CSM_Outside_map, seq num: 1, local addr:
209.165.200.225

     access-list CSM_IPSEC_ACL_1 extended permit ip 10.0.11.0
255.255.255.0.10.0.10.0 255.255.255.0
     local ident (addr/mask/prot/port) : (10.0.11.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port) : (10.0.10.0/255.255.255.0/0/0)
     current_peer: 209.165.202.129

     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
     #pkts decaps: 17, #pkts decrypt : 17, #pkts verify: 17
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp
failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created : 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 209.165.200.225/500, remote crypto endpt.:
209.165.202.129/500
     path mtu 1500, ipsec overhead 55(36), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi : B6F5EA53
     current inbound spi : 84348DEE
```

A. Site-to-site VPN preshared keys are mismatched.

B. Site-to-site VPN peers are using different encryption algorithms.

C. No split-tunnel policy is defined on the Firepower Threat Defense appliance.

D. The access control policy is not allowing VPN traffic in.

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

kerniger Highly Voted 5 years ago

A - vpn is established B - vpn is established C - Split Tunneling has nothing to do with a site-to-site VPN. D - we see traffic is comming in but no traffic is going into the tunnel so its likely a access policy wrong or missing

upvoted 29 times

zap_pap Highly Voted 5 years ago

A & B are ruled out by #pkts encaps #pkts decaps: traffic is flowing based on these lines, so the VPN is established. #pkts decaps: 17 - we are getting traffic in, so it is not blocked by the ACL. Only C is left.Perfect explanation! I agree with Cno no my friend...split-tunneling doesnt prevent vpns from operating but define what traffic should use the vpn tunnel and what traffic shoudnt so forget C...on FTD devices access policies shld also properly permit traffic provide vpn has been configured proper way...D sounds betterslpit-tunneling is never heard of in site 2 site vpns

upvoted 11 times

zap_pap 5 years ago

A & B are ruled out by #pkts encaps #pkts decaps: traffic is flowing based on these lines, so the VPN is established. #pkts decaps: 17 - we are getting traffic in, so it is not blocked by the ACL. Only C is left.

upvoted 11 times

jmosilva 5 years ago

Perfect explanation! I agree with C

upvoted 3 times

gondohwe 3 years, 3 months ago

no no my friend...split-tunneling doesnt prevent vpns from operating but define what traffic should use the vpn tunnel and what traffic shoudnt so forget C...on FTD devices access policies shld also properly permit traffic provide vpn has been configured proper way...D sounds better

upvoted 2 times

gondohwe 3 years, 3 months ago

no no my friend...split-tunneling doesnt prevent vpns from operating but define what traffic should use the vpn tunnel and what traffic shoudnt so forget C...on FTD devices access policies shld also properly permit traffic provide vpn has been configured proper way...D sounds betterslpit-tunneling is never heard of in site 2 site vpns

upvoted 2 times

gondohwe 3 years, 3 months ago

slpit-tunneling is never heard of in site 2 site vpns

upvoted 2 times

Rockbo47 Most Recent 2 years ago

As others have pointed out also, the correct answer can only be D for the reasons provided by others however there MUST be a typo in D because traffic is being successfully received as indicated by the decaps and decrypt packets. So the actual correct answer would be "The access control policy is not allowing VPN traffic OUT."

upvoted 2 times

Marshpillowz 2 years, 4 months ago

D is correct

upvoted 1 times

Alizade 2 years, 10 months ago

D. The access control policy is not allowing VPN traffic in.

upvoted 2 times

intirt 3 years, 8 months ago

D is correct

upvoted 2 times

ureis 3 years, 10 months ago

crypto map is not matching with ALC, so D is correct

upvoted 2 times

getafix 4 years, 2 months ago

A - cannot be true since the tunnel is established as we can see pkts decerypted and pkts encrypted --> zero B: Same as above, tunnel is up so Phase1 and Phase2 are both up and interesting traffic is passing C: Split tunneling works for remote access VPNs. It defines what traffic, when a user connects to a remote access VPN server, should go inside the VPN and what traffic should go out via his local home router. D: Since there are no encapsulations happening encaps:0bytes.....it evidently shows a problem with the access list

upvoted 8 times

somaaoo 4 years, 4 months ago

pkts encap are 0 , so D

upvoted 4 times

killbots 4 years, 4 months ago

I say its D. Split-Tunneling is only relevant to Remote Access VPNs not S2S. only one that makes sense is D.

upvoted 3 times

zheka 4 years, 8 months ago

Maybe it is another example of the stupid question/exhibit or a tricky one. If VPN is established and especially Phase 2 with all security associations created then two firewall peers negotiated everything which is matching. Of course nothing to do with split-tunneling on the site-to-site tunnel. The only explanation for this assymetry of counters for packets entering the tunnel and exiting is either missing NAT exemption rules or indeed access control policy rule which should be configured only if we stopped trusting the traffic that exits the tunnel (former sysopt connection permit-vpn)

upvoted 1 times

zeroC00L 4 years, 11 months ago

i would go with D and hoping this is just a typo (and it meant actually "out") because it seems to be the "less" wrong answer. C makes no sense from both wording and technically. If you do something wrong according to what to send into the tunnel it would either not come up at all or would throw erros about "proxy identity mismatch" (we dont have debugs so this cant be validated)

upvoted 6 times

Sarbi 4 years, 12 months ago

I agreed with C and VPN tunnel is established only traffic is not passing.

upvoted 1 times

Narcolepto 5 years, 1 month ago

I think the answer is D because if you look carefully at the access-list it is incorrectly formatted. There is an extra period between the mask of the source and the ip of the destination instead of a space - 255.255.255.0.10.0.10.0 instead of 255.255.255.0 10.0.10.0

upvoted 2 times

Narcolepto 5 years, 1 month ago

I think the answer is D because if you look carefully at the access-list it is incorrectly formatted. There is an extra period between the mask of the source and the ip of the destination instead of a space - 255.255.255.0.10.0.10.0 instead of 255.255.255.0 10.0.10.0This might me just a typo. In the next lines of the output, traffic selectors (local and remote idents) are parsed correctly.

upvoted 2 times

Dead_Adriano 5 years, 1 month ago

This might me just a typo. In the next lines of the output, traffic selectors (local and remote idents) are parsed correctly.

upvoted 1 times

Raajaa 5 years, 1 month ago

D is the answer

upvoted 1 times

Barish 5 years, 3 months ago

Answer D is correct

upvoted 2 times

Minipaf 5 years, 3 months ago

Hello, can anyone explain this answer ? I find that answer D makes more sense. thanks!

upvoted 1 times

Minipaf 5 years, 3 months ago

Hello, can anyone explain this answer ? I find that answer D makes more sense. thanks!A and B are incorrect because we can see the tunnel is up. We know it is up because we have 17 decap packets. This means traffic is coming from the peer to the ASA and it decrypts and sends it according to the routing table. C is incorrect because that is related to remote-access VPNs, not S2S VPNs. Since we have no encaps - which is traffic entering the ASA, being encrypted, and sent out the tunnel - this likely means the ASA has an inbound access-list on the 'inside' or whatever interface not allowing the interesting traffic in. So the traffic blocked entering into the ASA never giving it an option to be encrypted. D is therefore the answer.

upvoted 1 times

cciewannab 4 years, 11 months ago

A and B are incorrect because we can see the tunnel is up. We know it is up because we have 17 decap packets. This means traffic is coming from the peer to the ASA and it decrypts and sends it according to the routing table. C is incorrect because that is related to remote-access VPNs, not S2S VPNs. Since we have no encaps - which is traffic entering the ASA, being encrypted, and sent out the tunnel - this likely means the ASA has an inbound access-list on the 'inside' or whatever interface not allowing the interesting traffic in. So the traffic blocked entering into the ASA never giving it an option to be encrypted. D is therefore the answer.

upvoted 7 times

Question #95 *Topic 1*

Refer to the exhibit. A network administrator configured a site-to-site VPN tunnel between two Cisco IOS routers, and hosts are unable to communicate between two sites of VPN. The network administrator runs the debug crypto isakmp sa command to track VPN status. What is the problem according to this command output?

```
*Jun 30 16:52:33.287: ISAKMP: (1002) : retransmitting phase 1 MM_KEY_ECH…
*Jun 30 16:52:33.287: ISAKMP: (1002) : incrementing error counter on sa, attempt 4
of 5: retransmit phase 1
*Jun 30 16:52:33.287: ISAKMP: (1002) : retransmitting phase 1 MM_KEY_EXCH
*Jun 30 16:52:33.287: ISAKMP: (1002) : sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 16:52:33.291: ISAKMP: (1002) : Sending an IKE IPv4 Packet.
*Jun 30 16:52:33.791: ISAKMP: (1002) : received packet from 10.10.12.2 dport 500
sport 500 Global (I) MM_KEY_EXCH
*Jun 30 16:52:33.795: ISAKMP: (1002) : phase 1 packet is a duplicate of a previous
packet
R1#
*Jun 30 16:52:33.795: ISAKMP: (1002) : retransmission skipped for phase 1 (time
since last transmission 504)
R1#
*Jun 30 16:52:40.183: ISAKMP: (1001) : purging SA., SA=68CEE058, delme=68CEE058
R1#
*Jun 30 16:52:43.291: ISAKMP: (1002) : retransmitting phase 1 MM_KEY_EXCH…
*Jun 30 16:52:43.291: ISAKMP: (1002) : incrementing error counter on sa, attempt 5
of 5: retransmit phase 1
*Jun 30 16:52:43.295: ISAKMP: (1002) : retransmitting phase 1 MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP: (1002) : sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP: (1002) :Sending an IKE IPv4 Packet.
R1#
*Jun 30 16:52:53.299: ISAKMP: (1002) : retransmitting phase 1 MM_KEY_EXCH…
*Jun 30 16:52:53.291: ISAKMP: (1002) :peer does not do paranoid keepalives.

*Jun 30 16:52:53.299: ISAKMP: (1002) :deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.303: ISAKMP: (1002) :deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.307: ISAKMP: Unlocking peer struct 0x68287318 for
isadb_mark_sa_deleted {}, count 0
*Jun 30 16:52:53.307: ISAKMP: Deleting peer node by peer_reap for 10.10.12.2:
68287318
*Jun 30 16:52:53.311: ISAKMP: (1002) :deleting node 79875537 error FALSE reason "IKE
deleted"
R1#
*Jun 30 16:52:53.311: ISAKMP: (1002) :deleting node -484575753 error FALSE reason
"IKE deleted"
*Jun 30 16:52:53.315: ISAKMP: (1002) :Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL
*Jun 30 16:52:53.319: ISAKMP: (1002) :Old State = IKE_I_M5 New State = IKE_DEST_SA
```

A. interesting traffic was not applied

B. encryption algorithm mismatch

C. authentication key mismatch

D. hashing algorithm mismatch

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (77%) B (23%)

dr4gn00t Highly Voted 4 years, 6 months ago

Googling for MM_KEY_EXCH retransmission seems to indicate mismatch between shared secret

upvoted 20 times

denverfly Highly Voted 4 years, 6 months ago

Answer:C https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html n the show crypto isakmp sa output, the state should always be QM_IDLE. If the state is MM_KEY_EXCH, it means either the configured pre-shared key is not correct or the peer IP addresses are different.I agree with this. Even though the command is "show crypto isakmp sa" not "ebug crypto isakmp sa command" but same idea

upvoted 15 times

denverfly 4 years, 6 months ago

Answer:C https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html n the show crypto isakmp sa output, the state should always be QM_IDLE. If the state is MM_KEY_EXCH, it means either the configured pre-shared key is not correct or the peer IP addresses are different.

upvoted 15 times

CyberSecurity80 4 years, 6 months ago

I agree with this. Even though the command is "show crypto isakmp sa" not "ebug crypto isakmp sa command" but same idea

upvoted 1 times

Premium_Pils Most Recent 2 years ago

based on below explanation for MM_KEY_EXCH retransmission

upvoted 1 times

Marshpillowz 2 years, 4 months ago

C is correct

upvoted 1 times

JavierAcuna 3 years, 3 months ago

C MM_KEY_EXCH ANswer is C

upvoted 2 times

Carlis 3 years, 4 months ago

MM_KEY_EXCH indicates key exchange mismatch MM_NO_STATE would indicate isakmp policy mismatch (e.g.encryption)

upvoted 4 times

iratus_umbra 3 years, 4 months ago

100% C is correct.

upvoted 1 times

Vlad_Is_Love_ua 3 years, 5 months ago

C is CORRECT, because MM_KEY_EXCH = MisMatch Key ExchangeMM_KEY_EXCH = Main Mode Key Exchange

upvoted 2 times

Vlad_Is_Love_ua 3 years, 5 months ago

Selected Answer: C

C is CORRECT, because MM_KEY_EXCH = MisMatch Key Exchange

upvoted 2 times

Stevens0103 2 years, 7 months ago

MM_KEY_EXCH = Main Mode Key Exchange

upvoted 2 times

ddev3737_111 3 years, 6 months ago

C because B would right but paranoid keepalives message only occurs after MM_KEY_EXC error messageKeepalives are messages exchanged between the peers to ensure that the VPN tunnel is still alive and functioning. The "paranoid keepalives" message suggests that the peer (10.10.12.2) does not support or engage in the paranoid keepalives mechanism. The "MM_KEY_EXCH" messages, on the other hand, specifically refer to Main Mode Key Exchange during IKE negotiation. These messages are part of the process of establishing a secure communication channel between the VPN peers. They are distinct aspects of the overall VPN establishment process.

upvoted 2 times

ddev3737 3 years, 6 months ago

C because B would right but paranoid keepalives message only occurs after MM_KEY_EXC error message

upvoted 2 times

Stevens0103 2 years, 7 months ago

Keepalives are messages exchanged between the peers to ensure that the VPN tunnel is still alive and functioning. The "paranoid keepalives" message suggests that the peer (10.10.12.2) does not support or engage in the paranoid keepalives mechanism. The "MM_KEY_EXCH" messages, on the other hand, specifically refer to Main Mode Key Exchange during IKE negotiation. These messages are part of the process of establishing a secure communication channel between the VPN peers. They are distinct aspects of the overall VPN establishment process.

upvoted 1 times

psuoh 3 years, 7 months ago

More likely mismatched authentication key issue... https://www.networkworld.com/article/2288666/chapter-4--common-ipsec-vpn-issues.html?page=3

upvoted 1 times

Emlia1 3 years, 8 months ago

It's C

upvoted 2 times

Hereim 3 years, 10 months ago

It should be B - since the error message states "peer does not do paranoid keepalives" meaning PFS is tuned on at one end and off on the other end. If it was key mismatch we should see that in the debug.

upvoted 1 times

SulSulEi 3 years, 11 months ago

Answet is C, please check below, https://www.google.com/amp/s/www.networkworld.com/article/2288666/chapter-4--common-ipsec-vpn-issues.amp.html

upvoted 2 times

surforlife 4 years ago

all over the retry MM_KEY_EXCH, it means Mismatch Key Exchange! "C" is correctthats main mode key exchange. not mismatch

upvoted 2 times

surforlife 4 years ago

all over the retry MM_KEY_EXCH, it means Mismatch Key Exchange! "C" is correct

upvoted 2 times

west33637 3 years, 8 months ago

thats main mode key exchange. not mismatch

upvoted 1 times

Bezos 4 years, 1 month ago

C is the answer https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

upvoted 3 times

getafix 4 years, 2 months ago

Debugging isakmp logs show the actual message of key mismatch if there is a key mismatch. The exhibit in the question does not show the "key mismatch" message. The resulting logs would be due to a proposal mismatch

upvoted 2 times

Sattm1 4 years, 3 months ago

B and D show specific items that could be wrong - but we don't know which (or it could be mismatched secrets/auth methods). Here's a very basic ISAKMP config: C is the generic key mismatch - aka ISAKMP has failed- and that's all we see in the logs R3(config)# crypto isakmp policy 10 R3(config-isakmp)# authentication pre-share R3(config-isakmp)# encryption 3des R3(config-isakmp)# hash sha R3(config-isakmp)# group 2

upvoted 2 times

Question #96 *Topic 1*

Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?

A. group policy

B. access control policy

C. device management policy

D. platform settings policy

Suggested Answer: *D*

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/platform_settings_policies_for_managed_devices.pdf

Community vote distribution

D (100%)

Vic25H Highly Voted 5 years, 8 months ago

It's platform SETTINGS policy

upvoted 11 times

Seawanderer 4 years, 7 months ago

close enough :-)

upvoted 2 times

Marshpillowz Most Recent 1 year, 10 months ago

Selected Answer: D

D is correct

upvoted 1 times

sull3y 3 years ago

D:https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Platform_Settings_Policies_for_Managed_Devices.pdf

upvoted 3 times

Question #97 *Topic 1*

The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic.
Where must the ASA be added on the Cisco UC Manager platform?

A. Certificate Trust List

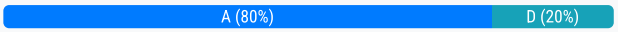
B. Endpoint Trust List

C. Enterprise Proxy Service

D. Secured Collaboration Proxy

Suggested Answer: *A*
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/special/unified-communications/guide/unified-comm/unified-comm-tlsproxy.html

Community vote distribution



red_sparrow_Gr Highly Voted 2 years, 3 months ago
Incorporating the Firewall into the Unified Communications System Configuring the ASA is not enough to fully incorporate the firewall into the Cisco Unified Communications system. You must also add the ASA to the Certificate Trust List (CTL) using the Cisco Certificate Trust List Client, which is part of the Unified Communications Manager. https://www.cisco.com/c/en/us/td/docs/security/asa/special/unified-communications/unified-communications-guide/tls-proxy-for-encrypted-voice-inspection.html?bookSearch=true
upvoted 7 times

surforlife Highly Voted 3 years, 7 months ago
"A" is correct. The security appliance acts as a TLS proxy between the Cisco IP Phone and Cisco UCM. The proxy is transparent for the voice calls between the phone and the Cisco UCM. Cisco IP Phones download a Certificate Trust List from the Cisco UCM before registration which contains identities (certificates) of the devices that the phone should trust, such as TFTP servers and Cisco UCM servers. To support server proxy, the CTL file must contain the certificate that the security appliance creates for the Cisco UCMs.
upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago
I think A
upvoted 1 times

Alizade 2 years, 4 months ago
The ASA must be added to the Cisco UC Manager platform as the Secured Collaboration Proxy.
upvoted 2 times

DWizard 2 years, 7 months ago
This question is horrible. It is about where to put the certificate or is it about the option in the menu in the CUCM to configure the TLS proxy or anything else?
upvoted 1 times

Question #98 *Topic 1*

Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two.)

A. SIP

B. inline normalization

C. SSL

D. packet decoder

E. modbus

Suggested Answer: *A, C*

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application_Layer_Preprocessors.html

Community vote distribution

AC (100%)

sull3y Highly Voted 3 years ago

A. SIP C. SSL SIP (Session Initiation Protocol) Preprocessor and SSL (Secure Sockets Layer) Preprocessor are two of the application layer preprocessors that are used by Firepower Next Generation Intrusion Prevention System (NGIPS). SIP preprocessor inspects and analyzes SIP traffic, and SSL preprocessor inspects and analyzes SSL traffic. These preprocessors work in conjunction with the overall NGIPS system to provide a comprehensive security solution for protecting networks from a variety of attacks.

upvoted 6 times

roolmereyes Highly Voted 2 years, 6 months ago

These are all available preprocessors: The DCE/RPC Preprocessor The DNS Preprocessor The FTP/Telnet Decoder The HTTP Inspect Preprocessor The Sun RPC Preprocessor The SIP Preprocessor The GTP Preprocessor The IMAP Preprocessor The POP Preprocessor The SMTP Preprocessor The SSH Preprocessor The SSL Preprocessor

upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago

A and C are correct

upvoted 1 times

Question #99 *Topic 1*

Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

A. quality of service

B. time synchronization

C. network address translations

D. intrusion policy

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

crh23 Highly Voted 5 years, 7 months ago

Correct B Synchronizing Time on Classic Devices https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_Software_Platform_Settings.html#task_EF18AE3D5CA9457AB65791B9654FD46C

upvoted 6 times

Marshpillowz Most Recent 1 year, 10 months ago

B is correct

upvoted 1 times

Question #100 *Topic 1*

Which information is required when adding a device to Firepower Management Center?

A. username and password

B. encryption method

C. device serial number

D. registration key

Suggested Answer: *D*

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html#ID-2242- 0000069d

Community vote distribution

D (100%)

pfunkylol Highly Voted 4 years, 3 months ago

correct.

upvoted 7 times

Marshpillowz Most Recent 1 year, 10 months ago

Selected Answer: D

D is correct

upvoted 1 times

gc999 2 years, 10 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html Please refer to the procedure Step 5 when adding devices to the FMC.

upvoted 4 times

Toni_Su91 2 years, 11 months ago

> configure manager add [IP address] [KEY]

upvoted 3 times

Question #101 *Topic 1*

What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?

A. Cisco Umbrella

B. External Threat Feeds

C. Cisco Threat Grid

D. Cisco Stealthwatch

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

CiscoTech Highly Voted 5 years, 7 months ago
I think the answer is B. https://www.cisco.com/c/en/us/support/docs/storage-networking/security/214859-configure-and-troubleshoot-cisco-threat.html
upvoted 19 times

MoII 4 years, 3 months ago
Answer should be B https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKDEV-2456.pdf Page 28 Cisco Threat Intelligence Director (TID) Step 1 Ingest third-party Cyber Threat Intelligence (CTI) Step 2 Publish observables to sensors Step 3 Detect and alert on incidents
upvoted 5 times

CyberGhost666 Most Recent 1 year, 1 month ago
B. External Threat Feed
upvoted 1 times

Marshpillowz 1 year, 10 months ago
B is correct
upvoted 1 times

brownbear505 3 years, 12 months ago
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_director__tid_.html
upvoted 5 times

Sun2sun 4 years ago
should be B
upvoted 2 times

pr0fectus 4 years, 1 month ago
TID is used to leverage external threat feeds. ThreatGrid is already integrated with the AMP capability of FTD.
upvoted 2 times

MoII 4 years, 3 months ago
Answer should be B https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligence-director
upvoted 4 times

zeroC00L 4 years, 4 months ago
i would go with B here. Because the TID is used if you want to use external (not cisco provided) Security Information / Observables, in addition to what you get from cisco -> "The Cisco Threat Intelligence Director (TID) operationalizes threat intelligence data, helping you aggregate intelligence data, configure defensive actions, and analyze threats in your environment. This feature is intended to supplement other Firepower functionality, offering an additional line of defense against threats" https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_director__tid_.html and for AMP you dont need the TID. AMP(for Networks) comes with its own configuration o the FMC for example where you can define the cloud you want to use etc.
upvoted 2 times

Sarbi 4 years, 5 months ago

It looks to me C.As it the cisco exam.Cisco treat grid"Secure Malware Analytics (formerly Threat Grid) combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware."

upvoted 2 times

Sarbi 4 years, 5 months ago

It looks to me C.As it the cisco exam.Cisco treat grid

upvoted 2 times

andrewj511 4 years, 5 months ago

"Secure Malware Analytics (formerly Threat Grid) combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware."

upvoted 2 times

Raajaa 4 years, 7 months ago

B sounds correct to me

upvoted 2 times

Kris92 4 years, 11 months ago

I went with C at first, but B makes more sense. External threat feed is a option on ESA, but I don't see any example of using TID. TID is usually added to FP in intelligence sources.

upvoted 1 times

user636 5 years, 1 month ago

The answer is B, there no possibility to integrate ThreatGrid with TID at all. You could check the administration guide of TID.

upvoted 5 times

JAckThePip 5 years, 2 months ago

The answer is B: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0110001.html

upvoted 2 times

myccnptest 5 years, 2 months ago

Looks like it might be "B" https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_director__tid_.html Feature introduced: Lets you use threat intelligence from external sources to identify and process threats.

upvoted 4 times

avl83 5 years, 6 months ago

the answer is C. More information take a look in, chapter 11, page 654, book "ccnp and ccie security Core"

upvoted 2 times

avl83 5 years, 6 months ago

the answer is C. More information take a look in, chapter 11, page 654, book "ccnp and ccie security Core"The question is about the TID, not CTR. Correct answer is BB

upvoted 2 times

essie007 Highly Voted 5 years, 4 months ago

The question is about the TID, not CTR. Correct answer is BB

upvoted 6 times

Question #102 *Topic 1*

Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?

A. aaa server radius dynamic-author

B. auth-type all

C. aaa new-model

D. ip device-tracking

Suggested Answer: *A*
Official Answer: A

Community vote distribution
C (72%) A (28%)

Ampersand Highly Voted 5 years, 4 months ago
aaa new-model Enables authentication, authorization, and accounting (AAA) globally.

aaa server radius dynamic-author Sets up the local AAA server for the dynamic authorization service, which must be enabled to support the CoA functionality to push the policy map in an input and output direction, and enters dynamic authorization local server configuration mode.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html
upvoted 25 times

jpapas Highly Voted 3 years ago
Selected Answer: A
Guys, you need reverse logic here. > if you issue an "aaa new-model" you dont have CoA support as is disabled by default on all devices. > if you issue "aaa server radius dynamic-author" this will activate CoA globally (assuming that aaa new-model is already there)
upvoted 5 times

jpapas 3 years ago
... and says "so that CoA >>IS<< supported..." so the command activated CoA.

If the Q wording was different i.e. "... so that to be able to support CoA..." , then the right answer would be C "aaa new-model" (but not with the above wording, which makes A the correct answer).
upvoted 1 times

CyberGhost666 Most Recent 1 year, 1 month ago
Selected Answer: C
C. aaa new-model command enables AAA globally, which is required for CoA to function on the device.
upvoted 1 times

sem_jeka 1 year, 11 months ago
A is correct
upvoted 1 times

Rockbo47 2 years ago
Selected Answer: C
The question is "Which Cisco command enables authentication, authorization, and accounting globally" - the rest is irrelevant here. With that being the case, the only correct answer is C. Once AAA is enabled globally, THEN you would use the command "aaa server radius dynamic-author" to enable CoA
upvoted 2 times

Tthurston1 2 years, 1 month ago
Selected Answer: C
To enable AAA, you need to configure the 'aaa new-model' command in global configuration mode. Until this command is enabled, ALL OTHER AAA commands are hidden.

https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

upvoted 2 times

Korndal 2 years, 1 month ago

Selected Answer: C

It's C. you cannot enable anything without first issuing "aaa new-model". So all AAA commands are not available befor you add "aaa new-model" therefor the answer is C

upvoted 3 times

XvidalX 2 years, 5 months ago

Selected Answer: C

simple.. dynamic author enables COA , aaa new model permits COA to be enabled.. C ir the correct.

upvoted 2 times

xziomal9 2 years, 9 months ago

Answer C

upvoted 1 times

cyberwhizzy0 3 years, 1 month ago

Selected Answer: C

Step 3 aaa new-model

Example: Device(config)# aaa new-model Enables authentication, authorization, and accounting (AAA) globally.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html

upvoted 2 times

Leogxn 3 years, 1 month ago

Selected Answer: A

aaa new-model Enables authentication, authorization, and accounting (AAA) globally

I think the aaa server radius dynamic-author command has to be enabled globally to support the CoA

upvoted 2 times

jku2cya 3 years, 1 month ago

Selected Answer: A

Exactly what Ampersand and Jessie45785 said

upvoted 2 times

Jessie45785 3 years, 2 months ago

Selected Answer: A

A is correct answer don't be fooled:

Proof: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-xe-3se-3850-cr-book/sec-a1-xe-3se-3850-cr-book_chapter_01.html#wp4234596077

aaa new-model: To enable the authentication, authorization, and accounting (AAA) access control model, issue the aaa new-model command in global configuration mode. To disable the AAA access control model, use the no form of this command.

aaa server radius dynamic-author: (to facilitate interaction with an external policy server)

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the aaa server radius dynamic-authorcommand in global configuration mode. To remove this configuration, use the no form of this command.

upvoted 2 times

YooAndI 3 years, 3 months ago

It's C. Cisco states that Step 3: aaa new-model "Enables authentication, authorization, and accounting (AAA) globally." This command goes before Step 4: aaa server radius dynamic-author, which "Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests. Configures the device as a AAA server to facilitate interaction with an external policy server." So the command aaa new-model is needed BEFORE aaa server radius dynamic-author, in order for it to function. Answer is C. Source: Cisco RADIUS Change of Authorization paper - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xe-16-10/sec-usr-aaa-xe-16-10-book/sec-rad-coa.pdf

upvoted 1 times

stalkr3 3 years, 4 months ago

Selected Answer: C

aaa server radius dynamic-author does not enable aaa globally. Therefore C

upvoted 2 times

Jessie45785 3 years, 4 months ago

Selected Answer: C

definitely C

upvoted 1 times

Tuxzinator 3 years, 6 months ago

Selected Answer: C

So both commands, "aaa new-model" and "aaa server radius dynamic-author," can be used to enable CoA on a Cisco device, but they serve different purposes. The "aaa new-model" command is used to enable AAA globally on the device, while the "aaa server radius dynamic-author" command is used to configure a RADIUS server for dynamic authorization.

upvoted 3 times

Question #103 *Topic 1*

What is a characteristic of Firepower NGIPS inline deployment mode?

A. ASA with Firepower module cannot be deployed

B. It cannot take actions such as blocking traffic

C. It is out-of-band from traffic

D. It must have inline interface pairs configured

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

surforlife Highly Voted 3 years, 7 months ago

"D" https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html#anc2

upvoted 8 times

CyberGhost666 Most Recent 1 year, 1 month ago

D. It must have inline interface pairs configured

upvoted 1 times

Marshpillowz 1 year, 10 months ago

I think D

upvoted 1 times

LTLnetworker 2 years, 1 month ago

Inline pairs should not be confused with IPS inline mode. https://community.cisco.com/t5/security-blogs/demystifying-firepower-deployment-modes/bc-p/4994822#M2570 https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html Without any inline pairs, an FTD in routed mode usually performs IPS functions in inline mode (i. e. capable of dropping packets if intrusion is detected). None of the answers are correct.

upvoted 2 times

Question #104 *Topic 1*

A mall provides security services to customers with a shared appliance. The mall wants separation of management on the shared appliance. Which ASA deployment mode meets these needs?

A. routed mode

B. multiple zone mode

C. multiple context mode

D. transparent mode

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

Marshpillowz Most Recent 1 year, 10 months ago

C is correct

upvoted 1 times

gondohwe 2 years, 9 months ago

multi-context mode allows creation of several firewall instances within a single physical firewall for multi-tenancy purposes

upvoted 1 times

gondohwe 2 years, 9 months ago

multi-context mode allows creation of several firewall instances within a single physical firewall for multi-tenancy purposesC is the correct choice

upvoted 1 times

gondohwe 2 years, 9 months ago

C is the correct choice

upvoted 1 times

Question #105 *Topic 1*

What is managed by Cisco Security Manager?

A. Cisco WLC

B. Cisco ESA

C. Cisco WSA

D. Cisco ASA

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

Correct Answer is D.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

D is correct

upvoted 1 times

sull3y 3 years ago

D:Cisco Security Manager (CSM) is a security management solution for Cisco security devices, such as Cisco ASA, Cisco Firepower, and Cisco ISR. It is used to manage and configure Cisco security devices, including firewall policies, VPNs, and intrusion prevention. CSM provides a centralized management platform that allows network administrators to manage multiple Cisco security devices from a single console, including device discovery, inventory management, policy provisioning and compliance reporting. With CSM, administrators can deploy consistent security policies across multiple devices, reducing the risk of security breaches and simplifying security management.

upvoted 1 times

TesterDude 3 years, 9 months ago

Based on the wording, I think bhbh2020 is right; however, I believe the wording on the test will be "Cisco Content Security Manager Appliance (SMA)", which is covered heavily in the book and manages ESA and WSA:

"Cisco Content SMA provides centralized management and monitoring (reporting) of Cisco WSAs and Cisco ESAs. The Cisco SMA simplifies the planning and administration of Cisco ESA and Cisco WSA deployments." Santos, Omar. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide (p. 624). Pearson Education. Kindle Edition.

upvoted 2 times

TesterDude 3 years, 9 months ago

Based on the wording, I think bhbh2020 is right; however, I believe the wording on the test will be "Cisco Content Security Manager Appliance (SMA)", which is covered heavily in the book and manages ESA and WSA: "Cisco Content SMA provides centralized management and monitoring (reporting) of Cisco WSAs and Cisco ESAs. The Cisco SMA simplifies the planning and administration of Cisco ESA and Cisco WSA deployments." Santos, Omar. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide (p. 624). Pearson Education. Kindle Edition."Security Manager" is different compared to "Security Management Appliance" which you refers to. On Cisco site they are different. Manager/Management... tricky but not the same word. D is the correct one.

upvoted 2 times

Mjestic 3 years, 3 months ago

"Security Manager" is different compared to "Security Management Appliance" which you refers to. On Cisco site they are different. Manager/Management... tricky but not the same word. D is the correct one.

upvoted 1 times

Question #106 *Topic 1*

An organization is trying to improve their Defense in Depth by blocking malicious destinations prior to a connection being established. The solution must be able to block certain applications from being used within the network. Which product should be used to accomplish this goal?

A. Cisco Firepower

B. Cisco Umbrella

C. Cisco ISE

D. Cisco AMP

Suggested Answer: *A*

Official Answer: A

Community vote distribution



aalnman Highly Voted 5 years, 1 month ago

Answer = B I work with Umbrella and Firepower daily. You can do this with Firepower, Umbrella whole existence is for blocking DNS connections to malicious sites before they are made, and blocking applications from launching on the internal network. For example, our users can't access Pandora, FB, Google Docs while on our internal network based on a policy configured in Umbrella.if you're working with them daily, how does umbrella handle connections to the same resources when using IP instead of FQDN?

upvoted 17 times

aalnman Highly Voted 5 years, 1 month ago

Answer = B I work with Umbrella and Firepower daily. You can do this with Firepower, Umbrella whole existence is for blocking DNS connections to malicious sites before they are made, and blocking applications from launching on the internal network. For example, our users can't access Pandora, FB, Google Docs while on our internal network based on a policy configured in Umbrella.

upvoted 17 times

MerlinTheWizard 1 year ago

if you're working with them daily, how does umbrella handle connections to the same resources when using IP instead of FQDN?

upvoted 1 times

AS04 5 years ago

A is correct, Firepower has AVC feature that can block traffic based on application.B is correct. AVC on Firepower can not block applications from being used within the network. Firepower can only block these applications if they pass through the firewall. Umbrella can block connections to malicious sites before the connection is made based on the DNS lookup. Umbrella also installs an endpoint supplicant or can be used as an Anyconnect module. This way you can push an application policy to the endpoints blocking even applications 'within the network'. Same as aalnman, I have used this at work and at home.

upvoted 7 times

AS04 5 years ago

A is correct, Firepower has AVC feature that can block traffic based on application.

upvoted 7 times

west33637 3 years, 8 months ago

B is correct. AVC on Firepower can not block applications from being used within the network. Firepower can only block these applications if they pass through the firewall. Umbrella can block connections to malicious sites before the connection is made based on the DNS lookup. Umbrella also installs an endpoint supplicant or can be used as an Anyconnect module. This way you can push an application policy to the endpoints blocking even applications 'within the network'. Same as aalnman, I have used this at work and at home.

upvoted 7 times

Silexis Most Recent 7 months ago

For the yr 2026, this is a very complicate question as now Cisco Umbrella is evolving to Cisco Secure Access which has a lot of security features (some as add-ons). Looking at this question in the simpler way, I think that Cisco FPR is the right answer as it can be deployed as well for traffic within the network at Layer 2. Using app control, url filtering/reputation and geoip fencing, FPR can block a connection before that being established either on IP or FQDN as well as control the traffic within the network. I will go with A for the above reasons

upvoted 1 times

Rakinor 11 months, 1 week ago

Blocking the Application. Not the DNS Query, so i would go for AMP

upvoted 1 times

ITPro21 1 year, 4 months ago

Acts as a first line of defense, blocking threats before they reach the network or endpoints.

upvoted 1 times

kloug 1 year, 9 months ago

Answer b

upvoted 1 times

luismg 1 year, 11 months ago

I would say is D Umbrella cannot stop ip connections firepower just traffic that goes through it. amp is host ralated, it can block any connection

upvoted 1 times

Premium_Pils 2 years ago

Block the process right at the beginning, i.e. at the DNS request step, before making a connection to the bad website. - Bhttps://umbrella.cisco.com/products/sig-product The question would fit for umbrella, except that it is about blocking access within the network. (However, they did not specify which network.) Did someone find a relevant documentation about AMP?Block from being used within the network... So, the application could reside on the internet, but being inaccessible in the organisation network. I think, it is what umbrella does.

upvoted 1 times

Premium_Pils 2 years ago

Selected Answer: B

Block the process right at the beginning, i.e. at the DNS request step, before making a connection to the bad website. - B

upvoted 1 times

Premium_Pils 1 year, 10 months ago

https://umbrella.cisco.com/products/sig-product The question would fit for umbrella, except that it is about blocking access within the network. (However, they did not specify which network.) Did someone find a relevant documentation about AMP?

upvoted 1 times

Premium_Pils 1 year, 10 months ago

https://umbrella.cisco.com/products/sig-product The question would fit for umbrella, except that it is about blocking access within the network. (However, they did not specify which network.) Did someone find a relevant documentation about AMP?Block from being used within the network... So, the application could reside on the internet, but being inaccessible in the organisation network. I think, it is what umbrella does.

upvoted 1 times

Premium_Pils 1 year, 10 months ago

Block from being used within the network... So, the application could reside on the internet, but being inaccessible in the organisation network. I think, it is what umbrella does.

upvoted 1 times

4pelos 2 years, 5 months ago

Correct answer B. Checked in securitytut

upvoted 2 times

xziomal9 2 years, 9 months ago

Answer B

upvoted 1 times

jorg32 3 years ago

Umbrella, is trying to block the start of the conversation with bad websites, why block the application when you know you can block way earlier on the traffic flow?

upvoted 1 times

Jessie45785 3 years, 2 months ago

The solution must be able to block certain applications from being used within the network I really think it is D cause: - NGFW cannot stop it in L2 - Umbrella can block only DNS protocol - what about all the other ones - wont be able to detect it - WSA - proxy will definitely will not help here ... but AMP can block application from being able to start hence cutting it from TCP stack and fulfilling a requirement of "blocking malicious destinations prior to a connection being established" but it is Cisco so you never know :/

upvoted 2 times

F0rtyx40 3 years, 2 months ago

It's B, Umbrella can block the connection before firepower L7 application detectors kick in.

upvoted 1 times

gc999 3 years, 3 months ago

I think most of us already get the keywords here "prior to a connection being established" and "within the network". Can I make an example that if there are two internal users, let say User-1 and User-2, within the network, which solution can block the certain application being send from User-1 to User-2?

upvoted 1 times

SegaMasterSystemAdmin 3 years, 3 months ago

This is a tricky one, the question is weird because the keywords are "prior to a connection being established" and "must be able to block certain applications". It is true that Umbrella blocks the DNS traffic so that it does that take care of "prior to a connection being established". However, Umbrella does not block the application itself just the DNS traffic, so if the application does not utilize DNS and is IP based, it will not block anything, Firepower on the other hand can block the applications and with a "Block with Reset" it does not allow any connection to be established. Also, both can block based on malicious destination. I will still go with B though.

upvoted 1 times

KPzee 3 years, 4 months ago

A is correct a firewall will block certain applications that might already be on the network.

upvoted 1 times

Toni_Su91 3 years, 5 months ago

Prior to a connection being established - This is classic Umbrella - DNS security is first line of defence.

upvoted 2 times

Question #107 *Topic 1*

An engineer notices traffic interruptions on the network. Upon further investigation, it is learned that broadcast packets have been flooding the network. What must be configured, based on a predefined threshold, to address this issue?

A. Storm Control

B. embedded event monitoring

C. access control lists

D. Bridge Protocol Data Unit guard

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Marshpillowz Most Recent 1 year, 10 months ago

Selected Answer: A

A - Storm Control

upvoted 1 times

sis_net_sec 3 years, 6 months ago

correct Answer is A Explanation: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr- book/eem-cr-e1.html

upvoted 2 times

Question #108 *Topic 1*

What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

A. Multiple NetFlow collectors are supported.

B. Advanced NetFlow v9 templates and legacy v5 formatting are supported.

C. Secure NetFlow connectors are optimized for Cisco Prime Infrastructure

D. Flow-create events are delayed.

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (66%) D (34%)

Reece_S Highly Voted 5 years, 1 month ago
A is the answer. While events can be delayed they are not delayed by default. The flow-create event is exported as soon as the flow is created if the flow-export delay flow-create command is not configured.
upvoted 14 times

ureis 3 years, 7 months ago
Multiple NetFlow collectors are supported in "Flexible Netflow"
upvoted 1 times

Smileebloke 4 years, 4 months ago
https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.pdf
upvoted 2 times

nep1019 Highly Voted 3 years ago
Selected Answer: A
Whew this is a hard question. Is A because as previously mentioned, delaying the export of flow-create events is NOT a default action. A is the "more correct" answer. Cisco exams are a racket.
upvoted 6 times

NETeng01 Most Recent 11 months ago
Selected Answer: A
To clarify, the flow-create event itself is not delayed—the event (the creation of a new flow) happens in real time on the ASA. What is delayed is the sending (export) of the flow-create event record to the NetFlow collector.

In other words:

The ASA detects and creates the flow immediately. The ASA can be configured to wait a specified amount of time before sending the flow-create event record to the NetFlow collector. This delay helps avoid logging very short-lived flows that might be torn down quickly, reducing unnecessary log entries.

So, A is correct
upvoted 2 times

diverjim64 11 months, 3 weeks ago
Selected Answer: A
D. is incorrect because "export" isn't in the answer.

From the provided link: Filters NSEL events based on the traffic and event type through Modular Policy Framework, then sends records to different collectors. Traffic is matched based on the order in which classes are configured. After a match is found, no other classes are checked. The supported event types are flow-create, flow-denied, flow-teardown, flow-update, and all. Records can be sent to different collectors. For example, with two collectors, you can do the following: – Log all flow-denied events that match ACL 1 to collector 1. – Log all flow-create events to collector 1. – Log all flow-teardown events to collector 2. – Log all flow-update events to collector 1.

• Delays the export of flow-create events.

upvoted 1 times

CyberGhost666 1 year, 1 month ago

Selected Answer: A

I'll go with A since Cisco ASA supports configuring multiple NetFlow collectors, which allows flow data to be sent to more than one monitoring or analytics platform

upvoted 1 times

Diegosuarezb 1 year, 4 months ago

Selected Answer: A

A since NFSEL one of the most distinguished characteristics its to send data to multiple collectors simultaneously

upvoted 1 times

kloug 1 year, 10 months ago

A is correct

upvoted 1 times

Marshpillowz 2 years, 4 months ago

Selected Answer: A

I think A is most accurate

upvoted 1 times

Stevens0103 2 years, 7 months ago

Selected Answer: A

The option D's wording implies that flow-create events are always delayed and this default action is a feature. However, flow-create events are actually optional and it is exactly this optionality makes it a feature.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/monitor_nsel.html

upvoted 4 times

Stevens0103 2 years, 7 months ago

correction: "...delayed flow-create events is actually optional..."

upvoted 1 times

jpapas 3 years ago

Selected Answer: D

Question translates to : "What is a feature [only] of Cisco NSEL ?" > A , its true for all Netflow implementations : IOS/IOS-XR/IOS-XE etc > B,C are wrong

D is true and exists only on ASA's NSEL. So is the correct answer (even if delay is optional).

ref: https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/monitor_nsel.html

upvoted 2 times

jku2cya 3 years, 1 month ago

Selected Answer: D

Multiple references to the correct information "Delays the export of flow-create events"

upvoted 1 times

dabance 3 years, 2 months ago

D. https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.pdf Ref: page 2

upvoted 1 times

gc999 3 years, 2 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.html#:~:text=Delays%20the%20export%20of%20flow%2Dcreate%20events

upvoted 1 times

gc999 3 years, 2 months ago

Selected Answer: D

Some guys already pointed out the main point in the link "https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.pdf"

The ASA and ASASM implementations of NSEL provide the following major functions: - Delays the export of flow-create events

I don't see any related keyword "Multiple" for Netflow in the document.

upvoted 1 times

gc999 3 years, 2 months ago

Besides, "Multiple NetFlow collectors are supported" is not a kind of core feature. From the link "https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nsel.html", it said it can support to send to "different" collectors , but it still cannot send to "multiple" collectors once it matches.

upvoted 1 times

Emlia1 3 years, 8 months ago

D could be

upvoted 2 times

francojaraba 4 years, 1 month ago

Selected Answer: A

Answer is A.

Based on the link -https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.pdf. What is delayed is the export not the flow-create.

upvoted 2 times

Pwned 4 years, 2 months ago

Selected Answer: A

A is the correct answer

upvoted 1 times

Question #109 *Topic 1*

What is a key difference between Cisco Firepower and Cisco ASA?

A. Cisco Firepower provides identity based access control while Cisco ASA does not.

B. Cisco AS provides access control while Cisco Firepower does not.

C. Cisco ASA provides SSL inspection while Cisco Firepower does not.

D. Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

sull3y Highly Voted 3 years ago

Cisco Firepower and Cisco ASA are both network security products offered by Cisco, but they have different capabilities and are typically used for different purposes. Cisco ASA (Adaptive Security Appliance) is a firewall and VPN device that provides perimeter security for networks. It can be used to control access to resources, block unauthorized traffic, and create secure VPN connections. ASA does not provide intrusion prevention capabilities, it is focused on network perimeter security. Cisco Firepower, on the other hand, is a more advanced security product that provides both firewall and intrusion prevention capabilities. It is designed to protect networks from advanced threats, such as malware and zero-day attacks. Firepower uses a combination of technologies, such as threat intelligence and machine learning, to detect and block malicious traffic. Firepower includes features such as advanced malware protection, threat hunting, and incident response capabilities.

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Answer is D.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

D is correct

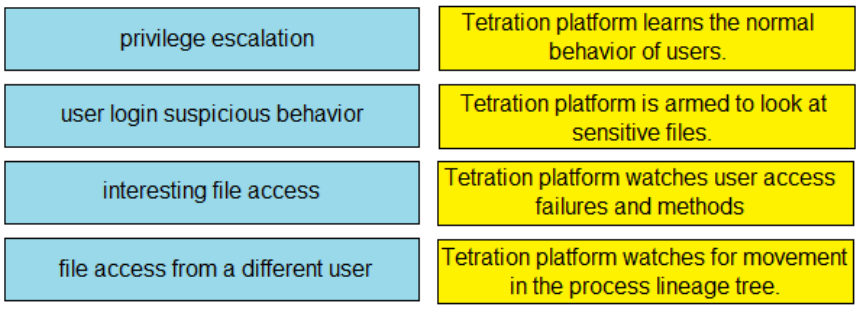
upvoted 2 times

Question #110 *Topic 1*

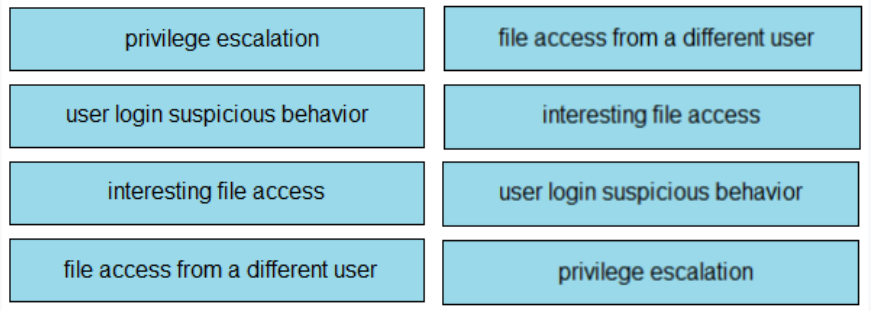
DRAG DROP -

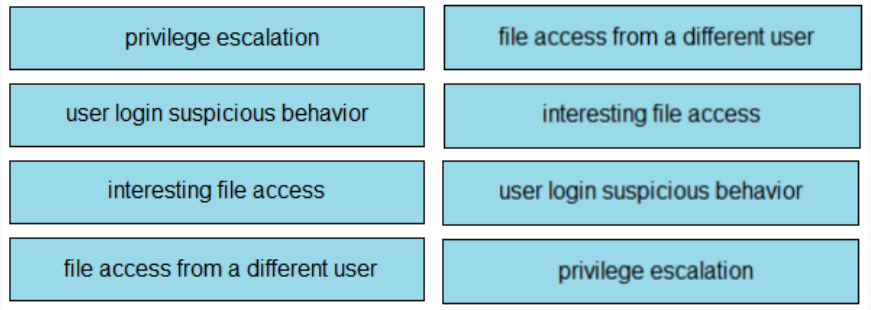
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.

Select and Place:



Suggested Answer:





Kyle1776 Highly Voted 3 years, 11 months ago

Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree. User login suspicious behavior: Cisco Secure Workload platform watches user login failures and user login methods. Interesting file access: Cisco Secure Workload platform can be armed to look at sensitive files. File access from a different user: Cisco Secure Workload platform learns the normal behavior of which file is accessed by which user. https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.htmlhttps://web.archive.org/web/20191129023324/https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html#_Toc509550184

upvoted 11 times

Kyle1776 Highly Voted 3 years, 11 months ago

Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.

User login suspicious behavior: Cisco Secure Workload platform watches user login failures and user login methods.

Interesting file access: Cisco Secure Workload platform can be armed to look at sensitive files.

File access from a different user: Cisco Secure Workload platform learns the normal behavior of which file is accessed by which user.

https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html

upvoted 11 times

MPoels Most Recent 1 year, 11 months ago

https://web.archive.org/web/20191129023324/https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html#_Toc509550184

upvoted 1 times

Question #111 *Topic 1*

What is a benefit of using Cisco FMC over Cisco ASDM?

A. Cisco FMC uses Java while Cisco ASDM uses HTML5.

B. Cisco FMC provides centralized management while Cisco ASDM does not.

C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.

D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices.

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (88%) D (12%)

RemiK 2 years, 2 months ago

Selected Answer: D

Am I the only one who has already managed several ASAs via ASDM? “Managing multiple ASAs” is not another definition of “centralized management”? Although, I agree, the possibility of a new “centralized management” apparatus is a far cry from what ASDM proposes. B says "Cisco ASDM does not" Regarding this, D seems the correct one

upvoted 1 times

RemiK 2 years, 2 months ago

Am I the only one who has already managed several ASAs via ASDM? “Managing multiple ASAs” is not another definition of “centralized management”? Although, I agree, the possibility of a new “centralized management” apparatus is a far cry from what ASDM proposes. B says "Cisco ASDM does not" Regarding this, D seems the correct onea central management is a management of multiple devices simultaneously in a single place. Per your understanding of central management, even superputty could be a central management for asa.

upvoted 1 times

MerlinTheWizard Most Recent 1 year ago

a central management is a management of multiple devices simultaneously in a single place. Per your understanding of central management, even superputty could be a central management for asa.

upvoted 1 times

Marshpillowz 2 years, 4 months ago

B is correct

upvoted 1 times

KPzee 3 years, 4 months ago

B is correct. FMC allows for centralized management of many devices e.g if there is several firepower NGFW devices, they can be managed via a single FMC device whereas ASDM can only manage a single appliance.

upvoted 3 times

sull3y 3 years, 6 months ago

B:Cisco FMC provides centralized management, meaning that it allows administrators to manage multiple firewall devices from a single console. This can improve efficiency and reduce the potential for errors that can occur when managing multiple devices individually. Cisco ASDM, on the other hand, is a device-specific management tool that can only be used to manage a single Cisco ASA device at a time.

upvoted 3 times

MUKD 4 years, 2 months ago

its B.FMC cannot manage ASA

upvoted 3 times

pr0fectus 4 years, 7 months ago

Let's not complicate the question. Main questions is "what is the benefit". FMC does provide centralized management of FTDs/FirePOWER service(note that FMC cannot manage ASA) while ASDM can only manage one ASA w/ FirePOWER service at a time.

upvoted 3 times

zheka 4 years, 8 months ago

But if by centralized management they mean managing IPS, AVC, AMP and all other security components then of course it is B

upvoted 2 times

zheka 4 years, 8 months ago

Disagree about D, FMC doesn't support firewalls running ASA code, it has to be FTD only. The term "centralized management" is vague. What do they mean by it? Managing more than one device ? You can manage more than one ASA from ASDM by the way. But you can't push configuration from ASDM to ASA, it's instantaneous change without going through "Deploy/push" procedure. I'm not sure if it is a benefit or not, to me rather architectural feature. So I'm inclined to think it is C

upvoted 1 times

shaikat 4 years, 8 months ago

I think B is more appropriate. Because ASA is not used for centralized management for all firewalls but only for a ASA management.

upvoted 2 times

Thusi26 4 years, 8 months ago

D should be it. Both ASA and FMC are being used for centralized management.

upvoted 1 times

Thusi26 4 years, 8 months ago

D should be it. Both ASA and FMC are being used for centralized management.Need to be careful in reading the choices. Note that FMC can only manage FirePOWER services of ASA (not the ASA) and Firepower appliance onboarded with FTD.connection manager in ASDM i dont think would be considered CM as you have to relogin to each firewall you want to manageYou need CSM to manage multiple ASA. ASDM cant manage multiple ASA.

upvoted 1 times

pr0fectus 4 years, 7 months ago

Need to be careful in reading the choices. Note that FMC can only manage FirePOWER services of ASA (not the ASA) and Firepower appliance onboarded with FTD.

upvoted 1 times

bob511 4 years, 5 months ago

connection manager in ASDM i dont think would be considered CM as you have to relogin to each firewall you want to manage

upvoted 1 times

1M4hqQ9G 4 years, 3 months ago

You need CSM to manage multiple ASA. ASDM cant manage multiple ASA.

upvoted 1 times

Question #112 *Topic 1*

Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?

A. Threat Intelligence Director

B. Encrypted Traffic Analytics.

C. Cognitive Threat Analytics.

D. Cisco Talos Intelligence

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

sull3y Highly Voted 3 years ago

A. Threat Intelligence Director Cisco FMC's Threat Intelligence Director allows security teams to integrate security intelligence observables from various sources, such as Cisco Talos, into their Cisco FMC environment. This allows the FMC to push updated security intelligence to its sensors, enabling them to better detect and respond to potential threats.

upvoted 5 times

Marshpillowz Most Recent 1 year, 10 months ago

A is correct

upvoted 1 times

Jamesy 3 years, 4 months ago

A is correct. Cheers

upvoted 3 times

freddycisco 4 years, 6 months ago

How does it work? As shown in the image, on the FMC you have to configure sources from where you would like to download threat intelligence information. The FMC then pushes that information (observables) to sensors. When the traffic matches the observables, the incidents appear in the FMC user interface (GUI). https://www.cisco.com/c/en/us/support/docs/storage-networking/security/214859-configure-and-troubleshoot-cisco-threat.html

upvoted 2 times

Question #113 *Topic 1*

A Cisco FirePower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose two.)

A. permit

B. allow

C. reset

D. trust

E. monitor

Suggested Answer: *B, D*

Official Answer: BD

Community vote distribution



rad9899 Highly Voted 5 years, 3 months ago

D. trust E. monitorIn case you are still nervy about the above answers, then this diagram will calm your nerves :) https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/access_control_rules.html#ID-2190-00000005https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/access_control_rules.html?bookSearch=true#ID-2190-0000023b There is an exception, however. If a Monitor rule contains layer 7 conditions—such as an application condition—the system allows early packets to pass and the connection to be established (or the SSL handshake to complete)

upvoted 32 times

rad9899 Highly Voted 5 years, 3 months ago

D. trust E. monitor

upvoted 31 times

loiphin 4 years, 7 months ago

In case you are still nervy about the above answers, then this diagram will calm your nerves :) https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/access_control_rules.html#ID-2190-00000005https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/access_control_rules.html?bookSearch=true#ID-2190-0000023b There is an exception, however. If a Monitor rule contains layer 7 conditions—such as an application condition—the system allows early packets to pass and the connection to be established (or the SSL handshake to complete)

upvoted 12 times

loiphin 4 years, 7 months ago

In case you are still nervy about the above answers, then this diagram will calm your nerves :)

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/access_control_rules.html#ID-2190-00000005

upvoted 12 times

Fugashi 4 years, 2 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/access_control_rules.html?bookSearch=true#ID-2190-0000023b There is an exception, however. If a Monitor rule contains layer 7 conditions—such as an application condition—the system allows early packets to pass and the connection to be established (or the SSL handshake to complete)

upvoted 3 times

west33637 3 years, 7 months ago

create a monitor rule that matches the application. Then create a trust rule right below it.

upvoted 6 times

SomKeat Most Recent 2 months, 2 weeks ago

B & D is correct Trust: This action allows traffic to pass without any further inspection, though it is still subject to identity requirements and rate limiting. Trusted traffic bypasses network discovery, intrusion inspection, and malware inspection. Allow: This action allows traffic to pass but still subjects it to optional deep inspection such as intrusion and file policies. However, if the goal is to allow traffic without inspection, "Trust" is the more direct choice. "Allow" permits traffic but can include inspection if configured.

upvoted 2 times

ezpzls 4 months, 1 week ago

You need to create the rule to allow (Permit) the traffic and also inspect it (Allow) smh..

upvoted 1 times

Ernestokoro 11 months ago

in Cisco Firepower, the "Trust" condition in an Access Control Policy does not inspect traffic for intrusions or files; it allows the traffic to pass to its destination without further deep inspection. However, it is still subject to certain operations like identity requirements, rate limiting, and pre-defined SSL decryption, as these happen before the access control policy evaluation No, a Cisco Firepower "monitor" condition itself does not inspect traffic; its primary purpose is to log and track network traffic for later analysis without taking action to permit or deny it. The actual deep inspection of the traffic, such as for intrusions or malware, happens when traffic matches a separate Intrusion or File policy.

upvoted 1 times

DANT7 1 year, 3 months ago

In Cisco Firepower, "allow" passes traffic but still inspects it. "Trust" passes traffic without inspection. Since the question asks for allowing traffic without inspection, the correct answers are D. trust and E. monitor.

upvoted 1 times

Diegosuarezb 1 year, 4 months ago

B & D makes more sense to me

upvoted 1 times

Basuso 1 year, 9 months ago

It's Trust & Monitor. Trust applies fast-path to traffic, and Monitor only Logs the traffic. Allow will inspect traffic.

upvoted 2 times

mhd96far 2 years, 4 months ago

never seen on the network

upvoted 1 times

Pakawat 2 years, 8 months ago

Trust and Monitor

upvoted 1 times

xziomal9 2 years, 9 months ago

Answer DE

upvoted 1 times

HOUSSE 2 years, 10 months ago

TRUST AND MONITOR ALLOW IS NOT A GOOD ANSWER BECAUSE TRAFFIC WILL PASS UNDER INSPECTION

upvoted 1 times

Pakawat 2 years, 11 months ago

Trust and Monitor as the question mention that "without inspection".

upvoted 1 times

F0rtyx40 3 years, 1 month ago

D and E , allow rules are still subject to L7 processing

upvoted 1 times

bobie 3 years, 3 months ago

The allow action, If it does only file inspection, intrusion inspection, or neither, it signifies that it will not be inspected because the application is unknown. Without a doubt, the trust action is one of the proper answers.

upvoted 2 times

Emlia1 3 years, 8 months ago

D, E

Explanation Each rule also has an action, which determines whether you monitor, trust, block, or allow matching traffic. Note: With action “trust”, Firepower does not do any more inspection on the traffic. There will be no intrusion protection and also no file-policy on this traffic.

upvoted 1 times

YooAndI 3 years, 3 months ago

Step 1: Monitor Step 2: Trust --> No inspection --> Reaches Destination Allow is further down on the process, Step 4, after Step 3: Block.

upvoted 2 times

dique 4 years ago

D and E (Trust and monitor.)

upvoted 1 times

psuoh 3 years, 7 months ago

The system does not perform deep inspection on trusted, blocked, or encrypted traffic. You monitor to log the session to use when "configuring a rule to allow a new application..."

upvoted 2 times

Question #114 *Topic 1*

What is a characteristic of a bridge group in a Cisco ASA Firewall running in transparent mode?

A. It has an IP address on its BVI interface and is used for management traffic.

B. It allows ARP traffic with a single access rule.

C. It includes multiple interfaces and access rules between interfaces are customizable.

D. It is a Layer 3 segment and includes one port and customizable access rules.

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (62%) A (38%)

leptonius Highly Voted 3 years, 11 months ago
It's C https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/general/asa-94-general-config/intro-fw.html
upvoted 12 times

sull3y Highly Voted 2 years, 6 months ago
C. It includes multiple interfaces and access rules between interfaces are customizable.

In transparent mode, a Cisco ASA firewall acts as a bridge instead of a router. A bridge group is a collection of interfaces that are bridged together and forward traffic between them. A bridge group in transparent mode includes multiple interfaces, and the access rules between interfaces are customizable, meaning that the administrator can configure filtering and access control policies to restrict traffic between different interfaces. This allows the firewall to forward traffic between different VLANs or segments while still applying security policies.
upvoted 6 times

Silexis Most Recent 7 months ago
Selected Answer: A
I will go with A here due to Transparent Mode keyword. The management traffic should not be confused with Management Interface, and an IP address is required for traffic to/from the device. This is the link:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa919/configuration/general/asa-919-general-config/interface-routed-tfw.html
upvoted 1 times

ytsionis 1 year, 11 months ago
C is the correct.

++if you configure an access control rule to block Questionable sites (level 5), it also blocks all 4,3,2, through Untrusted (level 1) sites. (Firepower Management Center Configuration Guide, Version 6.5) https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html#id_17110
upvoted 1 times

Jessie45785 2 years, 4 months ago
Selected Answer: A
NOT C - access rules between interfaces are customizable - how they can be since they are bridged ?!?
upvoted 1 times

Jessie45785 2 years, 3 months ago
C - IS CORRECT - I have to correct myself, indeed C is correct:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/firewall/asa-97-firewall-config/access-rules.html

Extended access rules (Layer 3+ traffic) assigned to Bridge Virtual Interfaces (BVI; routed mode)—If you name a BVI, you can apply separate rule sets in the inbound and outbound direction, and you can also apply rule sets to the bridge group member interfaces. When both the BVI and member interface have access rules, the order of processing depends on direction. Inbound, the member access rules are evaluated first, then the BVI access rules. Outbound, the BVI rules are considered first, then the member interface rules.
upvoted 2 times

kjubo 2 years, 9 months ago

Selected Answer: C

BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.

upvoted 3 times

leowulf 2 years, 11 months ago

I believe answer is C

https://integratingit.wordpress.com/2021/05/30/asa-transparent-mode/#:~:text=Bridge%20groups%20are%20used%20to,the%20ASA%20to%20pass%20traffic.

upvoted 2 times

getafix 3 years, 1 month ago

Selected Answer: C

A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place. Each bridge group includes a Bridge Virtual Interface (BVI). The ASA uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.

Only bridge group member interfaces are named and can be used with interface-based features.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/general/asa-94-general-config/intro-fw.html#ID-2106-00000012

While we can use BVIs for Firewall Management purposes, it isn't ONLY used for management. Answer C seems correct

upvoted 2 times

Metgatz 3 years, 3 months ago

Selected Answer: A

A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are supported in both transparent and routed firewall mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place

upvoted 1 times

dr4gn00t 3 years, 6 months ago

Why not A? BVI can be assigned IP and be used for management afaik

upvoted 2 times

Laryoul 3 years, 4 months ago

I think that in case of multiple bridge group, this answer as no sense ... there is only one route table.

upvoted 1 times

beeker98106 3 years, 9 months ago

more specific from below doc:

About Bridge Groups A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place

upvoted 1 times

Question #115 *Topic 1*

While using Cisco Firepower's Security Intelligence policies, which two criteria is blocking based upon? (Choose two.)

A. IP addresses

B. URLs

C. port numbers

D. protocol IDs

E. MAC addresses

Suggested Answer: *A, B*

Official Answer: AB

Community vote distribution

AB (100%)

idto Highly Voted 4 years, 2 months ago

"Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects or groups.)" Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/security_intelligence_blacklisting.html#ID-2192-0000002b

upvoted 6 times

Marshpillowz Most Recent 1 year, 10 months ago

A and B

upvoted 1 times

sull3y 3 years ago

A. IP addresses B. URLs Cisco Firepower's Security Intelligence policies allows to block traffic based on IP addresses and URLs. IP addresses can be used to block traffic from specific IPs or ranges of IPs, or to block traffic that is going to specific IPs or ranges of IPs. URLs can be used to block traffic to specific websites or web pages, or to block traffic that is coming from specific websites or web pages.

upvoted 3 times

Question #116 *Topic 1*

What features does Cisco FTDv provide over Cisco ASAv?

A. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not.

B. Cisco FTDv runs on VMware while Cisco ASAv does not.

C. Cisco FTDv runs on AWS while Cisco ASAv does not.

D. Cisco FTDv supports URL filtering while Cisco ASAv does not.

Suggested Answer: *D*

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2018/pdf/BRKSEC-2064.pdf

Community vote distribution

D (100%)

cisco_guy Most Recent 1 year, 8 months ago

Clearly none of the other commenters have actually tested this out. URL filtering on ASAv 9.4 and newer 100% supports URL filtering. It requires a regex and class map type inspect http to do so, but it will block a URL and also log when the URL is matched on.

upvoted 1 times

Marshpillowz 2 years, 4 months ago

D is correct

upvoted 1 times

sull3y 3 years, 6 months ago

D. Cisco FTDv supports URL filtering while Cisco ASAv does not. Cisco FTDv (Firepower Threat Defense Virtual) is a next-generation firewall (NGFW) solution that provides advanced security features and capabilities beyond what is offered by Cisco ASAv (Adaptive Security Appliance Virtual). One key feature that Cisco FTDv provides over Cisco ASAv is support for URL filtering. This feature allows administrators to block or allow traffic to specific websites or web pages, based on predefined policies. Additionally, FTDv provides a centralized management platform for firewall, VPN, and advanced threat protection services, while ASAv is a traditional firewall with VPN capabilities. Both Cisco FTDv and ASAv run on VMware and AWS, and both support 1GB of firewall throughput.

upvoted 3 times

psuoh 3 years, 7 months ago

https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/adapt-security-virtual-appliance-ds.html

upvoted 1 times

Raajaa 5 years, 1 month ago

D is the answer

upvoted 3 times

Question #117 *Topic 1*

A network engineer is deciding whether to use stateful or stateless failover when configuring two Cisco ASAs for high availability. What is the connection status in both cases?

A. need to be reestablished with stateful failover and preserved with stateless failover

B. preserved with both stateful and stateless failover

C. need to be reestablished with both stateful and stateless failover

D. preserved with stateful failover and need to be reestablished with stateless failover

Suggested Answer: *D*

Official Answer: D

Community vote distribution



sull3y Highly Voted 3 years ago

D. preserved with stateful failover and need to be reestablished with stateless failover In stateful failover, the primary and secondary devices share state information, meaning that they have the same view of the current connections and the connection status is preserved. If the primary device fails, the secondary device takes over and continues to manage the existing connections without interruption. In contrast, In stateless failover, the primary and secondary devices do not share state information, meaning that they have different views of the connections. If the primary device fails, the secondary device takes over but the connection status need to be reestablished.

upvoted 5 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct answer is D.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

D is correct

upvoted 1 times

johnnybgud 2 years, 8 months ago

D. Stateful = Maintain Sessions Stateless = Sessions need to be reestablished

upvoted 3 times

Question #118 *Topic 1*

Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco Talos?

A. authoring

B. consumption

C. sharing

D. analysis

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

dzef13 Highly Voted 4 years, 8 months ago

we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower Management Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector - Answer B Consumption

upvoted 18 times

Marshpillowz Most Recent 1 year, 10 months ago

B is correct

upvoted 1 times

yong08321 2 years, 9 months ago

The correct answer is B. Consumption. Cisco Firepower is a security solution that provides threat detection, prevention, and response capabilities for networks. One of the key features of Firepower is its integration with Cisco Talos, a global threat intelligence organization that provides real-time information on the latest security threats and vulnerabilities. When Firepower downloads threat intelligence updates from Talos, this process is called consumption. Firepower uses this information to update its own threat intelligence database and to identify and block any new threats that may be present on the network. Authoring refers to the process of creating or writing security rules and policies for a network. Sharing refers to the ability to share threat intelligence and other security information with other organizations or security solutions. Analysis refers to the process of examining and interpreting security data to identify potential threats or vulnerabilities.

upvoted 1 times

haiderzaid 2 years, 10 months ago

The process of downloading these updates is commonly referred to as "threat intelligence consumption"

upvoted 1 times

Emlia1 3 years, 2 months ago

It's B

upvoted 2 times

francojaraba 3 years, 7 months ago

The answer is consumption (B) - https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligence-director "TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists""Cisco Talos Intelligence Group (Talos) feeds—Talos provides access to regularly updated security intelligence feeds. Sites representing security threats such as malware, spam, botnets, and phishing appear and disappear faster than you can update and deploy custom configurations. The system downloads feed updates regularly, and thus new threat intelligence is available without requiring you to redeploy the configuration." - https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-sec-intel.html

upvoted 3 times

francojaraba 3 years, 7 months ago

The answer is consumption (B) - https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligence-director "TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists"

upvoted 3 times

francojaraba 3 years, 7 months ago

"Cisco Talos Intelligence Group (Talos) feeds—Talos provides access to regularly updated security intelligence feeds. Sites representing security threats such as malware, spam, botnets, and phishing appear and disappear faster than you can update and deploy custom configurations. The system downloads feed updates regularly, and thus new threat intelligence is available without requiring you to redeploy the configuration." - https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-sec-intel.html

upvoted 2 times

Laryoul 3 years, 10 months ago

like all people say correct answer is B

upvoted 4 times

efongvan 4 years, 1 month ago

B is correct answer.

upvoted 4 times

Sarbi 4 years, 5 months ago

The correct answer is consumption only.

upvoted 3 times

Seawanderer 4 years, 7 months ago

While I can't find any reference at all, "sharing" makes more sense to me. Firepower is not consuming anything (yet), but Talos is sharing the intelligence with other devices.

upvoted 1 times

Raajaa 4 years, 7 months ago

B looks correct

upvoted 4 times

statikd 4 years, 8 months ago

I wonder how Analysis was chosen as the answer. I can not find any good answer online or in the official cert guide. Closest thing is from https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligence-director

upvoted 1 times

entitty 4 years, 8 months ago

I leaning toward consumption - B

upvoted 3 times

Question #119 *Topic 1*

An administrator is configuring a DHCP server to better secure their environment. They need to be able to rate-limit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?

A. Set a trusted interface for the DHCP server.

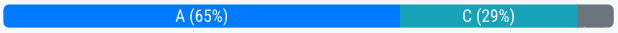
B. Set the DHCP snooping bit to 1.

C. Enable ARP inspection for the required VLAN.

D. Add entries in the DHCP snooping database.

Suggested Answer: *A*
Official Answer: A

Community vote distribution



zheka Highly Voted 4 years, 8 months ago

Folks, we have lots of wrong answers verified and provided by "experts", there's no need to supply wrong answers by ourselves here. You can't add entries to DHCP snooping database. It's wrong answer. The only case when you create mapping of IP to MAC and VLAN and port is configuring "ip source guard" but it is not the same as DHCP snooping.

Unless you explicitly configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/dam/en/us/td/docs/switches/lan/catalyst4500/XE35-0XO/configuration/guide/dhcp.fm/jcr:content/renditions/config_dhcp.html.xml

upvoted 14 times

Random000 Highly Voted 3 years, 10 months ago

So, it's A ?

upvoted 6 times

psuoh 3 years, 7 months ago

Answer is C

upvoted 2 times

BoxX 3 years, 1 month ago

If you won't to configure DAI (Dynamic ARP Inspection) and IP Source Guard (IPSG) you must add statically assigned IP addresses to the DHCP snooping database, as DAI and IPSG are using it.

Depending on platform and version you can add static entries into the DHCP snooping database: - Router# ip dhcp snooping binding binding_id vlan vlan_id interface interface expiry lease_time - Switch# ip dhcp snooping binding mac-addr vlan vlan ipaddr interface ifname expiry lease-in-seconds

Please, do not call someone "expert" just because you are not.

upvoted 2 times

Rododendron2 2 years, 3 months ago

Not valid comment You can add entries manually: Router# ip dhcp snooping binding mac_address vlan vlan_ID ip_address interface ifname expiry lease_in_seconds eg. https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/snoodhcp.pdf command.

upvoted 2 times

diverjim64 Most Recent 11 months, 3 weeks ago

Selected Answer: A

OCG p. 339. "DHCP Snooping...rate-limits DHCP traffic from trusted and untrusted interfaces."

upvoted 1 times

CyberGhost666 1 year, 1 month ago

Selected Answer: A

Answer is A.

upvoted 2 times

Premium_Pils 1 year, 10 months ago

Selected Answer: A

Basically, DHCP snooping drops DHCP offers on untrusted ports. However, Catalyst switches do not forward DHCP discovers on untrusted ports. If do not trust the port of the valid DHCP server, then the legitimate discovers will be dropped. That is why I choose A. See source below:
https://networklessons.com/switching/dhcp-snooping

upvoted 2 times

Demon_Queen_Velverosa 1 year, 11 months ago

This answer is A as shown below from the offical cert guide, don't over think it.

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, the DHCP snooping feature filters messages and rate-limits traffic from untrusted sources. The following steps are required to implement DHCP snooping on your network:

Step 1. Define and configure the DHCP server. Configuration of this step does not take place on the switch or router and is beyond the scope of this book. Step 2. Enable DHCP snooping globally. Step 3. Enable DHCP snooping on at least one VLAN. By default, DHCP snooping is inactive on all VLANs. Step 4. Ensure that the DHCP server is connected through a trusted interface. By default, the trust state of all interfaces is untrusted. Step 5. Configure the DHCP snooping database agent. This step ensures that database entries are restored after a restart or switchover.

upvoted 2 times

Rododendron2 2 years, 3 months ago

Selected Answer: D

It's possible to do this with D , eg. downloading the snooping database from tftp server (taken from DHCP server)... but cumbersome ... I am not sure if enough answer shall be A or D .... source - any IOS , IIS-XE, NX-OS ... DHCP snoopoing config guide ...
https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus3548/103x/configuration/security/cisco-nexus-3548-nx-os-security-configuration-guide-103x/m-configuring-dhcp-snooping.pdf

upvoted 1 times

4pelos 2 years, 5 months ago

Correct answer A Checked with securitytut

upvoted 1 times

xziomal9 2 years, 9 months ago

Selected Answer: C

Answer C

upvoted 1 times

kvothe86 2 years, 12 months ago

Answer is not A, I know because this is one of my few mistakes a couple of days ago. Admin, if you are reading this please provide the correct answer and I ask you not to post this comment

upvoted 1 times

Cokamaniako 3 years, 1 month ago

Aswer A

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, the DHCP snooping feature filters messages and rate-limits traffic from untrusted sources.

upvoted 1 times

BoxX 3 years, 1 month ago

Vote for A

Ensure that legitimate requests are not dropped (without trusted interface the traffic is dropped). This will also satisfy the request "able to rate-limit the traffic". "Able to", meaning it can be configured.

upvoted 2 times

Bandito 3 years, 2 months ago

ARP inspection rate-limits ARP packets, not DHCP requests. I vote for A

upvoted 1 times

gc999 3 years, 2 months ago

Selected Answer: A

I choose "A". The question said "An administrator is configuring a DHCP server", the DHCP server is a new setup, so it should not have trust interface before, we need to setup it once the DHCP server is newly installed.

upvoted 2 times

gc999 3 years, 2 months ago

Finally, I choose "C". The rate limiting would not be enabled by default when ip dhcp snooping is configured. However, it will be enabled on untrust interface once the arp inspection is enabled.

upvoted 2 times

gc999 3 years, 2 months ago

Please refer to this video at 13:22 https://www.youtube.com/watch?v=HwbTKaIvL6s&ab_channel=Jeremy%27sITLab

upvoted 1 times

Jessie45785 3 years, 2 months ago

Selected Answer: C

DHCP snooping has no default rate limit

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf

hence only C make sense

upvoted 1 times

Dorr20 3 years, 3 months ago

Selected Answer: C

As zheka said, answer is C

upvoted 1 times

angry 3 years, 5 months ago

D is the correct answer! A enable trust on the interface connected to the DHCP server. the trust statement has nothng to do with rate limit! C is also not correct! you can't set rate limit on ARP inpection. But with D, Switch(config-if)#ip dhcp snooping limit rate ? DHCP snooping rate limit Switch(config-if)#ip dhcp snooping limit rate

upvoted 1 times

Totosos1 3 years, 5 months ago

D is saying to add entries in the DHCP Snooping DB, you're statement is for setting the rate limit? It's still not clear what the answer is here!

upvoted 1 times

Question #120 *Topic 1*

What is a prerequisite when integrating a Cisco ISE server and an AD domain?

A. Configure a common administrator account.

B. Place the Cisco ISE server and the AD server in the same subnet.

C. Synchronize the clocks of the Cisco ISE server and the AD server.

D. Configure a common DNS server.

Suggested Answer: *C*

Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215233-identity-service-engine-ise-and-active.html#anc1

Community vote distribution

C (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

C) When integrating Cisco Identity Services Engine (ISE) with Microsoft Active Directory (AD), time synchronization is a critical requirement.

upvoted 1 times

Marshpillowz 1 year, 10 months ago

C is correct

upvoted 1 times

F0rtyx40 2 years, 9 months ago

This is a tricky one because DNS records are also crcucial, A will break more functionality for sure.I mean C *

upvoted 1 times

F0rtyx40 2 years, 9 months ago

This is a tricky one because DNS records are also crcucial, A will break more functionality for sure.

upvoted 1 times

F0rtyx40 2 years, 9 months ago

I mean C *

upvoted 1 times

sis_net_sec 3 years, 4 months ago

C is correct answer The following are the prerequisites to integrate Active Directory with Cisco ISE. + Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI. + If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that Get Latest & Actual 350-701 Exam's Question and Answers from Passleader. http://www.passleader.com 99 trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation. + You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE. Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5 C9CF5D582B77BB24F

upvoted 2 times

harvey227 3 years, 6 months ago

Answer is C. Otherwise you may get Kerberos Auth errors due to clock skew

upvoted 3 times

Question #121 *Topic 1*

When configuring ISAKMP for IKEv1 Phase 1 on a Cisco IOS router, an administrator needs to input the command crypto isakmp key cisco address 0.0.0.0.
The administrator is not sure what the IP address in this command is used for. What would be the effect of changing the IP address from 0.0.0.0 to 1.2.3.4?

A. The key server that is managing the keys for the connection will be at 1.2.3.4.

B. The address that will be used as the crypto validation authority.

C. All IP addresses other than 1.2.3.4 will be allowed.

D. The remote connection will only be allowed from 1.2.3.4.

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

CyberGhost666 Most Recent 1 year, 1 month ago
D is the correct option.
upvoted 1 times

illwill 1 year, 8 months ago
"D" is the correct answer because mask is optional and only needed if the peer device is using the mask command. (Optional) Specify the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)
https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfike.html#wp1017897
upvoted 1 times

gondohwe 2 years, 2 months ago
the command "crypto isakamp key xxxx address x.x.x.x " is used to specify the shared secret and the peer is expected at the other end of the connecton.....so D is the right choice
upvoted 2 times

Anonymous983475 2 years, 6 months ago
I think none of the answers are correct or the question itself is wrong. If you do not add a subnet mask at the end of the command the default class is assumed. The default class for 1.2.3.4 is class A, which has mask 255.0.0.0 or 8 bits. This means that all addresses from the 1.0.0.0/8 network will be accepted for authentication with that key.
upvoted 4 times

Question #122 *Topic 1*

A network administrator is configuring SNMPv3 on a new router. The users have already been created, however an additional configuration is needed to facilitate access to the SNMP views. What must the administrator do to accomplish this?

A. define the encryption algorithm to be used by SNMPv3

B. set the password to be used for SNMPv3 authentication

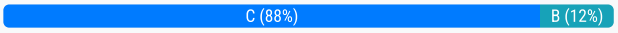
C. map SNMPv3 users to SNMP views

D. specify the UDP port used by SNMP

Suggested Answer: *C*

Official Answer: C

Community vote distribution



kornman Highly Voted 5 years, 1 month ago

I think the correct answer is C - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3e/snmp-xe-3e-book/nm-snmp-snmpv3-comm-supp.htmlhttps://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-e/snmp-15-e-book.pdf C is true

upvoted 14 times

kornman Highly Voted 5 years, 1 month ago

I think the correct answer is C - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3e/snmp-xe-3e-book/nm-snmp-snmpv3-comm-supp.html

upvoted 14 times

jaciro11 4 years, 9 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-e/snmp-15-e-book.pdf C is true

upvoted 2 times

thetaken 5 years, 1 month ago

It looks like none of the options given make sense: A and B are part of the user creation command, C does not make any sense since views can be assigned to groups, not users and D is wrong because it only makes sense if a SNMP host is being configured.

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct Option is C.

upvoted 1 times

Demon_Queen_Velverosa 1 year, 11 months ago

Don't Overthink the question A network administrator is configuring SNMPv3 on a new router. The users have already been created, however an additional configuration is needed to facilitate access to the SNMP views. What must the administrator do to accomplish this? The question is stating the users have been created, but never said any other commands had been used. Thus they ask "an additional config is needed to access SNMP views". At the moment we only have Users, but no views. Thus only logical answer would be map SNMPv3 users to SNMPv3 views. As that had not been done yet as we only had users.Answer is C

upvoted 2 times

Demon_Queen_Velverosa 1 year, 11 months ago

Don't Overthink the question

A network administrator is configuring SNMPv3 on a new router. The users have already been created, however an additional configuration is needed to facilitate access to the SNMP views. What must the administrator do to accomplish this?

The question is stating the users have been created, but never said any other commands had been used. Thus they ask "an additional config is needed to access SNMP views". At the moment we only have Users, but no views.

Thus only logical answer would be map SNMPv3 users to SNMPv3 views. As that had not been done yet as we only had users.

upvoted 2 times

Demon_Queen_Velverosa 1 year, 11 months ago

Answer is C

upvoted 1 times

bobie 3 years, 3 months ago

I'll go with B because I believe the user is using the noAuth command. The following example shows how to configure a remote user to receive traps at the “noAuthNoPriv” security level when the SNMPv3 security model is enabled: Device(config)# snmp-server group group1 v3 noauth Device(config)# snmp-server user remoteuser1 group1 remote 10.12.8.4 Device(config)# snmp-server host 10.12.8.4 informs version 3 noauth remoteuser config

upvoted 1 times

psuoh 3 years, 7 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3e/snmp-xe-3e-book/nm-snmp-snmpv3-comm-supp.html

upvoted 1 times

sis_net_sec 3 years, 10 months ago

Yes Tjhe correct Answer is C https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-e/snmp-15-e-book.pdf

upvoted 1 times

nomanlands 4 years, 1 month ago

"however an additional configuration is needed to facilitate access to the SNMP views" Need to give the user or groups access to the view

upvoted 2 times

surforlife 4 years, 1 month ago

"B" For requests to be authenticated, the manager and the agent must share knowledge of the authentication password associated with the username. For requests to be encrypted, the manager and the agent must additionally share knowledge of the privacy password associated with the username.

upvoted 1 times

surforlife 4 years, 1 month ago

"B" For requests to be authenticated, the manager and the agent must share knowledge of the authentication password associated with the username. For requests to be encrypted, the manager and the agent must additionally share knowledge of the privacy password associated with the username.setting the password for SNMPv3 authentication is also a required step in configuring SNMPv3, but it is not directly related to facilitating access to SNMP views,

upvoted 1 times

haiderzaid 3 years, 4 months ago

setting the password for SNMPv3 authentication is also a required step in configuring SNMPv3, but it is not directly related to facilitating access to SNMP views,

upvoted 2 times

surforlife 4 years, 1 month ago

"B" The secure management of SNMPv3 is an important enabling technology for safe configuration and control operations. SNMPv3 provides security with authentication and privacy, and its administration offers logical contexts, view-based access control, and remote configuration.

upvoted 1 times

killbots 4 years, 4 months ago

I agree with C. You can assign users or groups to views

upvoted 3 times

denverfly 4 years, 6 months ago

It is A • 2.8 Configure secure network management of perimeter security and infrastructure devices (secure device management, SNMPv3, views, groups, users, authentication, and encryption, secure logging, and NTP with authentication)

upvoted 2 times

zheka 4 years, 8 months ago

Agree with C, here's what Cisco document says about it: To configure a Simple Network Management Protocol Version 3 (SNMPv3) server user, specify an SNMP group or a table that maps SNMPv3 users to SNMP views.

upvoted 1 times

coentror 4 years, 8 months ago

It is C, on Cisco site: "To configure a Simple Network Management Protocol Version 3 (SNMPv3) server user, specify an SNMP group or a table that maps SNMPv3 users to SNMP views."

upvoted 1 times

u777 4 years, 11 months ago

The question is what is SNMP v3 according to Cisco (table 3): The SNMP Version 3 feature is used to provide secure access to devices by authenticating and encrypting data packets over the network. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-

3se/5700/snmp-xe-3se-5700-book/nm-snmp-snmpv3.pdf Then we need to provide SNMP Priv mode with both authentication and encryption, that is answer A+B. or only A if we consider the authentication is already provided.

upvoted 1 times

kerniger 4 years, 11 months ago

I think you have to configure a view to be able to configure a group. You need a group to be able to configure a user. The PW and encryption is set while creating the user. So if the user is already created, a group and a view is also created. This leaves me with D which makes me not happy.

upvoted 1 times

Reece_S 5 years, 1 month ago

This question is too vague to properly answer. When you create the user, you assign them to the group and this provides access to the view. C would be plausible if you mapped users to views but you don' t map users to views, you assign users to groups which provides access to views. The group and user option would enough in a NoAuth model. the answer wording is questionable C but it could be the answer based on NoAuth.

Since we don't know the model that is being used. It's hard to say. With AuthNoPriv you would need the auth password. With AuthPriv you would need both the auth password and encryption. However in no case would just the encryption be enough by itself to allow access. For A to be correct, we'd have to assume that the user has been assigned to the group and that the auth password is correct.

upvoted 1 times

Reece_S 5 years, 1 month ago

This question is too vague to properly answer. When you create the user, you assign them to the group and this provides access to the view. C would be plausible if you mapped users to views but you don' t map users to views, you assign users to groups which provides access to views. The group and user option would enough in a NoAuth model. the answer wording is questionable C but it could be the answer based on NoAuth. Since we don't know the model that is being used. It's hard to say. With AuthNoPriv you would need the auth password. With AuthPriv you would need both the auth password and encryption. However in no case would just the encryption be enough by itself to allow access. For A to be correct, we'd have to assume that the user has been assigned to the group and that the auth password is correct.Correction. C Could not be the answer at all. The question clearly states that the user has been created. The user is assigned to a group when the command is entered to create the user. Views are provided based on the group.Yeah, vague... But I would go with option B here.Agree with B Configuring SNMP Version 3 When you configure SNMPv3 and you want to use the SNMPv3 security mechanism for handling SNMP packets, you must establish SNMP groups and users with passwords. SNMPv3 is a security model. A security model is an authentication strategy that is set up for a user and the group in which the user resides. No default values exist for authentication or privacy algorithms when you configure the snmp-server group command. Also, no default passwords exist. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/12-4t/snmp-12-4t-book/nm-snmp-cfg-snmp-support.html

upvoted 1 times

Reece_S 5 years, 1 month ago

Correction. C Could not be the answer at all. The question clearly states that the user has been created. The user is assigned to a group when the command is entered to create the user. Views are provided based on the group.

upvoted 1 times

Reece_S 5 years, 1 month ago

Correction. C Could not be the answer at all. The question clearly states that the user has been created. The user is assigned to a group when the command is entered to create the user. Views are provided based on the group.Yeah, vague... But I would go with option B here.Agree with B Configuring SNMP Version 3 When you configure SNMPv3 and you want to use the SNMPv3 security mechanism for handling SNMP packets, you must establish SNMP groups and users with passwords. SNMPv3 is a security model. A security model is an authentication strategy that is set up for a user and the group in which the user resides. No default values exist for authentication or privacy algorithms when you configure the snmp-server group command. Also, no default passwords exist. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/12-4t/snmp-12-4t-book/nm-snmp-cfg-snmp-support.html

upvoted 1 times

klu16 5 years ago

Yeah, vague... But I would go with option B here.

upvoted 2 times

klu16 5 years ago

Yeah, vague... But I would go with option B here.Agree with B Configuring SNMP Version 3 When you configure SNMPv3 and you want to use the SNMPv3 security mechanism for handling SNMP packets, you must establish SNMP groups and users with passwords. SNMPv3 is a security model. A security model is an authentication strategy that is set up for a user and the group in which the user resides. No default values exist for authentication or privacy algorithms when you configure the snmp-server group command. Also, no default passwords exist. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/12-4t/snmp-12-4t-book/nm-snmp-cfg-snmp-support.html

upvoted 2 times

MoII 4 years, 9 months ago

Agree with B Configuring SNMP Version 3 When you configure SNMPv3 and you want to use the SNMPv3 security mechanism for handling SNMP packets, you must establish SNMP groups and users with passwords. SNMPv3 is a security model. A security model is an authentication strategy that is set up for a user and the group in which the user resides. No default values exist for authentication or privacy algorithms when you configure the snmp-server group command. Also, no default passwords exist. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/12-4t/snmp-12-4t-book/nm-snmp-cfg-snmp-support.html

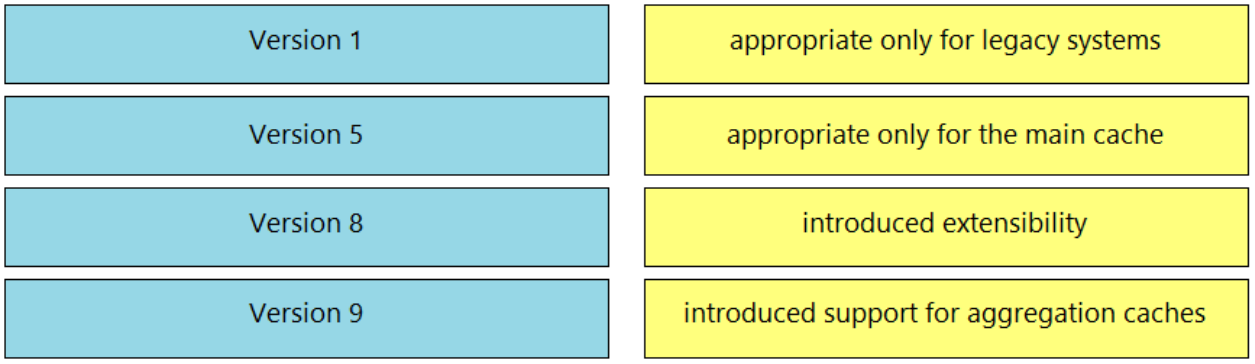
upvoted 2 times

Question #123 *Topic 1*

DRAG DROP -

Drag and drop the NetFlow export formats from the left onto the descriptions on the right.

Select and Place:



Suggested Answer:



Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2015/pdf/BRKNMS-3132.pdf

Laryoul Highly Voted 3 years, 1 month ago

Version 1 is for legacy systems Version 5 export format is suitable only for the main cache Version 8 export format is available only for aggregation caches Version 9 the format is extensible https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfg-nflow-data-expt.html

upvoted 11 times

A_Wolf Most Recent 11 months, 3 weeks ago

The URL referenced in the answer does not exist

upvoted 1 times

ddev3737_111 2 years ago

so version 9 introduced extensibility indeed

upvoted 1 times

ddev3737 2 years ago

so version 9 introduced extensibility indeed

upvoted 1 times

ddev3737_111 2 years ago

Version 9 You need to export data from various technologies, such as Multicast, DoS, IPv6, and BGP next hop. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, and BGP next hop. The Version 9 export format supports export from the main cache and from aggregation caches. Version 8 You need to export data from aggregation caches. The Version 8 export format is available only for export from aggregation caches. Version 5 You need to export data from the NetFlow main cache, and you are not planning to support new features. Version 5 export format does not support export from aggregation caches. Version 1 You need to export data to a legacy collection system that requires Version 1 export format. Otherwise, do not use Version 1 export format. Use Version 9 or Version 5 export format.

upvoted 2 times

ddev3737 2 years ago

Version 9

You need to export data from various technologies, such as Multicast, DoS, IPv6, and BGP next hop. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, and BGP next hop.

The Version 9 export format supports export from the main cache and from aggregation caches.

Version 8

You need to export data from aggregation caches. The Version 8 export format is available only for export from aggregation caches.

Version 5

You need to export data from the NetFlow main cache, and you are not planning to support new features.

Version 5 export format does not support export from aggregation caches.

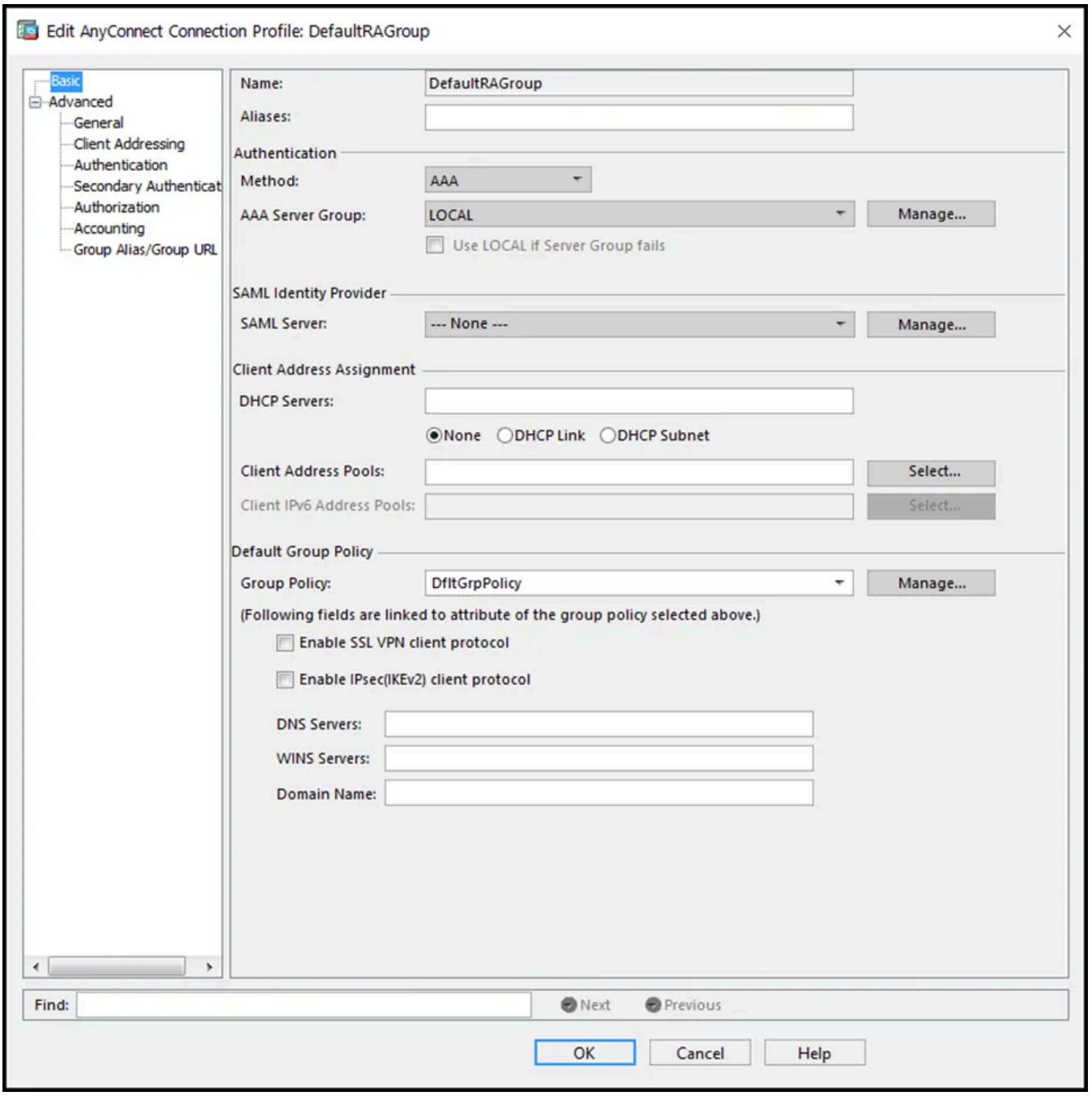
Version 1

You need to export data to a legacy collection system that requires Version 1 export format. Otherwise, do not use Version 1 export format. Use Version 9 or Version 5 export format.

upvoted 2 times

Question #124 *Topic 1*

Refer to the exhibit. When configuring a remote access VPN solution terminating on the Cisco ASA, an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication using machine certificates. Which configuration item must be modified to allow this?



A. Method

B. SAML Server

C. AAA Server Group

D. Group Policy

Suggested Answer: *C*

Official Answer: C

Community vote distribution

A (82%) C (18%)

aalnman Highly Voted 5 years, 1 month ago

C - is correct. Method (A) is already specified in the question if you read it closely. It wants external tokens when the configuration is set to local. C is what needs to be changed.

upvoted 9 times

Reece_S Highly Voted 5 years ago

AAA server group is correct. It's looking for what to use in conjunction with AAA. The method is already selected. Most likely you will change the "local" under server group to "ldap" to use AD for authentication rather than local creds defined on the ASA.Yea its method. I re-read the question. It a wants to use local & another method. So you'll need to select Both in the drop-down.

upvoted 9 times

Reece_S 5 years ago

AAA server group is correct. It's looking for what to use in conjunction with AAA. The method is already selected. Most likely you will change the "local" under server group to "ldap" to use AD for authentication rather than local creds defined on the ASA.

upvoted 9 times

Reece_S 5 years ago

Yea its method. I re-read the question. It a wants to use local & another method. So you'll need to select Both in the drop-down.

upvoted 7 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct answer is C.

upvoted 1 times

ITPro21 1 year, 4 months ago

https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client-v4x/212483-configure-asa-as-the-ssl-gateway-for-any.html

upvoted 1 times

Premium_Pils 2 years ago

C - AAA method is already set, but "local" needs to be changed - as mentioned below

upvoted 1 times

xziomal9 2 years, 9 months ago

Answer A

upvoted 1 times

[Removed] 2 years, 9 months ago

Method offers following options to select: - AAA - AAA and certificate - Certificate only - SAML - Multiple certificates and AAA - Multiple certificates In order to utilize an external token authentication mechanism in conjunction with AAA authentication using maching certificates you must change the method to "AAA and certificate". Answer is A = Method.Correct, a lot of people are overlooking the fact that it states "utilize an external token authentication mechanism in conjunction with AAA authentication USING MACHINE CERTIFICATES"

upvoted 5 times

[Removed] 2 years, 9 months ago

Selected Answer: A

Method offers following options to select: - AAA - AAA and certificate - Certificate only - SAML - Multiple certificates and AAA - Multiple certificates

In order to utilize an external token authentication mechanism in conjunction with AAA authentication using maching certificates you must change the method to "AAA and certificate". Answer is A = Method.

upvoted 5 times

Rockbo47 1 year, 11 months ago

Correct, a lot of people are overlooking the fact that it states "utilize an external token authentication mechanism in conjunction with AAA authentication USING MACHINE CERTIFICATES"

upvoted 1 times

rishard 3 years, 1 month ago

Thx @psuoh for the YT link. Answer A it is - Method.

upvoted 1 times

Jessie45785 3 years, 2 months ago

C - to my understanding secondary authentication tokens are configured ander sever groups:
https://kb.swivelsecure.com/w/index.php/Cisco_AnyConnect

upvoted 2 times

majster88 3 years, 2 months ago

The key here is "conjunction with AAA authentication using machine certificates". To use machine certificate as authentication method we need to change Method from AAA to AAA + certificate as a first step. Then we need to create AAA group of type RADIUS/SDI (depends of integration type

with Token solution) and change the AAA server group from LOCAL to group we created as the second step. Actually both A and C are correct, but A needs to be first.

upvoted 2 times

webwalker00 3 years, 3 months ago

It is A, the Method dictates what security mechanism to use, aaa server group defines those mechanisms.

upvoted 1 times

YooAndI 3 years, 3 months ago

A. Method - In order to use AAA along with an external token authentication mechanism, set the Method as “Both” in the Authentication. We don't just use AAA in this case.

upvoted 1 times

bmayer 3 years, 6 months ago

The correct answer is A- Method. Select method then from the drop down then select AAA and Certificates option.

upvoted 4 times

Jamesy 3 years, 6 months ago

Hi Guys, appreciate all your answers. Question says "an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication" which is the Method we all know! I think they are asking next in the configuration -> AAA Server Group options. Hope this helps. Thanks

upvoted 1 times

psuoh 3 years, 7 months ago

https://i.imgur.com/sdfzVeC.png https://www.youtube.com/watch?v=Er5toSsbM8I

upvoted 5 times

Emlia1 3 years, 8 months ago

It should be A

upvoted 2 times

sis_net_sec 3 years, 10 months ago

https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client-v4x/212483-configure-asa-as-the-ssl-gateway-for-any.html

upvoted 2 times

Question #125 *Topic 1*

An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco
Firepower. Which feature should be used to accomplish this?

A. Network Discovery

B. Access Control

C. Packet Tracer

D. NetFlow

Suggested Answer: *D*
Official Answer: D

Community vote distribution
A (100%)

Raajaa Highly Voted 5 years, 1 month ago
A is the answer as the Q specifies without using metadata
upvoted 8 times

Demon_Queen_Velverosa 1 year, 11 months ago
The Demon Queen sees you all are overthinking this XD. This question is to throw you off and took me time to get why its netflow and checked multiple sources.

An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

As in the question says we want to know what apps are being used on the network. However they throw you off by saying "but does not want the network devices to send metadata to Cisco Firepower.". Ask your self, Why do we care about Cisco FirePower in this question? We don't as we want to know what apps are on the network. By using netflow you have the network devices including firepower sending flow data out to be analyzed to other devices to analyze, but not sending data to the firepower device. They never said firepower could not be used as a sensor. The key word here is not "send" to firepower, but nothing about sending from firepower
upvoted 1 times

xziomal9 2 years, 9 months ago
Answer A
upvoted 1 times

KPzee 3 years, 4 months ago
It cannot be D as Netflow is concerned with metadata.
upvoted 2 times

Emlia1 3 years, 8 months ago
I prefer A
upvoted 1 times

sis_net_sec 3 years, 10 months ago
Selected Answer: A
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Network_Discovery_Policies.html The network discovery policy has a single default rule in place, configured to discover applications from all observed traffic. The rule does not exclude any networks, zones, or ports, host and user discovery is not configured, and the rule is not configured to monitor a NetFlow exporter. This policy is deployed by default to any managed devices when they are registered to the Firepower Management Center. To begin collecting host or user data, you must add or modify discovery rules and re-deploy the policy to a device.
upvoted 2 times

francojaraba 4 years, 1 month ago
Selected Answer: A

As long the questions indicates that no metada is required the answer is A - https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-c11-736595.html

Netflow are based on metadata - https://learning.oreilly.com/library/view/ccna-cyber-ops/9780134608938/ch04.html#ch04lev1sec1

upvoted 4 times

networkexpert 4 years, 3 months ago

Selected Answer: A

I am eliminating D

upvoted 1 times

semi1750 4 years, 4 months ago

Selected Answer: A

Opt for A. Cisco doc says Applications can be discovered by "non-NetFlow discovery rules" without Option D

You can disable detection of application protocols in discovery rules configured to monitor NetFlow exporters, but not in discovery rules configured to monitor Firepower System managed devices. If you enable host or user discovery in non-NetFlow discovery rules, applications are automatically discovered.

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/working_with_discovery_events.html

upvoted 3 times

pohqinan 4 years, 5 months ago

keyword network devices = switch / router therefore netflow. Network Discover usually is PC client send out

upvoted 2 times

NikoNiko 4 years, 1 month ago

"determine which applications" are running... and "does NOT want the network devices to send metadata to Cisco Firepower"

Correct answer is Network Discovery - a Firepower feature, which fingerprints devices and applications in LAN by their communication parameters.

upvoted 2 times

Floki_viking7 4 years, 5 months ago

An Overview of the NetFlow Protocol: NetFlow is a protocol used to collect metadata on IP traffic flows traversing a network device. Developed by Cisco Systems, NetFlow is used to record metadata about IP traffic flows traversing a network device such as a router, switch, or host

upvoted 1 times

zheka 4 years, 8 months ago

Someone below gave an example that Netflow operates with metadata and if we don't want to send them to Cisco FMC then we need to select Netflow as the answer, simple as 123. And yes, you can discover applications by network discoveries by Firepower. Just checked in real production environment

upvoted 1 times

zeroC00L 4 years, 10 months ago

i would go with A here. Because the Network Discovery feature on the FMC/FTD/Firepower stuff works like a passive monitor. The Firewalls are looking into the traffic which is passing through them and use the information they get from there to build up host information you can view from within FMC. So there is no need to send (active do something) metadata the firewalls can get this passively by using network discovery policy.

upvoted 1 times

kapplejacks 4 years, 11 months ago

Correct answer is A:

Question asks for "Firepower", I wish they would specify but I believe they are refering to ASA with firePOWER not FTD. If they say Firepower, cisco usually also includes Threat Defense so its for the ASA.

The ASA does know about are on the network using network discovery and can be view in ASDM without (also a key, the question asks "but does not want to send metadata") so it has to be network discovery

upvoted 2 times

kapplejacks 4 years, 11 months ago

Also its called FireSight, it enables you to see HTTP related info or basically application traffic in a GUI connected to your ASA.

FireSight.

upvoted 1 times

Sarbi 4 years, 11 months ago

I think the answer is A. As Netflow used metedata to analysise the flow. Rather than always relying on full packet capture, protocols like NetFlow and IPFIX can generate valuable metadata for less-intensive network monitoring. This metadata is similar to how your phone bill shows your calls, displaying the source, destination and volume rather than showing the actual content of the conversations. With this information, you can gain useful insights at a lower impact on your network management strategy. But which approach or metadata protocol is right for your network monitoring needs?

upvoted 1 times

kerniger 4 years, 12 months ago

I think A is not true because its based on metadata from firepower by default With NetFlow you can detect applications without metadata at firepower.

upvoted 1 times

zap_pap 5 years ago

- A "The network discovery policy has a single default rule in place, configured to discover applications from all observed traffic."

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Network_Discovery_Policies.html

upvoted 3 times

Pwned 4 years, 2 months ago

This is correct!!

upvoted 1 times

Nian Most Recent 1 year, 5 months ago

Yep.. "Discovery rules within the policy specify which networks and ports the Firepower System monitors to generate discovery data based on network data in traffic, and the zones to which the policy is deployed. Within a rule, you can configure whether hosts, applications, and non-authoritative users are discovered" https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Network_Discovery_Policies.html

upvoted 1 times

Question #126 *Topic 1*

An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command ntp authentication-key 1 md5 Cisc392481137. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however is unable to do so. Which command is required to enable the client to accept the server's authentication key?

A. ntp server 1.1.1.2 key 1

B. ntp peer 1.1.1.2 key 1

C. ntp server 1.1.1.1 key 1

D. ntp peer 1.1.1.1 key 1

Suggested Answer: *C*

Reference: https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch14s13.html

Community vote distribution

C (73%) A (27%)

SulSulEi Highly Voted 1 year, 11 months ago

Answer is C according to the below link, https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch14s13.html

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct Answer is C.

upvoted 1 times

killbots 2 years, 4 months ago

server is at 1.1.1.1 so on the client you need to specify the Server IP.

upvoted 4 times

Kyle1776 2 years, 5 months ago

For the client to be enabled it needs the server and the key. Answer C would be the command configured on the client to enable NTP to the server.

upvoted 3 times

u0815 2 years, 6 months ago

"to enable the client"

upvoted 3 times

Jetnor 2 years, 7 months ago

Selected Answer: A

Actually the question says 1.1.1.1 wants to authenticate ti 1.1.1.2:

the server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however is unable to do so. Which command is required to enable the client to accept the server's authentication key?

so config should be done on server side. Answer is A

upvoted 4 times

Jetnor 2 years, 7 months ago

Actually the question says 1.1.1.1 wants to authenticate ti 1.1.1.2: the server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however is unable to do so. Which command is required to enable the client to accept the server's authentication key? so config should be done on server side. Answer is AMy Bad: Which command is required to enable the client to accept the server's authentication key? it says which command on the Client so its C.it actually says "Which command is required to enable the client to accept the server's authentication key?" the important part is "to enable the (client to accept) the (server's authentication)" which indicates the command is coming from the server to the client the answer is A

upvoted 4 times

Jetnor 2 years, 7 months ago

My Bad: Which command is required to enable the client to accept the server's authentication key? it says which command on the Client so its C.it actually says "Which command is required to enable the client to accept the server's authentication key?" the important part is "to enable the (client to accept) the (server's authentication)" which indicates the command is coming from the server to the client the answer is A

upvoted 4 times

Jetnor 2 years, 7 months ago

My Bad: Which command is required to enable the client to accept the server's authentication key? it says which command on the Client so its C.

upvoted 4 times

bob511 2 years, 5 months ago

it actually says "Which command is required to enable the client to accept the server's authentication key?" the important part is "to enable the (client to accept) the (server's authentication)" which indicates the command is coming from the server to the client the answer is A

upvoted 1 times

MoII 2 years, 9 months ago

Agree, correct answer is C

upvoted 4 times

Question #127 *Topic 1*

Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps. Which two actions must be taken to ensure that interfaces are put back into service? (Choose two.)

A. Enable the snmp-server enable traps command and wait 300 seconds.

B. Use EEM to have the ports return to service automatically in less than 300 seconds

C. Ensure that interfaces are configured with the error-disable detection and recovery feature.

D. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the preconfigured interval.

E. Enter the shutdown and no shutdown commands on the interfaces.

Suggested Answer: *C, E*

Official Answer: CE

Community vote distribution

CE (100%)

LTLnetworker 2 years, 7 months ago

EEM is a possible method tooYes, I agree. Probably, Cisco want us to select more specific answers. EEM is part of ccnp R&S (encore+enarsi), but not ccnp security.

upvoted 2 times

LTLnetworker 2 years, 7 months ago

EEM is a possible method too

upvoted 2 times

Premium_Pils Most Recent 2 years ago

Yes, I agree. Probably, Cisco want us to select more specific answers. EEM is part of ccnp R&S (encore+enarsi), but not ccnp security.

upvoted 1 times

Felice44 3 years, 5 months ago

https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html#anc13 "After you fix the root problem, the ports are still disabled if you have not configured errdisable recovery on the switch. In this case, you must reenable the ports manually. Issue the shutdown command and then the no shutdown interface mode command on the associated interface in order to manually reenable the ports. The errdisable recovery command allows you to choose the type of errors that automatically reenable the ports after a specified amount of time. The show errdisable recovery command shows the default error-disable recovery state for all the possible conditions."

upvoted 2 times

Question #128 *Topic 1*

Refer to the exhibit. An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMC. The Cisco FTD uses a registration key of Cisc392481137 and is not behind a NAT device. Which command is needed to enable this on the Cisco FTD?



A. configure manager add 16

B. configure manager add DONTRESOLVE FTD123

C. configure manager add

D. configure manager add DONTRESOLVE

Suggested Answer: *C*

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_command_line_reference.html#ID- 2201-000004b4

Community vote distribution

C (57%) A (43%)

BennyTheK Highly Voted 5 years ago

The anwser is C. A is wrong (would need DONTRESOLVE to work in case on NAT device between FTD and FMC) B is wrong (would need 16 instead of FTD123, again in case on NAT device between FTD and FMC) C is correct:) D is wrong, DONTRESOLVE, KEY & NAT_ID is needed (again in case on NAT device between FTD and FMC)Indeed! My vote also for option C ;)

upvoted 15 times

BennyTheK Highly Voted 5 years ago

The anwser is C. A is wrong (would need DONTRESOLVE to work in case on NAT device between FTD and FMC) B is wrong (would need 16 instead of FTD123, again in case on NAT device between FTD and FMC) C is correct:) D is wrong, DONTRESOLVE, KEY & NAT_ID is needed (again in case on NAT device between FTD and FMC)

upvoted 15 times

klu16 5 years ago

Indeed! My vote also for option C ;)

upvoted 5 times

Luc_10 5 years, 1 month ago

I think the correct answer is C, as this is stated in the Official Cert Guide: "When you add a managed device to the Cisco FMC, you must provide an IP addresses of the managed device along with a registration key for authentication. The Cisco FMC and the managed device use the registration key and a NAT ID (instead of IP addresses in the case that the device is behind NAT) to authenticate and authorize for initial registration." But in this case is not behind a NAT, so....C

upvoted 14 times

CyberGhost666 Most Recent 1 year, 1 month ago

Answer is C

upvoted 2 times

XvidalX 2 years, 5 months ago

If you used a NAT ID during device setup, expand in the Advanced section and enter the same NAT ID in the Unique NAT ID field."

upvoted 2 times

LTLnetworker 2 years, 6 months ago

FMC 6.6 guide: "If you used a NAT ID during device setup, expand in the Advanced section and enter the same NAT ID in the Unique NAT ID field."Correct (A), see https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/device_management_basics.html#ID-2242-0000069dsuper agreeRead the Question it states that the device is not behind a NAT device. The answer is C

upvoted 3 times

LTLnetworker 2 years, 6 months ago

Selected Answer: A

FMC 6.6 guide: "If you used a NAT ID during device setup, expand in the Advanced section and enter the same NAT ID in the Unique NAT ID field."

upvoted 3 times

MPoels 2 years, 5 months ago

Correct (A), see https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/device_management_basics.html#ID-2242-0000069d

upvoted 1 times

XvidalX 2 years, 5 months ago

super agree

upvoted 1 times

XvidalX 2 years, 5 months ago

super agreeRead the Question it states that the device is not behind a NAT device. The answer is C

upvoted 1 times

BECAUSE 1 year, 10 months ago

Read the Question it states that the device is not behind a NAT device. The answer is C

upvoted 1 times

Ko13 2 years, 9 months ago

A is correct, I worked with FTDs for a long time, even if there is no Nat device in between, if you use NAT ID on one side then you have to use it on the other side too, the exhibit has nat ID 16 on it so the FTD's command has to match it.i have tried this out in gns3, he's right, when specifying a nat id in the fmc, the nat id has to match on the device as well, otherwise it wont be able to communicate

upvoted 5 times

Ko13 2 years, 9 months ago

Selected Answer: A

A is correct, I worked with FTDs for a long time, even if there is no Nat device in between, if you use NAT ID on one side then you have to use it on the other side too, the exhibit has nat ID 16 on it so the FTD's command has to match it.

upvoted 5 times

KnackerTopf1 2 years, 8 months ago

i have tried this out in gns3, he's right, when specifying a nat id in the fmc, the nat id has to match on the device as well, otherwise it wont be able to communicate

upvoted 5 times

psuoh 3 years, 7 months ago

Answer is C

upvoted 2 times

psuoh 3 years, 7 months ago

https://w_w_w.youtube.com/watch?v=v_uZ9GbICBk

upvoted 1 times

psuoh 3 years, 7 months ago

https://i.imgur.com/LdBgjED.png https://www.youtube.com/watch?v=v_uZ9GbICBk

upvoted 1 times

psuoh 3 years, 7 months ago

https://www.youtube.com/watch?v=v_uZ9GbICBk https://i.imgur.com/LdBgjED.png

upvoted 1 times

harvey227 4 years ago

C is correct answer. You don't need DONOTRESOLVE unless you are behind a NAT device. You need the NATID number.

upvoted 1 times

mecacig953 4 years, 4 months ago

Syntax configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id] where {hostname | IPv4_address | IPv6_address | DONTRESOLVE} specifies the DNS host name or IP address (IPv4 or IPv6) of the Firepower Management Center that manages this device. If the Firepower Management Center is not directly addressable, use DONTRESOLVE. If you useDONTRESOLVE, nat_id is required. regkey is the unique alphanumeric registration key required to register a device to the Firepower Management Center. nat_id is an optional alphanumeric string used during the registration process between the Firepower Management Center and the device. It is required if the hostname is set to DONTRESOLVE.

upvoted 1 times

brownbear505 4 years, 5 months ago

Firepower Management Center Configuration Guide, Version 6.1 - Device Management Basics [Cisco Firepower Management Center] - Cisco

upvoted 1 times

u0815 4 years, 6 months ago

100%, did it myself

upvoted 3 times

u0815 4 years, 6 months ago

see Luc and all others

upvoted 1 times

NullNull88 4 years, 8 months ago

C is the correct answer ,..unless your FMC's IP address is "DONTRESOLVE" which makes zero sense at all and the questions says it is not behind NAT

upvoted 1 times

Dead_Adriano 5 years ago

The answer is most probably C although it's not clear whe NAT ID is specified in FMC options. Regarding A: IP address + NAT ID can be specified on FTD in 2 cases: when FTD itself is behind NAT or when it's not but this is just another option to register device. But in both those cases IP of the device should be blank in FMC. This is explained here: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#ID-2242-00000191

upvoted 1 times

Dead_Adriano 5 years ago

The answer is most probably C although it's not clear whe NAT ID is specified in FMC options. Regarding A: IP address + NAT ID can be specified on FTD in 2 cases: when FTD itself is behind NAT or when it's not but this is just another option to register device. But in both those cases IP of the device should be blank in FMC. This is explained here: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#ID-2242-00000191If the FMC is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example: Example: > configure manager add DONTRESOLVE regk3y78 natid90 If the FTD is behind a NAT device, enter a unique NAT ID along with the FMC IP address or hostname, for example: Example: > configure manager add 10.70.45.5 regk3y78 natid56 https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#ID-2242-00000191 same link

upvoted 1 times

MoII 4 years, 9 months ago

If the FMC is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example: Example: > configure manager add DONTRESOLVE regk3y78 natid90 If the FTD is behind a NAT device, enter a unique NAT ID along with the FMC IP address or hostname, for example: Example: > configure manager add 10.70.45.5 regk3y78 natid56 https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#ID-2242-00000191 same link

upvoted 1 times

Question #129 *Topic 1*

A network administrator needs to find out what assets currently exist on the network. Third-party systems need to be able to feed host data into Cisco Firepower.
What must be configured to accomplish this?

A. a Network Analysis policy to receive NetFlow data from the host

B. a File Analysis policy to send file data into Cisco Firepower

C. a Network Discovery policy to receive data from the host

D. a Threat Intelligence policy to download the data from the host

Suggested Answer: *C*
Official Answer: C

abdulmalik_mail Highly Voted 4 years, 1 month ago
It's C, https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/network_discovery_policies.html
upvoted 7 times

abdulmalik_mail Highly Voted 4 years, 1 month ago
It's C, https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/network_discovery_policies.htmlyes, C is correct. From your link (and from my practice): "The network discovery policy on the Firepower Management Center controls how the system collects data on your organization's network assets and which network segments and ports are monitored. ... You can also add sources for host input and NetFlow exporters to monitor." - i. e. data from external devices.
upvoted 7 times

NikoNiko 3 years, 7 months ago
yes, C is correct. From your link (and from my practice): "The network discovery policy on the Firepower Management Center controls how the system collects data on your organization's network assets and which network segments and ports are monitored. ... You can also add sources for host input and NetFlow exporters to monitor." - i. e. data from external devices.
upvoted 2 times

iluvmicrosoft Most Recent 1 year, 10 months ago
statement 1, statement 2, what must be configured to accomplish this?? not these?? assets on the network = Network Discovery Policy third party systems feed FMC = Threat Intelligence Director horrible questions imo.. I do think the answer is C however, because even if we were using Threat Intelligence Director.. the feed wouldn't be from the "host"
upvoted 3 times

flejd 4 years, 1 month ago
its D. Network Discovery is a passive mechanizm. You want data from third party ? use TiD
upvoted 2 times

flejd 4 years, 1 month ago
its D. Network Discovery is a passive mechanizm. You want data from third party ? use TiDWe are looking for "assets" on the network. TID is used for threat feeds not discovering assets on the network.
upvoted 2 times

pr0fectus 4 years, 1 month ago
We are looking for "assets" on the network. TID is used for threat feeds not discovering assets on the network.
upvoted 5 times

Question #130 *Topic 1*

Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?

A. file access from a different user

B. user login suspicious behavior

C. privilege escalation

D. interesting file access

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

dzef13 Highly Voted 4 years, 8 months ago
should be A
upvoted 12 times

networkexpert Highly Voted 3 years, 9 months ago
Please, see Drag and Drop question 110 as well. so it should be AAgree as weird that question is , A indeed is a right answer
upvoted 6 times

networkexpert 3 years, 9 months ago
Please, see Drag and Drop question 110 as well. so it should be A
upvoted 6 times

Jessie45785 2 years, 9 months ago
Agree as weird that question is , A indeed is a right answer
upvoted 1 times

A_Wolf Most Recent 11 months, 3 weeks ago
The question is very unclear, however I'll go with A. t's important to clarify the core function of Tetration. It's designed to learn the normal behavior of workloads and applications, not necessarily the suspicious patterns of individual users. By understanding what "normal" looks like, it can then more easily detect deviations from that baseline, which are the truly suspicious events.
upvoted 1 times

Jessie45785 2 years, 9 months ago
networkexpert 12 months ago - gots a point: Please, see Drag and Drop question 110 as well. so it should be Ahttps://web.archive.org/web/20191129023324/https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html#_Toc509550184
upvoted 4 times

Jessie45785 2 years, 9 months ago
Selected Answer: A
networkexpert 12 months ago - gots a point:

Please, see Drag and Drop question 110 as well. so it should be A
upvoted 4 times

MPoels 1 year, 11 months ago
https://web.archive.org/web/20191129023324/https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html#_Toc509550184
upvoted 1 times

loser4fun 2 years, 11 months ago
I would go with B. user login suspicious behavior. The Cisco Tetration platform uses behavior-based anomaly detection to learn the normal behavior of users, applications, and network traffic, and to identify deviations from that normal behavior that may indicate a security threat. One of the behaviors that it looks for is user login suspicious behavior, such as repeated failed login attempts or login attempts from unusual locations or at unusual times. By analyzing these patterns of behavior, the platform can establish a baseline for normal user behavior and identify deviations that

may indicate a potential security threat. Once an anomaly is detected, the platform can take action to mitigate the threat and prevent it from causing damage to the network or applications.

upvoted 4 times

Kyle1776 3 years, 11 months ago

File access from a different user: Cisco Secure Workload platform learns the normal behavior of which file is accessed by which user. https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html

upvoted 3 times

jaciro11 4 years, 3 months ago

Should be A no ! Its A ! https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html

upvoted 5 times

kapplejacks 4 years, 3 months ago

Anwer: A Table 1. Cisco Tetration platform primary features and benefits Feature Benefit Zero-trust model using microsegmentation ● Cisco Tetration platform allows only the required traffic between application components and users, blocking everything else. This approach prevents a persistent threat from entering or searching for additional vulnerabilities. Also allows for micro segmentation so you can deny file access from different users. https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/cisco/data-center-tetration-data-sheet.pdf

upvoted 5 times

Sarbi 4 years, 5 months ago

What about b.If a user login from a US location and after 10 min the same user tries to login for Asia.

upvoted 2 times

kerniger 4 years, 5 months ago

i really dont get the question. https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html#CiscoSecureWorkloadplatformandapplicationbehaviorallowedlisting So SecureWorkload (Tetration) uses all of them but B C and D is not a "learning" machanism of users behavior while A is?

upvoted 2 times

Question #131 *Topic 1*

Which attribute has the ability to change during the RADIUS CoA?

A. authorization

B. NTP

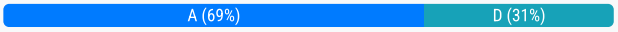
C. accessibility

D. membership

Suggested Answer: *A*

Official Answer: A

Community vote distribution



Kyle1776 Highly Voted 3 years, 5 months ago

CoA stands for change of Authorization so im gonna go with Authorization

upvoted 13 times

A_Wolf Most Recent 11 months, 3 weeks ago

Selected Answer: A

Although A (authorization) is not strictly an attribute bt the process. The word membership does not make any sense in technical terms is assigned to a VLAN, it is not called membership. will stick to A

upvoted 2 times

CyberGhost666 1 year, 1 month ago

Selected Answer: D

D is the correct answer.

> Authorization is the process of assigning permissions and access rights based on policies, not a changeable attribute by itself. > CoA is triggered due to a change in authorization, but the actual attribute that changes is usually something like VLAN membership, access control list, or policy group membership

upvoted 1 times

user_topic 1 year, 3 months ago

Selected Answer: A

Answer A - I work with ISE on a daily basis.

upvoted 4 times

Pierre_Bouvier 1 year, 6 months ago

Selected Answer: D

RADIUS Change of Authorization (CoA) allows dynamic updates to a user's session attributes after the session is already active.

upvoted 1 times

[Removed] 1 year, 9 months ago

Selected Answer: A

The name CoA (Change of Authorization) explains itself enough.

upvoted 2 times

Pierre_Bouvier 1 year, 6 months ago

"authorization" itself is not an attribute but rather a process or state.

upvoted 1 times

Cokamaniako 2 years, 1 month ago

Selected Answer: A

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated

upvoted 3 times

littlewilly 2 years, 2 months ago

Selected Answer: D

It's membership

upvoted 2 times

Terry0987 2 years, 8 months ago

Selected Answer: D

shouldn't it be D ? It's asking about a specific attribute !

upvoted 1 times

SegaMasterSystemAdmin Highly Voted 2 years, 3 months ago

membership? like a gym membership? lol

upvoted 5 times

abdulmalik_mail 3 years, 7 months ago

It's A, Radius CoA provides a mechanism to change the attributes of anauthentication, authorization, and accounting (AAA).

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xe-16-10/sec-usr-aaa-xe-16-10-book/sec-rad-coa.pdf

upvoted 4 times

Question #132 *Topic 1*

An administrator configures new authorization policies within Cisco ISE and has difficulty profiling the devices. Attributes for the new Cisco IP phones that are profiled based on the RADIUS authentication are seen; however, the attributes for CDP or DHCP are not. What should the administrator do to address this issue?

A. Configure a service template within the switch to standardize the port configurations so that the correct information is sent to Cisco ISE.

B. Configure the ip dhcp snooping trust command on the DHCP interfaces to get the information to Cisco ISE.

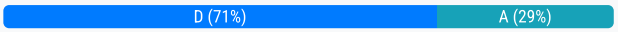
C. Configure the authentication port-control auto feature within Cisco ISE to identify the devices that are trying to connect.

D. Configure the device sensor feature within the switch to send the appropriate protocol information.

Suggested Answer: *D*

Official Answer: D

Community vote distribution



klu16 Highly Voted 4 years, 12 months ago

I would choose D... Device sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by Device Sensor can come from the following protocols: Cisco Discovery Protocol (CDP) Link Layer Discovery Protocol (LLDP) Dynamic Host Configuration Protocol (DHCP)https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html

upvoted 21 times

klu16 Highly Voted 4 years, 12 months ago

I would choose D... Device sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by Device Sensor can come from the following protocols: Cisco Discovery Protocol (CDP) Link Layer Discovery Protocol (LLDP) Dynamic Host Configuration Protocol (DHCP)

upvoted 21 times

andrewj511 4 years, 11 months ago

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html

upvoted 7 times

sy0_061 Most Recent 1 year ago

D - Device sensor is configured to send DHCP, CDP, and LLDP info to ISE. Since this is a Cisco phone, CDP and DHCP are the relevant here. The CDP, LLDP, and DHCP attributes are grouped together first. Then, the 'device-sensor' command is used to export those groupings to ISE.

upvoted 2 times

Premium_Pils 2 years ago

D - As others pointed out

upvoted 2 times

Korndal 2 years, 1 month ago

Answer is D. Other answer that should have been there, would be that den ip helper-address hasn't been configured to point to ISE, and therefor ISE does not get copies of the dhcp requests of the clients

upvoted 1 times

4pelos 2 years, 5 months ago

Correct answer D. Checked with securitytut

upvoted 1 times

nekkrokvlt 2 years, 11 months ago

It is D. Device sensor sends cdp / lldp attributes as radius accounting data for profiling

upvoted 2 times

gc999 3 years, 2 months ago

I eventually choose "D" after reading this https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_1_se/device_sensor/guide/sensor_guide.html

upvoted 3 times

Jessie45785 3 years, 4 months ago

D - cannot be correct cause device sensor is configured on ISE, NOT on the switch https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html#anc6 A- service templates can be locally configured on the switch: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html#anc6it was really late D- IS CORRECT: switch#show device-sensor cache interface g1/0/13 Device: 20bb.c0de.06ae on port GigabitEthernet1/0/13 ---------- ---------- Proto Type:Name Len Value LLDP 6:system-description 40 0C 26 43 69 73 63 6F 20 49 50 20 50 68 6F 6E 65 20 38 39 34 31 2C 20 56 33 2C 20 53 43 43 50 20 39 2D 33 2D 34 2D 31 37 CDP 6:platform-type 24 00 06 00 18 43 69 73 63 6F 20 49 50 20 50 68 6F 6E 65 20 38 39 34 31 20 CDP 28:secondport-status-type 7 00 1C 00 07 00 02 00

upvoted 4 times

Jessie45785 3 years, 4 months ago

Selected Answer: A

D - cannot be correct cause device sensor is configured on ISE, NOT on the switch https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html#anc6

A- service templates can be locally configured on the switch: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html#anc6

upvoted 4 times

Jessie45785 3 years, 3 months ago

it was really late D- IS CORRECT: switch#show device-sensor cache interface g1/0/13 Device: 20bb.c0de.06ae on port GigabitEthernet1/0/13 ---------- ---------- Proto Type:Name Len Value LLDP 6:system-description 40 0C 26 43 69 73 63 6F 20 49 50 20 50 68 6F 6E 65 20 38 39 34 31 2C 20 56 33 2C 20 53 43 43 50 20 39 2D 33 2D 34 2D 31 37 CDP 6:platform-type 24 00 06 00 18 43 69 73 63 6F 20 49 50 20 50 68 6F 6E 65 20 38 39 34 31 20 CDP 28:secondport-status-type 7 00 1C 00 07 00 02 00

upvoted 4 times

sis_net_sec 3 years, 10 months ago

D is correct Device sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by Device Sensor can come from the following protocols: + Cisco Discovery Protocol (CDP) + Link Layer Discovery Protocol (LLDP) + Dynamic Host Configuration Protocol (DHCP) Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292- ConfigureDevice-Sensor-for-ISE-Profilin.html

upvoted 2 times

JGW 4 years, 4 months ago

D is correct, use link provided by andrewj511 and coentror. Answer C is incorrect, as that command needs to be executed on the switch and not on the ISE server

upvoted 1 times

jaciro11 4 years, 5 months ago

Configure the device sensor feature within the switch to send the appropriate protocol information

upvoted 1 times

efongvan 4 years, 7 months ago

I will go with D.

upvoted 1 times

coentror 4 years, 8 months ago

It is D https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html

upvoted 4 times

testtaker13 4 years, 9 months ago

Seems D is the correct one

upvoted 4 times

Sarbi 4 years, 11 months ago

I will go with D.

upvoted 4 times

Sarbi 4 years, 12 months ago

Ans is A.

upvoted 2 times

Question #133 *Topic 1*

An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralized solution. The organization does not have a local VM but does have existing Cisco ASA that must migrate over to Cisco FTDs. Which solution meets the needs of the organization?

A. Cisco FMC

B. CDO

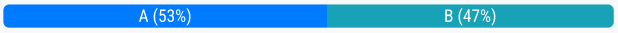
C. CSM

D. Cisco FDM

Suggested Answer: *B*

Official Answer: B

Community vote distribution



eazy99 Highly Voted 4 years, 10 months ago

What a tricky question, but I think I just got you the perfect answer and the perfect link from Cisco. The correct answer is A, not B. The reason why, According to Cisco, if you want to migrate your ASA to FTD and want to manage them both through "CDO and FDM" then use (CDO), but if you want to migrate ASA to FTD and manage both in the same time (Centralized) then use FMC" So the answer is absolutely A, and here is the link: https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide-CDO/ASA2FTD_Using_CDO/ASA2FTD_with_FP_Migration_Tool_cdo_chapter_011.html

upvoted 26 times

eazy99 Highly Voted 4 years, 10 months ago

What a tricky question, but I think I just got you the perfect answer and the perfect link from Cisco. The correct answer is A, not B. The reason why, According to Cisco, if you want to migrate your ASA to FTD and want to manage them both through "CDO and FDM" then use (CDO), but if you want to migrate ASA to FTD and manage both in the same time (Centralized) then use FMC" So the answer is absolutely A, and here is the link: https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide-CDO/ASA2FTD_Using_CDO/ASA2FTD_with_FP_Migration_Tool_cdo_chapter_011.htmlbut there's another tricky part which is the organization doesn't have a local VM which makes the answer is Byou can have physical FMC deployment. A is correct!Just want to confirm that FMC can also support Cloud Deployment. Right? https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.htmlAnswer A seems to be right (with a physical FMC appliance). Official ASA-2-FTD migration tool exists several years (so CDO built-in migration tool isn't needed): https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_00.html Consideration why not using CDO (in this scenario): When using device credentials to connect CDO to a device, it is a best practice to download and deploy an SDC in your network to manage the communication between CDO and the device. This procedure describes how to install an SDC in your network, using CDO's VM image. This is the preferred, easiest, and most reliable way to create an SDC. (see https://docs.defenseorchestrator.com/r_how-it-works_cdo.html#!t_deploy-a-sdc-using-cdos-vm-image.html)

upvoted 26 times

loser4fun 3 years, 5 months ago

but there's another tricky part which is the organization doesn't have a local VM which makes the answer is B

upvoted 4 times

loser4fun 3 years, 5 months ago

but there's another tricky part which is the organization doesn't have a local VM which makes the answer is Byou can have physical FMC deployment. A is correct!Just want to confirm that FMC can also support Cloud Deployment. Right? https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.htmlAnswer A seems to be right (with a physical FMC appliance). Official ASA-2-FTD migration tool exists several years (so CDO built-in migration tool isn't needed): https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_00.html Consideration why not using CDO (in this scenario): When using device credentials to connect CDO to a device, it is a best practice to download and deploy an SDC in your network to manage the communication between CDO and the device. This procedure describes how to install an SDC in your network, using CDO's VM image. This is the preferred, easiest, and most reliable way to create an SDC. (see https://docs.defenseorchestrator.com/r_how-it-works_cdo.html#!t_deploy-a-sdc-using-cdos-vm-image.html)

upvoted 4 times

angry 3 years, 5 months ago

you can have physical FMC deployment. A is correct!

upvoted 5 times

gc999 3 years, 4 months ago

Just want to confirm that FMC can also support Cloud Deployment. Right? https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html

upvoted 2 times

MPoels 2 years, 5 months ago

Answer A seems to be right (with a physical FMC appliance). Official ASA-2-FTD migration tool exists several years (so CDO built-in migration tool isn't needed): https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_00.html Consideration why not using CDO (in this scenario): When using device credentials to connect CDO to a device, it is a best practice to download and deploy an SDC in your network to manage the communication between CDO and the device. This procedure describes how to install an SDC in your network, using CDO's VM image. This is the preferred, easiest, and most reliable way to create an SDC. (see https://docs.defenseorchestrator.com/r_how-it-works_cdo.html#!t_deploy-a-sdc-using-cdos-vm-image.html)

upvoted 3 times

semi1750 4 years, 4 months ago

Vote for B FMC will manage only Firepower images (FTD or Firepower module Services). CDO is able to centrally manage your ASAs, FTD, Meraki security policies and AWS VPC security policies. For FMC, you need to have a local VM (with some resources like 32G RAM) and need to manage the redundancy as well. CDO is cloud based (could have a local VM with small resources to communicate with the cloud and not expose your devices management). You need to see CDO like the Meraki portal for Cisco Security Firewalls. https://community.cisco.com/t5/network-security/a-classic-cdo-vs-fmc/td-p/4070116

upvoted 9 times

F0rtyx40 Most Recent 3 months, 2 weeks ago

The firepower migration tool that converts ASA to FTD only supports FMC not CDO, not yet at least.

upvoted 1 times

Eluis007 7 months ago

A For true centralized management of multiple FTDs, FMC is the primary and intended solution.

upvoted 1 times

TanHK 7 months, 3 weeks ago

Cisco Defense Orchestrator (CDO) is a cloud-based management platform, so it does not require a local virtual machine. It provides centralized management for multiple FTDs and includes migration tools to convert ASA configurations to FTD, which directly addresses the migration requirement. A. Cisco FMC (Firepower Management Center) Requires a local or cloud VM and does not fit the “no local VM” constraint. C. CSM (Cisco Security Manager) Legacy product used for ASA management; does not manage FTD. D. Cisco FDM (Firepower Device Manager) Local, device-level management only; not centralized.

upvoted 1 times

Ernestokoro 11 months ago

I have deployed a physical cisco FMC. so it must not use a VM which make A correct for me

upvoted 1 times

luismg 1 year, 11 months ago

I would say is CDO because FMC is usually a VM.

upvoted 1 times

Ko13 2 years, 9 months ago

It is B. CDO . The FMC cannot help with the ASA-to-FTD migration, you do that using the Firepower Migration Tool, then the config is loaded in to the FMC once migrated. CDO on the other hand does allow you to migrate ASA to FTD (managed using FDM thou), but it also allows you to then manage thouse FDM FTDs too. https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide-CDO/ASA2FTD_Using_CDO/ASA2FTD_with_FP_Migration_Tool_cdo_chapter_011.html
https://www.cisco.com/c/en/us/td/docs/security/cdo/managing-ftd-with-cdo/managing-ftd-with-cisco-defense-orchestrator/managing-ftd-with-cdo.html

upvoted 1 times

DWizard 3 years, 1 month ago

The answer can be A) FMC using an appliance, not a virtual machine, or B) CDO without SDCs... it's a hard one, but I would go for A, has more sense if it must be a "centralized solution"

upvoted 2 times

ffaiz 3 years, 2 months ago

"The organization does not have a local VM" 1-FDM(manage device locally) 2-CDO(cloud based central management no need VM) 3-FMC(VM based central management)

upvoted 2 times

Jessie45785 3 years, 2 months ago

It is Cisco question do not overthink it - if you cannot use VM you are left with CDO https://www.cisco.com/c/en/us/td/docs/security/firepower/620/asa2ftd-migration/asa2ftd-migration-guide-620/asa2ftd_migration_procedure.pdf FMC: Step 1 Download one of the following images from Support: • Firepower Management Center Virtual for VMware • Firepower Management Center Virtual for KVM Step 2 Use the image file to install a dedicated Firepower Management Center Virtual, as described in the appropriate guide: • Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide • Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide Step 3 Connect to the Firepower Management Center via ssh, using the admin username. Step 4 Log in to the root shell: sudo su - Step 5 Run the following command: enableMigrationTool.pl After the process completes, refresh any web interface sessions running on the Firepower Management Center to use the migration tool.

upvoted 3 times

littlewilly 3 years, 2 months ago

Answer is CDO

upvoted 1 times

alexyozgat24 3 years, 3 months ago

i came cross this situation for deploying FPR1150 firewalls. basically you will have 3 options 1-FDM(manage device locally) 2-CDO(cloud based central management no need VM) 3-FMC(VM based central management) so for this question you need to manage them from controller but not from the VM you manage, answer is CDO . so B.

upvoted 3 times

Tuxzinator 3 years, 6 months ago

Selected Answer: A

B is incorrect.

CDO (Cisco Defense Orchestrator) is a cloud-based management solution that can manage multiple Cisco security products, including ASA (Adaptive Security Appliance) and FTD. However, it requires a local VM to be deployed in order to manage on-premises devices.

upvoted 3 times

KPzee 3 years, 4 months ago

A is correct. FMC supports both physical and virtual appliances, hence it can be deployed as a virtual machine on an existing server infrastructure or as a physical appliance. also FMC supports the migration of Cisco ASA configurations to Cisco FTD

upvoted 1 times

Tuxzinator 3 years, 6 months ago

B is incorrect. CDO (Cisco Defense Orchestrator) is a cloud-based management solution that can manage multiple Cisco security products, including ASA (Adaptive Security Appliance) and FTD. However, it requires a local VM to be deployed in order to manage on-premises devices.No, as long as those on-premises devices have Internet access https://www.cisco.com/c/en/us/td/docs/security/cdo/managing-asa-with-cdo/managing-asa-with-cisco-defense-orchestrator/basics-of-cisco-defense-orchestrator.html

upvoted 3 times

DWizard 3 years, 1 month ago

No, as long as those on-premises devices have Internet access https://www.cisco.com/c/en/us/td/docs/security/cdo/managing-asa-with-cdo/managing-asa-with-cisco-defense-orchestrator/basics-of-cisco-defense-orchestrator.html

upvoted 1 times

Hereim 3 years, 9 months ago

I will go with B. Very good comparison between CDO and FMC pros and cons in this link https://community.cisco.com/t5/network-security/a-classic-cdo-vs-fmc/td-p/4070116 Main two points here to note: there is no local VM as per the question. FMC needs a local VM. Secondly, the question clearly says the existing ASA must migrate over to FTD - CDO can do that however FMC you need to do separate migration tool.

upvoted 4 times

Emlia1 3 years, 8 months ago

A is correct

upvoted 1 times

Hereim 3 years, 9 months ago

I will go with B. Very good comparison between CDO and FMC pros and cons in this link https://community.cisco.com/t5/network-security/a-classic-cdo-vs-fmc/td-p/4070116 Main two points here to note: there is no local VM as per the question. FMC needs a local VM. Secondly, the question clearly says the existing ASA must migrate over to FTD - CDO can do that however FMC you need to do separate migration tool.But here said that FMC can be deployed either physical or virtual, or from the Cloud. https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html

upvoted 4 times

sis_net_sec 3 years, 10 months ago

Selected Answer: A

cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/firepower_threat_defense_logical_devices.html

upvoted 1 times

gc999 3 years, 3 months ago

But here said that FMC can be deployed either physical or virtual, or from the Cloud.

https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html

upvoted 3 times

Question #134 *Topic 1*

What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

A. Telemetry uses push and pull, which makes it more secure than SNMP.

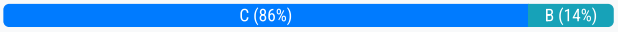
B. Telemetry uses push and pull, which makes it more scalable than SNMP.

C. Telemetry uses a push method, which makes it faster than SNMP.

D. Telemetry uses a pull method, which makes it more reliable than SNMP.

Suggested Answer: *C*
Official Answer: C

Community vote distribution



idto Highly Voted 4 years, 2 months ago

Selected Answer: C

SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts.

The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data.

Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.

Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics

https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming-telemetry

upvoted 11 times

Zatingke 3 years ago

The above says, does not scale. So it should be B then.

upvoted 1 times

MPoels 1 year, 11 months ago

The crucial difference is "uses push method" (not "push and pull"). So answer C seems to be right.

upvoted 2 times

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: C

C. Telemetry uses a push method, which makes it faster than SNMP.

upvoted 1 times

sull3y 2 years, 10 months ago

The benefit of using telemetry over SNMP to configure new routers for monitoring purposes is that telemetry uses a push method, which makes it faster than SNMP.

SNMP (Simple Network Management Protocol) is a widely used protocol for network monitoring and management. SNMP uses a pull model where the management system sends a request to the device to retrieve information. The device responds to the request with the requested data. This can result in a delay between when a change occurs and when the monitoring system is made aware of it.

Telemetry, on the other hand, uses a push model where the device sends data to the management system in near real-time. This makes telemetry faster than SNMP and can reduce the time between when a change occurs and when the monitoring system is made aware of it.

Therefore, the answer is C: Telemetry uses a push method, which makes it faster than SNMP.

upvoted 3 times

Zatingke 3 years ago

Selected Answer: B

Pull model, such as SNMP, does not scale when what you want is near real-time data.

upvoted 2 times

Question #135 *Topic 1*

Refer to the exhibit. A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced. What is the cause of this issue?

```
ntp authentication-key 10 md5 cisco123
ntp trusted-key 10
```

A. The hashing algorithm that was used was MD5, which is unsupported.

B. The key was configured in plain text.

C. NTP authentication is not enabled.

D. The router was not rebooted after the NTP configuration updated.

Suggested Answer: *C*
Official Answer: C

Toni_Su91 Highly Voted 1 year, 11 months ago

The following example shows how to configure the system to synchronize only to systems providing authentication keys 1 to 3 in their NTP packets:

Router(config)# ntp authenticate Router(config)# ntp authentication-key 1 md5 key1 Router(config)# ntp authentication-key 2 md5 key2 Router(config)# ntp authentication-key 3 md5 key3 Router(config)# ntp trusted-key 1 - 3

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/command/bsm-cr-book/bsm-cr-n1.html#wp2849112306

ntp authenticate - Enables NTP authentication.

upvoted 8 times

abdulmalik_mail 3 years, 1 month ago

It's C, we need put command ntp authentication enable

upvoted 3 times

Question #136 *Topic 1*

An engineer has been tasked with configuring a Cisco FTD to analyze protocol fields and detect anomalies in the traffic from industrial systems. What must be done to meet these requirements?

A. Enable traffic analysis in the Cisco FTD.

B. Implement pre-filter policies for the CIP preprocessor.

C. Configure intrusion rules for the DNP3 preprocessor.

D. Modify the access control policy to trust the industrial traffic.

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

klu16 Highly Voted 4 years, 11 months ago
I will go with C here... First of all, you need special kind of preprocessors (Modbus/DNP3/CIP) to analyze the industrial system traffic, so enabling "default" traffic analysis in FTD is not enough.
upvoted 11 times

klu16 Highly Voted 4 years, 11 months ago
I will go with C here... First of all, you need special kind of preprocessors (Modbus/DNP3/CIP) to analyze the industrial system traffic, so enabling "default" traffic analysis in FTD is not enough.Can confirm Bacnet and modbus for chillers and irrigation
upvoted 11 times

SrStew Most Recent 4 months, 2 weeks ago
Can confirm Bacnet and modbus for chillers and irrigation
upvoted 1 times

zeroC00L 4 years, 11 months ago
i would opt for C. DNP3 is a SCADA Protocol which in turn is widly used in the industrial network world. "The DNP3 preprocessor detects anomalies in DNP3 traffic and decodes the DNP3 protocol for processing by the rules engine, which uses DNP3 keywords to access certain protocol fields." https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada_preprocessors.htmlIts definitely not widely used, Id say CIP or Modbus are going to be used 90% of the time or better with CIP likely being dominant in at least the US plus cisco and Rockwell partnered to create the CIP/ethernet Ethernet/IP protocol and it is a cisco exam. Also looking at the preprocessor for CIP, "The CIP preprocessor detects CIP and ENIP traffic running on TCP or UDP and sends it to the intrusion rules engine." So id personally go with CIP preprocessor over intrusion rules with DNP3. But im not yet super familiar with the Firepower processes to be fair.
upvoted 8 times

zeroC00L 4 years, 11 months ago
i would opt for C. DNP3 is a SCADA Protocol which in turn is widly used in the industrial network world. "The DNP3 preprocessor detects anomalies in DNP3 traffic and decodes the DNP3 protocol for processing by the rules engine, which uses DNP3 keywords to access certain protocol fields." https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada_preprocessors.html
upvoted 8 times

brownb 4 years, 9 months ago
Its definitely not widely used, Id say CIP or Modbus are going to be used 90% of the time or better with CIP likely being dominant in at least the US plus cisco and Rockwell partnered to create the CIP/ethernet Ethernet/IP protocol and it is a cisco exam. Also looking at the preprocessor for CIP, "The CIP preprocessor detects CIP and ENIP traffic running on TCP or UDP and sends it to the intrusion rules engine." So id personally go with CIP preprocessor over intrusion rules with DNP3. But im not yet super familiar with the Firepower processes to be fair.
upvoted 5 times

CyberGhost666 1 year, 1 month ago
Correct Answer is C.
upvoted 1 times

Premium_Pils 2 years ago
Pre-filter policy skips snort engine. C seems to be correct.
upvoted 1 times

Jessie45785 3 years, 4 months ago

definitely C (as mentioned by @zeroCOOL DNP3 is part of SCADA) and SCADA is typical industrial system)

upvoted 2 times

surforlife 4 years ago

It does not matter which of the 3 you like the most. It does not matter which one you choose between Modbus, CIP or DNP3. What matters is where you set them to be trusted by FTD. Policies > Access Control, then click Network Analysis Policies or Policies > Access Control > Intrusion, then click Network Analysis Policies. Note If your custom user role limits access to the first path listed here, use the second path to access the policy. Step 2 Click Edit (edit icon) next to the policy you want to edit. If View (view button) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration. Step 3 Click Settings in the navigation panel. "D" is the correct answer.

upvoted 2 times

NikoNiko 4 years, 1 month ago

C is correct - Configure Intrusion Rules... because IR also automatically enable required pre-processors, which handle detection of anomalies (as required in the question). A - "enable traffic analysis" - means nothing specific B - Pre-filter policies for CIP -> Pre-filters are used to bypass Snort engine completely, optional first step of access control, rules that match simple values like IP's and ports (like ASA ACL). There is no deep packet inspection nor anomaly detection.[2][3] [2] https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212700-configuration-and-operation-of-ftd-prefi.html [3] https://networkdirection.net/articles/firewalls/firepowermanagementcentre/prefilterpolicies/ D - Set Access Control Policy to trust industrial traffic - Action TRUST = allow WITHOUT inspection & anomaly detection.C - "configure INTRUSION RULES for DNP3" -> Documentation states, that enabling INTRUSION RULES is mandatory for CIP to work + required preprocessors (in Network Access Policy - NAP) will be enabled automatically: "If you want the CIP preprocessor rules listed in the following table to generate events, you MUST enable them. See Setting Intrusion Rule States for information on enabling rules." "If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings, although the preprocessor remains disabled in the web interface for the corresponding network analysis policy." [1] https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada_preprocessors.html

upvoted 2 times

NikoNiko 4 years, 1 month ago

C is correct - Configure Intrusion Rules... because IR also automatically enable required pre-processors, which handle detection of anomalies (as required in the question).

A - "enable traffic analysis" - means nothing specific

B - Pre-filter policies for CIP -> Pre-filters are used to bypass Snort engine completely, optional first step of access control, rules that match simple values like IP's and ports (like ASA ACL). There is no deep packet inspection nor anomaly detection.[2][3] [2] https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212700-configuration-and-operation-of-ftd-prefi.html [3] https://networkdirection.net/articles/firewalls/firepowermanagementcentre/prefilterpolicies/

D - Set Access Control Policy to trust industrial traffic - Action TRUST = allow WITHOUT inspection & anomaly detection.

upvoted 2 times

NikoNiko 4 years, 1 month ago

C - "configure INTRUSION RULES for DNP3" -> Documentation states, that enabling INTRUSION RULES is mandatory for CIP to work + required preprocessors (in Network Access Policy - NAP) will be enabled automatically: "If you want the CIP preprocessor rules listed in the following table to generate events, you MUST enable them. See Setting Intrusion Rule States for information on enabling rules." "If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings, although the preprocessor remains disabled in the web interface for the corresponding network analysis policy." [1] https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada_preprocessors.html

upvoted 2 times

getafix 4 years, 1 month ago

SCADA: There are two supervisory control and data acquisition (SCADA) protocols for which the Cisco Firepower NGIPS offers preprocessors: DNP3 and Modbus. These protocols monitor and control industrial facilities. The SCADA preprocessors monitor the DNP and Modbus protocols for anomalies and decode their messages for further rule inspection. From the Cisco Official Cert Guide

upvoted 2 times

pr0fectus 4 years, 7 months ago

Pre-filter policy skips snort engine.

upvoted 5 times

MoII 4 years, 9 months ago

"the system does not inspect blocked or trusted traffic" https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/an_overview_of_network_analysis_and_intrusion_policies.htmldiagram shows, in a simplified fashion, the order of traffic analysis in an inline, intrusion prevention and AMP for Networks deployment. It illustrates how the access control policy invokes other policies to examine traffic, and in which order those policies are invoked. The network analysis and intrusion policy selection phases are highlighted. https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/an_overview_of_network_analysis_and_intrusion_policies.html In a newly created access control policy, one default network analysis policy governs preprocessing for all traffic for all intrusion policies invoked by the same parent access control policy.

upvoted 1 times

MoII 4 years, 9 months ago

"the system does not inspect blocked or trusted traffic" https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/an_overview_of_network_analysis_and_intrusion_policies.html

upvoted 1 times

MoII 4 years, 9 months ago

diagram shows, in a simplified fashion, the order of traffic analysis in an inline, intrusion prevention and AMP for Networks deployment. It illustrates how the access control policy invokes other policies to examine traffic, and in which order those policies are invoked. The network analysis and intrusion policy selection phases are highlighted. https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/an_overview_of_network_analysis_and_intrusion_policies.html In a newly created access control policy, one default network analysis policy governs preprocessing for all traffic for all intrusion policies invoked by the same parent access control policy.

upvoted 1 times

andrewj511 4 years, 10 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada_preprocessors.html If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings...

upvoted 4 times

fabio3wz 4 years, 11 months ago

I think the answer should be C. If you're going to detect any kind of anomalies I suppose Intrusion rules is a must.

upvoted 5 times

Question #137 *Topic 1*

An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices. The default management port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?

A. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices.

B. Set the sftunnel port to 8305.

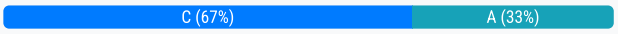
C. Manually change the management port on Cisco FMC and all managed Cisco FTD devices.

D. Set the sftunnel to go through the Cisco FTD.

Suggested Answer: *C*

Official Answer: C

Community vote distribution



MoII Highly Voted 3 years, 9 months ago

Answer should be C https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Security__Internet_Access__and_Communication_Ports.html 8305/tcp Securely communicate between appliances in a deployment. " If you change this port, you must change it for all appliances in the deployment. We recommend you keep the default."

upvoted 13 times

eazy99 Highly Voted 3 years, 11 months ago

The answer is C from Cisco website and specifically this paragraph, " In this case you must also change the port on FMC (Configuration > Management Interfaces > Shared Settings). This affects all other devices that are already registered to the same FMC. Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate together."

And here is the link https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

upvoted 9 times

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: C

Option C.

Cisco FMC (Firepower Management Center) communicates with Cisco FTD (Firepower Threat Defense) devices using a management channel established during the registration process. This channel uses a default TCP port (8305) for SFTunnel, which is a secure transport mechanism for FMC-to-FTD communication.

If the default port (e.g., 8305) conflicts with other applications on your network, you need to: > Manually update the port on both Cisco FMC and each FTD device. > There is no automatic push or sync of the new port from FMC to FTD. > For me option A is not correct since FMC cannot push this change, because the port is used to establish the connection in the first place.

upvoted 1 times

Alizade 1 year, 10 months ago

Selected Answer: C

C. Manually change the management port on Cisco FMC and all managed Cisco FTD devices.

upvoted 1 times

Tuxzinator 2 years, 6 months ago

Selected Answer: C

The answer is C. However if you overthink it it could also be A. however in the form the question is asked it should be C.

Cisco FMC has the ability to push configuration changes to managed Cisco FTD devices automatically, so changing the management port on the FMC can be propagated to all managed FTD devices without the need for manual intervention on each device. This can be done through the use of FlexConfigs or the Configuration Deployments feature in the FMC.

FlexConfigs allow for the execution of custom commands on managed devices, including configuration changes. The FMC can be configured to push a FlexConfig that changes the management port on all managed FTD devices at once.

upvoted 2 times

Emlia1 2 years, 8 months ago

I prefer C

upvoted 1 times

sis_net_sec 2 years, 10 months ago

Selected Answer: A

Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate with each other.

upvoted 3 times

francojaraba 3 years, 1 month ago

Selected Answer: C

Answer is C. The sftunnel is created once the communication is stablished - https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

"Once the registration is done the FTD and the FMC establish a secure tunnel called sftunnel (the name derives from the Sourcefire tunnel)."

upvoted 1 times

Laryoul 3 years, 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

Minion2021 3 years, 5 months ago

The answer is C

upvoted 2 times

klu16 3 years, 11 months ago

The answer is C... When you change the default port, you have to change it manually on all FTD devices in the deployment.

upvoted 3 times

fabio3wz 3 years, 11 months ago

C should be the correct answer; we can change the port manually: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html#anc7

upvoted 2 times

Question #138 *Topic 1*

An administrator is establishing a new site-to-site VPN connection on a Cisco IOS router. The organization needs to ensure that the ISAKMP key on the hub is used only for terminating traffic from the IP address of 172.19.20.24. Which command on the hub will allow the administrator to accomplish this?

A. crypto isakmp identity address 172.19.20.24

B. crypto ca identity 172.19.20.24

C. crypto enrollment peer address 172.19.20.24

D. crypto isakmp key Cisco0123456789 172.19.20.24

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

testtaker13 Highly Voted 2 years, 1 month ago

probably D. However the correct command should be crypto isakmp key address

upvoted 10 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct option is D. This command tells the router to only accept and use the specified key (Cisco0123456789) when communicating with the peer at IP 172.19.20.24.

upvoted 1 times

itashraf 2 years, 5 months ago

Ans: D

upvoted 3 times

Question #139 *Topic 1*

A Cisco FTD engineer is creating a newIKEv2 policy called s2s00123456789 for their organization to allow additional protocols to terminate network devices with.
They currently only have one policy established and need the new policy to be a backup in case some devices cannot support the stronger algorithms listed in the primary policy. What should be done in order to support this?

A. Change the encryption to AES* to support all AES algorithms in the primary policy.

B. Make the priority for the primary policy 10 and the new policy 1.

C. Change the integrity algorithms to SHA* to support all SHA algorithms in the primary policy.

D. Make the priority for the new policy 5 and the primary policy 1.

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

CyberGhost666 Most Recent 1 year, 1 month ago
Correct option is D.
upvoted 1 times

sis_net_sec 1 year, 10 months ago
All IKE policies on the device are sent to the remote peer regardless of what is in the selected policy section. The first IKE Policy matched by the remote peer will be selected for the VPN connection. Choose which policy is sent first using the priority field. Priority 1 will be sent first. Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike- protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html
upvoted 1 times

MoII 2 years, 9 months ago
Correct answer should be D The lower the number, the higher the priority.
https://docs.defenseorchestrator.com/Configuration_Guides/Objects/Configuring_the_Global_IKE_Policy/Managing_FTD_IKEv2_Policies Priority—The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
upvoted 4 times

Question #140 *Topic 1*

What is a functional difference between a Cisco ASA and Cisco IOS router with Zone-Based Policy Firewall?

A. The Cisco ASA can be configured for high availability, whereas the Cisco IOS router with Zone-Based Policy Firewall cannot.

B. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability, whereas the Cisco ASA cannot.

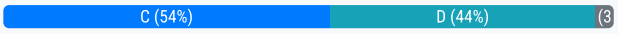
C. The Cisco ASA denies all traffic by default, whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces.

D. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas Cisco ASA starts out by allowing traffic until rules are added.

Suggested Answer: *C*

Official Answer: C

Community vote distribution



majster88 Highly Voted 3 years, 2 months ago

Selected Answer: C

Correct is C, why? On ASA by default all interfaces with ip address and nameif are configured with security level 0. Without "same-security-level inter/intra-traffic" (which is not by default) all traffic through ASA is denied (traffic between interfaces with the same security level). On other hand, with ZBFW by default all interfaces with ip address are not assigned to a zone. Traffic between interfaces not assigned to a zone is allowed.

upvoted 5 times

Winux29 Most Recent 6 months, 2 weeks ago

Selected Answer: C

Cisco ASA (Adaptive Security Appliance):

Default behavior: All interfaces are untrusted by default, and all traffic is denied

Cisco IOS Router with Zone-Based Policy Firewall (ZBFW):

Default behavior: Traffic between zones is permitted unless explicitly denied, depending on the policy maps.

upvoted 2 times

Silexis 7 months ago

Selected Answer: A

Cisco ASA supports clustering and stateful failover, while the Cisco IOS ZBFR is not able to produce a true HA in terms of firewalling. Answer D is not correct due to the fact that Cisco IOS ZBFR is not blocking ALL traffic by default, allowing same-zone inter interface flows. Cisco ASA, on the other hand, will allow by default traffic from high to low security level interfaces but blocking same level interface traffic. C is not right because Cisco IOS ZBFR is blocking all intra-zones trraffic. B is not correct because Cisco ASA CAN be configured and was designed with HA in mind. It remains A, as a functional difference between these 2 type of devices: ASA can function as part of a Cluster while Cisco IOS not. While you can use NHRP on routers or interfaces redundancy, propagating state of the connections to provide HA for clients won't be possible in case of IOS

upvoted 1 times

TanHK 7 months, 3 weeks ago

Selected Answer: C

The ASA enforces a global implicit deny, while ZBFW only controls traffic between defined zones. Untrusted interfaces (not in any zone) on a router with ZBFW will allow traffic until explicitly placed in a zone and governed by policies.

So, I vote for C.

upvoted 4 times

Ernestokoro 11 months, 1 week ago

Selected Answer: C

Remember that firewalls are deny by default whereas routers are allow by default. so do no allow them to confuse you with common basics. Answer is C guys

upvoted 2 times

Demon_Queen_Velverosa 1 year, 11 months ago

Don't over think this one and only read the question and answer.

What is a functional difference between a Cisco ASA and Cisco IOS router with Zone-Based Policy Firewall?

A. The Cisco ASA can be configured for high availability, whereas the Cisco IOS router with Zone-Based Policy Firewall cannot. B. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability, whereas the Cisco ASA cannot. C. The Cisco ASA denies all traffic by default, whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces. D. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas Cisco ASA starts out by allowing traffic until rules are added.

upvoted 1 times

Demon_Queen_Velverosa 1 year, 11 months ago

First the question asks us the difference between an ASA and a Cisco IOS “router” with a zone-based policy firewall. The first hint is CISCO IOS router and the second hint is ASA firewall. However they are only saying the IOS router has the zone-based policy firewall feature and did not say the IOS router is currently using zone-based firewall functionality. They state "IOS router With Zone-based policy firewall" and did not say IOS router configured with zone-based policy firewall.

upvoted 1 times

Demon_Queen_Velverosa 1 year, 11 months ago

Answers cannot be A or B as this is a firewall and a router making me surprised if they could not be used for high availability. The answer cannot be D as we are dealing with two different devices that are not the same. A firewall explicit device (ASA) and a router device (IOS) but it has extra features aka firewall. a firewall by default will have an implicit deny which is the ASA, but a IOS router? It would not have an implicit deny. why? Because, it is still a router when you pull it out of the box and routing is the primary function of a router. Thus you will need to enable or utilize the zone-based firewall policy feature in order for firewall rules to start to apply. Don't let the words "firewall" or "zone-based policy firewall".

Now the Demon Queen will go drink some wine and continue planning for world domination.

upvoted 2 times

Premium_Pils 1 year, 10 months ago

https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router. https://networklessons.com/cisco/asa-firewall/cisco-asa-access-list Without any access-lists, the ASA will allow traffic from a higher security level to a lower security level https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/217679-asa-access-control-list-configuration-ex.html By default, traffic that passes from a lower security level interface to a higher security level interface is denied whereas traffic from a higher security level interface to a lower security level interface is allowed. This behavior can also be overridden with an ACL. D) is the closest answer.

upvoted 2 times

Silexis 7 months ago

It is actually NOT due to the keyword "all". In IOS ZBFR, traffic between same-zone interfaces are allowed!!! I will vote for A, due to the fact that in real life, Cisco ASA supports stateful failover while such a mechanism cannot be accomplished on a CIsco IOS Router. The question is about "functional difference"

upvoted 1 times

luismg 1 year, 11 months ago

Selected Answer: D

D IOS router denies traffic by default ASA it depends of the security level on the interface.

upvoted 1 times

Premium_Pils 2 years ago

Selected Answer: D

Based on my work experience with both ZFW and ASA, by default no traffic is allowed to pass between zones. Whereas ASA allows traffic from high level security interfaces to low level security interfaces by default.

upvoted 1 times

XvidalX 2 years, 5 months ago

Selected Answer: D

D is correct - ASA starts perminting higher security level interface to access any ohter security level interfaces by default , until a access list applied

upvoted 2 times

red_sparrow_Gr 2 years, 8 months ago

Selected Answer: D

correct id D https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html#anc11

search for the following : ZFW default policy between zones is deny all. If no policy is explicitly configured, all traffic that moves between zones is blocked.

upvoted 2 times

XvidalX 2 years, 5 months ago

ZFW default policy between zones is deny all. If no policy is explicitly configured, all traffic that moves between zones is blocked <----------

upvoted 2 times

kylesam2017 2 years, 8 months ago

"C" is the correct answer. Here is the link: "One difference is that the IOS router starts out by allowing all traffic [on your untrusted interfaces], where as the ASA starts by denying all traffic. Consequently you have to configure the actual hardening of your IOS router. "

https://community.cisco.com/t5/network-security/ios-firewall-vs-asa/td-p/2133822#:~:text=One%20difference%20is%20that%20the,hardening%20of%20your%20IOS%20router.

upvoted 4 times

red_sparrow_Gr 2 years, 9 months ago

Selected Answer: C

Cisco ASA vs IOS Router with Zone-Based Firewall Some prefer to have a single device do both routing and security, but others opt for dedicated security devices. The ASA denies all traffic by default, while the IOS router starts out by allowing all traffic, even on your untrusted interfaces.

upvoted 1 times

Pakawat 2 years, 11 months ago

Selected Answer: C

C https://community.cisco.com/t5/network-security/ios-firewall-vs-asa/td-p/2133822

upvoted 2 times

fdl543 3 years ago

Selected Answer: D

D. "even on untrusted" kills alternative C...

upvoted 2 times

Cokamaniako 3 years, 1 month ago

Selected Answer: C

The ASA denies all traffic by default, while the IOS router starts out by allowing all traffic, even on your untrusted interfaces. You can eliminate this disadvantage, however, by hardening your router.

upvoted 2 times

zamkljo 3 years, 1 month ago

C https://www.linkedin.com/pulse/cisco-zone-based-firewall-reporting-anna-mcelhany/

upvoted 3 times

Jessie45785 3 years, 4 months ago

Selected Answer: D

C - is not correct:

All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router.

https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html

only D make sense

upvoted 3 times

Question #141 *Topic 1*

An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1.1.1.1 using the flow record Stealthwatch406143794 command. Which additional command is required to complete the flow record?

A. cache timeout active 60

B. destination 1.1.1.1

C. match ipv4 ttl

D. transport udp 2055

Suggested Answer: *C*

Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/config-trouble-netflow-stealth.pdf

Community vote distribution

C (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

C. match ipv4 ttl

upvoted 1 times

psuoh 2 years ago

https://www.networkingwithehsan.com/cisco-stealthwatch-netflow-configuration https://i.imgur.com/xKO1BYq.png FLOW RECORD command allows MATCH https://i.imgur.com/eCXKsRm.png

upvoted 2 times

nomanlands 2 years, 7 months ago

May have a mistype in the answer but flow records are made of match and collect commandsExample shows how to configure version 9 export for Flexible NetFlow. ! flow exporter EXPORTER-1 destination 172.16.10.2 export-protocol netflow-v9 transport udp 90 exit ! flow record v4_r1 match ipv4 tos match ipv4 protocol match ipv4 source address match ipv4 destination address match transport source-port match transport destination-port collect counter bytes long collect counter packets long ! flow monitor FLOW-MONITOR-1 record v4_r1 exporter EXPORTER-1 ! ip cef ! interface GigabitEthernet 0/0/0 ip address 172.16.6.2 255.255.255.0 ip flow monitor FLOW-MONITOR-1 input https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnf-v9-export.htmlSo C is correct: match ipv4 ttl Exporter = specifications of NetFlow protocol parameters and dest. IP of Collector. Record = specifications of information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. “match” and “collect” commands tell which fields to include in the outgoing NetFlow PDU. “match” = key fields used to determine the uniqueness of the flow. “collect” = extra fields to include for more detail to the collector for reporting and analysis. Monitor = pairs Record with Exporter and is applied to network interface from which we want to collect NetFlow statistics & data. https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf

upvoted 3 times

nomanlands 2 years, 7 months ago

Selected Answer: C

May have a mistype in the answer but flow records are made of match and collect commands

upvoted 3 times

NikoNiko 2 years, 7 months ago

Example shows how to configure version 9 export for Flexible NetFlow. ! flow exporter EXPORTER-1 destination 172.16.10.2 export-protocol netflow-v9 transport udp 90 exit ! flow record v4_r1 match ipv4 tos match ipv4 protocol match ipv4 source address match ipv4 destination address match transport source-port match transport destination-port collect counter bytes long collect counter packets long ! flow monitor FLOW-MONITOR-1 record v4_r1 exporter EXPORTER-1 ! ip cef ! interface GigabitEthernet 0/0/0 ip address 172.16.6.2 255.255.255.0 ip flow monitor FLOW-MONITOR-1 input

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnf-v9-export.html

upvoted 3 times

NikoNiko 2 years, 7 months ago

Example shows how to configure version 9 export for Flexible NetFlow. ! flow exporter EXPORTER-1 destination 172.16.10.2 export-protocol netflow-v9 transport udp 90 exit ! flow record v4_r1 match ipv4 tos match ipv4 protocol match ipv4 source address match ipv4 destination address match transport source-port match transport destination-port collect counter bytes long collect counter packets long ! flow monitor FLOW-MONITOR-1

record v4_r1 exporter EXPORTER-1 ! ip cef ! interface GigabitEthernet 0/0/0 ip address 172.16.6.2 255.255.255.0 ip flow monitor FLOW-MONITOR-1 input https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnf-v9-export.htmlSo C is correct: match ipv4 ttl Exporter = specifications of NetFlow protocol parameters and dest. IP of Collector. Record = specifications of information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. “match” and “collect” commands tell which fields to include in the outgoing NetFlow PDU. “match” = key fields used to determine the uniqueness of the flow. “collect” = extra fields to include for more detail to the collector for reporting and analysis. Monitor = pairs Record with Exporter and is applied to network interface from which we want to collect NetFlow statistics & data. https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf

upvoted 4 times

NikoNiko 2 years, 7 months ago

So C is correct: match ipv4 ttl Exporter = specifications of NetFlow protocol parameters and dest. IP of Collector. Record = specifications of information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. “match” and “collect” commands tell which fields to include in the outgoing NetFlow PDU. “match” = key fields used to determine the uniqueness of the flow. “collect” = extra fields to include for more detail to the collector for reporting and analysis. Monitor = pairs Record with Exporter and is applied to network interface from which we want to collect NetFlow statistics & data. https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf

upvoted 2 times

otzu1 2 years, 9 months ago

is ttl a legit parameter tho?

upvoted 1 times

otzu1 2 years, 9 months ago

is ttl a legit parameter tho?yes, it is valid sw3X50(config)# flow record LANCOPE1 sw3X50(config-flow-record)# description NetFlow record for StealthWatch sw3X50(config-flow-record)# match datalink mac source address input sw3X50(config-flow-record)# match datalink mac destination address input sw3X50(config-flow-record)# match ipv4 ttl
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf

upvoted 1 times

NikoNiko 2 years, 7 months ago

yes, it is valid sw3X50(config)# flow record LANCOPE1 sw3X50(config-flow-record)# description NetFlow record for StealthWatch sw3X50(config-flow-record)# match datalink mac source address input sw3X50(config-flow-record)# match datalink mac destination address input sw3X50(config-flow-record)# match ipv4 ttl https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf

upvoted 2 times

Smileebloke 2 years, 9 months ago

B

Once the Flow Record has been created you would tie it to a Flow Exporter. Flow Exporter configuration defines the physical or virtual Flow Collector IP Address to which NetFlow data is sent. It also defines the source interface from which the Flow Exporter device will send NetFlow data, this can be a physical or logical address; it is also worth considering using a Loopback interface to source NetFlow data from as a Loopback typically will remain up even when other interfaces fail therefore enabling continuous transport (where routing permits) This is also where the transport protocol (TCP or UDP) and destination port is defined; the destination port is specific to the NetFlow Collector and in this case refers to the port used by the Stealthwatch Flow Collector. To define a Flow Exporter, follow these steps: flow exporter Stealthwatch_Exporter description Stealthwatch Export to Flow Collector destination [Collector_IP_Address] source [Physical_Interface | Logical_Interface] transport udp 2055

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/config-trouble-netflow-stealth.pdf

upvoted 2 times

Smileebloke 2 years, 9 months ago

B Once the Flow Record has been created you would tie it to a Flow Exporter. Flow Exporter configuration defines the physical or virtual Flow Collector IP Address to which NetFlow data is sent. It also defines the source interface from which the Flow Exporter device will send NetFlow data, this can be a physical or logical address; it is also worth considering using a Loopback interface to source NetFlow data from as a Loopback typically will remain up even when other interfaces fail therefore enabling continuous transport (where routing permits) This is also where the transport protocol (TCP or UDP) and destination port is defined; the destination port is specific to the NetFlow Collector and in this case refers to the port used by the Stealthwatch Flow Collector. To define a Flow Exporter, follow these steps: flow exporter Stealthwatch_Exporter description Stealthwatch Export to Flow Collector destination [Collector_IP_Address] source [Physical_Interface | Logical_Interface] transport udp 2055
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/config-trouble-netflow-stealth.pdfIgnore previous comment C: flow record Stealthwatch_FlowRecord description Flow Record for Export to Stealthwatch (optional) match ipv4 source address match ipv4 destination address match ipv4 protocol match ipv4 tos match transport source-port match transport destination-port match interface input match flow direction collect routing next-hop address ipv4 collect ipv4 dscp collect ipv4 ttl minimum collect ipv4 ttl maximum collect transport tcp flags collect interface

output collect counter bytes collect counter packets collect timestamp sys-uptime first collect timestamp sys-uptime lasthttps://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/command/fnf-cr-book/fnf-m1.html#wp8173096590

upvoted 2 times

Smileebloke Highly Voted 2 years, 9 months ago

Ignore previous comment C: flow record Stealthwatch_FlowRecord description Flow Record for Export to Stealthwatch (optional) match ipv4 source address match ipv4 destination address match ipv4 protocol match ipv4 tos match transport source-port match transport destination-port match interface input match flow direction collect routing next-hop address ipv4 collect ipv4 dscp collect ipv4 ttl minimum collect ipv4 ttl maximum collect transport tcp flags collect interface output collect counter bytes collect counter packets collect timestamp sys-uptime first collect timestamp sys-uptime lasthttps://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/command/fnf-cr-book/fnf-m1.html#wp8173096590

upvoted 5 times

Smileebloke Highly Voted 2 years, 9 months ago

Ignore previous comment

C:

flow record Stealthwatch_FlowRecord description Flow Record for Export to Stealthwatch (optional) match ipv4 source address match ipv4 destination address match ipv4 protocol match ipv4 tos match transport source-port match transport destination-port match interface input match flow direction collect routing next-hop address ipv4 collect ipv4 dscp collect ipv4 ttl minimum collect ipv4 ttl maximum collect transport tcp flags collect interface output collect counter bytes collect counter packets collect timestamp sys-uptime first collect timestamp sys-uptime last

upvoted 5 times

Smileebloke 2 years, 9 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/command/fnf-cr-book/fnf-m1.html#wp8173096590

upvoted 4 times

Question #142 *Topic 1*

An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE. The engineer wants to authenticate users using their account when they log into network devices. Which action accomplishes this task?

A. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within Cisco ISE.

B. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE.

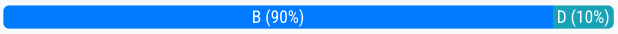
C. Modify the current policy with the condition MFA: SourceSequence:DUO=true in the authorization conditions within Cisco ISE.

D. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO.

Suggested Answer: *B*

Reference: https://duo.com/docs/authproxy-reference

Community vote distribution



nomanlands Highly Voted 2 years, 1 month ago

Selected Answer: B

B is the correct answer. You would have to authenticate first successfully before DUO is triggered for MFA, DUO would not handle authentication directly.

upvoted 5 times

nomanlands Highly Voted 2 years, 1 month ago

B is the correct answer. You would have to authenticate first successfully before DUO is triggered for MFA, DUO would not handle authentication directly.Yes, B is correct. Scheme & explanation: https://community.cisco.com/t5/security-knowledge-base/duo-mfa-integration-with-ise-for-tacacs-device-administration/ta-p/3881767 DUO scheme: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214813-configure-duo-two-factor-authentication.html A - "configure DUO external Active Directory connector + tie it to the policy set within Cisco ISE" - DUO uses own Authentication Proxy server, which connects to AD (not called "AD connector") and more importantly - it is impossible to configure ISE policy with DUO AD connector. Nonsense. In policy can be used only "AD connector", which is ISE connection to AD (i. e. AD Join Point) but it has nothing to do with DUO. C - not existing condition in ISE https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_segmentation.html#ID37 D - nonsense, ISE doesn't have any Identity Policy as I know (I also Googled it for sure)

upvoted 5 times

NikoNiko 2 years, 1 month ago

Yes, B is correct. Scheme & explanation: https://community.cisco.com/t5/security-knowledge-base/duo-mfa-integration-with-ise-for-tacacs-device-administration/ta-p/3881767 DUO scheme: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214813-configure-duo-two-factor-authentication.html A - "configure DUO external Active Directory connector + tie it to the policy set within Cisco ISE" - DUO uses own Authentication Proxy server, which connects to AD (not called "AD connector") and more importantly - it is impossible to configure ISE policy with DUO AD connector. Nonsense. In policy can be used only "AD connector", which is ISE connection to AD (i. e. AD Join Point) but it has nothing to do with DUO. C - not existing condition in ISE https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_segmentation.html#ID37 D - nonsense, ISE doesn't have any Identity Policy as I know (I also Googled it for sure)

upvoted 3 times

CyberGhost666 Most Recent 1 year, 1 month ago

B. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE.

upvoted 1 times

sis_net_sec 1 year, 10 months ago

https://community.cisco.com/t5/security-documents/duo-mfa-integration-with-ise-for-tacacs- device-administration/ta-p/3881767

upvoted 3 times

wenorex222 2 years, 2 months ago

The correct answer should be d.

upvoted 1 times

Question #143 *Topic 1*

What is the function of the crypto isakmp key cisc406143794 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel?

A. It prevents all IP addresses from connecting to the VPN server.

B. It configures the pre-shared authentication key.

C. It configures the local address for the VPN server.

D. It defines what data is going to be encrypted via the VPN.

Suggested Answer: *B*

This command is used to configure pre-shared-key for IPsec remote acess users on the Cisco router. Address is mentioned as 0.0.0.0 0.0.0.0 because the users will be connecting from random ip addresses and it is almost impossible to mention all the ip addresses. Hence, 0.0.0.0 0.0.0.0 is used to allow all public ip addresses.

Community vote distribution

B (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: B

Correct Answer is B.

upvoted 1 times

Orez1589 2 years, 1 month ago

They really like to ask this question ^^

upvoted 4 times

Question #144 *Topic 1*

An administrator is adding a new switch onto the network and has configured AAA for network access control. When testing the configuration, the RADIUS authenticates to Cisco ISE but is being rejected. Why is the ip radius source-interface command needed for this configuration?

A. Only requests that originate from a configured NAS IP are accepted by a RADIUS server.

B. The RADIUS authentication key is transmitted only from the defined RADIUS source interface.

C. RADIUS requests are generated only by a router if a RADIUS source interface is defined.

D. Encrypted RADIUS authentication requires the RADIUS source interface be defined.

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfrad.html#wp1027454

Community vote distribution

A (100%)

loser4fun Highly Voted 2 years, 5 months ago

I would go with A When configuring AAA for network access control, the ip radius source-interface command is needed to specify the interface that the switch uses to send RADIUS requests to the server. The source interface is important because it determines the IP address that is used as the NAS-IP-Address attribute in the RADIUS packet. If the RADIUS server is configured to only accept requests that originate from a specific NAS IP address, then the switch must use that address as the source for its requests, or the authentication will fail. This is often the case in enterprise networks where strict access controls are in place. Therefore, the ip radius source-interface command is needed to ensure that the switch sends RADIUS requests from the correct IP address and that the RADIUS server will accept them. Without this command, the authentication may fail or be rejected by the RADIUS server.

upvoted 7 times

CyberGhost666 Most Recent 1 year, 1 month ago

A) ISE uses the NAS IP to match policies and shared secrets.

upvoted 2 times

Ko13 1 year, 9 months ago

The RADIUS NAS-IP-Address Attribute Configurability feature allows you to configure an arbitrary IP address to be used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets. This feature may be used for situations in which service providers are using a cluster of small network access servers (NASs) to simulate a large NAS to improve scalability. This feature allows the NASs to behave as a single RADIUS client from the perspective of the RADIUS server.

https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/12_2sba/feature/guide/sbsiara.html

upvoted 2 times

Tutsi 3 years, 1 month ago

When the Radius policy is configured on the radius server, to prevent unauthorised devices from matching the policy, NAS IP can be specified within the policy. I do this configuration very often...

upvoted 2 times

Cyberops 3 years, 3 months ago

I would go with B. It says Network Access control not Server.Not sure on this one. Couldn't delete my previous comment but i would have if i could.

upvoted 1 times

Cyberops 3 years, 3 months ago

I would go with B.

It says Network Access control not Server.

upvoted 1 times

Cyberops 3 years, 3 months ago

Not sure on this one. Couldn't delete my previous comment but i would have if i could.

upvoted 1 times

Question #145 *Topic 1*

Which statement about the configuration of Cisco ASA NetFlow v9 Secure Event Logging is true?

A. To view bandwidth usage for NetFlow records, the QoS feature must be enabled.

B. A sysopt command can be used to enable NSEL on a specific interface.

C. NSEL can be used without a collector configured.

D. A flow-export event type must be defined under a policy.

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

I'll go with D. A flow-export event type must be defined under a policy.

upvoted 1 times

Edy79 1 year, 10 months ago

Answer D Prerequisites for NSEL NSEL has the following prerequisites: IP address and hostname assignments must be unique throughout the NetFlow configuration. You must have at least one configured collector before you can use NSEL. You must configure NSEL collectors before you can configure filters via Modular Policy Framework.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_nsel.html#87790

upvoted 1 times

Thusi26 3 years, 11 months ago

D it is

upvoted 4 times

Question #146 *Topic 1*

Which feature requires a network discovery policy on the Cisco Firepower NGIPS?

A. security intelligence

B. impact flags

C. health monitoring

D. URL filtering

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

yenp Highly Voted 2 years, 7 months ago
B right answer as One of the most valuable analysis tools is the impact flag indicator. You will see impact flag calculated for your intrusion events. To help you evaluate the impact that an event has on your network, the Cisco FMC displays an impact level in the table view of intrusion events. For each event, the system adds an impact level icon, whose color indicates the correlation between intrusion data, network discovery data, and vulnerability information
upvoted 16 times

CyberGhost666 Most Recent 1 year, 1 month ago
Impact Flags in Cisco Firepower NGIPS (Next-Generation Intrusion Prevention System) are used to indicate how critical or impactful a threat is to the network. This requires a Network Discovery Policy.
upvoted 1 times

otzu1 1 year, 9 months ago
You can configure the system to alert you whenever an intrusion event with a specific impact flag occurs. Impact flags help you evaluate the impact an intrusion has on your network by correlating intrusion data, network discovery data, and vulnerability information.
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/external_alerting_with_alert_responses.html#ID-2197-00000299
upvoted 1 times

brownbear505 1 year, 12 months ago
Because of the Network Discovery Policy you gain the use of impact flags to evaluate the severity that intrusion events have on your network. That knowledge makes possible the ability to tune intrusion rule states so that they provide maximum protection for your network assets.
upvoted 1 times

NullNull88 2 years, 2 months ago
B is correct for this one
upvoted 1 times

Raajaa 2 years, 7 months ago
B is the answer
upvoted 1 times

bazinga31 2 years, 8 months ago
i believe its B
upvoted 1 times

deathfrom 2 years, 8 months ago
B https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3300.pdf
upvoted 4 times

Question #147 *Topic 1*

Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

A. correlation

B. intrusion

C. access control

D. network discovery

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

The Network Discovery Policy on Cisco Firepower NGIPS is specifically designed to capture host information by passively monitoring network traffic. This includes: • Host IP addresses • Operating systems • Applications • Users • Ports and protocols This information allows Firepower to build a network map, which is crucial for context-aware security (e.g., assigning impact flags to intrusion events).

upvoted 1 times

Question #148 *Topic 1*

What is a characteristic of traffic storm control behavior?

A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.

B. Traffic storm control cannot determine if the packet is unicast or broadcast.

C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.

D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/12-1E/configuration/guide/storm.html

Community vote distribution

A (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval

upvoted 1 times

NikoNiko 2 years, 1 month ago

Storm Control behavior:

•If you enable broadcast traffic storm control, and broadcast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast traffic until the end of the traffic storm control interval.

•If you enable broadcast and multicast traffic storm control, and the COMBINED BROADCAST and MULTICAST traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control DROPS ALL BROADCAST and MULTICAST traffic until the end of the traffic storm control interval.

•If you enable broadcast and multicast traffic storm control, and broadcast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval.

•If you enable broadcast and multicast traffic storm control, and multicast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval. Default Traffic Storm Control Configuration

https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/storm.html

upvoted 2 times

NikoNiko 2 years, 1 month ago

Storm Control behavior: •If you enable broadcast traffic storm control, and broadcast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast traffic until the end of the traffic storm control interval. •If you enable broadcast and multicast traffic storm control, and the COMBINED BROADCAST and MULTICAST traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control DROPS ALL BROADCAST and MULTICAST traffic until the end of the traffic storm control interval. •If you enable broadcast and multicast traffic storm control, and broadcast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval. •If you enable broadcast and multicast traffic storm control, and multicast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval. Default Traffic Storm Control Configuration
https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/storm.htmlSo correct is A - Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.

upvoted 2 times

NikoNiko 2 years, 1 month ago

So correct is A - Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.

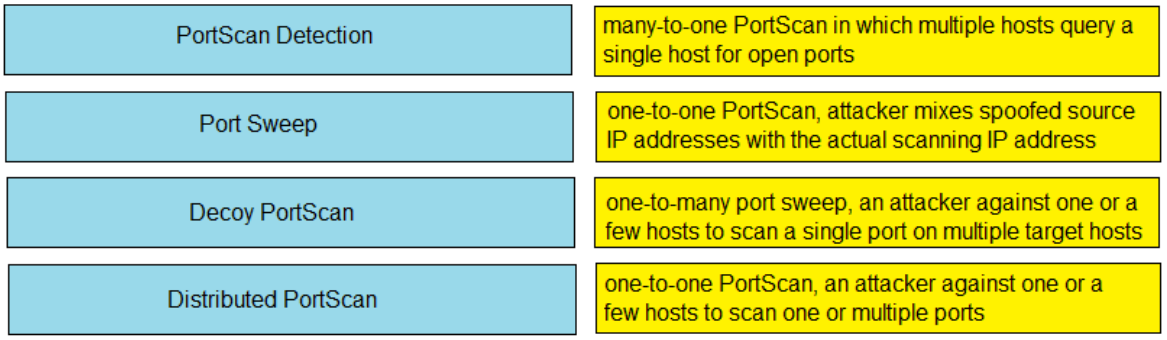
upvoted 4 times

Question #149 *Topic 1*

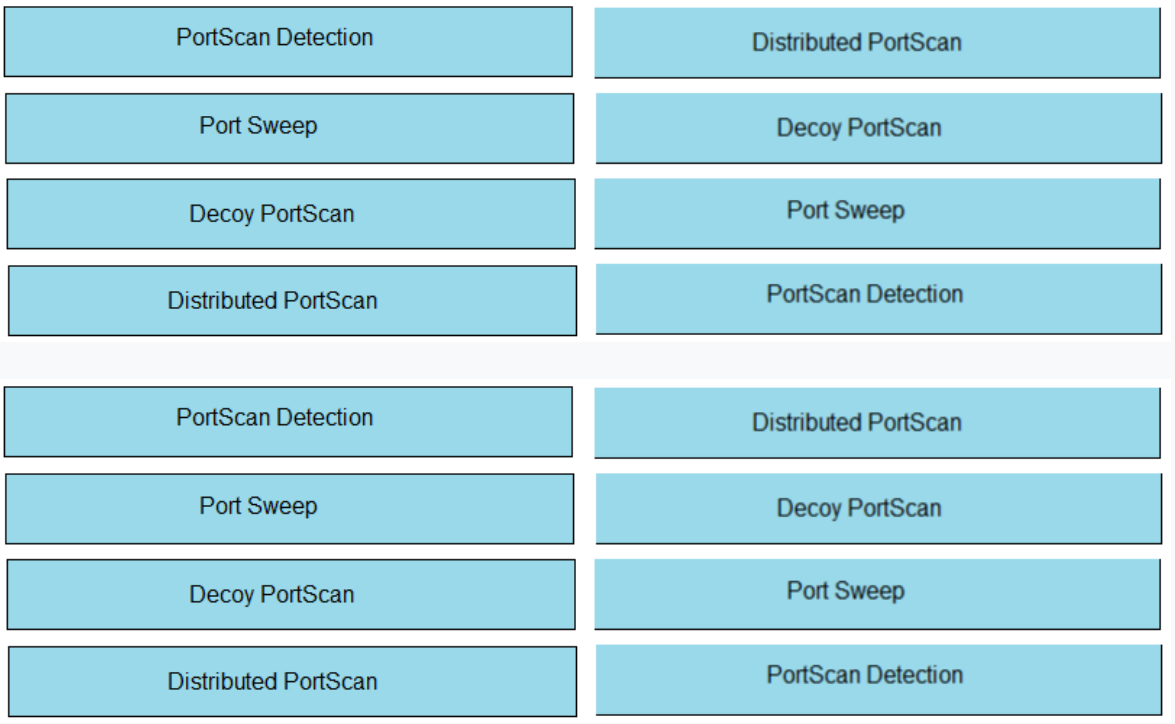
DRAG DROP -

Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

Select and Place:



Suggested Answer:



Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/detecting_specific_threats.html

otzu1 Highly Voted 1 year, 9 months ago

PortScan Detection Keyword "portscan" Port Sweep Keyword "sweep" Decoy PortScan Keyword "Spoofed" Distributed PortScan Keyword "many-to-one"

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Detecting_Specific_Threats.html#ID-2236-000000bb

upvoted 12 times

Question #150 *Topic 1*

Refer to the exhibit. Which statement about the authentication protocol used in the configuration is true?

```
aaa new-model

radius-server host 10.0.0.12 key secret12
```

A. The authentication request contains only a password

B. The authentication request contains only a username

C. The authentication and authorization requests are grouped in a single packet.

D. There are separate authentication and authorization request packets.

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

testtaker42 Highly Voted 4 years, 1 month ago

C does seem to be the most correct. "RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization." Source: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

upvoted 12 times

CyberGhost666 Most Recent 1 year, 1 month ago

C. The authentication and authorization requests are grouped in a single packet.

upvoted 1 times

kwong328 1 year, 11 months ago

Correct answer is C, "In RADIUS, authentication and authorization are coupled together" https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html You can find the answer in the "RADIUS Authentication and Authorization Sequence" diagram

upvoted 2 times

NikoNiko 2 years, 7 months ago

RADIUS open standard protocol It uses UDP as a transmission protocol It uses UDP port number 1812 for authentication and authorization and 1813 for accounting. Authentication and Authorization are COMBINED in RADIUS. Only the password is encrypted while the other information such as username, accounting information, etc are not encrypted. No external authorization of commands is supported. No multiprotocol support. Used for network access

upvoted 3 times

Raajaa 3 years, 7 months ago

Answer is C

upvoted 4 times

Question #151 *Topic 1*

Which deployment model is the most secure when considering risks to cloud adoption?

A. public cloud

B. hybrid cloud

C. community cloud

D. private cloud

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Raajaa Highly Voted 3 years, 7 months ago

D is the answer

upvoted 5 times

CyberGhost666 Most Recent 1 year, 1 month ago

Correct Option is D. The Private Cloud model is considered the most secure because: • It is dedicated to a single organization. • Offers greater control over data, infrastructure, and security policies. • Can be hosted on-premises or in a dedicated off-premises environment. • Reduces the risk of data leakage or multi-tenancy vulnerabilities present in public cloud models.

upvoted 1 times

hdrnzienlaoroljol 1 year, 9 months ago

D is the answer

upvoted 1 times

Question #152 *Topic 1*

What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?

A. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously.

B. It discovers and controls cloud apps that are connected to a company's corporate environment.

C. It deletes any application that does not belong in the network.

D. It sends the application information to an administrator to act on.

Suggested Answer: *B*

Reference: https://www.cisco.com/c/en/us/products/security/cloudlock/index.html#~features

Community vote distribution

B (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

Correct option is B.

upvoted 1 times

abdulmalik_mail 2 years, 1 month ago

It's B The Cloudlock Apps Firewall discovers and controls cloud apps connected to your corporate environment

https://www.cisco.com/c/en/us/products/security/cloudlock/index.html

upvoted 4 times

Question #153 *Topic 1*

Which exfiltration method does an attacker use to hide and encode data inside DNS requests and queries?

A. DNS tunneling

B. DNSCrypt

C. DNS security

D. DNSSEC

Suggested Answer: *A*

Reference: https://learn-umbrella.cisco.com/cloud-security/dns-tunneling

Community vote distribution

A (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

A) DNS tunneling is a technique attackers use to hide stolen data inside DNS requests. Since DNS traffic is usually allowed through firewalls, they sneak data out of a network by encoding it inside DNS queries.

upvoted 1 times

abdulmalik_mail 2 years, 1 month ago

It's A DNS tunneling can establish command and control. Or, it can exfiltrate data. https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/

upvoted 2 times

Question #154 *Topic 1*

Which technology reduces data loss by identifying sensitive information stored in public computing environments?

A. Cisco SDA

B. Cisco Firepower

C. Cisco HyperFlex

D. Cisco Cloudlock

Suggested Answer: *D*

Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloudlock/cisco-cloudlock-cloud-data-security-datasheet.pdf

Community vote distribution

D (100%)

abdulmalik_mail Highly Voted 2 years, 1 month ago

It's D Cloudlock's data loss prevention (DLP) technology continuously monitors cloud environments to detect and secure sensitive information.
https://www.cisco.com/c/en/us/products/security/cloudlock/index.html#~features

upvoted 6 times

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: D

D) if you're trying to secure sensitive info in the cloud, the tool you want is Cisco Cloudlock.

upvoted 1 times

Question #155 *Topic 1*

In which cloud services model is the tenant responsible for virtual machine OS patching?

A. IaaS

B. UCaaS

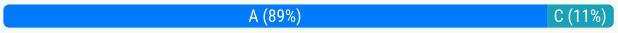
C. PaaS

D. SaaS

Suggested Answer: *A*

Reference: https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php

Community vote distribution



CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: A

Option A is correct.

upvoted 1 times

Cokamaniako 2 years, 1 month ago

Selected Answer: A

Infrastructure as a Service (IaaS)

To deploy your applications to the Cloud, you have to install OS images and relatedapplication software on the cloud infrastructure. In this model, it'syour responsibility to patch/update/maintain the OSand any application software you install.

Answer A

upvoted 1 times

loser4fun 2 years, 5 months ago

I believe the conflict here came from the responsibility For first sight I thought it's C as in PaaS you own the OS, but in fact vendor handing over OS but you use it for your own application, so you're responsible for Application only

On the other hand IaaS you have the Infra including OS, but you're responsible for everything including OS patching.

If the question was about what model where you have OS then it's PaaS

The correct answer is A

upvoted 2 times

Emlia1 2 years, 7 months ago

Selected Answer: A

A is correct

upvoted 2 times

FortiSherlock 3 years ago

IaaS cannot be wrong, because it is the model where you are responsible for most of the things. Only hardware patching is cloud responsibility. So all the people who say PaaS is correct - it might be an ADDITIONAL answer for you, but everything you are responsible for in PaaS you are also responsible for in IaaS.

upvoted 1 times

nomanlands 3 years, 1 month ago

Selected Answer: A

IaaS is the only one where you are responsible for the OS

upvoted 2 times

Jardator 3 years, 3 months ago

tenant is key-word so Cisco again, sorry its A

upvoted 1 times

Jardator 3 years, 3 months ago

Selected Answer: C

IaaS: In this model, it's your responsibility to patch/update/maintain the OS and any application software you install.

upvoted 1 times

asdasd123123iu 3 years, 2 months ago

So it's A (IaaS), not C.

upvoted 2 times

Sattm1 3 years, 3 months ago

Selected Answer: A

This link has a nice diagram showing the difference between infrastructure, platform and software (as a service) https://azure.microsoft.com/en-us/overview/what-is-paas/#:~:text=Platform%20as%20a%20service%20(PaaS,%2C%20cloud%2Denabled%20enterprise%20applications.

upvoted 2 times

abdulmalik_mail 3 years, 7 months ago

It's A SAAS = Application like SharePoint online, O365 PAAS = Operating system like Windows Azure, Database like SQL Azure IAAS = Windows Azure Virtual Machine and Network, Storage https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php (same link with admin reference)

upvoted 2 times

Question #156 *Topic 1*

What is the function of Cisco Cloudlock for data security?

A. data loss prevention

B. controls malicious cloud apps

C. detects anomalies

D. user and entity behavior analytics

Suggested Answer: *A*

Reference: https://umbrella.cisco.com/products/casb

Community vote distribution

A (100%)

bobby14 Highly Voted 5 years, 6 months ago

Cloudlock use DLP to prevent data exfiltrate to internet.

upvoted 12 times

Demon_Queen_Velverosa Most Recent 1 year, 11 months ago

Remember This question explicitly mentions data security as the want to know. Thus It can only be A as that answer has to do with data loss which is data security. the other questions don't have anything to do with data security.

upvoted 2 times

Ko13 2 years, 9 months ago

https://www.cisco.com/c/en/us/products/security/cloudlock/index.html#~features Data security Cloudlock's data loss prevention (DLP) technology continuously monitors cloud environments to detect and secure sensitive information. It provides countless out-of-the-box policies as well as highly tunable custom policies.

upvoted 1 times

ExamMoney 5 years, 7 months ago

Such a bad question. Cloudlock can provide all the services mentioned in the question and all of them can offer data security whether directly or indirectly.In the reference link, under the Data Security section, it specifically states: "Protect against exposures and a data security breach with highly-configurable data loss prevention engine with automated, policy-driven response actions" While you're correct (it IS a terrible question), given the specific context of the question, answer "A" is correct.

upvoted 1 times

ExamMoney 5 years, 7 months ago

Such a bad question. Cloudlock can provide all the services mentioned in the question and all of them can offer data security whether directly or indirectly.

upvoted 1 times

bigdadzzz Highly Voted 5 years, 7 months ago

In the reference link, under the Data Security section, it specifically states: "Protect against exposures and a data security breach with highly-configurable data loss prevention engine with automated, policy-driven response actions" While you're correct (it IS a terrible question), given the specific context of the question, answer "A" is correct.

upvoted 10 times

Question #157 *Topic 1*

Which feature is supported when deploying Cisco ASAv within AWS public cloud?

A. multiple context mode

B. user deployment of Layer 3 networks

C. IPv6

D. clustering

Suggested Answer: *B*

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96-qsg/asav-aws.html

Community vote distribution

B (100%)

abdulmalik_mail Highly Voted 3 years, 7 months ago

Yes It's B. The ASAv on AWS supports the following features: 1. Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instance family. 2.Deployment in the Virtual Private Cloud (VPC) 3.Enhanced networking (SR-IOV) where available 4.Deployment from Amazon Marketplace 5.Maximum of four vCPUs per instance 6.User deployment of L3 networks 7.Routed mode (default)

upvoted 8 times

DWizard Most Recent 2 years, 1 month ago

The right option is B, here are listed the unsupported features which include IPv6, clustering and multiple context mode: https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/asav/quick-start-book/asav-910-qsg/asav_aws.html#id_45810

upvoted 2 times

Question #158 *Topic 1*

Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

A. PaaS

B. XaaS

C. IaaS

D. SaaS

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Thusi26 Highly Voted 4 years, 8 months ago

It's PaaS PaaS Platform-as-a-service (PaaS) is another step further from full, on-premise infrastructure management. It is where a provider hosts the hardware and software on its own infrastructure and delivers this platform to the user as an integrated solution, solution stack, or service through an internet connection.

upvoted 10 times

Demon_Queen_Velverosa Most Recent 1 year, 11 months ago

what is XaaS? XaaS (Anything-as-a-Service) is an umbrella term that refers to the delivery of products, services, or resources as a service over the internet.

upvoted 1 times

Emlia1 3 years, 7 months ago

A is correct

upvoted 1 times

Thusi26 4 years, 8 months ago

SaaS Software-as-a-service (SaaS), also known as cloud application services, is the most comprehensive form of cloud computing services, delivering an entire application that is managed by a provider, via a web browser

upvoted 1 times

Thusi26 4 years, 8 months ago

SaaS Software-as-a-service (SaaS), also known as cloud application services, is the most comprehensive form of cloud computing services, delivering an entire application that is managed by a provider, via a web browserPaaS is the correct answer. With SaaS, the customer will only use the application, they won't have to develop nor deploy anything.

upvoted 1 times

pr0fectus Highly Voted 4 years, 7 months ago

PaaS is the correct answer. With SaaS, the customer will only use the application, they won't have to develop nor deploy anything.

upvoted 15 times

Question #159 *Topic 1*

Which risk is created when using an Internet browser to access cloud-based service?

A. misconfiguration of Infra, which allows unauthorized access

B. intermittent connection to the cloud connectors

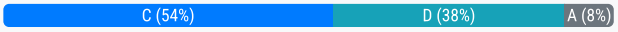
C. vulnerabilities within protocol

D. insecure implementation of API

Suggested Answer: *C*

Official Answer: C

Community vote distribution



zheka Highly Voted 4 years, 8 months ago

Disagree with protocol vulnerabilities. The answer is about insecure implementation of API https://www.imperva.com/blog/top-10-cloud-security-concerns/API and Internet Browser? Definetly not!Agreed as stated the user is using a Web browser thus it cannot be API, the correct answer is C

upvoted 9 times

zheka Highly Voted 4 years, 8 months ago

Disagree with protocol vulnerabilities. The answer is about insecure implementation of API https://www.imperva.com/blog/top-10-cloud-security-concerns/

upvoted 9 times

dummyy 4 years, 6 months ago

API and Internet Browser? Definetly not!Agreed as stated the user is using a Web browser thus it cannot be API, the correct answer is C

upvoted 4 times

dummyy 4 years, 6 months ago

API and Internet Browser? Definetly not!

upvoted 4 times

larn 4 years, 3 months ago

Agreed as stated the user is using a Web browser thus it cannot be API, the correct answer is C

upvoted 5 times

madboy2 Most Recent 1 year, 4 months ago

When using an Internet browser to access cloud-based services, the primary risk is vulnerabilities within the communication protocols (e.g., HTTP, HTTPS, TLS, or WebSockets). Attackers can exploit these vulnerabilities through man-in-the-middle (MITM) attacks, SSL/TLS weaknesses, or browser-based exploits.

upvoted 3 times

kloug 1 year, 9 months ago

Answer c

upvoted 1 times

Premium_Pils 2 years ago

I think it is about securing APIs. A web API can be accessed via web browser. https://stackoverflow.com/questions/29105007/how-to-make-basic-rest-api-calls-using-a-browser

upvoted 1 times

4pelos 2 years, 5 months ago

Correct answer C. Checked with securitytut

upvoted 1 times

xziomal9 2 years, 9 months ago

Answer D

upvoted 1 times

zamkljo 3 years, 1 month ago

insecure API: A malicious user gained access to an organization's database from a cloud-base application programming interface that lacked strong authentication control. (from 350 - 701 practice exam)

upvoted 2 times

stalkr3 3 years, 4 months ago

another showcase question why Cisco exams are utter garbage.

upvoted 3 times

Tuxzinator 3 years, 6 months ago

Vulnerabilities within protocol: Cross-site scripting (XSS) vulnerabilities: These allow attackers to inject malicious scripts into web pages viewed by other users.

upvoted 4 times

Zatingke 3 years, 6 months ago

Should be D. A poorly designed or implemented API could allow users accessing confidential data unintentionally, e.g. with a typo in the address box of a browser. A. Wrong. Misconfiged infra, not specificly vulnerable to browsers B. Wrong. not that significant, although it is an availability issue in security perspective, but also nothing to do with a browser. C. Wrong, vulnerable within protocol? then which protocol? specific to a browser? then should be http or https, however, that also affects non-cloud-based services as well, right?

upvoted 2 times

Emlia1 3 years, 7 months ago

I prefer C

upvoted 1 times

FortiSherlock 4 years ago

VM might be publicly reachable and WebUI is weakly protected by a default password like Cisco123.

upvoted 1 times

NikoNiko 4 years, 1 month ago

A - Misconfiguration of Infra, which leads to unauthorized access is CORRECT for me --> it joins 2 most often security issues of public cloud in one answer (see link below) Question states BROWSER so API is probably not an option (D). Vulnerabilities within protocol (C) - this is not specific to cloud, PROTOCOLS are being used everywhere and they are years old tuned standards with minimum vulnerabilities. Option B - connection stability (?) --> means service availability, which is also security aspect but it is not such a big issue as option A and networks are reliable today (risk is DoS / DDoS but they are not asking about it). A is correct. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

upvoted 3 times

NikoNiko 4 years, 1 month ago

A - Misconfiguration of Infra, which leads to unauthorized access is CORRECT for me --> it joins 2 most often security issues of public cloud in one answer (see link below) Question states BROWSER so API is probably not an option (D). Vulnerabilities within protocol (C) - this is not specific to cloud, PROTOCOLS are being used everywhere and they are years old tuned standards with minimum vulnerabilities. Option B - connection stability (?) --> means service availability, which is also security aspect but it is not such a big issue as option A and networks are reliable today (risk is DoS / DDoS but they are not asking about it). A is correct. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/That is also my answer. You are responsible for configuring users and authentication / authorization for your Cloud, so if you do that in a dumb way it is insecure. Your AWS instances might be publicly reachable for SSL with a Cisco123 password - what do you think ?

upvoted 3 times

FortiSherlock 4 years ago

That is also my answer. You are responsible for configuring users and authentication / authorization for your Cloud, so if you do that in a dumb way it is insecure. Your AWS instances might be publicly reachable for SSL with a Cisco123 password - what do you think ?

upvoted 2 times

Sparrsh 4 years, 4 months ago

Answer is D

Vulnerabilities within protocols that can expose confidential data

upvoted 2 times

Sparrsh 4 years, 4 months ago

Answer is D Vulnerabilities within protocols that can expose confidential dataVulnerabilities within protocols that can expose confidential data. That is C! not D

upvoted 2 times

Iarn 4 years, 3 months ago

Vulnerabilities within protocols that can expose confidential data. That is C! not D

upvoted 3 times

Question #160 *Topic 1*

What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

A. Cisco AppDynamics

B. Cisco Cloudlock

C. Cisco Umbrella

D. Cisco AMP

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

sull3y Highly Voted 2 years ago

Cisco Cloudlock is a cloud-based security platform that helps organizations reduce the risk of data breaches and application risks in an environment that is not on-premise. It is an API-based broker that provides a comprehensive set of security controls and tools to secure data in the cloud. With Cloudlock, organizations can easily monitor and secure data in cloud-based services such as Google Apps, Microsoft Office 365, Salesforce, and more. Cloudlock uses advanced security analytics and machine learning to identify and prevent threats such as data theft, malicious insider activity, and account takeover attacks. It also provides continuous monitoring and reporting to help organizations understand their security posture and identify potential risks. By using Cloudlock, organizations can reduce the risk of compromises, application risks, and data breaches, and ensure the security of their data and systems in a cloud-based environment.it is B

upvoted 6 times

sull3y Highly Voted 2 years ago

Cisco Cloudlock is a cloud-based security platform that helps organizations reduce the risk of data breaches and application risks in an environment that is not on-premise. It is an API-based broker that provides a comprehensive set of security controls and tools to secure data in the cloud. With Cloudlock, organizations can easily monitor and secure data in cloud-based services such as Google Apps, Microsoft Office 365, Salesforce, and more.

Cloudlock uses advanced security analytics and machine learning to identify and prevent threats such as data theft, malicious insider activity, and account takeover attacks. It also provides continuous monitoring and reporting to help organizations understand their security posture and identify potential risks.

By using Cloudlock, organizations can reduce the risk of compromises, application risks, and data breaches, and ensure the security of their data and systems in a cloud-based environment.

upvoted 6 times

sull3y 2 years ago

it is B

upvoted 2 times

FortiSherlock 2 years, 6 months ago

Cloudlock is a CASB - Cloud Access Security BROKER. It is in the name.

upvoted 2 times

abdulmalik_mail 3 years, 1 month ago

It's B https://learn-umbrella.cisco.com/i/781077-cisco-umbrella-and-cloudlock/1?

upvoted 3 times

Raajaa 3 years, 7 months ago

B is the answer

upvoted 3 times

Question #161 *Topic 1*

Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two.)

A. middleware

B. applications

C. virtualization

D. operating systems

E. data

Suggested Answer: *B, E*
Official Answer: BE

sull3y Highly Voted 2 years, 6 months ago

The two aspects of the cloud PaaS model that are managed by the customer but not the provider are: B. applications: The customer is responsible for developing, deploying, and managing the applications that run on the platform. This can include custom applications or third-party applications that are integrated with the platform. E. data: The customer is responsible for storing and managing their data, including backups and disaster recovery. This may include data that is stored in databases or file systems, or data that is transmitted between different components of the application. The provider is responsible for managing the underlying infrastructure and platform components, such as virtualization, operating systems, middleware, and other components that support the applications.

upvoted 5 times

Speckbrot Most Recent 2 years ago

Answer is B and E! See https://i0.wp.com/fourweekmba.com/wp-content/uploads/2020/12/what-is-saas.png?resize=1024%2C772&ssl=1

upvoted 3 times

zheka 3 years, 8 months ago

Both answers are correct: https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php

upvoted 4 times

Question #162 *Topic 1*

Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

A. Google Cloud Platform

B. Red Hat Enterprise Virtualization

C. Amazon Web Services

D. VMware ESXi

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

pr0fectus Highly Voted 2 years, 7 months ago

As of this writing, GCP is now supported. So if ever the exam changes and asks for 2 answers then A & C would be the correct one.

upvoted 9 times

ITVI Most Recent 1 year, 4 months ago

This must be an older question since the three power house cloud providers now supports them: AWS, Azure, GCP.

upvoted 2 times

geppo81 2 years, 1 month ago

If multiple choice are required Deployment modes:Routed, transparent (inline set — IPS-only), and passive; AWS, Azure, GCP and OCI: routed mode only https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html

upvoted 3 times

Question #163 *Topic 1*

What is an attribute of the DevSecOps process?

A. security scanning and theoretical vulnerabilities

B. development security

C. isolated security team

D. mandated security controls and check lists

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (64%) D (36%)

Premium_Pils 2 years ago
As sis_net_sec an others wrote, it should be Bhttps://blogs.cisco.com/developer/flavorsofdevops01 https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/devsecops-addressing-security-challenges.html
upvoted 1 times

Premium_Pils 2 years ago
Selected Answer: B
As sis_net_sec an others wrote, it should be B
upvoted 1 times

Premium_Pils Most Recent 2 years ago
https://blogs.cisco.com/developer/flavorsofdevops01 https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/devsecops-addressing-security-challenges.html
upvoted 1 times

MPoels 2 years, 5 months ago
Like statikd about the mentioned DevSecOps manifesto wrote: "Enabling businesses to address their most critical security requirements over a checklist or security mandates." Which is an attribute listed in the DevSecOps manifesto. Development security is overall what DevSecOps does, it's a given. https://blogs.cisco.com/security/devsecops-win-win-for-all see also: https://www.base4sec.com/research/en/DevSecOps-Checklist/ and https://www.devsecops.org/blog/tag/DevSecOps+Explained
upvoted 4 times

DWizard 3 years, 1 month ago
I'd go for B, even though it's not written in correct English, it should be security development: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/devsecops-infographic.pdf "Using clearly defined guiding principles to drive security throughout the development process helps establish mutual trust among the Engineering, Operations and Security teams"
upvoted 1 times

sis_net_sec 4 years ago
DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to IT and business objectives. Three key things make a real DevSecOps environment: + Security testing is done by the development team. + Issues found during that testing is managed by the development team. + Fixing those issues stays within the development team. https://blogs.cisco.com/security/devsecops-win-win-for-all
upvoted 3 times

brownbear505 4 years, 5 months ago
The drive toward shorter and more iterative development cycles, with a focus on delivering mission needs, is leading agencies to adopt DevSecOps (development, security, and operations) methodologies that enable development, security, and IT teams to work more closely and collaboratively. https://www.cisco.com/c/en/us/solutions/collateral/industries/government/cloud-ready-networks.html
upvoted 2 times

coentror 4 years, 8 months ago
It is B. D can never be because it goes againts the principles of Agile "mandate"
upvoted 2 times

hulisani 4 years, 9 months ago

based on this both B and D are correct answers What is an attribute of the DevSecOps? What is an attribute of the DevSecOps process? security scanning and theoretical vulnerabilities. development security. isolated security team. mandated security controls and check lists

upvoted 1 times

kapplejacks 4 years, 11 months ago

Just from a very basic angle, D is correct. "development security" is not proper grammar and broken English or something. Read the question then the answer, does it flow and sound like a Cisco answer? If i get this on the test and it really does say "development security" I am picking D. If it says "security development" I would pick B.

upvoted 1 times

itisfakemaillol 5 years, 1 month ago

B. development security

upvoted 2 times

dzef13 5 years, 2 months ago

B DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to IT and business objectives. Three key things make a real DevSecOps environment: + Security testing is done by the development team. + Issues found during that testing is managed by the development team. + Fixing those issues stays within the development team.

upvoted 2 times

wfexco 5 years, 2 months ago

It is a terrible question. I could see it being either B or D. I would go with D though. DevOps is a deliberate effort to align the application development team with the application operations team, while SecDevOps introduces additional processes within the framework, to mitigate the chances that the Continuous Integration and Continuous Deployment (CI/CD) operational tempo will compromise application security.

upvoted 1 times

trickbot 5 years, 3 months ago

If I get this question on the Exam, I will be answering B) Development Security. For reference, search "Cisco's DevSecOps Manifesto, where it explicitly states it's mission is to solve security problems with "Consumable Security Services over Mandated Security Controls" and "Collaboration to Securely enable Business, over Mandates" its a very Agile-ish manifesto. I found it here. https://blogs.cisco.com/security/devsecops-win-win-for-allBut this same blog states: "Enabling businesses to address their most critical security requirements over a checklist or security mandates." Which is an attribute listed in the DevSecOps manifesto. Development security is overall what DevSecOps does, it's a given. I think the answer is DMan exactly that's the best answer they don´t ask about overall work of DevSecops. They ask about attribute.... Answer D

upvoted 3 times

trickbot 5 years, 3 months ago

If I get this question on the Exam, I will be answering B) Development Security. For reference, search "Cisco's DevSecOps Manifesto, where it explicitly states it's mission is to solve security problems with "Consumable Security Services over Mandated Security Controls" and "Collaboration to Securely enable Business, over Mandates" its a very Agile-ish manifesto. I found it here. https://blogs.cisco.com/security/devsecops-win-win-for-all

upvoted 3 times

statikd Highly Voted 5 years, 1 month ago

But this same blog states: "Enabling businesses to address their most critical security requirements over a checklist or security mandates." Which is an attribute listed in the DevSecOps manifesto. Development security is overall what DevSecOps does, it's a given. I think the answer is D

upvoted 8 times

statikd 5 years, 1 month ago

But this same blog states: "Enabling businesses to address their most critical security requirements over a checklist or security mandates." Which is an attribute listed in the DevSecOps manifesto. Development security is overall what DevSecOps does, it's a given. I think the answer is DMan exactly that's the best answer they don´t ask about overall work of DevSecops. They ask about attribute.... Answer D

upvoted 8 times

jaciro11 Highly Voted 4 years, 8 months ago

Man exactly that's the best answer they don´t ask about overall work of DevSecops. They ask about attribute.... Answer D

upvoted 10 times

Question #164 *Topic 1*

On which part of the IT environment does DevSecOps focus?

A. application development

B. wireless network

C. data center

D. perimeter network

Suggested Answer: *A*
Official Answer: A

sull3y Highly Voted 2 years ago

A. DevSecOps focuses on the application development part of the IT environment. DevSecOps is a software development philosophy that emphasizes collaboration and communication between development, operations, and security teams in order to secure the entire software development life cycle. DevSecOps aims to integrate security into the development process, starting from the design phase, through to deployment and ongoing management. By focusing on the application development environment, DevSecOps aims to improve the security of software applications, reduce the risk of vulnerabilities, and ensure that applications are secure from the start.

upvoted 6 times

Jeeves69 Highly Voted 3 years, 11 months ago

Answer: A - Application development https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/devsecops-infographic.pdf

upvoted 5 times

Question #165 *Topic 1*

In a PaaS model, which layer is the tenant responsible for maintaining and patching?

A. hypervisor

B. virtual machine

C. network

D. application

Suggested Answer: *D*
Reference: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

Currently there are no comments in this discussion, be the first to comment!

Question #166 *Topic 1*

Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two.)

A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS

B. Cisco FTDv with one management interface and two traffic interfaces configured

C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises

D. Cisco FTDv with two management interfaces and one traffic interface configured

E. Cisco FTDv configured in routed mode and IPv6 configured

Suggested Answer: *A, C*
Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html

micruguy Highly Voted 3 years, 6 months ago
A & C are correct. Management console for NGFW Virtual FMC can be deployed on ESXi, KVM and in AWS Required for configuration, management & checking events NGFWv in cloud can be managed by FMC in AWS or FMC on premise (physical or virtual) FMC dashboard provides complete visibility

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-2064.pdf
upvoted 5 times

micruguy Highly Voted 3 years, 6 months ago
A & C are correct. Management console for NGFW Virtual FMC can be deployed on ESXi, KVM and in AWS Required for configuration, management & checking events NGFWv in cloud can be managed by FMC in AWS or FMC on premise (physical or virtual) FMC dashboard provides complete visibility
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-2064.pdfA & C
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-2064.pdf Page 56
upvoted 5 times

Cokamaniako Most Recent 2 years, 1 month ago
A & C https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-2064.pdf Page 56
upvoted 1 times

abdulmalik_mail 3 years, 7 months ago
Correct, It's A and C Based on reference "Cisco NGFWv in AWS (routed mode), Cisco NGFWv is deployed in routed mode and managed by an on premises FMC or FMC running in AWS"
upvoted 4 times

Thusi26 3 years, 8 months ago
A and C Communications paths: Management interface—Used to connect the ASAv to the ASDM; can't be used for through traffic. Inside interface (required)—Used to connect the ASAv to inside hosts. Outside interface (required)—Used to connect the ASAv to the public network. DMZ interface (optional)—Used to connect the ASAv to the DMZ network when using the c3.xlarge interface.it seems 4 interfaces are required, even to boot, as per video (interface section). https://www.youtube.com/watch?v=ycjTZhl_acQ&embeds_euri=https%3A%2F%2Fwww.google.com%2F&feature=emb_rel_pause
upvoted 1 times

Thusi26 3 years, 8 months ago
A and C

Communications paths:

Management interface—Used to connect the ASAv to the ASDM; can't be used for through traffic.

Inside interface (required)—Used to connect the ASAv to inside hosts.

Outside interface (required)—Used to connect the ASAv to the public network.

DMZ interface (optional)—Used to connect the ASAv to the DMZ network when using the c3.xlarge interface.
upvoted 1 times

Joseph47 2 years, 6 months ago

it seems 4 interfaces are required, even to boot, as per video (interface section). https://www.youtube.com/watch?v=ycjTZhl_acQ&embeds_euri=https%3A%2F%2Fwww.google.com%2F&feature=emb_rel_pause

upvoted 1 times

jccastiyo 3 years, 9 months ago

I'd say A and B because C states "Physical" on premise and we can do both physical and virtual on premise. https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html B is closer to right since we have 1 management and 2 data interfaces for FTDv in AWS, ignoring the diagnostic interface(eth0) since it's not mentioned here.https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-gsg/ftdv-aws-intro.html Firepower Threat Defense Virtual Limitations The c4.xlarge is the recommended instance; the c3.xlarge instance has limited availability across AWS regions. You must have two management interfaces configured during launch. You must have two traffic interfaces and two management interfaces to launch, for a total of four interfaces.

upvoted 1 times

jccastiyo 3 years, 9 months ago

I'd say A and B because C states "Physical" on premise and we can do both physical and virtual on premise.

https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html

B is closer to right since we have 1 management and 2 data interfaces for FTDv in AWS, ignoring the diagnostic interface(eth0) since it's not mentioned here.

upvoted 1 times

duck_hat 3 years, 8 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-gsg/ftdv-aws-intro.html Firepower Threat Defense Virtual Limitations The c4.xlarge is the recommended instance; the c3.xlarge instance has limited availability across AWS regions. You must have two management interfaces configured during launch. You must have two traffic interfaces and two management interfaces to launch, for a total of four interfaces.

upvoted 2 times

Raajaa 4 years, 1 month ago

A and C

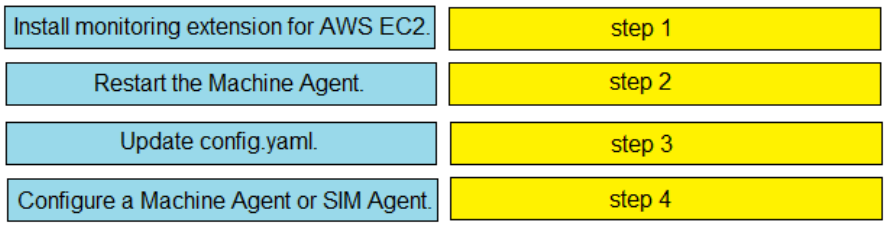
upvoted 2 times

Question #167 *Topic 1*

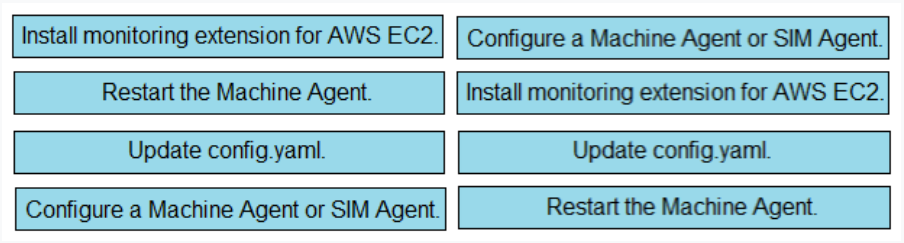
DRAG DROP -

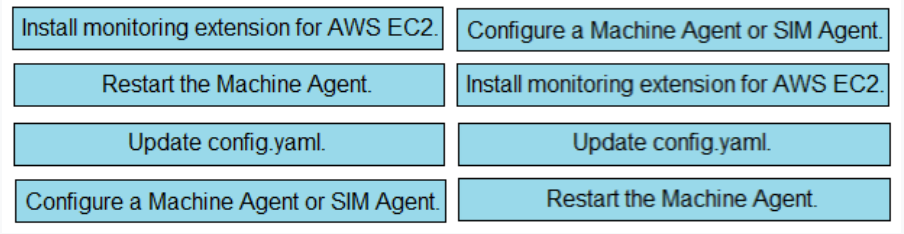
Drag and drop the steps from the left into the correct order on the right to enable Cisco AppDynamics to monitor an EC2 instance in AWS.

Select and Place:



Suggested Answer:





Reece_S Highly Voted 4 years, 6 months ago

Actually the answer is correct. According to this https://www.appdynamics.com/community/exchange/extension/aws-ec2-monitoring-extension/ The prerequisites states that you need a Standalone JAVA Machine Agent or SIM Agent; Which means you need to have that configured first before you can install the monitoring extension.config install update restart https://web.archive.org/web/20200807125050/https://www.appdynamics.com/community/exchange/extension/aws-ec2-monitoring-extension/

upvoted 14 times

Reece_S Highly Voted 4 years, 6 months ago

Actually the answer is correct. According to this https://www.appdynamics.com/community/exchange/extension/aws-ec2-monitoring-extension/

The prerequisites states that you need a Standalone JAVA Machine Agent or SIM Agent; Which means you need to have that configured first before you can install the monitoring extension.

upvoted 14 times

MPoels 1 year, 11 months ago

config install update restart https://web.archive.org/web/20200807125050/https://www.appdynamics.com/community/exchange/extension/aws-ec2-monitoring-extension/

upvoted 2 times

jshow 4 years, 7 months ago

install config update restart Run 'mvn clean install' from aws-ec2-monitoring-extension Copy and unzip AWSEC2Monitor- .zip from 'target' directory into /monitors/ The metricPrefix of the extension has to be configured as specified here. Please make sure that the right metricPrefix is chosen based on your machine agent deployment, otherwise this could lead to metrics not being visible in the controller. Edit config.yml file in AWSEC2Monitor and provide the required configuration (see Configuration section) Restart the Machine Agent. https://www.appdynamics.com/community/exchange/extension/aws-ec2-monitoring-extension/

upvoted 10 times

laribando98 Most Recent 11 months ago

Correct Answer The answer has been elaborated furter within the solution chart. Review carefully. Config Install Update Restart

upvoted 1 times

Tuxzinator 3 years ago

it is recommended to install and configure the machine agent or the sim agent before installing the monitoring extension for AWS EC2. This is because the agent is required to run the monitoring extension and collect the necessary data for monitoringSo are you saying it should be: 1. Config 2. Install 3. Update 4. Restart Can someone confirm, the AppDynamics link is a little misleading? Many thanks,

upvoted 3 times

Tuxzinator 3 years ago

it is recommended to install and configure the machine agent or the sim agent before installing the monitoring extension for AWS EC2. This is because the agent is required to run the monitoring extension and collect the necessary data for monitoring

upvoted 3 times

Totosos1 2 years, 11 months ago

So are you saying it should be: 1. Config 2. Install 3. Update 4. Restart Can someone confirm, the AppDynamics link is a little misleading? Many thanks,

upvoted 1 times

nomanlands 3 years, 7 months ago

Must configure the agent first as a pre-req. Install the AWS monitoring extension. Configure yaml file Restart

upvoted 1 times

otzu1 3 years, 10 months ago

Makes sense, you first need a machine to install the AWS EC2. Also Update the Yaml.config so when you restart it can be pushed back if needed. Config Machine Agent Install AWS EC2 Update YAML Restart

upvoted 2 times

litespirit 3 years, 11 months ago

The link below has been mostly misinterpreted. Reece_S is correct... Config [Pre-requisite] Install Update Restart ---- PreReq: AppDynamics Monitoring Extensions require either a Server Infrastructure and Monitoring (SIM) Agent or a stand-alone Machine Agent (MA) to report metrics to the AppDynamics Controller. IMPORTANT | AppDynamics Extensions are only supported if there is a single instance of either a Machine Agent with APM Agents or a SIM Agent on a physical host. Multiple instances of Machine Agent or SIM on a single physical host are not supported for extensions installation.

upvoted 3 times

Seawanderer 4 years, 7 months ago

Install 1, configure 2

upvoted 1 times

Question #168 *Topic 1*

What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?

A. Enable IP Layer enforcement.

B. Activate the Cisco AMP license.

C. Activate SSL decryption.

D. Enable Intelligent Proxy.

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

sull3y Highly Voted 3 years ago
The Secure Internet Gateway is a security solution that helps protect your organization's network and users from online threats such as malware. To enable malware file scanning, it is necessary to have the Intelligent Proxy feature enabled. The Intelligent Proxy provides an additional layer of security by examining and filtering out malicious traffic, including malware files, before they can reach your network. Without this feature, the Secure Internet Gateway may not be able to detect and prevent malware from entering your network.
upvoted 5 times

MPoels Most Recent 1 year, 11 months ago
Selected Answer: D
Toggle on Enable Intelligent Proxy. When enabled, you have access to the following options: Inspect Files [...]

https://docs.umbrella.com/deployment-msp/docs/enable-the-intelligent-proxy

btw Support for the intelligent proxy is deprecated and only available for legacy deployments of the MSP console. The intelligent proxy is not available for new deployments of the MSP console.
upvoted 2 times

Dorr20 2 years, 10 months ago
This question is bad at so many levels. The "File Inspection" in SIG is included in all Bundles, so there is no need to activate it, but still there is a warning on Cisco's website and I guess this makes it the correct answer.

My educated answer is B This is way:

All terms are part of the "Advanced Settings" in the "DNS Policy" (the SIG adds us a "Web Policy" section).

IP Layer enforcement is a protection against malicious servers and it is end of life for over a year now (so A is wrong) Turning on SSL decryption allows HTTPS URL blocking (so C is wrong). Intellignet Proxy gains us visibility into threats, content or apps for risky domains (only). If the question was not about SIG, I would go with this answer, BUT It's not a true malware inspection like SIG has to offer (and that is way i think D is wrong).

In order to use File Analysis in SIG you need to make sure you have a license (see link below), enable HTTPS inspection etc.
https://docs.umbrella.com/umbrella-user-guide/docs/manage-file-analysis
upvoted 1 times

Tuxzinator 3 years ago
stop posting umbrella link's. SIG = not umbrella.
upvoted 1 times

Toni_Su91 2 years, 11 months ago
https://umbrella.cisco.com/trends-threats/secure-internet-gateway

Cisco Umbrella SIG unifies multiple security capabilities in the cloud to secure cloud adoption and direct internet access
upvoted 2 times

Tuxzinator 3 years ago

Don't you need a license before it actually works?

upvoted 4 times

mecacig953 3 years, 10 months ago

Selected Answer: D

https://docs.umbrella.com/deployment-umbrella/docs/configure-advanced-settings Advanced Settings let you enable various security settings including Umbrella's intelligent proxy, which gives Umbrella the ability to intercept and proxy requests for malicious files embedded within certain so-called "grey" domains. With the intelligent proxy, if a site is considered potentially suspicious or could host malicious content, we'll return the IP address of the intelligent proxy. The request to that domain is then routed through our cloud-based secure gateway, and malicious content is found and stopped before it's sent to you.

upvoted 1 times

Question #169 *Topic 1*

A company is experiencing exfiltration of credit card numbers that are not being stored on-premise. The company needs to be able to protect sensitive data throughout the full environment. Which tool should be used to accomplish this goal?

A. Cisco ISE

B. Web Security Appliance

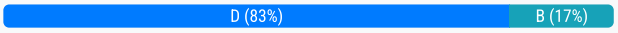
C. Security Manager

D. Cloudlock

Suggested Answer: *D*

Official Answer: D

Community vote distribution



sull3y Highly Voted 2 years ago

The answer is D, Cloudlock. Cisco Cloudlock is an API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise. It provides protection of sensitive data throughout the full environment and helps secure cloud-based email, file storage, and web applications. Cloudlock detects and protects sensitive data across all cloud services, including cloud storage and collaboration services such as AWS, Box, Dropbox, Google Drive, Microsoft OneDrive, Salesforce, and more

upvoted 7 times

Moe1416 2 years, 2 months ago

A company is experiencing exfiltration of credit card numbers that are NOT being stored on-premise. Its NOT on premise Answer is D

upvoted 3 times

Jariaya1 2 years, 3 months ago

B = Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

upvoted 1 times

nomanlands 2 years, 7 months ago

Cloudlock DLP

upvoted 2 times

DarkestHour 2 years, 7 months ago

It says NOT on premise. So I suspect B is incorrect.

upvoted 3 times

wenorex222 2 years, 8 months ago

Selected Answer: B

Correct answer is B, keyword on premise. https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/solution-overview-c22-732948.html

upvoted 1 times

wenorex222 2 years, 8 months ago

Correct answer is B, keyword on premise. https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/solution-overview-c22-732948.htmlNo, the key word is said before on promise: "NOT being stored on-premise"

upvoted 1 times

GoldFree Most Recent 1 year, 8 months ago

No, the key word is said before on promise: "NOT being stored on-premise"

upvoted 2 times

Question #170 *Topic 1*

What are the two types of managed Intercloud Fabric deployment models? (Choose two.)

A. Service Provider managed

B. User managed

C. Public managed

D. Hybrid managed

E. Enterprise managed

Suggested Answer: *A, E*

Official Answer: AE

Community vote distribution

AE (100%)

Medusa8 Most Recent 2 years, 2 months ago

https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Intercloud_Fabric_1.html#pgfId-2319061

upvoted 3 times

cesardgrd 3 years ago

AE without a doubt

upvoted 1 times

abdulmalik_mail 3 years, 1 month ago

Correct, It's AE https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric.pdf, please see on page 8 and 9 on PDF

upvoted 3 times

VI_Vershinin 3 years, 7 months ago

It's a correct answer. Cisco Intercloud Fabric addresses the cloud deployment requirements appropriate for two hybrid cloud deployment models: Enterprise Managed and Service Provider Managed.

upvoted 3 times

Question #171 *Topic 1*

An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?

A. CASB

B. Cisco Cloudlock

C. Adaptive MFA

D. SIEM

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

netwguy Highly Voted 4 years, 2 months ago

its clearly B

upvoted 11 times

itisfakemaillol Highly Voted 4 years, 1 month ago

It's Cisco exam, so the correct answer is - B. Cisco Cloudlock

upvoted 9 times

Eluis007 Most Recent 7 months ago

with other cloud solutions , so, this is Cloud solution, BBBBBBBBB

upvoted 1 times

cyberwhizzy0 2 years, 1 month ago

The question is the definition of CASB but CASB is just the technology not that solution. Cloudlock, which is a cloud-native CASB, is the solution. Compare with Q184

upvoted 3 times

ddev3737 2 years, 6 months ago

Although Cisco exam, the most correction answer would be D Cisco has SIEM Cisco's Stealthwatch Cloud but that is not an option here. If that were present then it would stealthwatch instead of Cloudlock. I vote for D siem

upvoted 2 times

ddev3737_111 2 years, 6 months ago

Although Cisco exam, the most correction answer would be D Cisco has SIEM Cisco's Stealthwatch Cloud but that is not an option here. If that were present then it would stealthwatch instead of Cloudlock. I vote for D siem

upvoted 2 times

nomanlands 3 years, 1 month ago

B since this is a Cisco exam. A SIEM could do this if you set it up to do so.

upvoted 1 times

brownbear505 3 years, 5 months ago

Cisco Cloudlock for Google Workspace - Digital Marketplace https://www.digitalmarketplace.service.gov.uk/g-cloud/services/468189650542713

upvoted 2 times

Minion2021 3 years, 5 months ago

It should be B

upvoted 1 times

flejd 3 years, 7 months ago

A and B is the same. I'd pick D

upvoted 1 times

MoII 3 years, 9 months ago

Answer should be B

upvoted 2 times

ZanaHiwa 3 years, 10 months ago

Answer B

upvoted 2 times

Sarbi 3 years, 11 months ago

It is d.

upvoted 2 times

klu16 4 years ago

Come on guys, it's B... + Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy. + Cloudlock is API-based. + Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).

upvoted 7 times

Dinges 4 years, 1 month ago

A CASB, for any cloud solution. If the question specified a Cisco cloud solution, then B Cloudlock

upvoted 4 times

SirFrates24 4 years, 1 month ago

SIEM software works by collecting log and event data generated by an organizations applications, security devices and host systems and bringing it together into a single centralized platform. ... In this way it detects threats and creates security alerts.

upvoted 3 times

statikd 4 years, 1 month ago

I think it is D, SIEM (Security information and event management). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security-technology-partners/bn_cisco_siem.pdf "This guide focuses on Cisco products and discusses how those products integrate with any third party SIEM product. " "Customers need the ability to log, monitor, and report on security incidents in their data infrastructure, and to log, store, and report on large volumes of security event logs." Cisco Cloudlock is a Cloud-Based Security Broker (CASB). "A CASB provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware." So basically Cloudlock is a DLP device.

upvoted 4 times

Question #172 *Topic 1*

An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

A. Cisco Defense Orchestrator

B. Cisco Configuration Professional

C. Cisco Secureworks

D. Cisco DNA Center

Suggested Answer: *A*
Reference: https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html

sull3y Highly Voted 2 years ago

it is A Cloud-based Firewall Management Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms. Cisco Defense Orchestrator centrally manages elements of policy and configuration across: ● Cisco Secure Firewall ASA, both on-premises and virtual ● Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual ● Cisco Meraki™ MX ● Cisco IOS devices ● AWS security groups Cisco Defense Orchestrator also incorporates the cloud-delivered version of Firewall Management Center (FMC), providing a fully unified experience between on-premises and cloud-based firewall management. This expands management of policy and configuration to: ● Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual ● Cisco Secure IPS (formerly Firepower NGIPS) ● Cisco Firewall Threat Defense for ISR

upvoted 5 times

jshow 3 years, 7 months ago

A is correct

upvoted 3 times

Question #173 *Topic 1*

Which factor must be considered when choosing the on-premise solution over the cloud-based one?

A. With an on-premise solution, the provider is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the customer is responsible for it.

B. With a cloud-based solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.

C. With an on-premise solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.

D. With an on-premise solution, the customer is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the provider is responsible for it.

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

Happy_Shepherd26 Most Recent 1 year, 9 months ago

Selected Answer: D

Obviously D

upvoted 2 times

Question #174 *Topic 1*

An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud-native CASB and cloud cybersecurity platform. What should be used to meet these requirements?

A. Cisco NGFW

B. Cisco Cloudlock

C. Cisco Cloud Email Security

D. Cisco Umbrella

Suggested Answer: *B*
Official Answer: B

statikd Highly Voted 4 years, 8 months ago

Cisco Cloudlock is a Cloud-Based Security Broker (CASB). "A CASB provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware." So basically Cloudlock is a DLP device.

upvoted 7 times

GARBADOUR Most Recent 1 year, 9 months ago

I've learnt that if Cloudlock is one of the possible solutions, the solution is always Cloudlock

upvoted 4 times

Question #175 *Topic 1*

In an IaaS cloud services model, which security function is the provider responsible for managing?

A. firewalling virtual machines

B. Internet proxy

C. hypervisor OS hardening

D. CASB

Suggested Answer: *A*

Official Answer: A

Community vote distribution

C (95%) (5%)

Dead_Adriano Highly Voted 5 years, 1 month ago

Why A for IaaS? Shouldn't it be C?Yes, it must be C

upvoted 14 times

Dead_Adriano 5 years, 1 month ago

Why A for IaaS? Shouldn't it be C?

upvoted 14 times

itisfakemaillol Highly Voted 5 years, 1 month ago

Yes, it must be C

upvoted 17 times

Totosos1 3 years, 5 months ago

https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/ According to IaaS, the provider is responsible for: Virtualization Servers Storage Networking Hypervisor being the "Virtualisation", therefore C is the correct answer!

upvoted 7 times

Demon_Queen_Velverosa Most Recent 1 year, 11 months ago

I noticed various individuals are a bit confused and overthinking it. This question is about IaaS (Infrastructure as a service) and the confusion relays with virtualization. The customer is responsible for the Virtual network, but the provider is only responsible for the Hypervisor. customer responsibility: - People - data - apps - runtime - middleware - OS - virtual network Provider responsible for: - Hypervisor - servers - storage - physical network

upvoted 1 times

Mohammad_h_tarawneh 2 years, 2 months ago

I think , option A and C is valid , but regarding Security , I think firewalling is more specific and should be done before O.S hardening ..

upvoted 1 times

mhd96far 2 years, 4 months ago

C. hypervisor OS hardening Most Voted

upvoted 1 times

xziomal9 2 years, 9 months ago

Answer C

upvoted 1 times

Ko13 2 years, 9 months ago

You have to take on account that there are multiple OSes here, Vendor is responsible for the hypervisor's OS version (currently Hyper-V Server 2022 is the latest as of today) while the VM's software version (Windows 11 for example) is not. https://comparacloud.com/wp-content/uploads/2019/09/saas-vs-paas-vs-iaas.jpg

upvoted 2 times

gc999 3 years, 4 months ago

At the first look, I would choose "C". But after a while, "A" maybe more suitable. It is because for the "services" model, Hypervisor would not do "serve" to Cloud users but virtual machine does. For me, even I am running hypervisor, I seldom to take care of it since the management network is isolated to the public access.

upvoted 1 times

Emlia1 3 years, 8 months ago

It's C

upvoted 4 times

tanri04 3 years, 9 months ago

With an IaaS model, the vendor is responsible for security of the physical data centers and other hardware that power the infrastructure -- including VMs, disks and networks. Users must secure their own data, operating systems and software stacks that run their applications. (my answer: C)How can your answer be C then. The question is asking "What is the Vendor responsible for" and you're reply is saying that user's are responsible for the Operating Systems, that means C is invalid based on your response?You have to take on account that there are multiple OSes here, Vendor is responsible for the hypervisor's OS version (currently Hyper-V Server 2022 is the latest as of today) while the VM's software version (Windows 11 for example) is not. https://comparacloud.com/wp-content/uploads/2019/09/saas-vs-paas-vs-iaas.jpg

upvoted 3 times

tanri04 3 years, 9 months ago

With an IaaS model, the vendor is responsible for security of the physical data centers and other hardware that power the infrastructure -- including VMs, disks and networks. Users must secure their own data, operating systems and software stacks that run their applications. (my answer: C)

upvoted 3 times

Totosos1 3 years, 5 months ago

How can your answer be C then. The question is asking "What is the Vendor responsible for" and you're reply is saying that user's are responsible for the Operating Systems, that means C is invalid based on your response?You have to take on account that there are multiple OSes here, Vendor is responsible for the hypervisor's OS version (currently Hyper-V Server 2022 is the latest as of today) while the VM's software version (Windows 11 for example) is not. https://comparacloud.com/wp-content/uploads/2019/09/saas-vs-paas-vs-iaas.jpg

upvoted 1 times

Totosos1 3 years, 5 months ago

How can your answer be C then. The question is asking "What is the Vendor responsible for" and you're reply is saying that user's are responsible for the Operating Systems, that means C is invalid based on your response?

upvoted 1 times

sis_net_sec 3 years, 10 months ago

Infrastructure as a Service (IaaS) in cloud computing is one of the most significant and fastest growing field. In this service model, cloud providers offer resources to users/machines that include computers as virtual machines, raw (block) storage, firewalls, load balancers, and network devices.

upvoted 1 times

FortiSherlock 4 years ago

Clearly C in an IaaS environment.

upvoted 1 times

nemeses667 4 years ago

Surely C? https://www.leanix.net/en/wiki/saas/iaas-vs-paas-vs-saas?utm_term=&utm_source=adwords&utm_medium=ppc&utm_campaign=UK+%7C+SMP+%7C+SaaS+Management+%7C+DSA+%7C+ENG&hsa_ver=3&hsa_cam=15150382310&hsa_grp=133953171750&hsa_acc=9751618594&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_src=g&hsa_tgt=dsa-1465784135448&hsa_ad=563932871660&gclid=Cj0KCQjw54iXBhCXARIsADWpsG-gPk26BNMvGPkFB34KtX0PVry-x1Wq5mNlSFBDBLJlkmIhvjrUF2caAn2AEALw_wcB

upvoted 1 times

getafix 4 years, 2 months ago

A. firewalling virtual machines - isn't correct because the virtual machine setup in IAAS belongs to the client and the client is responsible for deploying a firewall and other software as they want B. Internet proxy - isn't related C. hypervisor OS hardening - correct answer since the provider is responsible for all security on the baremetal server which runs the hypervisor OS D. CASB - isn't related as thats only a Cloud Access Security Broker

upvoted 5 times

TesterDude 4 years, 3 months ago

Answer is C Customer Responsibilities: Applications Data Middleware OS People Runtime Environment Virtual network and hosts Security and patching of an VMs Provider Responsibilities Hypervisors Servers Storage devices Physical Networ

upvoted 2 times

semi1750 4 years, 3 months ago

D. is correct you guys are all wrong. It is asking which security function responsible for managing in IaaS... C is security related task provider is responsible in IaaS environment. but not security fuction....

upvoted 1 times

JGW 4 years, 4 months ago

in IAAS the service provider is responsible up to the hypervisor. https://www.cisco.com/c/dam/en/us/solutions/collateral/design-zone/cisco-validated-profiles/safe-secure-cloud-architecture-guide.pdf page 7

upvoted 4 times

Question #176 *Topic 1*

An organization wants to secure users, data, and applications in the cloud. The solution must be API-based on operate as a cloud-native CASB. Which solution must be used for this implementation?

A. Cisco Cloud Email Security

B. Cisco Cloudlock

C. Cisco Umbrella

D. Cisco Firepower Nest-Generation Firewall

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

Swiz005 Most Recent 1 year, 7 months ago

If you see Cisco Cloudlock as the option. Just go for Cisco Cloudlock

upvoted 3 times

cristip 1 year, 9 months ago

B. Cisco Cloudlock

upvoted 1 times

Alizade 2 years, 4 months ago

B. Cisco Cloudlock

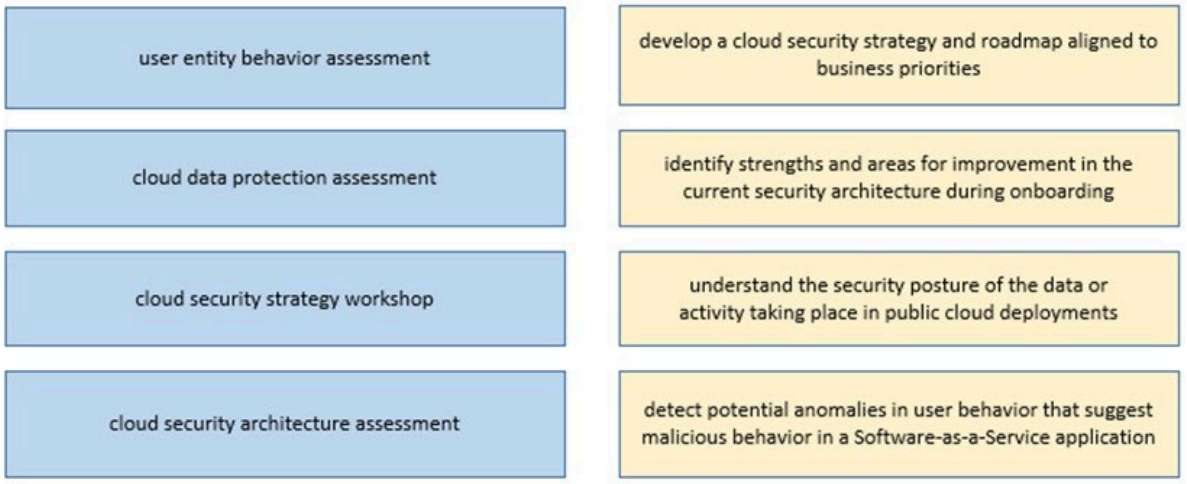
upvoted 1 times

Question #177 *Topic 1*

DRAG DROP -

Drag and drop the cloud security assessment components from the left onto the definitions on the right.

Select and Place:



Suggested Answer:



Max95 Highly Voted 3 years, 12 months ago

Answer should be cloud security strategy workshop cloud security architecture assessment cloud data protection assessment user entity behaviour assessment https://www.cisco.com/c/dam/m/en_sg/dc-innovation/assets/pdfs/securing-your-multicloud-journey.pdf

upvoted 38 times

ZanaHiwa Highly Voted 3 years, 10 months ago

the Answer is: cloud security strategy workshop cloud security architecture assessment cloud data protection assessment user entity behavior assessment

upvoted 5 times

Przemol 2 years, 1 month ago

cloud security strategy workshop cloud security architecture assessment cloud data protection assessment user entity behaviour assessment See Page 13 https://www.cisco.com/c/dam/m/en_sg/dc-innovation/assets/pdfs/securing-your-multicloud-journey.pdf

upvoted 1 times

Totosos1 2 years, 5 months ago

I have the following for the Drag & Drop, as I can't make sense of the below answers from Max95 & ZanaHiwa: 1 > 4 - User Behaviour 2 > 3 - Data Protection 3 > 1 - Strategy 4 > 2 - Security ArchitectureAll of you were basically telling the same thing. They clearly listed the results, you did not move the line in order but gave the movement.

upvoted 1 times

Totosos1 2 years, 5 months ago

I have the following for the Drag & Drop, as I can't make sense of the below answers from Max95 & ZanaHiwa:

1 > 4 - User Behaviour 2 > 3 - Data Protection 3 > 1 - Strategy 4 > 2 - Security Architecture

upvoted 1 times

Leogxn Most Recent 2 years, 1 month ago

All of you were basically telling the same thing. They clearly listed the results, you did not move the line in order but gave the movement.

upvoted 1 times

eazy99 3 years, 11 months ago

I agree with you guys, I found a slide that defines each from Cisco and gives the answers.
https://www.cisco.com/c/dam/en/us/products/security/security-strategy-advisory-aag.pdf

upvoted 4 times

Sarbi 3 years, 12 months ago

Agreed with Max 95

upvoted 2 times

Question #178 *Topic 1*

An organization wants to secure data in a cloud environment. Its security model requires that all users be authenticated and authorized. Security configuration and posture must be continuously validated before access is granted or maintained to applications and data. There is also a need to allow certain application traffic and deny all other traffic by default. Which technology must be used to implement these requirements?

A. virtual routing and forwarding

B. access control policy

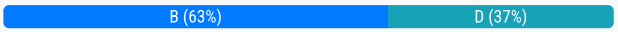
C. virtual LAN

D. microsegmentation

Suggested Answer: *D*

Official Answer: D

Community vote distribution



jaciro11 Highly Voted 4 years, 5 months ago

Microsegmentation is NOT for posturing checking. All the requirements criteria is met by Access Control Policies where you can define in ISE, Authentication, Authorization (Assign SGT in this part, which is the microsegmentation), then use Access List to deny or allow traffic Answer is BI see your point however, this is again one of those typical Cisco questions worded to throw you off balance. While Access Control Policy fits much better the question background and requirements, the question itself is "Which TECHNOLOGY must be used to implement these requirements?" if i get this question at the exam, I will go for D, MicrosegmentationI incline more to microsegmentation. Access control and Identity based access is without doubt necessary part of that, but the whole enforcement technology is microsegmentation.

upvoted 20 times

jaciro11 Highly Voted 4 years, 5 months ago

Selected Answer: B

Microsegmentation is NOT for posturing checking. All the requirements criteria is met by Access Control Policies where you can define in ISE, Authentication, Authorization (Assign SGT in this part, which is the microsegmentation), then use Access List to deny or allow traffic

Answer is B

upvoted 20 times

A_Wolf 11 months, 2 weeks ago

I see your point however, this is again one of those typical Cisco questions worded to throw you off balance. While Access Control Policy fits much better the question background and requirements, the question itself is "Which TECHNOLOGY must be used to implement these requirements?" if i get this question at the exam, I will go for D, Microsegmentation

upvoted 2 times

Rododendron2 2 years, 3 months ago

I incline more to microsegmentation. Access control and Identity based access is without doubt necessary part of that, but the whole enforcement technology is microsegmentation.

upvoted 3 times

Smileebloke 4 years, 4 months ago

The key point is all users must be authenticated / authorised (RBAC), using identity based access control, so ISE. Micro segmentation is also part of the solution using SGT. Access policy brings these components together. Answer: B

upvoted 6 times

SomKeat Most Recent 2 months, 2 weeks ago

D is the correct answer The technology that must be used to implement a security model in a cloud environment where all users are authenticated and authorized, security posture is continuously validated before access is granted or maintained, and certain application traffic is allowed while all other traffic is denied by default is microsegmentation.

upvoted 1 times

7d4c29f 3 months, 1 week ago

Micro segmentation (Zero Trust): User connects → Validate → Access granted → Continuously re-validate

upvoted 1 times

Happy_Shepherd26 1 year, 9 months ago

Micro-segmentation secures applications by expressly allowing particular application traffic and, by default, denying all other traffic.

upvoted 1 times

kloug 1 year, 9 months ago

D correct

upvoted 1 times

luismg 1 year, 11 months ago

In microsegmentation traffic doesn't need to be authenticated, for me is B.

upvoted 1 times

Premium_Pils 2 years ago

They meant the broader term, Access Control Policy.

upvoted 1 times

Tthurston1 2 years, 2 months ago

Have to agree with the others who voted for Option D. The keywords that stood out to me were "...allowing certain application traffic and deny all other traffic by default." This is possible ONLY with microsegmentation. With ACL's - the opposite of that is true - traffic is allowed by default unless explicitly stated otherwise with rules denying certain traffic. https://www.cisco.com/c/en/us/products/security/what-is-microsegmentation.html

upvoted 3 times

gorequill 2 years, 7 months ago

https://www.theasciiconstruct.com/post/sda_security_2/ D

upvoted 1 times

Alizade 2 years, 10 months ago

The answer is D. microsegmentation.

upvoted 1 times

Jessie45785 3 years, 4 months ago

they asking about the model, access control policy is not a model, microsegmentation is a security deployment model - I am going for B

upvoted 1 times

angry 3 years, 5 months ago

B is correct guys!

upvoted 2 times

Tuxzinator 3 years, 6 months ago

Its security model requires that all users be authenticated and authorized. How does micro segmentation do this?

upvoted 3 times

Emlia1 3 years, 8 months ago

Selected Answer: D

I prefer D

upvoted 2 times

psuoh 3 years, 6 months ago

Micro-segmentation software uses network virtualization technology to create increasingly granular secure zones in data centers and cloud deployments, which isolate each individual workload and secure it separately.

upvoted 1 times

4000000 3 years, 9 months ago

They r talking about and questioning technology..... Microsegmentation is the technology so D

upvoted 2 times

Anonymous983475 3 years, 7 months ago

I agree that it's D

upvoted 2 times

Question #179 *Topic 1*

Which cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group?

A. community

B. private

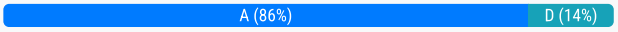
C. public

D. hybrid

Suggested Answer: *A*

Official Answer: A

Community vote distribution



XBfoundX Most Recent 1 week ago

As Fragalot is saying is this: A community cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group that share specific computing concerns such as, security, compliance or jurisdiction considerations. The community cloud can be either on-premises or off-premises, and can be governed by the participating organizations or by a third-party managed service provider. so is A community cloud.

upvoted 1 times

laribando98 11 months ago

Community cloud model

upvoted 1 times

Premium_Pils 2 years ago

community cloud model

upvoted 1 times

Thusi26 4 years, 2 months ago

community cloud model A community cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group that share specific computing concerns such as, security, compliance or jurisdiction considerations.

upvoted 3 times

NullNull88 4 years, 8 months ago

Selected Answer: D

This isn't Hybrid? Why not? Community? Isn't this a Cisco exam?

upvoted 1 times

NullNull88 4 years, 8 months ago

This isn't Hybrid? Why not? Community? Isn't this a Cisco exam?It's Community - https://blogs.cisco.com/datacenter/emerging-cloud-models-community-cloudHybrid is a mixture of public cloud and private cloud, so it is actually Community

upvoted 1 times

Fragalot Highly Voted 4 years, 8 months ago

It's Community - https://blogs.cisco.com/datacenter/emerging-cloud-models-community-cloud

upvoted 5 times

fukumoto0925 3 years, 9 months ago

Hybrid is a mixture of public cloud and private cloud, so it is actually Community

upvoted 4 times

Question #180 *Topic 1*

How does Cisco Workload Optimization Manager help mitigate application performance issues?

A. It automates resource resizing.

B. It sets up a workload forensic score.

C. It optimizes a flow path.

D. It deploys an AWS Lambda system.

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

idto Highly Voted 3 years, 2 months ago

"Workload Optimization Manager continuously analyzes workload consumption, costs, and compliance constraints and automatically allocates resources in real time." Source: https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-s-series-storage-servers/whitepaper-c11-741392.pdf

upvoted 7 times

XBfoundX Most Recent 1 week ago

Cisco Workload Optimization Manager is intelligent software that facilitates application performance by giving workloads the resources they need, when they need them.

upvoted 1 times

yong08321 1 year, 9 months ago

A. It automates resource resizing. Cisco Workload Optimization Manager is designed to automate the management of applications and workloads across hybrid IT environments. It continuously monitors the performance of workloads and applications and makes recommendations for optimizing resources such as compute, storage, and network to improve performance. It can also automatically resize resources based on performance metrics to ensure that the application has the resources it needs to run effectively.

upvoted 2 times

Question #181 *Topic 1*

Which DevSecOps implementation process gives a weekly or daily update instead of monthly or quarterly in the applications?

A. CI/CD pipeline

B. container

C. orchestration

D. security

Suggested Answer: *A*
Reference: https://devops.com/how-to-implement-an-effective-ci-cd-pipeline/

idto Highly Voted 1 year, 8 months ago

A is correct. "Unlike the traditional software life cycle, the CI/CD implementation process gives a weekly or daily update instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly." Source: https://devops.com/how-to-implement-an-effective-ci-cd-pipeline/amp/

upvoted 5 times

Question #182 *Topic 1*

Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?

A. SDLC

B. Lambda

C. Contiv

D. Docker

Suggested Answer: *D*

Reference: https://www.cisco.com/c/dam/global/es_es/pdfs/Cisco-cloudcenter-architecture-wp-c11-737224.pdf

Community vote distribution

C (100%)

Tuxzinator Highly Voted 2 years, 6 months ago

Selected Answer: C

C. Contiv With Contiv, cloud architects and IT admin teams can create, manage and consistently enforce operational policies such as multi-tenant traffic isolation, microsegmentation, bandwidth prioritization, latency requirements, and policies

upvoted 6 times

Tuxzinator Highly Voted 2 years, 6 months ago

C. Contiv With Contiv, cloud architects and IT admin teams can create, manage and consistently enforce operational policies such as multi-tenant traffic isolation, microsegmentation, bandwidth prioritization, latency requirements, and policiesAgree. https://blogs.cisco.com/cloud/introducing-contiv-1-0#:~:text=With%20Contiv%2C%20cloud%20architects%2C%20and%20IT%20admin%20teams%20can%20create%2C%20manage%20and%20consistently%20enforce%20operational%20policies%20such%20as%20multi%2Dtenant%20traffic%20isolation%2C%20microsegmentation

upvoted 6 times

gc999 2 years, 2 months ago

Agree. https://blogs.cisco.com/cloud/introducing-contiv-1-0#:~:text=With%20Contiv%2C%20cloud%20architects%2C%20and%20IT%20admin%20teams%20can%20create%2C%20manage%20and%20consistently%20enforce%20operational%20policies%20such%20as%20multi%2Dtenant%20traffic%20isolation%2C%20microsegmentation

upvoted 3 times

jku2cya Most Recent 2 years, 1 month ago

https://blogs.cisco.com/cloud/introducing-contiv-1-0 "create, manage and consistently enforce operational policies such as multi-tenant traffic isolation, microsegmentation..."

upvoted 4 times

yong08321 2 years, 3 months ago

Contiv is an open-source system that provides infrastructure-level virtualization and policy-based networking to facilitate microsegmentation and multi-tenancy services deployment with a policy-based container. It is designed to provide a unified networking fabric across multiple container clusters, hypervisors, and cloud platforms.

upvoted 3 times

sull3y 2 years, 6 months ago

C. Contiv Contiv is a system that facilitates deploying microsegmentation and multi-tenancy services with a policy-based container. Contiv provides a unified policy model for managing container networks, enabling administrators to easily segment traffic between different tenants and applications. The system allows administrators to define and enforce network security policies, providing a high degree of security and control over network traffic. With its focus on container-based deployment and its support for microsegmentation and multi-tenancy, Contiv provides a powerful solution for organizations looking to secure their containerized environments. By using a policy-based approach, Contiv helps organizations achieve a high level of network security and control, enabling them to securely deploy and manage containers at scale.

upvoted 3 times

Cyberops 3 years, 3 months ago

With Contiv, cloud architects and IT admin teams can create, manage and consistently enforce operational policies such as multi-tenant traffic isolation, microsegmentation, bandwidth prioritization, latency requirements, and policies

upvoted 3 times

HAckerGK 3 years, 3 months ago

its C. contiv

upvoted 2 times

ileri_sec 3 years, 3 months ago

http://contiv.ciscolive.com/pod5/Intro/contiv_intro

upvoted 2 times

Yuta1123 3 years, 3 months ago

Why C ? I think D is answer. Contive: Flexible Policy Control Contiv allows flexible policies to be applied to container networks, including per-application group policy control, bandwidth, QoS, etc.___Sorry, why D? I think C is answer.

upvoted 2 times

Yuta1123 3 years, 3 months ago

Selected Answer: C

Why C ? I think D is answer.

Contive: Flexible Policy Control Contiv allows flexible policies to be applied to container networks, including per-application group policy control, bandwidth, QoS, etc.___

upvoted 2 times

Yuta1123 3 years, 3 months ago

Sorry, why D? I think C is answer.

upvoted 1 times

Question #183 *Topic 1*

An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?

A. Infrastructure as a Service because the customer manages the operating system.

B. Platform as a Service because the service provider manages the operating system.

C. Infrastructure as a Service because the service provider manages the operating system.

D. Platform as a Service because the customer manages the operating system.

Suggested Answer: *B*
Reference: https://www.cisco.com/c/en/us/solutions/cloud/what-is-cloud-computing.html#~cloud-computing-services

Currently there are no comments in this discussion, be the first to comment!

Question #184 *Topic 1*

How does a cloud access security broker function?

A. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution.

B. It scans other cloud solutions being used within the network and identifies vulnerabilities.

C. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution.

D. It acts as a security information and event management solution and receives syslog from other cloud solutions.

Suggested Answer: *C*
Reference: https://www.cisco.com/c/en_in/products/security/cloudlock/index.html#~stickynav=2

sull3y Most Recent 2 years ago

C. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution.

A Cloud Access Security Broker (CASB) is a security solution that integrates with cloud solutions such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) via APIs. It monitors cloud usage and creates incidents based on events from the cloud solution. This allows organizations to gain visibility into and control over their cloud usage, helping to protect against security threats and ensure compliance with security policies and regulations. CASBs can perform a variety of security-related functions, including identity and access management, data loss prevention, threat protection, and compliance enforcement, among others. By acting as an intermediary between cloud solutions and the organization, CASBs help to bridge the gap between security and cloud adoption, allowing organizations to securely adopt and manage cloud services.

upvoted 3 times

Question #185 *Topic 1*

An organization has a requirement to collect full metadata information about the traffic going through their AWS cloud services. They want to use this information for behavior analytics and statistics. Which two actions must be taken to implement this requirement? (Choose two.)

A. Send syslog from AWS to Cisco Stealthwatch Cloud.

B. Configure Cisco Stealthwatch Cloud to ingest AWS information.

C. Send VPC Flow Logs to Cisco Stealthwatch Cloud.

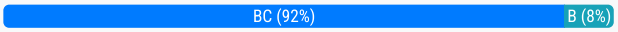
D. Configure Cisco Thousand Eyes to ingest AWS information.

E. Configure Cisco ACI to ingest AWS information.

Suggested Answer: *A, C*

Reference: https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch-cloud/at-a-glance-c45-739850.html

Community vote distribution



loser4fun Highly Voted 2 years, 5 months ago

C. Send VPC Flow Logs to Cisco Stealthwatch Cloud. VPC Flow Logs are a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs, which can be easily exported to Cisco Stealthwatch Cloud for analysis and monitoring. B. Configure Cisco Stealthwatch Cloud to ingest AWS information. Once the VPC Flow Logs are collected, they can be ingested into Cisco Stealthwatch Cloud for analysis and monitoring. This requires configuring Cisco Stealthwatch Cloud to ingest the AWS information and setting up the appropriate rules and policies for analysis and alerting. Therefore, options C and B are the correct answers.

upvoted 7 times

Yuta1123 Highly Voted 3 years, 3 months ago

Selected Answer: BC

I think BC is answer...

upvoted 6 times

Yuta1123 3 years, 3 months ago

I think BC is answer...Agree with you

upvoted 6 times

sajoz123 3 years, 3 months ago

Agree with you

upvoted 2 times

diverjim64 Most Recent 11 months, 3 weeks ago

Stealthwatch is now Cisco Secure Network Analytics.

upvoted 1 times

psuoh 2 years, 6 months ago

Configure AWS s3 bucket to store logs then grant Cisco Stealthwatch to read logs from it https://www.youtube.com/watch?v=rBz9jjMFdZc

upvoted 1 times

tanri04 2 years, 8 months ago

Yes correct answer: BC

upvoted 2 times

FortiSherlock 3 years ago

Configure StealthWatch Cloud and then send data from AWS to it.

upvoted 2 times

nomanlands 3 years, 1 month ago

Can't syslog out data from AWS. At best you can send logs to an AWS bucket and pick them up from there.

upvoted 1 times

Cyberops 3 years, 3 months ago

B and C

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/cloud/configuration/Public_Cloud_Monitoring_for_AWS_Quick_Start_Guide_DV_

2_0.pdf

upvoted 2 times

Question #186 *Topic 1*

An organization wants to implement a cloud-delivered and SaaS-based solution to provide visibility and threat detection across the AWS network. The solution must be deployed without software agents and rely on AWS VPC flow logs instead. Which solution meets these requirements?

A. NetFlow collectors

B. Cisco Cloudlock

C. Cisco Stealthwatch Cloud

D. Cisco Umbrella

Suggested Answer: *C*
Reference: https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html

loser4fun Most Recent 1 year, 11 months ago

C. Cisco Stealthwatch Cloud meets these requirements. It is a cloud-delivered and SaaS-based solution that provides visibility and threat detection across AWS networks. It uses AWS VPC flow logs for traffic analysis and does not require software agents to be installed. Cisco Umbrella is a cloud-based security platform for DNS and web traffic protection and does not rely on AWS VPC flow logs for its operation. NetFlow collectors are used for collecting and analyzing network traffic data and are not a complete solution for providing visibility and threat detection across AWS networks. Cisco Cloudlock is a cloud access security broker that provides visibility and control over cloud applications and data but does not provide threat detection across AWS networks.

upvoted 3 times

leowulf 2 years, 4 months ago

C

https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html

upvoted 1 times

Question #187 *Topic 1*

Where are individual sites specified to be blacklisted in Cisco Umbrella?

A. application settings

B. content categories

C. security settings

D. destination lists

Suggested Answer: *D*
Official Answer: D

idto Highly Voted 2 years, 2 months ago

D is correct. "To block a URL, simply enter it into a blocked destination list, or create a new blocked destination list just for URLs. To do this, navigate to Policies > Destination Lists, expand a Destination list, add a URL and then click Save." Source: https://support.umbrella.com/hc/en-us/articles/115004518146-Umbrella-Dashboard-New-Features-Custom-blocked-URLs

upvoted 9 times

Question #188 *Topic 1*

An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed through the Cisco Umbrella network. Which action tests the routing?

A. Ensure that the client computers are pointing to the on-premises DNS servers.

B. Enable the Intelligent Proxy to validate that traffic is being routed correctly.

C. Add the public IP address that the client computers are behind to a Core Identity.

D. Browse to http://welcome.umbrella.com/ to validate that the new identity is working.

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

juanlecho Highly Voted 4 years, 11 months ago

Correct answer is D https://docs.umbrella.com/deployment-umbrella/docs/protect-your-network

upvoted 29 times

hisho72 Highly Voted 4 years, 7 months ago

Correct Answer: Browse to http://welcome.umbrella.com/ to validate that the new identity is working. According to dump: Enable the Intelligent Proxy to validate that traffic is being routed correctly. Verify that your DNS connections are routed through Cisco Umbrella's global network by navigating to the following page in your client's browser: https://welcome.umbrella.com/. You should see the Welcome to Umbrella page. Note: You may need to restart your client's network interface or your computer. https://docs.umbrella.com/deployment-umbrella/docs/protect-your-network#section-step-4-test-yournetwork

upvoted 10 times

mrimmune Most Recent 3 years, 8 months ago

Correct is D

upvoted 1 times

TesterDude 3 years, 9 months ago

Selected Answer: D

The answer is D to test if Umbrella is protecting your network

upvoted 2 times

jaciro11 3 years, 11 months ago

Selected Answer: D

Correct answer is D

upvoted 3 times

Minion2021 3 years, 12 months ago

Obviously, the answer is D

upvoted 1 times

samismayilov 4 years, 9 months ago

http://welcome.umbrella.com/

upvoted 5 times

Question #189 *Topic 1*

How does Cisco Umbrella archive logs to an enterprise-owned storage?

A. by using the Application Programming Interface to fetch the logs

B. by sending logs via syslog to an on-premises or cloud-based syslog server

C. by the system administrator downloading the logs from the Cisco Umbrella web portal

D. by being configured to send logs to a self-managed AWS S3 bucket

Suggested Answer: *D*

Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

Community vote distribution

D (100%)

Happy_Shepherd26 Most Recent 1 year, 9 months ago

Where are Logs Stored? When you create a policy, activity logs are by default saved to the North America – California, US location of Umbrella's data warehouse. You can change the location of the data warehouse to Europe at any time. You can also optionally configure logging so that logs are also stored to an Amazon S3 bucket—either your own or one managed by Cisco.

upvoted 2 times

Kevbo02 4 years, 4 months ago

It is D. https://docs.umbrella.com/deployment-umbrella/docs/log-management says you can also save your logs to an Amazon S3 Bucket.

upvoted 4 times

Question #190 *Topic 1*

Which API is used for Content Security?

A. NX-OS API

B. IOS XR API

C. OpenVuln API

D. AsyncOS API

Suggested Answer: *D*

Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma12-0/api/b_SMA_API_12/test_chapter_01.html

Community vote distribution

D (100%)

sull3y Most Recent 1 year, 10 months ago

The AsyncOS API is used for content security. It is a set of REST APIs provided by Cisco to enable integration and automation of content security features, such as email and web security, into third-party applications or management systems. The AsyncOS API allows developers to interact with the content security platform, retrieve information, and perform actions such as blocking or quarantining emails or URLs based on various criteria.

upvoted 3 times

Anonymous983475 2 years, 1 month ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma12-0/api/b_SMA_API_12/test_chapter_01.html

upvoted 3 times

Question #191 *Topic 1*

Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?

A. IP Block List Center

B. File Reputation Center

C. AMP Reputation Center

D. IP and Domain Reputation Center

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

laribando98 Most Recent 11 months ago

IP and Domanin Repuatation cen

upvoted 1 times

Happy_Shepherd26 1 year, 9 months ago

d

upvoted 1 times

Zatingke 3 years, 6 months ago

Correct

upvoted 1 times

Question #192 *Topic 1*

What is the primary role of the Cisco Email Security Appliance?

A. Mail Submission Agent

B. Mail Transfer Agent

C. Mail Delivery Agent

D. Mail User Agent

Suggested Answer: *B*
Official Answer: B

testtaker42 Highly Voted 5 years, 7 months ago
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-EmailSecurityUsingCiscoESADesignGuide-AUG14.pdf Third Paragraph in "Design Overview" section on Page 3."It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay."
upvoted 8 times

testtaker42 Highly Voted 5 years, 7 months ago
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-EmailSecurityUsingCiscoESADesignGuide-AUG14.pdf

Third Paragraph in "Design Overview" section on Page 3.
upvoted 8 times

Premium_Pils Most Recent 2 years ago
"It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay."
upvoted 2 times

testtaker13 4 years, 9 months ago
B - MTA is correct
upvoted 4 times

Question #193 *Topic 1*

Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two.)

A. DDoS

B. antispam

C. antivirus

D. encryption

E. DLP

Suggested Answer: *D, E*

Reference:

https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

Community vote distribution

DE (100%)

idto Highly Voted 4 years, 2 months ago

D and E are correct. According to the Cisco doc they shared in the (Reveal Solution)... "while the on-premises appliances provide granular control—protecting sensitive information with data loss prevention (DLP) and encryption technologies."

upvoted 8 times

laribando98 Most Recent 11 months ago

Encryption Data Loss Prevention and encryption technolgies

upvoted 1 times

gorequill 2 years ago

The cloud-based infrastructure is typically used for inbound email cleansing, while the on-premises appliances provide granular control—protecting sensitive information with data loss prevention (DLP) and encryption technologies.

upvoted 2 times

NikoNiko 3 years, 7 months ago

Sure, D. "The cloud-based infrastructure is typically used for inbound email cleansing, while the on-premises appliances provide granular control—protecting sensitive information with data loss prevention (DLP) and encryption technologies." Source (same as in Q response): https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

upvoted 2 times

Question #194 *Topic 1*

An organization is receiving SPAM emails from a known malicious domain. What must be configured in order to prevent the session during the initial TCP communication?

A. Configure the Cisco ESA to reset the TCP connection.

B. Configure policies to stop and reject communication.

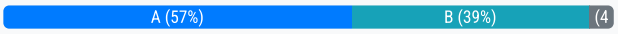
C. Configure the Cisco ESA to drop the malicious emails.

D. Configure policies to quarantine malicious emails.

Suggested Answer: *B*

Official Answer: B

Community vote distribution



west33637 Highly Voted 3 years, 7 months ago

A should be correct - TCPREFUSE resets the TCP connection. The question asks for preventing the session during the initial TCP communication. The remaining answers do not specify dropping the communication at TCP level.

upvoted 8 times

kerniger Highly Voted 5 years ago

hm it seems there is no clear valid answer A - probably the best answer because if you configure as "TCPREFUSE" it will send a "reset" at tcp. B - the client gehts responses at a higher level than tcp C - its not at tcp layer D - its not at tcp layer

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118179-configure-esa-00.html

upvoted 7 times

kerniger 5 years ago

hm it seems there is no clear valid answer A - probably the best answer because if you configure as "TCPREFUSE" it will send a "reset" at tcp. B - the client gehts responses at a higher level than tcp C - its not at tcp layer D - its not at tcp layer
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118179-configure-esa-00.htmlBased on this, I would go with B...
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00. html

upvoted 7 times

klu16 5 years ago

Based on this, I would go with B... https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00. html

upvoted 2 times

XBfoundX Most Recent 1 week ago

REJECT. Connection is initially accepted, but the client attempting to connect gets a 4XX or 5XX SMTP status code. No email is accepted. TCPREFUSE. Connection is refused at the TCP level. This question is anyway confusing, but the issue is that if we use the action REJECT we are saying that at least the TCP Session will be accepted, we will block then the SMTP session if the REJECT action.

upvoted 1 times

TanHK 7 months, 3 weeks ago

Why the Others Are Incorrect A. Reset the TCP connection Used for IP-based blocking, not domain-based identity C. Drop malicious emails Happens after the email is received D. Quarantine malicious emails Also post-acceptance

upvoted 1 times

A_Wolf 11 months, 2 weeks ago

I'd go for B. the question is PREVENT, a reset, resets the connecton (connection already took place) read this: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00.html You can configure your Email Security Appliance (ESA) to restrict connections by adding any of these items to Sender Groups which use Mail Flow Policies: IP range Specific host or domain name SenderBase Reputation Service (SBRS) "organization" classification SBRS score range DNS List query response Each Mail Flow Policy has an access rule, such as ACCEPT, REJECT, RELAY, CONTINUE, and TCPREFUSE. A host that attempts to establish a connection to your ESA and matches a Sender Group using a TCPREFUSE access rule is not allowed to connect to your ESA. From the standpoint of the sending server, it will appear as if your server is unavailable. Most MTAs will retry frequently in this case, which will create more traffic then answering once with a clear hard bounce, for example, REJECT.

upvoted 2 times

Demon_Queen_Velverosa 1 year, 11 months ago

The answer is B. The hint is TCP and not referring to anything high than TCP. A would only be valid if the TCP connection had already been established and if the ESA has that reset ability. in this case reset wouldn't even do anything as their is no connection to reset as a connection is trying to be established. C and D don't have anything to do with the question.

upvoted 1 times

Premium_Pils 2 years ago

Answer "B", REJECT would be the preferable solution based on this article: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00.html. However, answering with "554 SMTP error" seems to correspond with Layer 7, and not with Layer 4 (TCP). A TCP Reset acts at Layer 4. Thus, for me it is "A".

upvoted 2 times

4pelos 2 years, 5 months ago

Correct answer B. Checked with securitytut

upvoted 1 times

cristip 2 years, 7 months ago

I think it is B

upvoted 1 times

fdl543 3 years ago

A is correct. "prevent the session during the initial TCP communication" Only reset the TCP connection does this. B continues to communicate with the reject communication...

upvoted 2 times

jku2cya 3 years, 1 month ago

Typical ambiguous Cisco exam question. However I'd say A corresponds to TCPREFUSE and B corresponds to REJECT. B also mentions the word 'reject' in it. Also the link provided by multiple people in this thread states "A host that attempts to establish a connection to your ESA and encounters a REJECT will receive a 554 SMTP error (hard bounce)"

upvoted 1 times

DWizard 3 years, 1 month ago

Based on the links already shared, the best answer would be B. C and D does not work at the TCP level, and option A does not really reset the TCP connection, just ignore it, so the sender will try again to send the email. Option B will work in a similar way to A, but instead of ignoring the TCP connection, will reject it so the sender won't try again. It's a difficult one, I don't hope that everybody agrees with me.

upvoted 1 times

PeterHasse 3 years, 2 months ago

I think is A https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118214-configure-esa-00.html

upvoted 1 times

Jessie45785 3 years, 2 months ago

B - its cisco question must be B https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00.html

upvoted 1 times

theunnameddemon 3 years, 3 months ago

To prevent the session during the initial TCP communication with a known malicious domain and stop receiving spam emails, the appropriate action would be: A. Configure the Cisco ESA to reset the TCP connection. By configuring the Cisco ESA (Email Security Appliance) to reset the TCP connection, it would terminate the connection attempt during the initial handshake process. This prevents any further communication between the sender and the recipient, effectively blocking the spam emails from that malicious domain. Options B, C, and D are not specifically related to preventing the TCP session during initial communication: Option B: Configuring policies to stop and reject communication might be effective in blocking or filtering certain types of traffic or communication, but it doesn't specifically prevent the TCP session from being established.

upvoted 1 times

sis_net_sec 3 years, 10 months ago

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118219-configure- esa-00.html

upvoted 1 times

lucky2205 4 years, 1 month ago

Selected Answer: B

its B Each Mail Flow Policy has an access rule, such as ACCEPT, REJECT, RELAY, CONTINUE, and TCPREFUSE. A host that attempts to establish a connection to your ESA and matches a Sender Group using a TCPREFUSE access rule is not allowed to connect to your ESA. From the standpoint of the sending server, it will appear as if your server is unavailable. Most MTAs will retry frequently in this case, which will create more traffic then answering once with a clear hard bounce, for example, REJECT.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00.html

upvoted 2 times

NikoNiko 4 years, 1 month ago

"You can configure your Email Security Appliance (ESA) to restrict connections by adding any of these items to Sender Groups which use Mail Flow Policies: IP range Specific host or domain name SenderBase Reputation Service (SBRS) "organization" classification SBRS score range DNS List query response Each Mail Flow Policy has an access rule, such as ACCEPT, REJECT, RELAY, CONTINUE, and TCPREFUSE. A host that attempts to establish a connection to your ESA and matches a Sender Group using a TCPREFUSE access rule is not allowed to connect to your ESA." Source (2014): https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00.html Newer (2021) - the same but TCPREFUSE is replaced by "TCP refuse": https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216842-understand-parameters-related-to-mail-fl.html

upvoted 2 times

Dorr20 3 years, 4 months ago

A "reject" will send an NDR so it's not preventing the session. You also don't want a "known malicious" domain to know you are accepting message from other domains as you are trying to hide your ESA from attackers.

upvoted 2 times

Question #195 *Topic 1*

Refer to the exhibit. What is a result of the configuration?

```
Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S*   0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C        1.1.1.0 255.255.255.0 is directly connect, outside
S        172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C        192.168.100.0 255.255.255.0 is directly connected, inside
C        172.16.10.0 255.255.255.0 is directly connected, dmz
S          10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz

---------------------------------------------------------------

access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
 sfr fail-open

service-policy inside-policy global
```

A. Traffic from the DMZ network is redirected.

B. Traffic from the inside network is redirected.

C. All TCP traffic is redirected.

D. Traffic from the inside and DMZ networks is redirected.

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

LynenDutzow Highly Voted 5 years, 9 months ago

The answer is definitly D. The ACL's match 192.168.100.0 to 192.168.100.255 and 172.16.0.0 to 172.16.255.255. The DMZ and inside network fall in those ranges.

upvoted 14 times

getafix Highly Voted 4 years, 2 months ago

Traffic from both inside and DMZ networks is redirected. Inside networks are 192.168.100.0/24 and 172.16.0.0/16 DMZ network is 172.16.10.0/24 The redirect acl is permitting 192.168.100.0/24 and 172.16.0.0/16 (which also includes 172.16.10.0/24 --> traffic from DMZ networks)

upvoted 7 times

Alizade 2 years, 10 months ago

Answer: D

upvoted 1 times

TWu2 4 years, 7 months ago

10.10.10.0/24 (to DMZ) is not in the access-list. So the answer is B only.

upvoted 3 times

TWu2 4 years, 7 months ago

10.10.10.0/24 (to DMZ) is not in the access-list. So the answer is B only.I know this is late, but dont let this fool you as the /24 is apart of the /16 172.16.10.0/24 is apart of 172.16.0.0/16

upvoted 3 times

Demon_Queen_Velverosa Most Recent 1 year, 11 months ago

I know this is late, but dont let this fool you as the /24 is apart of the /16 172.16.10.0/24 is apart of 172.16.0.0/16

upvoted 1 times

Moll 4 years, 9 months ago

Yes, should be D

upvoted 2 times

statikd 5 years, 1 month ago

Answer is D 192.168.100.0 255.255.255.0 is directly connected, inside 172.16.10.0 255.255.255.0 is directly connected, dmz Both ACLs apply to these networks.

upvoted 3 times

oncledave 5 years, 7 months ago

What about the last static route 10.10.10.0/24 , part of the dmz ? The inside network, as well as part of the dmz fall in those ranges.D is correct. Answer D does not state that all networks from inside and DMZ are redirected, just the (some) traffic is redirected.correct answer would be: traffic from inside networks and traffic from DMZ DIRECTLY CONNECTED network are redirected. Teribly question as both B and D are can be considered correct answers.

upvoted 1 times

oncledave 5 years, 7 months ago

What about the last static route 10.10.10.0/24 , part of the dmz ? The inside network, as well as part of the dmz fall in those ranges.

upvoted 1 times

netwguy 5 years, 2 months ago

D is correct. Answer D does not state that all networks from inside and DMZ are redirected, just the (some) traffic is redirected.

upvoted 4 times

netwguy 5 years, 2 months ago

D is correct. Answer D does not state that all networks from inside and DMZ are redirected, just the (some) traffic is redirected.correct answer would be: traffic from inside networks and traffic from DMZ DIRECTLY CONNECTED network are redirected. Teribly question as both B and D are can be considered correct answers.

upvoted 4 times

dr4gn00t 4 years, 6 months ago

correct answer would be: traffic from inside networks and traffic from DMZ DIRECTLY CONNECTED network are redirected. Teribly question as both B and D are can be considered correct answers.

upvoted 2 times

Oz3006 5 years, 10 months ago

forget what is said, answer is D

upvoted 6 times

Oz3006 5 years, 10 months ago

answer is B If you look at the 172.16.10.0/24 for DMZ does not match the access list 172.16.0.0/16

upvoted 2 times

Oz3006 5 years, 10 months ago

answer is B If you look at the 172.16.10.0/24 for DMZ does not match the access list 172.16.0.0/16yes to this172.16.10.0 matches 172.16.0.0/16... 172.16.0.0 255.255.0.0 has rage of 172.16.0.0 - 172.16.255.255

upvoted 2 times

mecacig953 4 years, 4 months ago

yes to this

upvoted 2 times

Initial14 3 years, 10 months ago

172.16.10.0 matches 172.16.0.0/16... 172.16.0.0 255.255.0.0 has rage of 172.16.0.0 - 172.16.255.255

upvoted 1 times

Jimmyluckyone 5 years, 10 months ago

The access-list also matches the DMZ network 172.16.10.0 so D is correct

upvoted 4 times

AZak 5 years, 10 months ago

Is it D ? Im not 100% sure. Couldn't it maybe B ?

upvoted 1 times

Question #196 *Topic 1*

An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically. What must be configured to accomplish this?

A. Configure the Cisco WSA to modify policies based on the traffic seen.

B. Configure the Cisco ESA to modify policies based on the traffic seen.

C. Configure the Cisco WSA to receive real-time updates from Cisco Talos.

D. Configure the Cisco ESA to receive real-time updates from Cisco Talos.

Suggested Answer: *D*
Official Answer: D

Zatingke Most Recent 2 years ago
Correct
upvoted 2 times

Question #197 *Topic 1*

What are two differences between a Cisco WSA that is running in transparent mode and one running in explicit mode? (Choose two.)

A. The Cisco WSA responds with its own IP address only if it is running in explicit mode.

B. The Cisco WSA is configured in a web browser only if it is running in transparent mode.

C. The Cisco WSA responds with its own IP address only if it is running in transparent mode.

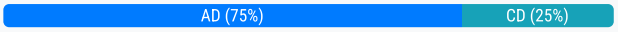
D. The Cisco WSA uses a Layer 3 device to redirect traffic only if it is running in transparent mode.

E. When the Cisco WSA is running in transparent mode, it uses the WSA's own IP address as the HTTP request destination.

Suggested Answer: *A, D*

Official Answer: AD

Community vote distribution



wfexco Highly Voted 5 years, 2 months ago

A and D are correct. - In explicit proxy mode, users are configured to use a web proxy and the web traffic is sent directly to the Cisco WSA. In contrast, in transparent proxy mode the Cisco WSA intercepts user's web traffic redirected from other network devices, such as switches, routers, or firewalls.

upvoted 21 times

Sarbi Highly Voted 4 years, 12 months ago

A and D is correct. No doubt it.

upvoted 5 times

Premium_Pils Most Recent 2 years ago

I am sure about "D" as a the traffic is redirected on a L3 device with PBR (or similar solution). "A" would be fine without the word "only". The WSA is a full proxy, maintaining separate sessions btw. client - proxy and proxy - webserver. The source IP of the response is surely the ip of the proxy in the client-proxy connection with Explicit mode, when the client directly communicates with the proxy. However, I am not sure the redirected Transparent mode, as again the proxy is sitting in between the client and the webserver. I assume that the client does not get the response directly from the webserver, but rather from the proxy. So the source ip should be from the proxy (or does it spoof the source ip?).

upvoted 2 times

squirrelzzz 2 years, 5 months ago

Transparent means it has no L3 interface

upvoted 1 times

Leogxn 3 years, 1 month ago

Selected Answer: CD

Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide-> Therefore in Transparent mode, WSA uses its own IP address to initiate a new connection the Web Server

upvoted 1 times

Leogxn 3 years, 1 month ago

Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide-> Therefore in Transparent mode, WSA uses its own IP address to initiate a new connection the Web ServerThe only problem is that that quote is nowhere in the OCG... It's AD: actual quote from the OCG: "When the Cisco WSA (as a web proxy) forwards a request, by default it changes the request source IP address to match its own address."

upvoted 1 times

Bubu3k 2 years ago

The only problem is that that quote is nowhere in the OCG... It's AD: actual quote from the OCG: "When the Cisco WSA (as a web proxy) forwards a request, by default it changes the request source IP address to match its own address."

upvoted 2 times

andrewj511 4 years, 11 months ago

When requests are being redirected to the WSA transparently, the WSA must pretend to be the OCS (origin content server), since the client is unaware of the existence of a proxy. On the contrary, if a request is explicitly sent to the WSA, the WSA will respond with it's own IP information.

upvoted 4 times

rad9899 5 years, 3 months ago

C&E is correct https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html

upvoted 1 times

rad9899 5 years, 3 months ago

C&E is correct https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.htmlNot C, But A - leaning toward D (wish it stated Layer4) When requests are being redirected to the WSA transparently, the WSA must pretend to be the OCS (origin content server), since the client is unaware of the existence of a proxy. On the contrary, if a request is explicitly sent to the WSA, the WSA will respond with it's own IP information.

upvoted 1 times

entitty 5 years, 2 months ago

Not C, But A - leaning toward D (wish it stated Layer4) When requests are being redirected to the WSA transparently, the WSA must pretend to be the OCS (origin content server), since the client is unaware of the existence of a proxy. On the contrary, if a request is explicitly sent to the WSA, the WSA will respond with it's own IP information.

upvoted 4 times

Question #198 *Topic 1*

Which technology is used to improve web traffic performance by proxy caching?

A. WSA

B. Firepower

C. FireSIGHT

D. ASA

Suggested Answer: *A*
Official Answer: A

Zatingke Most Recent 2 years ago
Correct, WSA can be a proxy cache
upvoted 1 times

Question #199 *Topic 1*

Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

A. transparent

B. redirection

C. forward

D. proxy gateway

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html

Community vote distribution

A (100%)

cyberwhizzy0 Most Recent 2 years, 1 month ago

How the WSA HTTP proxy obtains the client's request can be defined as one of two ways: Transparently or Explicitly. Deployment: Transparent Method: WCCP Description: A WCCP v2 enabled device (typically a router, switch, PIX, or ASA) redirects port 80 https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html

upvoted 4 times

gc999 2 years, 4 months ago

I guess this question should be rewritten as "Which mode must be used on Cisco WSA to redirect TCP traffic with WCCP?". There is no "transparent proxy mode", there is only "forward proxy mode".

upvoted 1 times

Question #200 *Topic 1*

What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

A. It decrypts HTTPS application traffic for unauthenticated users.

B. It alerts users when the WSA decrypts their traffic.

C. It decrypts HTTPS application traffic for authenticated users.

D. It provides enhanced HTTPS application detection for AsyncOS.

Suggested Answer: *D*
Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01011.html

ddev3737_111 Most Recent 2 years ago

D Decryption Option Description Decrypt for Authentication For users who have not been authenticated prior to this HTTPS transaction, allow decryption for authentication. Decrypt for End-User Notification Allow decryption so that AsyncOS can display the end-user notification. Note If the certificate is invalid and invalid certificates are set to drop, when running a policy trace, the first logged action for the transaction will be “decrypt”. Decrypt for End-User Acknowledgment For users who have not acknowledged the web proxy prior to this HTTPS transaction, allow decryption so that AsyncOS can display the end-user acknowledgment. Decrypt for Application Detection Enhances the ability of AsyncOS to detect HTTPS applications.
upvoted 2 times

ddev3737 2 years ago

D

Decryption Option

Description

Decrypt for Authentication

For users who have not been authenticated prior to this HTTPS transaction, allow decryption for authentication.

Decrypt for End-User Notification

Allow decryption so that AsyncOS can display the end-user notification.

Note If the certificate is invalid and invalid certificates are set to drop, when running a policy trace, the first logged action for the transaction will be “decrypt”. Decrypt for End-User Acknowledgment

For users who have not acknowledged the web proxy prior to this HTTPS transaction, allow decryption so that AsyncOS can display the end-user acknowledgment.

Decrypt for Application Detection

Enhances the ability of AsyncOS to detect HTTPS applications.
upvoted 2 times

Question #201 *Topic 1*

A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?

A. The ESA immediately makes another attempt to upload the file.

B. The file upload is abandoned.

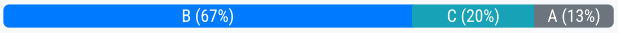
C. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.

D. The file is queued for upload when connectivity is restored

Suggested Answer: *B*

Official Answer: B

Community vote distribution



Seawanderer Highly Voted 5 years, 1 month ago

I'm not really sure about the answer, but it could be B

"The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.'

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html

upvoted 19 times

pohqinan 4 years, 5 months ago

Agree With this.

upvoted 1 times

kerniger Highly Voted 4 years, 12 months ago

its B

"The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more."

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html

upvoted 14 times

CyberGhost666 Most Recent 1 year, 1 month ago

Selected Answer: B

Network congestion is categorized as a connectivity problem, so ESA performs one upload attempt and then drops the file, not retrying it later.

upvoted 1 times

Demon_Queen_Velverosa 1 year, 11 months ago

The network is congested in this case so that means connectivity problems are occurring and so as many people have wrote but not emphasized. Theresa will drop the file and not upload it again because of connectivity issues.

upvoted 1 times

Demon_Queen_Velverosa 1 year, 11 months ago

Network congestion is a network connectivity issue as packets are being dropped because the network devices can't handle the absurd amount of network traffic.

upvoted 1 times

Mulema 2 years, 8 months ago

The correct answer to me even is D. The first part of the question is just noise to distract. The emphasis to me is the second half of the question - How will Cisco ESA handle any files which need analysis?

The Cisco ESA will not abandon the file upload. Instead, it will continue to attempt to upload the file until communication is restored. If the file is still not uploaded after a certain period of time, the Cisco ESA will cache the file and continue to attempt to upload it periodically

https://bard.google.com/chat/e3b8e30fe3160083

upvoted 3 times

Bandito 3 years, 1 month ago

Selected Answer: B

There is a video from a Cisco engineer. https://youtu.be/WD7UD70e2mo?t=453 I believe the answer is B.

upvoted 2 times

itsklk 3 years, 3 months ago

Selected Answer: A

Read this : https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html#anc5 Highlighting important notes:

If a file has recently been uploaded from any source, the file will not be uploaded again. For file analysis results for this file, search for the SHA-256 from the File Analysis reporting page. The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.

upvoted 1 times

ddev3737 3 years, 6 months ago

The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more

upvoted 1 times

Anonymous983475 3 years, 7 months ago

Selected Answer: C

The AMP first tries to compare file's hash to the cloud DB and if there is no such file it tries to upload it. It will retry if the upload fails.

upvoted 3 times

sis_net_sec 3 years, 10 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html

upvoted 1 times

lucky2205 4 years, 1 month ago

Selected Answer: B

its B the question clearly states that "The network is congested and is affecting communication." & its mentioned in ESA configuration guide "The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded."

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html

upvoted 7 times

bob511 4 years, 5 months ago

Cisco ESA adds a record of the SHA256 of this file to its internal database, where it is kept for up to 12 hours, and starts periodically querying if the analysis was complete, until it receives a positive response back from the file analysis service

i think C

upvoted 6 times

eazy99 4 years, 11 months ago

I actually believe the answer is D. I got it from Cisco website, here is the paragraph “The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.“ Please feel free to correct me if you think it’s not. This is the link: You will find it as the second point where they say Highly Important Notes: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html#anc1

upvoted 3 times

eazy99 4 years, 10 months ago

I apologize, I meant A not D.

upvoted 2 times

psuoh 3 years, 6 months ago

" If the failure was because the file analysis server was overloaded the upload will be attempted once more. " The network is congested as the question points out. The question doesnt mention about the analysis server being overloaded.

upvoted 1 times

kapplejacks 4 years, 11 months ago

There is NO (Zero) file upload, only a hash exchange making answer C the only correct answer.

upvoted 6 times

kapplejacks 4 years, 11 months ago

Cisco likes to do this, do not go down the path they are leading where they want you to over think. They would have said the file analysis server was overloaded if they wanted you to know about periodic upload. This question test your ability to know how AMP communicates about file reputation.

upvoted 5 times

Sarbi 4 years, 12 months ago

What about A. Highlighting important notes:

If a file has recently been uploaded from any source, the file will not be uploaded again. For file analysis results for this file, search for the SHA-256 from the File Analysis reporting page. The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.

upvoted 2 times

Question #202 *Topic 1*

An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address.
Which list contains the allowed recipient addresses?

A. SAT

B. BAT

C. HAT

D. RAT

Suggested Answer: *D*
Official Answer: D

sull3y Most Recent 1 year, 10 months ago

The correct answer is D. RAT (Recipient Access Table). The Cisco ESA (Email Security Appliance) can be used to control whether to accept or reject email messages to a recipient address. The list that contains the allowed recipient addresses is called the Recipient Access Table (RAT). The Recipient Access Table (RAT) is a list of email addresses that have been authorized to receive emails. When an email is received, the Cisco ESA checks the email address against the list in the RAT to determine whether to accept or reject the email.

upvoted 2 times

Kyle1776 2 years, 11 months ago

Overview of the Recipient Access Table (RAT) The Recipient Access Table defines which recipients are accepted by a public listener. At a minimum, the table specifies the address and whether to accept or reject it. The Recipient Access Table (RAT) page shows a listing of the entries in the RAT including the order, default action, and whether or not the entry has been configured to bypass LDAP accept queries.

upvoted 2 times

Cock 2 years, 11 months ago

AsyncOS uses the RAT for each Public Listener for managing acceptance or rejection of recipient addresses. Recipient addresses include these: Domains Email addresses Groups of email addresses By default, the RAT rejects all recipients to prevent the creation of an open relay.

upvoted 1 times

Question #203 *Topic 1*

Why would a user choose an on-premises ESA versus the CES solution?

A. Sensitive data must remain onsite.

B. Demand is unpredictable.

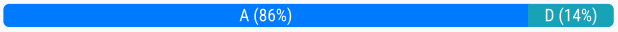
C. The server team wants to outsource this service.

D. ESA is deployed inline.

Suggested Answer: *A*

Official Answer: A

Community vote distribution



XBfoundX Most Recent 1 week ago

ESA is the appliance that you can run on prem, CES is Cloud Email Security, is an ESA appliance, running into the cloud.

upvoted 1 times

Demon_Queen_Velverosa 1 year, 11 months ago

It's A

upvoted 2 times

ZappBrannigan 2 years, 2 months ago

D - I think could be correct as well. Not sure how you can deploy a cloud based solution inline.

upvoted 1 times

Cock 4 years, 5 months ago

Cloud Email Security(CES)

upvoted 3 times

Question #204 *Topic 1*

Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two.)

A. Sophos engine

B. white list

C. RAT

D. outbreak filters

E. DLP

Suggested Answer: *A, D*

Official Answer: AD

Community vote distribution

AD (100%)

laribando98 Most Recent 11 months ago

Sophos engine Outbreak filters

upvoted 1 times

Pakawat 2 years, 1 month ago

Found this one in the exam

upvoted 3 times

san111 4 years, 3 months ago

A , D CVD-EmailSecurityUsingCiscoESADesignGuide-AUG14.pdf

upvoted 3 times

jshow 4 years, 6 months ago

A and D sophos is av engine

upvoted 1 times

jshow 4 years, 7 months ago

D for sure Cisco ESA uses a multilayer approach to fight viruses and malware: • The first layer of defense consists of outbreak filters, which the appliance downloads from Cisco SenderBase. They contain a list of known bad mail servers. These filters are generated by watching global email traffic patterns and looking for anomalies associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat. • The second layer of defense is using antivirus signatures to scan quarantined emails, to ensure that they do not carry viruses into the network. • Cisco ESA also scans outbound emails to provide antivirus protection.

upvoted 3 times

Question #205 *Topic 1*

After a recent breach, an organization determined that phishing was used to gain initial access to the network before regaining persistence. The information gained from the phishing attack was a result of users visiting known malicious websites. What must be done in order to prevent this from happening in the future?

A. Modify web proxy settings.

B. Modify outbound malware scanning policies.

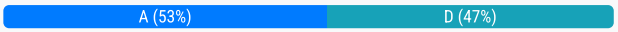
C. Modify identification profiles.

D. Modify an access policy.

Suggested Answer: *A*

Official Answer: A

Community vote distribution



entitty Highly Voted 5 years, 2 months ago

A - Configuring Web Proxy Settings - https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_0100.htmlWhy Intercepting Web Requests if we can block specific URL in a ACP policy ? D is the anwser imoFor future people who view this. Don't let this user throw you off and you start to over think. Even though they have a valid point the answer is still Afor a few reasons. 1 the attack already happened meaning what ever protections they had failed. Thus it doesn't matter if they block it or not as it won't protect from over website threats hence you modify the web security appliance proxy settings to hopefully prevent such attacks from other URL. It's being proactive. 2. The attack happened already, but now you block this one URL. So…. Your telling me your going to block every URL on the internet that attacks you or is bad with a ACL? Good luck trying to block the ocean as that not practical. Thus if you think blocking the URL is the way to go than you probably are not ready for a career in this field tbh.Really? Tbh I can ask the same question about you. Modify web proxy can mean anything while the ACP controls exactly what it is needed. For example, WebReputation and if that one can't correctly evaluate the url, than, manual blocking should do the trick. This doesn't mean u have to do it on the entire WWWIF i had a known CnC server that was involved with compromising my infrastructure i am 100% putting it on the firewall, 1 - Not all threat traffic egresses through http/https, 2 - Firewall will cover traffic for everything leaving the network, not juts the user groups using SWG.

upvoted 18 times

entitty Highly Voted 5 years, 2 months ago

A - Configuring Web Proxy Settings - https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_0100.html

upvoted 18 times

ureis 3 years, 8 months ago

Why Intercepting Web Requests if we can block specific URL in a ACP policy ? D is the anwser imoFor future people who view this. Don't let this user throw you off and you start to over think. Even though they have a valid point the answer is still Afor a few reasons. 1 the attack already happened meaning what ever protections they had failed. Thus it doesn't matter if they block it or not as it won't protect from over website threats hence you modify the web security appliance proxy settings to hopefully prevent such attacks from other URL. It's being proactive. 2. The attack happened already, but now you block this one URL. So…. Your telling me your going to block every URL on the internet that attacks you or is bad with a ACL? Good luck trying to block the ocean as that not practical. Thus if you think blocking the URL is the way to go than you probably are not ready for a career in this field tbh.Really? Tbh I can ask the same question about you. Modify web proxy can mean anything while the ACP controls exactly what it is needed. For example, WebReputation and if that one can't correctly evaluate the url, than, manual blocking should do the trick. This doesn't mean u have to do it on the entire WWWIF i had a known CnC server that was involved with compromising my infrastructure i am 100% putting it on the firewall, 1 - Not all threat traffic egresses through http/https, 2 - Firewall will cover traffic for everything leaving the network, not juts the user groups using SWG.

upvoted 5 times

ureis 3 years, 8 months ago

Why Intercepting Web Requests if we can block specific URL in a ACP policy ? D is the anwser imo

upvoted 5 times

Demon_Queen_Velverosa 1 year, 11 months ago

For future people who view this. Don't let this user throw you off and you start to over think. Even though they have a valid point the answer is still Afor a few reasons. 1 the attack already happened meaning what ever protections they had failed. Thus it doesn't matter if they block it or not as it won't protect from over website threats hence you modify the web security appliance proxy settings to hopefully prevent such attacks from other URL. It's being proactive. 2. The attack happened already, but now you block this one URL. So…. Your telling me your going to block every URL on the internet that attacks you or is bad with a ACL? Good luck trying to block the ocean as that not practical. Thus if you think blocking the URL is the way to go than you probably are not ready for a career in this field tbh.Really? Tbh I can ask the same question about you. Modify web proxy can mean anything while the ACP controls exactly what it is needed. For example, WebReputation and if that one can't correctly evaluate the url, than, manual blocking should do the trick. This doesn't mean u have to do it on the entire WWWIF i had a known CnC server that was involved with compromising my infrastructure i am 100% putting it on the firewall, 1 - Not all threat traffic egresses through http/https, 2 - Firewall will cover traffic for everything leaving the network, not juts the user groups using SWG.

upvoted 3 times

Demon_Queen_Velverosa 1 year, 11 months ago

For future people who view this. Don't let this user throw you off and you start to over think. Even though they have a valid point the answer is still Afor a few reasons.

1 the attack already happened meaning what ever protections they had failed. Thus it doesn't matter if they block it or not as it won't protect from over website threats hence you modify the web security appliance proxy settings to hopefully prevent such attacks from other URL. It's being proactive.

2. The attack happened already, but now you block this one URL. So…. Your telling me your going to block every URL on the internet that attacks you or is bad with a ACL? Good luck trying to block the ocean as that not practical. Thus if you think blocking the URL is the way to go than you probably are not ready for a career in this field tbh.

upvoted 3 times

Silexis 7 months ago

Really? Tbh I can ask the same question about you. Modify web proxy can mean anything while the ACP controls exactly what it is needed. For example, WebReputation and if that one can't correctly evaluate the url, than, manual blocking should do the trick. This doesn't mean u have to do it on the entire WWWIF i had a known CnC server that was involved with compromising my infrastructure i am 100% putting it on the firewall, 1 - Not all threat traffic egresses through http/https, 2 - Firewall will cover traffic for everything leaving the network, not juts the user groups using SWG.

upvoted 1 times

Silexis 7 months ago

Really? Tbh I can ask the same question about you. Modify web proxy can mean anything while the ACP controls exactly what it is needed. For example, WebReputation and if that one can't correctly evaluate the url, than, manual blocking should do the trick. This doesn't mean u have to do it on the entire WWW

upvoted 1 times

F0rtyx40 Most Recent 4 months, 1 week ago

IF i had a known CnC server that was involved with compromising my infrastructure i am 100% putting it on the firewall, 1 - Not all threat traffic egresses through http/https, 2 - Firewall will cover traffic for everything leaving the network, not juts the user groups using SWG.

upvoted 1 times

Iarn 4 years, 3 months ago

The Web Security appliance intercepts requests that are forwarded to it by clients or other devices over the network. The appliance works in conjunction with other network devices to intercept traffic. These may be ordinary switches, transparent redirection devices network taps,and other proxy servers or Web Security appliances.

upvoted 5 times

TanHK 7 months, 3 weeks ago

A. Modify web proxy settings: Adjusting proxy settings may affect traffic routing or authentication but does not inherently block malicious websites. It is a configuration step rather than a security policy change. Access Policy Control: Access policies define which websites users can visit based on URL filtering, reputation, and categories. Modifying these policies to block known malicious websites prevents users from accessing them, addressing the root cause described in the scenario.

upvoted 1 times

NETeng01 11 months ago

Modifying web proxy settings is the best way to prevent users from accessing known malicious websites and stop phishing attacks at the source.

upvoted 1 times

Basuso 1 year, 9 months ago

For me, you modify the Access Policy, so D choice. This is how you would enable URL Filtering and perform any actual security control for the traffic. Web Proxy Settings are usually what kind of port it would use to listen for HTTP/S Proxying, Caching settings, Authentication Settings, etc.

upvoted 2 times

Happy_Shepherd26 1 year, 9 months ago

On the WSA, to filter traffic based on Web Reputation you need to enable it on the Access Policies

upvoted 2 times

Demon_Queen_Velverosa 1 year, 11 months ago

To clarify this gives you a hint it's the was as it's not talking about only blocking that url but phishing attacks in general.

" What must be done in order to prevent this from happening in the future?"

upvoted 1 times

Demon_Queen_Velverosa 1 year, 11 months ago

To clarify this gives you a hint it's the was as it's not talking about only blocking that url but phishing attacks in general. " What must be done in order to prevent this from happening in the future?"I meant WSA as I am using my phone and stupid auto correct I am to lazy to turn off.

upvoted 1 times

Demon_Queen_Velverosa 1 year, 11 months ago

I meant WSA as I am using my phone and stupid auto correct I am to lazy to turn off.

upvoted 1 times

Demon_Queen_Velverosa 1 year, 11 months ago

It's A

upvoted 1 times

Premium_Pils 2 years ago

A - WSA. "Web reputation filtering protects client devices from visiting potentially harmful websites that contain malware or phishing links." + " URLs are checked against a list of known websites in the Cisco URL filtering database of more than 50 million blacklisted sites." https://study-ccnp.com/cisco-secure-web-appliance-cisco-wsa/ , https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_010000.html

upvoted 2 times

MPoels 2 years, 5 months ago

Selected Answer: D

Configure URL filters for Access Policy https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html#toc-hId--1455911870

upvoted 3 times

MPoels 2 years, 5 months ago

Configure URL filters for Access Policy https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html#toc-hId--1455911870Again don't fall for this comment as the ACL is not the way to go in this day and age as we have better security measures than an ACL. Remember the web security appliance can help find fishing attempts hence an attack was successful as it managed to sneak by the WSA. That's why an answer regarding modifying the web proxy config settings is the answer as the answer is the best solution to prevent future phishing attacks. This be a ok answer is the WSA was not mentioned as an answer.

upvoted 3 times

Demon_Queen_Velverosa 1 year, 11 months ago

Again don't fall for this comment as the ACL is not the way to go in this day and age as we have better security measures than an ACL. Remember the web security appliance can help find fishing attempts hence an attack was successful as it managed to sneak by the WSA. That's why an answer regarding modifying the web proxy config settings is the answer as the answer is the best solution to prevent future phishing attacks. This be a ok answer is the WSA was not mentioned as an answer.

upvoted 1 times

bobie 3 years, 3 months ago

I chose A since the term "malicious website" corresponds to the topic WSA.

upvoted 1 times

Dorr20 3 years, 4 months ago

WSA uses access policies to decide what to allow and what to block. "Settings" usually reffer to the appliance settings not to a policy. I'll go with - D

upvoted 1 times

Emlia1 3 years, 8 months ago

A or D

upvoted 2 times

pohqinan 4 years, 5 months ago

Answer is D https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Access_Control_Rules__URL_Filtering.html

upvoted 2 times

rbrain 4 years, 6 months ago

Selected Answer: D

Could it be D, i go for D: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html Tricky question.

upvoted 1 times

rbrain 4 years, 6 months ago

Could it be D, i go for D: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html Tricky question.Question is not focused on any specific product, therefore I think A is best answer in general, if you consider product can be WSA, Firepower, Umbrella or anything between..except you would modify an access policy to do this on FTD

upvoted 1 times

dr4gn00t 4 years, 6 months ago

Question is not focused on any specific product, therefore I think A is best answer in general, if you consider product can be WSA, Firepower, Umbrella or anything between..

upvoted 1 times

dr4gn00t 4 years, 6 months ago

Question is not focused on any specific product, therefore I think A is best answer in general, if you consider product can be WSA, Firepower, Umbrella or anything between..except you would modify an access policy to do this on FTD

upvoted 1 times

bob511 4 years, 5 months ago

except you would modify an access policy to do this on FTD

upvoted 2 times

Cock 4 years, 7 months ago

The answer is D

upvoted 1 times

testtaker13 4 years, 9 months ago

why not B?

upvoted 1 times

testtaker13 4 years, 9 months ago

why not B?B because the issue is with user requests to known malicious websites. Outbound malware scanning sounds more specific to the question.

upvoted 1 times

NullNull88 3 years, 10 months ago

B because the issue is with user requests to known malicious websites. Outbound malware scanning sounds more specific to the question.

upvoted 1 times

Question #206 *Topic 1*

An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly identifying all valid recipients. What must be done on the Cisco ESA to accomplish this goal?

A. Configure Directory Harvest Attack Prevention

B. Bypass LDAP access queries in the recipient access table.

C. Use Bounce Verification.

D. Configure incoming content filters.

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

kerniger Highly Voted 3 years, 6 months ago
i would choose A https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117847-technote-esa-00.html
upvoted 15 times

kerniger Highly Voted 3 years, 6 months ago
i would choose A https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117847-technote-esa-00.htmlDefinately A
upvoted 15 times

testtaker13 3 years, 3 months ago
Definately A
upvoted 2 times

yong08321 Most Recent 1 year, 9 months ago
To prevent malicious actors from quickly identifying all valid recipients, the engineer can use Directory Harvest Attack Prevention (DHAP) on the Cisco ESA. DHAP blocks SMTP messages to invalid recipient addresses and limits the number of messages that can be sent to the server, which helps prevent attackers from obtaining a complete list of valid email addresses. Therefore, option A is the correct answer. Option B, bypassing LDAP access queries in the recipient access table, does not provide any protection against Directory Harvest Attacks (DHAs). Option C, using Bounce Verification, is used to prevent backscatter, which is when an email system sends a bounce message to an innocent victim, who did not send the original message and who is not the intended recipient of the bounce message. Option D, configuring incoming content filters, is used to block unwanted emails based on message content.
upvoted 3 times

sull3y 1 year, 10 months ago
The correct answer is A. Configure Directory Harvest Attack Prevention. When LDAP (Lightweight Directory Access Protocol) accept queries are enabled on a listener, it is possible for malicious actors to quickly identify all valid recipients on the email server. This is known as a Directory Harvest Attack (DHA), and it can be used by spammers to collect valid email addresses to use for spamming. To prevent a DHA, the Cisco ESA (Email Security Appliance) must be configured with Directory Harvest Attack Prevention (DHAP). This feature limits the number of invalid queries a sender can make, and it can be used to detect and block DHA attempts.
upvoted 2 times

mecacig953 2 years, 10 months ago
The DHAP is a supported feature on the Cisco Content Security Appliances that can be enabled when Lightweight Directory Access Protocol (LDAP) acceptance validation is used. The DHAP feature keeps track of the number of invalid recipient addresses from a given sender. Once a sender crosses an administrator-defined threshold, the sender is deemed to be untrusted, and mail from that sender is blocked with no Network Design Requirement (NDR) or error code generation. You can configure the threshold based upon the reputation of the sender. For example, untrusted or suspicious senders can have a low DHAP threshold, and trusted or reputable senders can have a high DHAP threshold.
upvoted 1 times

nospampls 3 years, 6 months ago
i choose D For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used. Secondary actions include: Sending a copy to any custom quarantine or the Policy quarantine. Encrypt the message. The appliance only encrypts the message body. It does not encrypt the message headers. Altering the Subject header. Adding disclaimer text/HTML to the message. Sending the message to an alternate destination mailhost. Sending bcc copies of the message. Sending DLP violation

notification to the sender and/or other contacts. These actions are not mutually exclusive — you can combine some of them within different DLP policies for various processing needs for different user groups. We are going to implement the following DLP Actions: Encrypt These actions assume that Encryption is licensed and configured on the ESA and three profiles have been created for High, Medium, and Low security as was done in the earlier sections: CRES_HIGH CRES_MED CRES_LOW https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html#anc11

upvoted 1 times

jshow 3 years, 6 months ago

i believe its access policy....u can create an ips and attach it to the access policy to prevent

upvoted 1 times

Question #207 *Topic 1*

In which two ways does a system administrator send web traffic transparently to the Cisco WSA? (Choose two.)

A. use Web Cache Communication Protocol

B. configure AD Group Policies to push proxy settings

C. configure the proxy IP address in the web-browser settings

D. configure policy-based routing on the network infrastructure

E. reference a Proxy Auto Config file

Suggested Answer: *A, D*

Official Answer: AD

Community vote distribution

AD (100%)

entitty Highly Voted 3 years, 2 months ago

A&D.. transparent Any configuration on client device is explicit/forward

upvoted 31 times

entitty Highly Voted 3 years, 2 months ago

A&D.. transparent Any configuration on client device is explicit/forwardSticking with A & EIgnore my last comment

upvoted 31 times

deathfrom 3 years, 2 months ago

Sticking with A & E

upvoted 4 times

deathfrom 3 years, 2 months ago

Sticking with A & EIgnore my last comment

upvoted 4 times

deathfrom 3 years, 2 months ago

Ignore my last comment

upvoted 5 times

sathees_121 Most Recent 2 years, 1 month ago

A & D confirmed

upvoted 2 times

getafix 2 years, 1 month ago

When the Cisco WSA is in transparent mode, clients do not know there is a proxy deployed. Network infrastructure devices are configured to forward traffic to the Cisco WSA. In transparent mode deployments, network infrastructure devices redirect web traffic to the proxy. Web traffic redirection can be done using policy-based routing (PBR)—available on many routers —or using Cisco's Web Cache Communication Protocol (WCCP) on Cisco ASA, Cisco routers, or switches. Extract from Cisco OCG

upvoted 4 times

madcloud 2 years, 2 months ago

A&D is the right answer. For Transparent option : use PBR (policy based routing), WCCP or L4-L7 redirection. For explicit forwarding: configure Browser or use .PAC file

upvoted 2 times

djsonicdh 2 years, 3 months ago

Pbr a and D

upvoted 1 times

breezer 2 years, 4 months ago

A & D Using PAC Files is Explicit Mode - https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html

upvoted 1 times

mecacig953 2 years, 4 months ago

wccp and routing

upvoted 1 times

flejd 2 years, 7 months ago

PBR and WCCP

upvoted 1 times

MoII 2 years, 9 months ago

I'll go with A and D here

upvoted 2 times

Sarbi 2 years, 12 months ago

A and D

upvoted 2 times

ferari 3 years, 1 month ago

This question is not direct,direct traffic to WSA is by using explicit mode. The Transparent method is not direct to the WSA.It has to be redirected by a layer 3 device. The question is stating web traffic transparently (Direct). it seems B and C is the right answer.

upvoted 1 times

hisho72 3 years, 1 month ago

Answer E is relatede to explicit mode to configure proxy settings for clients

upvoted 3 times

itisfakemaillol 3 years, 1 month ago

A and D

upvoted 2 times

Question #208 *Topic 1*

What is the function of the Context Directory Agent?

A. reads the AD logs to map IP addresses to usernames

B. relays user authentication requests from Cisco WSA to AD

C. maintains users' group memberships

D. accepts user authentication requests on behalf of Cisco WSA for user identification

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_oveviw.html

Community vote distribution

A (100%)

mecacig953 Most Recent 1 year, 10 months ago

Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to).

upvoted 3 times

Question #209 *Topic 1*

A network administrator is configuring a rule in an access control policy to block certain URLs and selects the `Chat and Instant Messaging` category. Which reputation score should be selected to accomplish this goal?

A. 5

B. 10

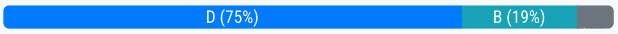
C. 3

D. 1

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Kuzi Highly Voted 3 years, 2 months ago

The answer is D. 1. A reputation score of 1 is the lowest possible score, and it indicates that the URL is considered to be very risky. This means that the network administrator should block all URLs with a reputation score of 1, in order to prevent users from accessing malicious websites. The other possible answers are incorrect. A reputation score of 5 is considered to be "neutral", while a reputation score of 10 is considered to be "good". This means that URLs with these scores should not be blocked. A reputation score of 3 is considered to be "suspect", and it may be necessary to block some URLs with this score, depending on the organization's specific policies and risk tolerance. Here is a table that shows the different reputation scores and their corresponding meanings: Reputation Score | Meaning ------ | ------- 1 | Very risky 3 | Suspect 5 | Neutral 10 | Good

upvoted 7 times

TanHK Most Recent 7 months, 3 weeks ago

To block all URLs within the "Chat and Instant Messaging" category, the network administrator should set the reputation score to the highest value available in the system (typically representing the strictest threshold). This ensures that even sites with a good reputation within that category are blocked. Given the reputation score scale is likely 1–10 (since 10 is an option), selecting 10 would block all sites in the category regardless of their individual reputation scores.

upvoted 1 times

Happy_Shepherd26 1 year, 9 months ago

We are talking about ACP (Access Control Policy) which is only to be found on Firepower. When you have an URL filtering license on your FMC you can enable URL filtering based on reputation which provides a score of 1 (Untrusted), 2 (Questionable) 3 (Neutral or Unknown) 4 (Favorable) and 5 (Trusted).

upvoted 1 times

iratus_umbra 3 years, 4 months ago

About URL Filtering with Category and Reputation With a URL Filtering license, you can control access to websites based on the category and reputation of requested URLs: Category—A general classification for the URL. For example, ebay.com belongs to the Auctions category, and monster.com belongs to the Job Search category. A URL can belong to more than one category. Reputation—How likely the URL is to be used for purposes that might be against your organization's security policy. Reputations range from Unknown risk (level 0) or Untrusted (level 1) to Trusted (level 5). In the URL Filtering Overview section https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html#Cisco_Reference.dita_72248e9a-706c-4e53-9bf1-de72f87b1bebquestion is about ESA. Why are you looking at firepower? why do you think the question is from ESA?Chat and Instant Messaging

upvoted 3 times

iratus_umbra 3 years, 4 months ago

Selected Answer: D

About URL Filtering with Category and Reputation With a URL Filtering license, you can control access to websites based on the category and reputation of requested URLs:

Category—A general classification for the URL. For example, ebay.com belongs to the Auctions category, and monster.com belongs to the Job Search category.

A URL can belong to more than one category.

Reputation—How likely the URL is to be used for purposes that might be against your organization's security policy. Reputations range from Unknown risk (level 0) or Untrusted (level 1) to Trusted (level 5).

In the URL Filtering Overview section https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html#Cisco_Reference.dita_72248e9a-706c-4e53-9bf1-de72f87b1beb

upvoted 3 times

jienBoq 3 years, 4 months ago

question is about ESA. Why are you looking at firepower?

upvoted 1 times

jienBoq 3 years, 4 months ago

question is about ESA. Why are you looking at firepower?why do you think the question is from ESA?Chat and Instant Messaging

upvoted 1 times

stalkr3 3 years, 3 months ago

why do you think the question is from ESA?Chat and Instant Messaging

upvoted 2 times

seb008 3 years, 1 month ago

Chat and Instant Messaging

upvoted 1 times

zsrite 3 years, 4 months ago

The appropriate reputation score to select in an access control policy to block URLs in the "Chat and Instant Messaging" category would depend on the organization's specific policies and risk tolerance. However, generally speaking, a higher reputation score would be more restrictive and block more URLs. Malicious (-10.0 to -6.0), Suspect (-5.9 to 5.9), Clean (6.0 to 10.0)

upvoted 2 times

Toni_Su91 3 years, 5 months ago

Selected Answer: C

In new FMC 7.2 When creating Access Policy Rule, you have a range from 1-5 in Reputation for Chat and Instant Messaging. 3 - Will block Neutral Reputation to Untruset 1 - Will block Untrusted Reputation

However there is more levels.

In old fmc it seems to be only 1-3 and 3 will block from Untrusted to Neutral.

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html#Cisco_Reference.dita_72248e9a-706c-4e53-9bf1-de72f87b1beb

upvoted 1 times

Toni_Su91 3 years, 5 months ago

In new FMC 7.2 When creating Access Policy Rule, you have a range from 1-5 in Reputation for Chat and Instant Messaging. 3 - Will block Neutral Reputation to Untruset 1 - Will block Untrusted Reputation However there is more levels. In old fmc it seems to be only 1-3 and 3 will block from Untrusted to Neutral. https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html#Cisco_Reference.dita_72248e9a-706c-4e53-9bf1-de72f87b1bebquestion is about ESA. Why are you looking at firepower?why do you think the question is from ESA?

upvoted 1 times

jienBoq 3 years, 4 months ago

question is about ESA. Why are you looking at firepower?why do you think the question is from ESA?

upvoted 1 times

stalkr3 3 years, 3 months ago

why do you think the question is from ESA?

upvoted 2 times

Tuxzinator 3 years, 6 months ago

I belove it was -10 to +10. -10 was block. 0 nutreal monitor. Weird question

upvoted 1 times

Zatingke 3 years, 6 months ago

No clue

upvoted 1 times

Question #210 *Topic 1*

A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?

A. The policy was created to send a message to quarantine instead of drop.

B. The file has a reputation score that is below the threshold.

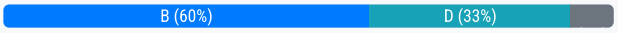
C. The file has a reputation score that is above the threshold.

D. The policy was created to disable file analysis.

Suggested Answer: *B*

Official Answer: B

Community vote distribution



Dinges Highly Voted 4 years, 7 months ago

I found B a possibility Quarantine is only for unrecognised files. When file is undetermined, reputation score is checked. Reputation 1-59: Deliver file / Reputation 60-100: Block file So B looks correct. Look at - Figure 1. Advanced Malware Protection Workflow for Public-Cloud File Analysis Deployments https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010000.html

upvoted 20 times

itisfakemaillol Highly Voted 4 years, 7 months ago

I am sure it is D. The policy was created to disable file analysis. When the reputation is not clear = undetermined, the file should be send for file analysis. It is not happening, so the file is not dropped.

upvoted 7 times

CyberGhost666 Most Recent 1 year, 1 month ago

D is correct

upvoted 1 times

Pierre_Bouvier 1 year, 6 months ago

Based on the Cisco documentation, files with an undetermined verdict (i.e., "Unscannable" or files without sufficient reputation data) can be configured to either be sent for further analysis or quarantined. If no policy action is set to quarantine or analyze such files, they may be released to the recipient. Given this, the most likely reason for the issue you're describing is: D. The policy was created to disable file analysis. Disabling file analysis would prevent undetermined verdicts from being processed correctly, leading to files not being dropped or quarantined as expected. https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-2-3/User_Guide/b_ESA_Admin_Guide_14-2-3/b_ESA_Admin_Guide_12_1_chapter_010001.html#con_1809437

upvoted 1 times

Ozzig 1 year, 9 months ago

Check the flow diagram, it's B https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-2-3/User_Guide/b_ESA_Admin_Guide_14-2-3/b_ESA_Admin_Guide_12_1_chapter_010001.html#con_1809437

upvoted 3 times

rishard 2 years, 6 months ago

The correct answer is B (it took me long to understand that) There is a difference between "Undetermined" (from the question), and "Unrecognized". Undetermined - It checks the file score (Which is in the question - Right answer - B). Unrecognize - Push file for analysis (Answer D - which is wrong in this case). https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010000.html

upvoted 3 times

rishard 2 years, 7 months ago

I would go with D. When a file's reputation verdict is undetermined, it means that the Cisco ESA's file analysis feature could not determine the reputation of the file. In a typical configuration, the Cisco ESA would have the ability to drop or quarantine files based on their reputation verdicts. However, if the policy is set to disable file analysis, it means that the Cisco ESA is not analyzing the files and therefore cannot drop them based on their reputation. Therefore, option D is the most likely cause of the issue described in the scenario.

upvoted 1 times

DWizard 2 years, 7 months ago

Option B is correct. Above figure 1 on the already shared link is the explanation.

upvoted 1 times

achille5 3 years ago

In the scenario described in the question, the issue is that the Cisco ESA is not dropping files that have an undetermined verdict. The undetermined verdict means that the reputation service did not have enough information to determine the file's reputation score. When the Cisco ESA encounters a file with an undetermined verdict, it checks the message filter to determine the action to take. If the message filter is configured to quarantine the message, then the file will be sent to the quarantine area, even if the reputation score is undetermined.

upvoted 1 times

nicklapa 3 years, 1 month ago

If the file is known to the reputation service but there is insufficient information for a definitive verdict, the reputation service returns a reputation score based on characteristics of the file such as threat fingerprint and behavioral analysis. If this score meets or exceeds the configured reputation threshold, the appliance applies the action that you have configured in the mail policy for files that contain malware .

upvoted 1 times

ureis 3 years, 3 months ago

Maybe the “newly installed service” in this Qmentions about Advanced Malware Protection (AMP) which can be used along with ESA. AMP allows superior protection across the attack continuum.

upvoted 1 times

Jamesy 3 years, 4 months ago

C is the correct answer. Cheers

upvoted 1 times

ChrisMT 3 years, 7 months ago

Answer B guys, please refer to the Figure 1. Advanced Malware Protection Workflow for Public-Cloud File Analysis Deployments The undetermined verdict with score 1- 59 will delivery the file to user The undetermined verdict with score 60- 100 will block the file So answer C, the reputation score is above the threshold is correct ! https://www.cisco.com/c/dam/en/us/td/i/400001-500000/410001-420000/415001-416000/415734.tif/_jcr_content/renditions/415734.jpg

upvoted 4 times

ChrisMT 3 years, 7 months ago

Answer B guys, please refer to the Figure 1. Advanced Malware Protection Workflow for Public-Cloud File Analysis Deployments The undetermined verdict with score 1- 59 will delivery the file to user The undetermined verdict with score 60- 100 will block the file So answer C, the reputation score is above the threshold is correct ! https://www.cisco.com/c/dam/en/us/td/i/400001-500000/410001-420000/415001-416000/415734.tif/_jcr_content/renditions/415734.jpgSorry for the typo, answer is CSorry, typo again, final the answer is B Confirmed! the old version of the doc shown below https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010001.htmlShould be this one: https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_14-0/b_ESA_Admin_Guide_ces_14-0/b_ESA_Admin_Guide_12_1_chapter_010001.html

upvoted 4 times

ChrisMT 3 years, 7 months ago

Sorry for the typo, answer is C

upvoted 2 times

ChrisMT 3 years, 7 months ago

Sorry for the typo, answer is CSorry, typo again, final the answer is B Confirmed! the old version of the doc shown below https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010001.htmlShould be this one: https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_14-0/b_ESA_Admin_Guide_ces_14-0/b_ESA_Admin_Guide_12_1_chapter_010001.html

upvoted 2 times

ChrisMT 3 years, 7 months ago

Sorry, typo again, final the answer is B Confirmed! the old version of the doc shown below https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010001.htmlShould be this one: https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_14-0/b_ESA_Admin_Guide_ces_14-0/b_ESA_Admin_Guide_12_1_chapter_010001.html

upvoted 1 times

ChrisMT 3 years, 7 months ago

Sorry, typo again, final the answer is B Confirmed! the old version of the doc shown below https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010001.html

upvoted 1 times

Stevens0103 2 years, 1 month ago

Should be this one: https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_14-0/b_ESA_Admin_Guide_ces_14-0/b_ESA_Admin_Guide_12_1_chapter_010001.html

upvoted 1 times

Orestesmc 3 years, 8 months ago

it is the reputation of the file that is being inspected, for an indeterminate verdict a score is set from 0 to 100 - C, its correct. https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide/b_ESA_Admin_Guide_ces_11_0/b_ESA_Admin_Guide_chapter_010000.pdf

upvoted 2 times

larn 3 years, 9 months ago

How are SenderBase Reputation Scores (SBRS) determined, and what do they mean? SenderBase scores are assigned to IP addresses based on a combination of factors, including email volume and reputation. Reputation scores in SenderBase may range from -10 to +10, reflecting the likelihood that a sending IP address is trying to send spam. Highly negative scores indicate senders who are very likely to be sending spam; highly positive scores indicate senders who are unlikely to be sending spam.

upvoted 1 times

semi1750 3 years, 10 months ago

B looks correct. "undetermined verdict" is located right before scoring within the "Recognized File" process under reputational service. once a file has undetermind verdict, there are only 2 options below, deliver or drop based on the reputation score. for D, I am not sure if you can make a policy to disable fily analysis service....you can enable or disable the service optionally....

upvoted 1 times

mecacig953 3 years, 10 months ago

https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_010000.html undetermined verdict below threshold on reputation score so delivered

upvoted 1 times

Question #211 *Topic 1*

An organization has a Cisco ESA set up with DLP policies and would like to customize the action assigned for violations. The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?

A. deliver and add disclaimer text

B. quarantine and send a DLP violation notification

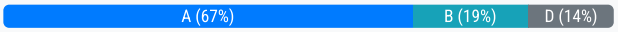
C. quarantine and alter the subject header with a DLP violation

D. deliver and send copies to other recipients

Suggested Answer: *B*

Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html

Community vote distribution



VI_Vershinin Highly Voted 5 years ago

It is B. Read chapter 5. Creating Data Loss Prevention Message Actions https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html

upvoted 17 times

VI_Vershinin Highly Voted 5 years ago

It is B. Read chapter 5. Creating Data Loss Prevention Message Actions https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.htmlAbsolutely B. This is from Chapter 5 Vershinin speaks of: About DLP Message Actions DLP message actions describe what actions that the ESA will take when it detects a DLP violation in an outgoing email. You can specify primary and secondary DLP Actions and different actions can be assigned for different violation types and severities. Primary actions include: Deliver Drop Quarantine For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used.Here is the rest (can't edit original post) Secondary actions include: Sending a copy to any custom quarantine or the 'Policy' quarantine. Encrypt the message. The appliance only encrypts the message body. It does not encrypt the message headers. Altering the Subject header. Adding disclaimer text/HTML to the message. Sending the message to an alternate destination mailhost. Sending bcc copies of the message. Sending DLP violation notification to the sender and/or other contacts.You meant A, wrote B. A) deliver and add disclaimer text - exactly as explained above

upvoted 17 times

aalnman 4 years, 10 months ago

Absolutely B. This is from Chapter 5 Vershinin speaks of: About DLP Message Actions

DLP message actions describe what actions that the ESA will take when it detects a DLP violation in an outgoing email. You can specify primary and secondary DLP Actions and different actions can be assigned for different violation types and severities.

Primary actions include: Deliver Drop Quarantine

For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used.

upvoted 3 times

aalnman 4 years, 10 months ago

Absolutely B. This is from Chapter 5 Vershinin speaks of: About DLP Message Actions DLP message actions describe what actions that the ESA will take when it detects a DLP violation in an outgoing email. You can specify primary and secondary DLP Actions and different actions can be assigned for different violation types and severities. Primary actions include: Deliver Drop Quarantine For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used.Here is the rest (can't edit original post) Secondary actions include: Sending a copy to any custom quarantine or the 'Policy' quarantine. Encrypt the message. The appliance only encrypts the message body. It does not encrypt the message headers. Altering the Subject header. Adding disclaimer text/HTML to the message. Sending the

message to an alternate destination mailhost. Sending bcc copies of the message. Sending DLP violation notification to the sender and/or other contacts.You meant A, wrote B. A) deliver and add disclaimer text - exactly as explained above

upvoted 3 times

aalnman 4 years, 10 months ago

Here is the rest (can't edit original post)

Secondary actions include:

Sending a copy to any custom quarantine or the 'Policy' quarantine. Encrypt the message. The appliance only encrypts the message body. It does not encrypt the message headers. Altering the Subject header. Adding disclaimer text/HTML to the message. Sending the message to an alternate destination mailhost. Sending bcc copies of the message. Sending DLP violation notification to the sender and/or other contacts.

upvoted 1 times

aalnman 4 years, 10 months ago

Here is the rest (can't edit original post) Secondary actions include: Sending a copy to any custom quarantine or the 'Policy' quarantine. Encrypt the message. The appliance only encrypts the message body. It does not encrypt the message headers. Altering the Subject header. Adding disclaimer text/HTML to the message. Sending the message to an alternate destination mailhost. Sending bcc copies of the message. Sending DLP violation notification to the sender and/or other contacts.You meant A, wrote B. A) deliver and add disclaimer text - exactly as explained above

upvoted 1 times

NikoNiko 4 years, 1 month ago

You meant A, wrote B. A) deliver and add disclaimer text - exactly as explained above

upvoted 7 times

itisfakemaillol 5 years, 1 month ago

It is definetely A. deliver and add disclaimer text

upvoted 12 times

Premium_Pils Most Recent 2 years ago

I would choos A based on this: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html#:~:text=Adding%20disclaimer%20text/HTML%20to%20the%20message -Sending bcc copies of the message. -Adding disclaimer text/HTML to the message.

upvoted 1 times

cbaina 2 years, 1 month ago

IT is D, look this scenario: Sending copies (bcc) of messages to other recipients. For example, you could copy messages with critical DLP violations to a compliance officer's mailbox for examination. ---------- Not A, Not B, Because not mentioned about "send a copy of message" Not B, Although you guys mentioned about the below secondary action in your comments, But in the second option (B) there is not any sign of a copy of message (((Secondary actions include: Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message.)))

upvoted 1 times

DaleC78 2 years, 3 months ago

B without a doubt. Emails violating internal DLP policies shouldn't be delivered, otherwise what's the point? The provided link explains it perfectly: 5. Creating Data Loss Prevention Message Actions Create DLP Quarantines If you'd like to keep a copy of messages violating DLP policies you can create individual Policy quarantines for each type of policy violation. This is especially useful when running a 'transparent' POV, where Outbound messages violating DLP policies are logged and delivered but no action is taken on the messages.Misreaded that one... Seems that's A

upvoted 1 times

DaleC78 2 years, 3 months ago

Selected Answer: B

B without a doubt. Emails violating internal DLP policies shouldn't be delivered, otherwise what's the point? The provided link explains it perfectly: 5. Creating Data Loss Prevention Message Actions Create DLP Quarantines

If you'd like to keep a copy of messages violating DLP policies you can create individual Policy quarantines for each type of policy violation. This is especially useful when running a 'transparent' POV, where Outbound messages violating DLP policies are logged and delivered but no action is taken on the messages.

upvoted 1 times

DaleC78 2 years, 2 months ago

Misreaded that one... Seems that's A

upvoted 1 times

red_sparrow_Gr 2 years, 9 months ago

the question states : ...The organization wants a copy of the message to be delivered... So B and C are excluded

upvoted 2 times

cyberwhizzy0 3 years, 1 month ago

I think B is correct (not too certain though) Primary actions include: Deliver Drop Quarantine Secondary actions include: Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message. https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html

upvoted 1 times

jku2cya 3 years, 1 month ago

As per the link Vl_Vershinin posted and under "Secondary actions include.."

upvoted 1 times

gc999 3 years, 2 months ago

Selected Answer: D

Here I will choose "D". The question said the organization wants a "copy of the message to be delivered". Only option "D" would do "sending copies.

Refer to "https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html#con_1304495", only this point can meet - "Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer's mailbox for examination.)".

upvoted 2 times

gc999 3 years, 2 months ago

Here I will choose "D". The question said the organization wants a "copy of the message to be delivered". Only option "D" would do "sending copies. Refer to "https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html#con_1304495", only this point can meet - "Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer's mailbox for examination.)".Wrong URL quoted, it should be "https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html"Sorry, I believe "A" is the answer https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html#:~:text=Adding%20disclaimer%20text/HTML%20to%20the%20message

upvoted 2 times

gc999 3 years, 2 months ago

Wrong URL quoted, it should be "https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html"

upvoted 1 times

gc999 3 years, 2 months ago

Wrong URL quoted, it should be "https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html"Sorry, I believe "A" is the answer https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html#:~:text=Adding%20disclaimer%20text/HTML%20to%20the%20message

upvoted 1 times

gc999 3 years, 2 months ago

Sorry, I believe "A" is the answer https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html#:~:text=Adding%20disclaimer%20text/HTML%20to%20the%20message

upvoted 1 times

angry 3 years, 5 months ago

Absolutely A!

upvoted 2 times

achille5 3 years, 6 months ago

deliver and add disclaimer text

upvoted 1 times

jienBoq 3 years, 6 months ago

as per https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html Primary actions include: Deliver Drop Quarantine For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used. Secondary actions include: Sending a copy to any custom quarantine or the

‘Policy’ quarantine. Encrypt the message. The appliance only encrypts the message body. It does not encrypt the message headers. Altering the Subject header. Adding disclaimer text/HTML to the message. Sending the message to an alternate destination mailhost. Sending bcc copies of the message. Sending DLP violation notification to the sender and/or other contacts.

upvoted 5 times

Emlia1 3 years, 7 months ago

A or B

upvoted 1 times

Emlia1 3 years, 8 months ago

I prefer A

upvoted 1 times

sathees_121 4 years, 1 month ago

It is D https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html

upvoted 1 times

sha2 4 years, 3 months ago

its deliver because the questions says "wants a copy of the message to be delivered" and in the Configuration guide "Note If you select Deliver, you can choose to have a copy of the message sent to a policy quarantine. The copy of the message is a perfect clone, including the Message ID." then add disclaimer text because the question says "to be delivered with a message added to flag it as a DLP violation" and in configuration guide it says : "To include disclaimer text when delivering messages with DLP violations or suspected violations, specify disclaimer text in Mail Policies" so answer is A

upvoted 5 times

Pupu 4 years, 5 months ago

Answer is D. In the referenced guide, it mentions that you can take two actions for DLP messages, primary and secondary. Here the primary would be "Deliver" and secondary "Sending DLP violation notification to the sender and/or other contacts." It also says: "For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used." Since the question clearly states that message needs to be delivered, the answer cannot be B or C. We're left with A and D. I am picking D because the secondary action it specifies is the only that sends violation notifications.

upvoted 1 times

Question #212 *Topic 1*

A Cisco ESA administrator has been tasked with configuring the Cisco ESA to ensure there are no viruses before quarantined emails are delivered. In addition, delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two.)

A. Deploy the Cisco ESA in the DMZ.

B. Use outbreak filters from SenderBase.

C. Configure a recipient access table.

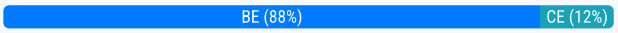
D. Enable a message tracking service.

E. Scan quarantined emails using AntiVirus signatures.

Suggested Answer: *B, E*

Official Answer: BE

Community vote distribution



Basuso Most Recent 1 year, 9 months ago

Guys, Recipient Table Address (RAT) is where you define which recipients can receive emails, not from where emails will be received from, that's on HAT. But since there isn't a HAT option then the closest thing for "known bad mail servers" is through Outbreak Filters which uses TALOS Global Threat Inteligence.

upvoted 2 times

ff001 4 years, 1 month ago

Cisco ESA uses a multilayer approach to fight viruses and malware: • The first layer of defense consists of outbreak filters, which the appliance downloads from Cisco SenderBase. They contain a list of known bad mail servers. These filters are generated by watching global email traffic patterns and looking for anomalies associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat. • The second layer of defense is using antivirus signatures to scan quarantined emails, to ensure that they do not carry viruses into the network. • Cisco ESA also scans outbound emails to provide antivirus protection.

upvoted 4 times

surforlife 4 years, 1 month ago

"B and E" Cisco ESA uses a multilayer approach to fight viruses and malware: • The first layer of defense consists of outbreak filters, which the appliance downloads from Cisco SenderBase. They contain a list of known bad mail servers. These filters are generated by watching global email traffic patterns and looking for anomalies associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat. • The second layer of defense is using antivirus signatures to scan quarantined emails, to ensure that they do not carry viruses into the network. • Cisco ESA also scans outbound emails to provide antivirus protection.

upvoted 1 times

nomanlands 4 years, 1 month ago

BE - C wouldn't stop known bad senders.

upvoted 1 times

semi1750 4 years, 4 months ago

Picked B & E Page 6 stated as follow Fighting Viruses and Malware Cisco ESA uses a multilayer approach to fight viruses and malware: • The first layer of defense consists of outbreak filters, which the appliance downloads from Cisco SenderBase. They contain a list of known bad mail servers. These filters are generated by watching global email traffic patterns and looking for anomalies associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat. • The second layer of defense is using antivirus signatures to scan quarantined emails, to ensure that they do not carry viruses into the network. • Cisco ESA also scans outbound emails to provide antivirus protection https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVD-EmailSecurityUsingCiscoESADesignGuide-AUG13.pdf

upvoted 1 times

Pupu 4 years, 5 months ago

I'm going with B and E. B: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0/b_ESA_Admin_Guide_12_1_chapter_0101.html E: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0/b_ESA_Admin_Guide_12_1_chapter_01101.html

upvoted 3 times

Cock 4 years, 5 months ago

The answer cannot be A. Either single-armed deployment or dual-armed deployment, Cisco ESA is separate from DMZ. ESA is connected to DMZ, not in the DMZ. B is not correct as well. What is outbreak filter? An outbreak occurs when messages with attachments containing never-before-seen viruses or variants of existing viruses spread quickly through private networks and the Internet. The question does not specify to new virus. C is correct. Recipient access table (RAT) acceptance or rejection of recipient addresses. E is correct.

upvoted 1 times

NullNull88 4 years, 8 months ago

"delivery of mail from known bad mail servers must be prevented" that isn't C. RAT?

upvoted 2 times

MoII 4 years, 9 months ago

Agree with A and B

upvoted 1 times

MoII 4 years, 9 months ago

Agree with A and BSorry I meant B and E

upvoted 1 times

MoII 4 years, 9 months ago

Sorry I meant B and E

upvoted 2 times

Question #213 *Topic 1*

An organization has noticed an increase in malicious content downloads and wants to use Cisco Umbrella to prevent this activity for suspicious domains while allowing normal web traffic. Which action will accomplish this task?

A. Use destination block lists.

B. Configure application block lists.

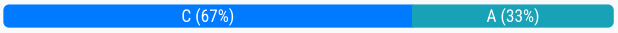
C. Configure the intelligent proxy.

D. Set content settings to High.

Suggested Answer: *C*

Official Answer: C

Community vote distribution



Seawanderer Highly Voted 4 years, 1 month ago

I'd say C, intelligent proxy

upvoted 11 times

sull3y Highly Voted 2 years, 6 months ago

C. Configure the intelligent proxy. Cisco Umbrella's intelligent proxy allows you to enforce security policies for web traffic based on various criteria, such as destination domain, IP address, or URL category. To prevent malicious content downloads, the organization can configure the intelligent proxy to block access to suspicious domains, while allowing normal web traffic. This can be done by creating a security policy that specifies which domains should be blocked and which should be allowed. Note: The intelligent proxy is a feature in Cisco Umbrella that can be used to enforce security policies for web traffic. Other Umbrella features, such as destination block lists and application block lists, can also be used to prevent malicious activity. However, the intelligent proxy is the best option for this specific task, as it allows you to enforce security policies based on domain, IP, or URL category

upvoted 6 times

NETeng01 11 months ago

A. Use destination block lists This blocks specific domains/IPs manually. Effective but not dynamic or scalable for suspicious domains. Too static for the scenario. C. Configure the intelligent proxy Correct Answer Umbrella's Intelligent Proxy: Intercepts requests to suspicious domains. Analyzes content before allowing or blocking it. Prevents malicious downloads while allowing legitimate traffic. This matches the requirement perfectly.

upvoted 1 times

CyberGhost666 1 year, 1 month ago

I'll go with A.

upvoted 1 times

Pierre_Bouvier 1 year, 6 months ago

The intelligent proxy helps in inspecting and analyzing web traffic but doesn't directly block access to domains. It may be useful for deeper inspection but isn't the primary method to block suspicious domains.

upvoted 1 times

Alizade 1 year, 10 months ago

C. Configure the intelligent proxy.

upvoted 1 times

F0rtyx40 2 years, 1 month ago

This is a standard destination list category that can be accomplished with simple DNS forwarding.

upvoted 1 times

nomanlands 3 years, 1 month ago

C - it will still allow normal web traffic

upvoted 1 times

TesterDude 3 years, 3 months ago

I'm going with A because it specifies that it only wants to perform that action for malicious domains, which will be identified by a destination list. Intelligent proxy Inspection of files would apply to all domainsI agree with this, this is a standard destination list category that can be accomplished with simple DNS forwarding.Not for alldomains!! Intelligent proxy will apply ontrols on unknown/suspicious domains which were not blocked by DNS

filtering, nor they have been allowed as trusted. Anything manual is not producing results because you don't know them and the bocking will be done after a host was compromised This is why, in my opinion, answer C is the correct one (download content can as well be files, not only web content)

upvoted 2 times

TesterDude 3 years, 3 months ago

Selected Answer: A

I'm going with A because it specifies that it only wants to perform that action for malicious domains, which will be identified by a destination list.

Intelligent proxy Inspection of files would apply to all domains

upvoted 2 times

F0rtyx40 2 years, 1 month ago

I agree with this, this is a standard destination list category that can be accomplished with simple DNS forwarding.

upvoted 1 times

Silexis Most Recent 7 months ago

Not for alldomains!! Intelligent proxy will apply ontrols on unknown/suspicious domains which were not blocked by DNS filtering, nor they have been allowed as trusted. Anything manual is not producing results because you don't know them and the bocking will be done after a host was compromised This is why, in my opinion, answer C is the correct one (download content can as well be files, not only web content)

upvoted 1 times

Pupu 3 years, 5 months ago

C is the answer.

upvoted 2 times

brownbear505 3 years, 5 months ago

The intelligent proxy is the ability for Umbrella to intercept and proxy requests for malicious files embedded within certain so-called "grey" domains. Some websites, especially those with large user communities or the ability to upload and share files, have content that most users want to access while also posing a risk because of the possibility of hosting malware. Administrators don't want to block access to the whole "grey" domain for everyone but they also don't want your users to access files that could harm their computers or compromise company data.

upvoted 5 times

Minion2021 3 years, 5 months ago

The Answer is C

upvoted 1 times

Floki_viking7 3 years, 6 months ago

I'd say C The intelligent proxy is the ability for Umbrella to intercept and proxy requests for malicious files embedded within certain so-called "grey" domains. Some websites, especially those with large user communities or the ability to upload and share files, have content that most users want to access while also posing a risk because of the possibility of hosting malware. Administrators wouldn't want to block access to the whole "grey" domain for everyone but they also don't want your users to access files that could harm their computers, compromise your company data or worse!

upvoted 2 times

coentror 3 years, 8 months ago

I would say C: How Cisco umbrella will manage traffic to a risky domain? With the intelligent proxy, if a site is considered potentially suspicious or could host malicious content, Umbrella returns the intelligent proxy's IP address. The request to that domain is then routed through our cloud-based secure gateway, and malicious content is found and stopped before it's sent to you.

upvoted 3 times

MoII 3 years, 9 months ago

I'd go with C here

upvoted 1 times

Steve122 3 years, 9 months ago

Support for the intelligent proxy is deprecated and only available for legacy deployments of the MSP console. The intelligent proxy is not available for new deployments of the MSP console.

upvoted 1 times

john_thomas 3 years, 9 months ago

i Passed and i Used [C. Configure the intelligent proxy.]

upvoted 5 times

Question #214 *Topic 1*

Which attack is preventable by Cisco ESA but not by the Cisco WSA?

A. SQL injection

B. phishing

C. buffer overflow

D. DoS

Suggested Answer: *D*

Official Answer: D

Community vote distribution

B (56%) D (44%)

ddev3737_111 Highly Voted 3 years, 6 months ago

but also B. Phishing Cisco ESA (Email Security Appliance) and Cisco WSA (Web Security Appliance) are both security products that provide protection against a variety of network-based threats. However, ESA is designed specifically to protect against email-based threats such as spam, phishing and malware, while WSA is designed to protect against web-based threats such as SQL injection, buffer overflow, and DoS attacks. So, Cisco ESA can prevent phishing but Cisco WSA can't.

upvoted 9 times

ddev3737 Highly Voted 3 years, 6 months ago

but also B. Phishing Cisco ESA (Email Security Appliance) and Cisco WSA (Web Security Appliance) are both security products that provide protection against a variety of network-based threats. However, ESA is designed specifically to protect against email-based threats such as spam, phishing and malware, while WSA is designed to protect against web-based threats such as SQL injection, buffer overflow, and DoS attacks. So, Cisco ESA can prevent phishing but Cisco WSA can't.

upvoted 9 times

MoII 4 years, 9 months ago

I'd go with B becasue the question is about "Preventable" meaning user should not get the email in the first place, that's ESA's job..

upvoted 7 times

F0rtyx40 Most Recent 3 months, 2 weeks ago

Answer is B Its true WSA can potentially block phishing urls but the goal is to try and stop them from ever getting delivered.

upvoted 1 times

Swiz005 1 year, 7 months ago

This should be B Cisco ESA (Email Security Appliance) - Cisco WSA (Web Security Appliance) has no business with emails

upvoted 2 times

kloug 1 year, 9 months ago

Answer b

upvoted 1 times

masal 1 year, 11 months ago

from https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117952-qanda-wsa-00.html WSA can prevent phishing attack. true answer is D.

upvoted 1 times

Stig_88 2 years, 3 months ago

b. Phishing. when an email came in, phishing already happens and WSA did not prevented it. Its the ESA which could prevent it from coming in. What WSA can prevent is when user clicks the link on the email, but that its not that phishing attack. the phishing attack starts when user received the phishing in his inbox.

upvoted 1 times

Premium_Pils 2 years ago

D - "Cisco ESA Bounce Verification to avoid the Denial of Service DOS of your email infrastructure." https://community.cisco.com/t5/security-blogs/cisco-esa-bounce-verification-to-avoid-the-denial-of-service-dos/ba-p/4431574 Not B: WSA - "Web reputation filtering protects client devices from visiting potentially harmful websites that contain malware or phishing links."

upvoted 1 times

Stig_88 2 years, 3 months ago

b. Phishing. when an email came in, phishing already happens and WSA did not prevented it. Its the ESA which could prevent it from coming in. What WSA can prevent is when user clicks the link on the email, but that its not that phishing attack. the phishing attack starts when user received the phishing in his inbox.Another thing to add here: Q: but not by the Cisco WSA When a web server is getting attacked by a DOS, can WSA not prevent it? I think it can. Maybe we are focusing more on email server and ignoring Web server that we are protecting as well. Nothing on the question states that it only considers email servers.

upvoted 1 times

XvidalX 2 years, 5 months ago

Selected Answer: D

WSA PROTECT against pishing!! ESA protect againsd DOS because have RATE LIMIT configuration for connections https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117952-qanda-wsa-00.html : Cisco Web Security Appliance (WSA) provides the industry's most comprehensive gateway defense against spyware and web-based malware. This includes everything from Adware (which causes the most supportability issues and consumes significant network resources) to more malicious threats such as Trojans, Browser Hijackers, Browser helper Objects, Phishing, Pharming, System Monitors, Keyloggers, Worms, etc.

upvoted 2 times

Stig_88 2 years, 3 months ago

Another thing to add here: Q: but not by the Cisco WSA When a web server is getting attacked by a DOS, can WSA not prevent it? I think it can. Maybe we are focusing more on email server and ignoring Web server that we are protecting as well. Nothing on the question states that it only considers email servers.

upvoted 1 times

XvidalX 2 years, 5 months ago

WSA PROTECT against pishing!! ESA protect againsd DOS because have RATE LIMIT configuration for connections https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117952-qanda-wsa-00.html : Cisco Web Security Appliance (WSA) provides the industry's most comprehensive gateway defense against spyware and web-based malware. This includes everything from Adware (which causes the most supportability issues and consumes significant network resources) to more malicious threats such as Trojans, Browser Hijackers, Browser helper Objects, Phishing, Pharming, System Monitors, Keyloggers, Worms, etc.Cisco ESA is specifically designed to prevent phishing attacks, which primarily occur via email, whereas WSA (Web Security Appliance) focuses on web-based threats and does not provide phishing protection for emails. Why not D. DoS? While ESA does offer rate limiting to mitigate email-based DoS attacks, it's not a dedicated DoS prevention solution. Rate limiting helps reduce email-based DoS risks, but network-wide DoS attacks (like volumetric DDoS attacks) are typically handled by firewalls, IPS, or specialized DDoS mitigation solutions. WSA also has protections against DoS-like behaviors by limiting connections and scanning web traffic, but its main focus is not DoS prevention. So, while ESA can help mitigate DoS effects, phishing is the unique attack type that ESA prevents but WSA does not.

upvoted 2 times

Pierre_Bouvier 1 year, 6 months ago

Cisco ESA is specifically designed to prevent phishing attacks, which primarily occur via email, whereas WSA (Web Security Appliance) focuses on web-based threats and does not provide phishing protection for emails. Why not D. DoS? While ESA does offer rate limiting to mitigate email-based DoS attacks, it's not a dedicated DoS prevention solution. Rate limiting helps reduce email-based DoS risks, but network-wide DoS attacks (like volumetric DDoS attacks) are typically handled by firewalls, IPS, or specialized DDoS mitigation solutions. WSA also has protections against DoS-like behaviors by limiting connections and scanning web traffic, but its main focus is not DoS prevention. So, while ESA can help mitigate DoS effects, phishing is the unique attack type that ESA prevents but WSA does not.

upvoted 2 times

mellohello 2 years, 6 months ago

Phishing

upvoted 1 times

itsklk 3 years, 3 months ago

Selected Answer: D

Question Does the Cisco Web Security Appliance (WSA) provide Malware/Spyware protection?

Cisco Web Security Appliance (WSA) provides the industry's most comprehensive gateway defense against spyware and web-based malware. This includes everything from Adware (which causes the most supportability issues and consumes significant network resources) to more malicious threats such as Trojans, Browser Hijackers, Browser helper Objects, Phhttps://www.examtopics.com/discussions/cisco/view/64650-exam-350-701-topic-1-question-214-discussion/#ishing, Pharming, System Monitors, Keyloggers, Worms, etc.

upvoted 1 times

JavierAcuna 3 years, 3 months ago

The Aswer is the B

upvoted 1 times

itsklk 3 years, 3 months ago

Question Does the Cisco Web Security Appliance (WSA) provide Malware/Spyware protection? Cisco Web Security Appliance (WSA) provides the industry's most comprehensive gateway defense against spyware and web-based malware. This includes everything from Adware (which causes the most supportability issues and consumes significant network resources) to more malicious threats such as Trojans, Browser Hijackers, Browser helper Objects, Phhttps://www.examtopics.com/discussions/cisco/view/64650-exam-350-701-topic-1-question-214-discussion/#ishing, Pharming, System Monitors, Keyloggers, Worms, etc.its asking not by WSA ? so why are we having link for WSA?

upvoted 1 times

alexyozgat24 3 years, 2 months ago

its asking not by WSA ? so why are we having link for WSA?

upvoted 1 times

achille5 3 years, 4 months ago

https://www.linkedin.com/pulse/you-using-cisco-wsa-security-appliance-vulnerable-dos-cyber-defence/

upvoted 1 times

ddev3737 3 years, 6 months ago

What about answer A A. SQL injection: Cisco ESA can prevent SQL injection attacks by inspecting the payload of the incoming email messages and identifying any SQL injection attempts. However, Cisco WSA is focused on web traffic and may not have the same level of protection against this type of attack. B. Phishing: Both Cisco ESA and Cisco WSA can prevent phishing attacks by using reputation-based filtering, SSL inspection, and anti-phishing capabilities. C. Buffer overflow: Cisco ESA can prevent buffer overflow attacks by inspecting the payload of incoming email messages and identifying any buffer overflow attempts. However, Cisco WSA is focused on web traffic and may not have the same level of protection against this type of attack. D. DoS: Both Cisco ESA and Cisco WSA can prevent DoS attacks by using rate-limiting, access controls, and other security measures to prevent the attack from overwhelming the system.

upvoted 1 times

rumble291 3 years, 5 months ago

The ESA is a Transfer Agent therefore will limit mail flow to the actual email server. Therefore stopping a DoS attack.

upvoted 1 times

ddev3737_111 3 years, 6 months ago

What about answer A A. SQL injection: Cisco ESA can prevent SQL injection attacks by inspecting the payload of the incoming email messages and identifying any SQL injection attempts. However, Cisco WSA is focused on web traffic and may not have the same level of protection against this type of attack. B. Phishing: Both Cisco ESA and Cisco WSA can prevent phishing attacks by using reputation-based filtering, SSL inspection, and anti-phishing capabilities. C. Buffer overflow: Cisco ESA can prevent buffer overflow attacks by inspecting the payload of incoming email messages and identifying any buffer overflow attempts. However, Cisco WSA is focused on web traffic and may not have the same level of protection against this type of attack. D. DoS: Both Cisco ESA and Cisco WSA can prevent DoS attacks by using rate-limiting, access controls, and other security measures to prevent the attack from overwhelming the system.

upvoted 1 times

CCNP21 3 years, 7 months ago

I believe B is the answer.

upvoted 1 times

intirt 3 years, 8 months ago

B is correct. ESA is email appliance, not firewall.

upvoted 1 times

Emlia1 3 years, 8 months ago

B is correct

upvoted 1 times

Question #215 *Topic 1*

An organization recently installed a Cisco WSA and would like to take advantage of the AVC engine to allow the organization to create a policy to control application specific activity. After enabling the AVC engine, what must be done to implement this?

A. Use security services to configure the traffic monitor.

B. Use URL categorization to prevent the application traffic.

C. Use an access policy group to configure application control settings.

D. Use web security reporting to validate engine functionality.

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

sull3y Highly Voted 2 years ago
C. Use an access policy group to configure application control settings.

The Application Visibility and Control (AVC) engine in Cisco Web Security Appliance (WSA) allows you to control application specific activity by creating policies based on the type of traffic. To implement this, you must use an access policy group to configure the application control settings.

An access policy group defines the set of security rules that the WSA applies to incoming web traffic. The AVC engine in the WSA allows you to categorize applications based on the type of traffic they generate, and then create policies that control how that traffic is handled. This can include allowing or blocking specific applications, controlling the bandwidth used by applications, and setting limits on the amount of data that can be downloaded.
upvoted 6 times

NikoNiko Highly Voted 2 years, 7 months ago
C is correct.

"The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in ACCESS POLICY GROUPS. You can block or allow applications individually or according to application type. You can also apply controls to particular application types. "

Source: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01111.html
upvoted 5 times

CyberGhost666 Most Recent 1 year, 1 month ago
Selected Answer: C
C) Use an access policy group to configure application control settings.
upvoted 1 times

Question #216 *Topic 1*

What is the role of Cisco Umbrella Roaming when it is installed on an endpoint?

A. to establish secure VPN connectivity to the corporate network

B. to enforce posture compliance and mandatory software

C. to ensure that assets are secure from malicious links on and off the corporate network

D. to protect the endpoint against malicious file transfers

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

Steve122 Highly Voted 2 years, 9 months ago

C Umbrella Roaming is a cloud-delivered security service for Cisco's next-generation firewall. It protects your employees even when they are off the VPN. No additional agents are required. Simply enable the Umbrella functionality in the Cisco AnyConnect client. You'll get seamless protection against malware, phishing, and command-and-control callbacks wherever your users go.

upvoted 6 times

ureis Most Recent 1 year, 9 months ago

Umbrella Roaming is a cloud-delivered security service for Cisco's next-generation firewall. It protects your employees even when they are "off the VPN"

upvoted 2 times

FortiSherlock 2 years ago

C - I do agree.

upvoted 1 times

beeker98106 2 years, 9 months ago

Nope, this is confirmed C. (on and off the network is the kicker, Umbrella also works while NOT connected view VPN)

upvoted 2 times

john_thomas 2 years, 9 months ago

Answer: A. to establish secure VPN connectivity to the corporate network

upvoted 1 times

Question #217 *Topic 1*

An administrator configures a Cisco WSA to receive redirected traffic over ports 80 and 443. The organization requires that a network device with specific WSA integration capabilities be configured to send the traffic to the WSA to proxy the requests and increase visibility, while making this invisible to the users. What must be done on the Cisco WSA to support these requirements?

A. Use PAC keys to allow only the required network devices to send the traffic to the Cisco WSA.

B. Configure transparent traffic redirection using WCCP in the Cisco WSA and on the network device.

C. Configure active traffic redirection using WPAD in the Cisco WSA and on the network device.

D. Use the Layer 4 setting in the Cisco WSA to receive explicit forward requests from the network device.

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

CyberGhost666 Most Recent 1 year, 1 month ago

B. Configure transparent traffic redirection using WCCP in the Cisco WSA and on the network device.

upvoted 1 times

mikexian 2 years ago

client does not have any feeling while use transparent mode

upvoted 1 times

Question #218 *Topic 1*

An administrator configures a new destination list in Cisco Umbrella so that the organization can block specific domains for its devices. What should be done to ensure that all subdomains of domain.com are blocked?

A. Configure the domain.com address in the block list.

B. Configure the *.domain.com address in the block list.

C. Configure the *.com address in the block list.

D. Configure the *domain.com address in the block list.

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

zeroC00L Highly Voted 4 years, 4 months ago

it is actually A -> https://docs.umbrella.com/deployment-umbrella/docs/wild-cards "Every domain in a block or allow destination list has an implied left side and right side wildcard"

upvoted 22 times

zeroC00L Highly Voted 4 years, 4 months ago

it is actually A -> https://docs.umbrella.com/deployment-umbrella/docs/wild-cards "Every domain in a block or allow destination list has an implied left side and right side wildcard"ZeroCool is correct. Same link also states: It is not possible to use an asterisk to wildcard a different part of the domain. The following will not work: *.domain.com subdomain.*.com sub*.com domain.* Adding domain.com to an allow list results in requests to domain.com or its subdomains, such as www.domain.com, being allowed. The result is the same for blocklists.

upvoted 22 times

aalnman 4 years, 4 months ago

ZeroCool is correct. Same link also states: It is not possible to use an asterisk to wildcard a different part of the domain. The following will not work: *.domain.com subdomain.*.com sub*.com domain.* Adding domain.com to an allow list results in requests to domain.com or its subdomains, such as www.domain.com, being allowed. The result is the same for blocklists.

upvoted 12 times

14LearningStuff 4 years, 5 months ago

I think it is A. Always add domains in the format "domain.com" rather than www.domain.com to ensure *.domain.com is included (a wildcard is implicit). However, if you only wish to block subdomain.domain.com, then be more specific when you define the entry here.

upvoted 10 times

CyberGhost666 Most Recent 1 year, 1 month ago

"Adding domain.com to an allow list results in requests to domain.com or its subdomains, such as www.domain.com, being allowed. The result is the same for blocklists." A

upvoted 1 times

Pakawat 2 years, 1 month ago

Found this one in the exam.

upvoted 1 times

loser4fun 2 years, 11 months ago

Answer B is more accurate To ensure that all subdomains of domain.com are blocked in Cisco Umbrella, the administrator should configure the *.domain.com address in the block list. The asterisk (*) is a wildcard character that represents any string of characters, including subdomains. By using the wildcard character in the block list, any subdomain of domain.com will be blocked, including subdomains that do not exist yet. If the administrator only configures the domain.com address in the block list, it will only block traffic to the root domain and not to any of its subdomains. Similarly, configuring the *.com address in the block list will block all traffic to any domain that ends with .com, not just domain.com and its subdomains. Configuring the *domain.com address in the block list will not have any effect, as it does not follow the correct syntax for blocking subdomains.You are incorrect. The answer is A.you can't use * in destination list, the system won't allow you. you configure a domian, not a URL so all subdomains are auto included.

upvoted 1 times

loser4fun 2 years, 11 months ago

Answer B is more accurate

To ensure that all subdomains of domain.com are blocked in Cisco Umbrella, the administrator should configure the *.domain.com address in the block list.

The asterisk (*) is a wildcard character that represents any string of characters, including subdomains. By using the wildcard character in the block list, any subdomain of domain.com will be blocked, including subdomains that do not exist yet.

If the administrator only configures the domain.com address in the block list, it will only block traffic to the root domain and not to any of its subdomains. Similarly, configuring the *.com address in the block list will block all traffic to any domain that ends with .com, not just domain.com and its subdomains. Configuring the *domain.com address in the block list will not have any effect, as it does not follow the correct syntax for blocking subdomains.

upvoted 1 times

iratus_umbra 2 years, 10 months ago

You are incorrect. The answer is A.

upvoted 1 times

Dorr20 2 years, 10 months ago

you can't use * in destination list, the system won't allow you. you configure a domian, not a URL so all subdomains are auto included.

upvoted 1 times

Emlia1 3 years, 2 months ago

A is correct

upvoted 1 times

ureis 3 years, 3 months ago

"Adding domain.com to an allow list results in requests to domain.com or its subdomains, such as www.domain.com, being allowed. The result is the same for blocklists." A

upvoted 1 times

Jamesy 3 years, 4 months ago

B is the correct answer. Cheers

upvoted 2 times

madcloud 3 years, 8 months ago

What you cannot add to a destination list 1. You cannot add wildcards. A wildcard is implicit in the way DNS is structured, so adding a domain covers all of the subdomains and there is no reason to add *.domain.com to cover this. https://support.umbrella.com/hc/en-us/articles/115006964927-Understanding-Destination-lists-supported-entries-and-error-messages

upvoted 2 times

jaciro11 4 years, 3 months ago

The answer is A Guys. https://docs.umbrella.com/deployment-umbrella/docs/wild-cardsImplied Wildcard

upvoted 7 times

jaciro11 4 years, 3 months ago

The answer is A Guys. https://docs.umbrella.com/deployment-umbrella/docs/wild-cards

upvoted 7 times

MoII 4 years, 2 months ago

Implied Wildcard

upvoted 3 times

john_thomas 4 years, 3 months ago

B. Configure the *.domain.com address in the block list.

upvoted 3 times

Sarbi 4 years, 5 months ago

The answer is B

upvoted 8 times

Question #219 *Topic 1*

An organization wants to use Cisco FTD or Cisco ASA devices. Specific URLs must be blocked from being accessed via the firewall, which requires that the administrator input the bad URL categories that the organization wants blocked into the access policy. Which solution should be used to meet this requirement?

A. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not.

B. Cisco ASA because it enables URL filtering and blocks malicious URLs by default, whereas Cisco FTD does not.

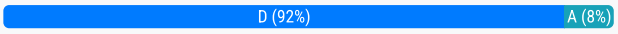
C. Cisco ASA because it includes URL filtering in the access control policy capabilities, whereas Cisco FTD does not.

D. Cisco FTD because it includes URL filtering in the access control policy capabilities, whereas Cisco ASA does not.

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Pupu 2 years, 5 months ago

The answer is D. URL Filtering is not enabled by default on FTD. Adding the license enables the Enable URL Filtering option, which then is required to be enabled by the admin. https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/url_filtering.html#id_74537

upvoted 11 times

Silexis Most Recent 7 months ago

Cisco ASA supports URL Filtering using MPF and Regex but NOT URL Categories. FTD supports both URL Categories and static URL filtering capabilities. URL categories have to be configured by administrators in FTD but once accomplished, it is done by default while Cisco ASA needs regexes for each URL you want to filter, requiring a manual input all the time and not a default action.

upvoted 1 times

cisco_guy 1 year, 7 months ago

I'm going with D as well, but you can do URL filtering on the ASA, you need an HTTP inspection policy with regex to do it. Both firewalls support it.

upvoted 1 times

Jamesy 1 year, 11 months ago

Hi guys, the answer is A please read carefully. I hope I am not confusing anyone. Thanks

upvoted 2 times

john_thomas 2 years, 9 months ago

A. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not.

upvoted 3 times

john_thomas 2 years, 9 months ago

A. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not.Agree with @janzeleny, correct answer is D, I noticed @john_thomas comments on a lot of the questions but normally gives wrong answers with no explanations. Be careful following his suggestions guys. Just a friendly PSA.The option for doing URL filtering and blocking malicious URLs is in FTD, but it's not doing it by default, you have to enable it and configure which URLs (categories) should be blocked. So the correct answer is D.URL Filtering can be done in ASA using MPF and Regex. The only difference between FTD and ASA is that FTD has the concept of URL categories, while cisco ASA does not - it requires static URLs definitions. This is why, in my opinion, Answer A is covering better the request URL categories.....

upvoted 3 times

lurker8000 Highly Voted 2 years, 7 months ago

Agree with @janzeleny, correct answer is D, I noticed @john_thomas comments on a lot of the questions but normally gives wrong answers with no explanations. Be careful following his suggestions guys. Just a friendly PSA.

upvoted 17 times

janzeleny Highly Voted 2 years, 9 months ago

The option for doing URL filtering and blocking malicious URLs is in FTD, but it's not doing it by default, you have to enable it and configure which URLs (categories) should be blocked. So the correct answer is D.

upvoted 14 times

janzeleny 2 years, 9 months ago

The option for doing URL filtering and blocking malicious URLs is in FTD, but it's not doing it by default, you have to enable it and configure which URLs (categories) should be blocked. So the correct answer is D.URL Filtering can be done in ASA using MPF and Regex. The only difference between FTD and ASA is that FTD has the concept of URL categories, while cisco ASA does not - it requires static URLs definitions. This is why, in my opinion, Answer A is covering better the request URL categories.....

upvoted 14 times

Silexis 7 months ago

URL Filtering can be done in ASA using MPF and Regex. The only difference between FTD and ASA is that FTD has the concept of URL categories, while cisco ASA does not - it requires static URLs definitions. This is why, in my opinion, Answer A is covering better the request URL categories.....

upvoted 1 times

Question #220 *Topic 1*

Which component of Cisco Umbrella architecture increases reliability of the service?

A. BGP route reflector

B. anycast IP

C. AMP Threat Grid

D. Cisco Talos

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

fabio3wz Highly Voted 4 years, 11 months ago
It should be anycast IP. Why Talos would incrase reliability'?
upvoted 14 times

Rabyn Highly Voted 4 years, 11 months ago
Anycast would increase the resiliency of the product. Reliability and resiliency are different. With Cisco Talos, the reliability of Cisco Umbrella threat detection is increased.
upvoted 8 times

Premium_Pils Most Recent 2 years ago
anycast ip: "Anycast routing is the key to reliability" - https://umbrella.cisco.com/blog/why-the-cisco-umbrella-global-network-uses-anycast-routing
upvoted 1 times

Alizade 2 years, 10 months ago
anycast IP
upvoted 1 times

sis_net_sec 3 years, 10 months ago
B is Correct Anycast would increase the resiliency of the product. Reliability and resiliency are different. With Cisco Talos, the reliability of Cisco Umbrella threat detection is increased.
upvoted 1 times

nomanlands 4 years, 1 month ago
Anycast for sure
upvoted 1 times

jaciro11 4 years, 5 months ago
anycast IP
upvoted 3 times

Pupu 4 years, 5 months ago
The answer is B Anycast. Check title "Anycast routing is the key to reliability" https://umbrella.cisco.com/blog/why-the-cisco-umbrella-global-network-uses-anycast-routing
upvoted 2 times

Minion2021 4 years, 5 months ago
It is B. Anycast IP
upvoted 2 times

lurker8000 4 years, 7 months ago
https://umbrella.cisco.com/blog/why-the-cisco-umbrella-global-network-uses-anycast-routing#:~:text=Anycast%20routing%20is%20the%20key%20to%20reliability B. Anycast IP
upvoted 3 times

sysadminshodan 4 years, 7 months ago
Creator of the question did not know "reliability" could been in a traditional network sense (Anycast) but also reliability in the accuracy of TALOs to accurately classify domains.Reliability in Networking refers to availabilities, so anycast is correct
upvoted 1 times

sysadminshodan 4 years, 7 months ago

Creator of the question did not know "reliability" could been in a traditional network sense (Anycast) but also reliability in the accuracy of TALOs to accurately classify domains.

upvoted 1 times

cyberwhizzy0 3 years, 1 month ago

Reliability in Networking refers to availabilities, so anycast is correct

upvoted 1 times

MoII 4 years, 8 months ago

Voting fo B here

upvoted 2 times

jaciro11 4 years, 9 months ago

B. anycast IP

upvoted 4 times

TonyVi 4 years, 9 months ago

B is the correct answer https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-1980.pdf

upvoted 3 times

beeker98106 4 years, 9 months ago

It's B. https://umbrella.cisco.com/blog/why-the-cisco-umbrella-global-network-uses-anycast-routing Above page has this paragraph: Anycast routing is the key to reliability

upvoted 4 times

john_thomas 4 years, 9 months ago

B. anycast IP

upvoted 3 times

Question #221 *Topic 1*

A customer has various external HTTP resources available including Intranet, Extranet, and Internet, with a proxy configuration running in explicit mode. Which method allows the client desktop browsers to be configured to select when to connect direct or when to use proxy?

A. Bridge mode

B. Transparent mode

C. .PAC file

D. Forward file

Suggested Answer: *C*
Official Answer: C

Jayde Highly Voted 3 years, 4 months ago

Answer is C

A Proxy Auto-Configuration (PAC) file contains a set of rules coded in JavaScript which allows a web browser to determine whether to send web traffic direct to the Internet or be sent via a proxy server.

PAC files can control how a web browser handles HTTP, HTTPS, and FTP traffic

http://findproxyforurl.com/pac-file-introduction/

upvoted 11 times

sull3y Most Recent 2 years ago

C. .PAC file

A .PAC (Proxy Auto-Config) file is a JavaScript file that is used to configure proxy settings for client desktop browsers. The .PAC file provides a set of instructions that determine whether a client should connect directly to a target resource or whether it should use a proxy. The .PAC file can be hosted on a web server and can be referenced by the client browser to automatically configure the proxy settings.

In explicit proxy mode, the client desktop browser must be configured to use the proxy for all outbound connections. With a .PAC file, the client desktop browser can be configured to select when to connect directly to a target resource or when to use the proxy based on the destination URL. This provides greater flexibility and control over proxy settings, and allows the client to easily access different types of external HTTP resources, such as Intranet, Extranet, and Internet, with different proxy configurations.

upvoted 1 times

Question #222 *Topic 1*

What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?

A. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA.

B. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA.

C. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.

D. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not.

Suggested Answer: *D*

Reference: https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/guide-c07-742373.html

Community vote distribution

D (100%)

Rododendron2 Most Recent 2 years, 2 months ago

Cisco Cloud Web Security - Retirement Notification The Cisco Cloud Web Security has been retired and is no longer supported. End-of-Sale Date: 2018-10-31 End-of-Support Date: 2019-10-31

upvoted 3 times

sis_net_sec 3 years, 10 months ago

Explanation: https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/guide-c07- 742373.html

upvoted 2 times

NikoNiko 4 years, 1 month ago

WSA • Mobile User Security improves integration with VPN Headend ASA • Client web traffic must be tunneled back to HQ CWS • Remote sites can utilise CWS directly. No VPN Backhaul! • On-the-Go users are filtered and secured direct to CWS infrastructure • Consistent policy applied whether in the office or not https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2018/pdf/BRKSEC-2042.pdf

upvoted 2 times

Question #223 *Topic 1*

An engineer needs to add protection for data in transit and have headers in the email message. Which configuration is needed to accomplish this goal?

A. Deploy an encryption appliance.

B. Provision the email appliance.

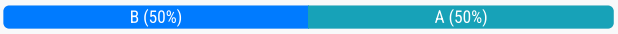
C. Map sender IP addresses to a host interface.

D. Enable flagged message handling.

Suggested Answer: *B*

Official Answer: B

Community vote distribution



sull3y Highly Voted 3 years, 6 months ago

B. Provision the email appliance Provisioning the email appliance, also known as an Email Security Gateway or Email Security Appliance, is a solution for protecting data in transit and adding headers to email messages. The email appliance acts as a security layer between the email servers and the Internet, and provides a range of security features such as encryption, anti-virus, anti-spam, and content filtering. These features help to ensure that emails are transmitted securely, and help to prevent unauthorized access to sensitive information. By provisioning the email appliance, the engineer can add protection for data in transit and have headers in the email message.A. Deploy an encryption appliance. Deploying an encryption appliance is the configuration that is needed to add protection for data in transit and have headers in the email message. An encryption appliance encrypts data before it is transmitted over a network, providing protection against eavesdropping and unauthorized access to sensitive information. By deploying an encryption appliance, the engineer can add protection for data in transit and ensure that headers are added to the email message. This solution provides a secure way to transmit data and helps to prevent unauthorized access to sensitive information.

upvoted 11 times

sull3y Highly Voted 3 years, 6 months ago

B. Provision the email appliance

Provisioning the email appliance, also known as an Email Security Gateway or Email Security Appliance, is a solution for protecting data in transit and adding headers to email messages. The email appliance acts as a security layer between the email servers and the Internet, and provides a range of security features such as encryption, anti-virus, anti-spam, and content filtering. These features help to ensure that emails are transmitted securely, and help to prevent unauthorized access to sensitive information. By provisioning the email appliance, the engineer can add protection for data in transit and have headers in the email message.

upvoted 11 times

sull3y 3 years, 6 months ago

A. Deploy an encryption appliance. Deploying an encryption appliance is the configuration that is needed to add protection for data in transit and have headers in the email message. An encryption appliance encrypts data before it is transmitted over a network, providing protection against eavesdropping and unauthorized access to sensitive information. By deploying an encryption appliance, the engineer can add protection for data in transit and ensure that headers are added to the email message. This solution provides a secure way to transmit data and helps to prevent unauthorized access to sensitive information.

upvoted 5 times

Kromwall 3 years, 3 months ago

After doing more research I will change my answer to A. To add protection for data in transit and have headers in the email message, an engineer needs to deploy an encryption appliance. This is discussed on page 1 of the Cisco Email Encryption PDF guide under the section "How to Encrypt Messages with a Local Key Server" and on page 11 under "Inserting Encryption Headers into Messages". Therefore, the correct answer is A. Deploy an encryption appliance. https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_010010.pdf

upvoted 5 times

XBfoundX Most Recent 1 week ago

the keyword here is add protection of the data in transit, for doing so there were dedicated hardware appliances called, Cisco ironport encryption appliance, now the service is used via cloud using: Secure Email Encryption Service https://www.cisco.com/site/us/en/products/security/secure-

email/secure-email-encryption-service/index.html

upvoted 1 times

G0909 1 month ago

Cisco AsyncOS handles this by utilizing either an on-premise physical/virtual encryption appliance

upvoted 1 times

7d4c29f 2 months, 3 weeks ago

According to Cisco's official Email Encryption documentation: "The Cisco IronPort Encryption appliance must be set up to handle flagged messages" and to insert encryption headers into messages — confirming the encryption appliance is the correct solution for both data in transit protection AND email headers

upvoted 1 times

jku2cya 3 years, 1 month ago

Selected Answer: B

I'd say B more than A, but who knows. Again another ambiguous exam question, to prove one knows Cisco Security knowledge..

upvoted 3 times

Pages 4 months, 2 weeks ago

The key requirements are: Protection for data in transit (encryption) Ability to add/modify headers in email messages The best answer is: B. Provision the email appliance. Why: An email appliance (such as a secure email gateway) is specifically designed to: Encrypt emails in transit Inspect, modify, and add email headers Enforce email security policies (DLP, TLS, etc.)

upvoted 1 times

Basuso 1 year, 9 months ago

Terrible question by Cisco, but let's get to facts: Encryption Appliances are out of support for almost a decade (were made EoS in 2015). Deploying the Email Appliance allows you to add protection for data in transit as you can encrypt the conversation with TLS and/or even encrypt the data itself with S/MIME. Also, using Content Filtering and other features you are able to add/edit Headers. Therefore I would go with B.

upvoted 2 times

cristip 2 years, 7 months ago

I Think it is A

upvoted 1 times

achille5 3 years, 5 months ago

Selected Answer: B

Correct B

upvoted 2 times

jku2cya 3 years, 1 month ago

I'd say B more than A, but who knows. Again another ambiguous exam question, to prove one knows Cisco Security knowledge..Just looked at this again. I'd stick with B. Question says "Which configuration is needed". The verb 'deploy' corresponds to adding in something new, like a new device. The verb 'configure' corresponds to changing something that already exists.

upvoted 3 times

achille5 3 years, 4 months ago

option A

upvoted 2 times

jku2cya 3 years, 1 month ago

Just looked at this again. I'd stick with B. Question says "Which configuration is needed". The verb 'deploy' corresponds to adding in something new, like a new device. The verb 'configure' corresponds to changing something that already exists.

upvoted 1 times

stalkr3 3 years, 4 months ago

option C

upvoted 1 times

Kromwall 3 years, 3 months ago

It's B. To add protection for data in transit and have headers in the email message, you need to insert encryption headers into messages using either a content filter or a message filter. The encryption header can override the encryption settings defined in the associated encryption profile, and it can apply specified encryption features to messages. Therefore, option B (provision the email appliance) is needed to accomplish this goal. Option A (deploy an encryption appliance) may also be necessary depending on your organization's needs. Options C (map sender IP addresses to a host interface) and D (enable flagged message handling) are not directly related to this goal.

upvoted 2 times

achille5 3 years, 5 months ago

Correct Boption Aoption Coption D

upvoted 2 times

achille5 3 years, 4 months ago

option Aoption Coption D

upvoted 2 times

stalkr3 3 years, 4 months ago

option Coption D

upvoted 1 times

stalkr3 3 years, 4 months ago

option D

upvoted 1 times

NikoNiko 4 years, 1 month ago

A is correct.

WSA: " AsyncOS enables you to add encryption settings to a message by inserting an SMTP HEADER into a message using either a content filter or a message filter. The encryption header can override the encryption settings defined in the associated encryption profile, and it can apply specified encryption features to messages.

NOTE: The Cisco Ironport ENCRYPTION APPLIANCE must be set up to handle flagged messages."

As question states that headers are already in the email messages, we need only Encryption Appliance to do its work.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_010010.html#task_1146822

upvoted 3 times

CCNP21 3 years, 7 months ago

The encryption header can override the encryption settings defined in the associated encryption profile, and it can apply specified encryption features to messages.

upvoted 1 times

Emlia1 3 years, 8 months ago

I prefer A

upvoted 1 times

4000000 3 years, 9 months ago

AsyncOS supports using encryption to secure inbound and outbound email. To use this feature, you create an encryption profile that specifies characteristics of the encrypted message and connectivity information for the key server. The key server may either be: The Cisco Registered Envelope Service (managed service), or An Cisco Encryption appliance (locally managed server) 😝it should b (A) as to locally manage one must first deploy it.

upvoted 1 times

NikoNiko 4 years, 1 month ago

A is correct. WSA: " AsyncOS enables you to add encryption settings to a message by inserting an SMTP HEADER into a message using either a content filter or a message filter. The encryption header can override the encryption settings defined in the associated encryption profile, and it can apply specified encryption features to messages. NOTE: The Cisco Ironport ENCRYPTION APPLIANCE must be set up to handle flagged messages." As question states that headers are already in the email messages, we need only Encryption Appliance to do its work. https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_010010.html#task_1146822The Cisco IronPort Encryption Appliance is now obsolete (past End-of-Life and End-of-Support status). End-of-Sale Date: 2012-07-19 End-of-Support Date: 2015-07-31 => Either this question is outdated since almost 10 years or this functionality is somehow merged in the ESA itself.

upvoted 3 times

FortiSherlock 4 years ago

The Cisco IronPort Encryption Appliance is now obsolete (past End-of-Life and End-of-Support status). End-of-Sale Date: 2012-07-19 End-of-Support Date: 2015-07-31 => Either this question is outdated since almost 10 years or this functionality is somehow merged in the ESA itself.

upvoted 3 times

Question #224 *Topic 1*

Which Cisco platform processes behavior baselines, monitors for deviations, and reviews for malicious processes in data center traffic and servers while performing software vulnerability detection?

A. Cisco Tetration

B. Cisco ISE

C. Cisco AnyConnect

D. Cisco AMP for Network

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/white_papers/Cisco-IT-Tetration-Deployment-Part-2-of-2.html

Community vote distribution

A (100%)

Felice44 Most Recent 1 year, 11 months ago

Cisco Secure Workload (formerly Tetration) seamlessly delivers a zero-trust approach to securing your application workloads across any cloud and on-premises data center environments by reducing the attack surface, preventing lateral movement, identifying workload behavior anomalies, and remediating threats quickly.

upvoted 3 times

azertyu 2 years ago

https://www.cisco.com/c/en_sg/products/data-center-analytics/tetration-analytics/index.html

upvoted 1 times

Question #225 *Topic 1*

A network engineer must configure a Cisco ESA to prompt users to enter two forms of information before gaining access. The Cisco ESA must also join a cluster machine using preshared keys. What must be configured to meet these requirements?

A. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA GUI.

B. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA CLI.

C. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA GUI.

D. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA CLI.

Suggested Answer: *A*
Official Answer: A

Community vote distribution
D (100%)

Yuta1123 Highly Voted 2 years, 9 months ago
I think D is the answer. Sorce:https://www.cisco.com/c/ja_jp/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_fs/b_ESA_Admin_Guide_fs_chapter_0101000.html
upvoted 8 times

Toni_Su91 Highly Voted 1 year, 11 months ago
Document Updated on March6, 2023 https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200885-ESA-Cluster-Requirements-and-Setup.html Cluster configuration options must be done via the CLI on the ESA and cannot be created or joined in the GUI. Note: If you run the PREPJOIN option, you need to commit your changes to the primary ESA before you run clusterconfig on the secondary ESA and join that appliance to your newly configured cluster. This is noted from the output throughout the operation: to join this appliance to a cluster with pre-shared keys, log in to the cluster machine, run the clusterconfig > prepjoin > new command , enter the next details, and commit your changes. So I believe it is D
upvoted 5 times

Jessie45785 Most Recent 1 year, 8 months ago
Check ans from q412 ---> Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG CLI D - is correct
upvoted 1 times

Tuxzinator 1 year, 12 months ago
horrible question. The ability to join a cluster using the Cisco ESA GUI was introduced in version 13.5.
upvoted 2 times

ross123 2 years, 1 month ago
Answer is D. See: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200885-ESA-Cluster-Requirements-and-Setup.html under "Requirements" section.
upvoted 1 times

a7mad150 2 years, 3 months ago
joining the cluster-only can be only CLI and ESA only supports radius
upvoted 1 times

sis_net_sec 2 years, 3 months ago
https://www.cisco.com/c/ja_jp/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_fs/b_ESA_Admin_Guide_fs_chapter_0101000.html
upvoted 1 times

NikoNiko 2 years, 7 months ago
"You cannot create or join a cluster from the Graphical User Interface (GUI). You must use the Command Line Interface (CLI) to create, join, or configure clusters of machines. Once you have created a cluster, you can change configuration settings from either the GUI or the CLI. ... Although you cannot create or join clusters or administer cluster specific settings from the GUI (the equivalent of the clusterconfig command), you can browse machines in the cluster, create, delete, copy, and move settings among the cluster, groups, and machines (that is, perform the equivalent of the clustermode and clusterset commands) from within the GUI." https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_11_1_chapter_0101000.html#con_1122438
upvoted 2 times

geppo81 2 years, 7 months ago

I found also these links: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_0100000.html https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_0100000.html#id_50726

upvoted 3 times

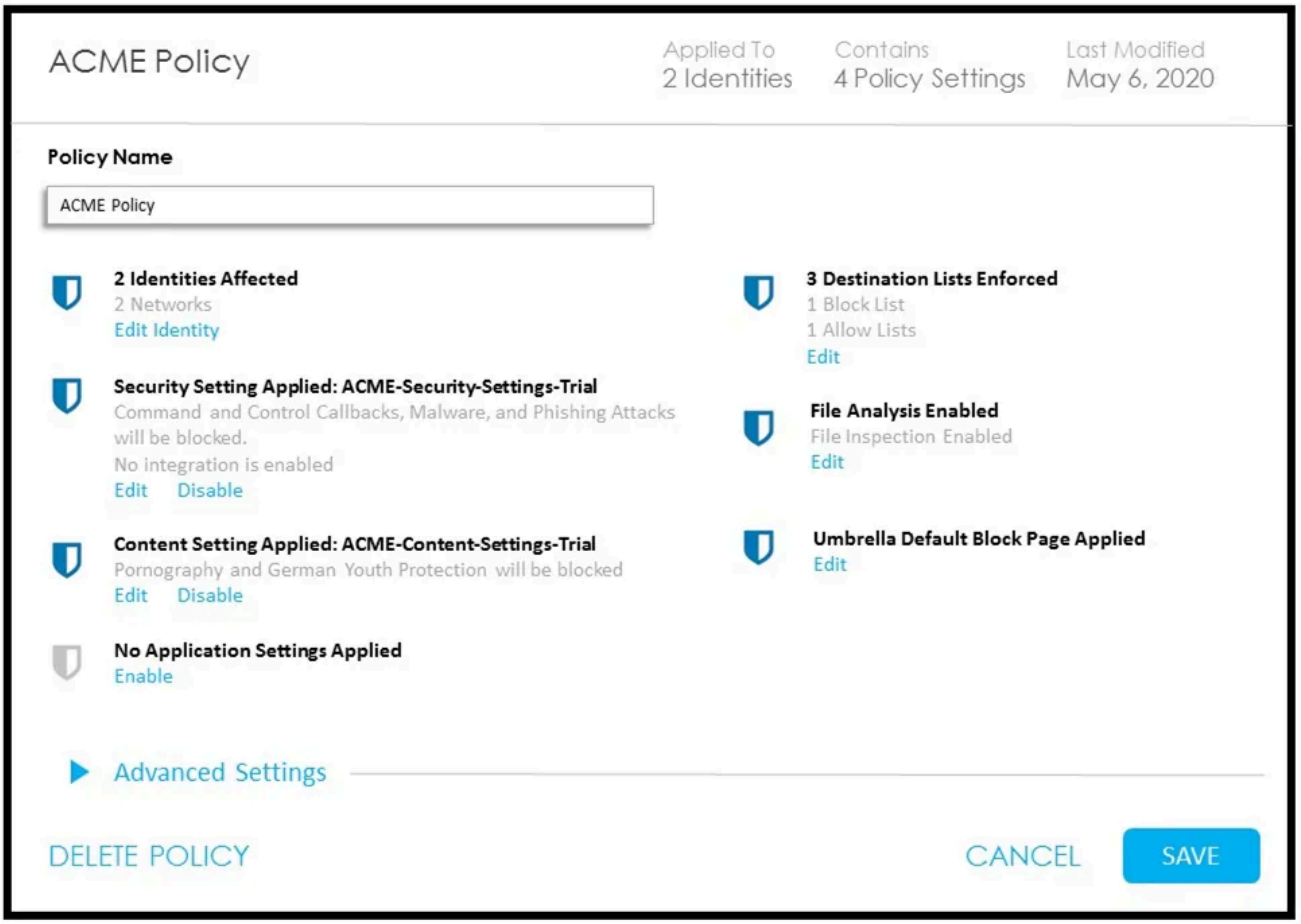
Jardator 2 years, 9 months ago

initial joining the cluster-only CLI can be used

upvoted 4 times

Question #226 *Topic 1*

Refer to the exhibit. How does Cisco Umbrella manage traffic that is directed toward risky domains?



A. Traffic is managed by the application settings, unhandled and allowed.

B. Traffic is managed by the security settings and blocked.

C. Traffic is proxied through the intelligent proxy.

D. Traffic is allowed but logged.

Suggested Answer: *B*

Official Answer: B

Community vote distribution

C (54%) B (46%)

PiX2 Highly Voted 3 years, 5 months ago

Selected Answer: B

Output clearly shows that risky domains (C&C, Malware, Phishing) will be blocked by "Security Settings". Intelligent Proxy (answer C) is configured under the "Advanced settings", which is not visible on the output.

upvoted 11 times

PiX2 Highly Voted 3 years, 5 months ago

Output clearly shows that risky domains (C&C, Malware, Phishing) will be blocked by "Security Settings". Intelligent Proxy (answer C) is configured under the "Advanced settings", which is not visible on the output.Yes but where do you see "Newly Seen Domains" enabled?File analyzer require intelligent proxy to be enabledI agree. it is security settings and blocked based on the picture.Sorry for this comment, I needed to look at it closer to see that B is not correct here. C is the right one. I will deliver the details soon.

upvoted 11 times

F0rtyx40 3 months, 2 weeks ago

Yes but where do you see "Newly Seen Domains" enabled?

upvoted 1 times

haiderzaid 3 years, 4 months ago

File analyzer require intelligent proxy to be enabled

upvoted 3 times

Premium_Pils 2 years ago

I agree. it is security settings and blocked based on the picture.

upvoted 1 times

Premium_Pils 2 years ago

I agree. it is security settings and blocked based on the picture.Sorry for this comment, I needed to look at it closer to see that B is not correct here. C is the right one. I will deliver the details soon.

upvoted 1 times

Premium_Pils 1 year, 9 months ago

Sorry for this comment, I needed to look at it closer to see that B is not correct here. C is the right one. I will deliver the details soon.

upvoted 2 times

F0rtyx40 Most Recent 3 months, 2 weeks ago

C: As others have stated if you look closer "Newly Seen Domains" nor "Potentially Harmful Domains" are checked. We are talking about "Risky" domains not malicious domains

upvoted 1 times

Premium_Pils 1 year, 9 months ago

Selected Answer: C

a) Application Settings: NO - Traffic is not handled by application settings as these are not applied. b) Security Settings: NO - It would be logical handle risky domains here, but as the picture shows, no such a thing was set here. For blocking risky domains, you would need to choose Security Settings -> Potentially Harmful Domains. Now we can see that the category for blocking "Potentially Harmful Domains" is not selected. They only selected blocking: Command and Control Callbacks, Malware, and Phishing Attacks, but nothing else. So, Security Settings are not managing risky domains.

upvoted 3 times

diverjim64 12 months ago

Agree with answer provided by Pils. Verified in lab.

upvoted 1 times

user_topic 1 year, 3 months ago

File analysis > Intelligent proxy (risky domains) > SSL Decryption (optional)

upvoted 1 times

Premium_Pils 1 year, 9 months ago

a) Application Settings: NO - Traffic is not handled by application settings as these are not applied. b) Security Settings: NO - It would be logical handle risky domains here, but as the picture shows, no such a thing was set here. For blocking risky domains, you would need to choose Security Settings -> Potentially Harmful Domains. Now we can see that the category for blocking "Potentially Harmful Domains" is not selected. They only selected blocking: Command and Control Callbacks, Malware, and Phishing Attacks, but nothing else. So, Security Settings are not managing risky domains.Here you can see, how Security Settings would look like when "Potentially Harmful Domains" are added. It is not the case on the picture in our question. "Potentially Harmful Domains" have not been added, so B) is not correct.C) Intelligent Proxy: YES - Why? Because File Analysis is Enabled! The pre-requisite to be able to enable this feature is to turn on the Intelligent Proxy! Otherwise, you won't be able to switch this to be "enabled" and a message would be displayed under "File Analysis" that this "Requires Intelligent Proxy". Now that we understand that this feature is activated, we can also conclude that the Intelligent Proxy is ON.This page shows what is displayed when Intelligent Proxy has not been enabled yet. So, you can see that in our case, on the picture of the question, the Intelligent Proxy is already ON: https://docs.umbrella.com/deployment-umbrella/docs/enable-the-intelligent-proxy About Intelligent Proxy: https://docs.umbrella.com/deployment-umbrella/docs/enable-the-intelligent-proxy Umbrella's intelligent proxy intercepts and proxies requests for URLs, potentially malicious files, and domain names associated with certain uncategorized or unknown domains. About File Inspection: " File Inspection inspects files hosted on risky domains for DNS policies." https://docs.umbrella.com/umbrella-user-guide/docs/manage-file-analysisRisky domains: The intelligent proxy is the abil

upvoted 3 times

Premium_Pils 1 year, 9 months ago

C) Intelligent Proxy: YES - Why? Because File Analysis is Enabled! The pre-requisite to be able to enable this feature is to turn on the Intelligent Proxy! Otherwise, you won't be able to switch this to be "enabled" and a message would be displayed under "File Analysis" that this "Requires Intelligent Proxy". Now that we understand that this feature is activated, we can also conclude that the Intelligent Proxy is ON.

upvoted 3 times

Premium_Pils 1 year, 9 months ago

This page shows what is displayed when Intelligent Proxy has not been enabled yet. So, you can see that in our case, on the picture of the question, the Intelligent Proxy is already ON: https://docs.umbrella.com/deployment-umbrella/docs/enable-the-intelligent-proxy

About Intelligent Proxy: https://docs.umbrella.com/deployment-umbrella/docs/enable-the-intelligent-proxy Umbrella's intelligent proxy intercepts and proxies requests for URLs, potentially malicious files, and domain names associated with certain uncategorized or unknown domains.

About File Inspection: " File Inspection inspects files hosted on risky domains for DNS policies." https://docs.umbrella.com/umbrella-user-guide/docs/manage-file-analysis

upvoted 2 times

Premium_Pils 1 year, 9 months ago

Here you can see, how Security Settings would look like when "Potentially Harmful Domains" are added. It is not the case on the picture in our question. "Potentially Harmful Domains" have not been added, so B) is not correct.

upvoted 1 times

Premium_Pils 1 year, 9 months ago

C) Intelligent Proxy: YES - Why? Because File Analysis is Enabled! The pre-requisite to be able to enable this feature is to turn on the Intelligent Proxy! Otherwise, you won't be able to switch this to be "enabled" and a message would be displayed under "File Analysis" that this "Requires Intelligent Proxy". Now that we understand that this feature is activated, we can also conclude that the Intelligent Proxy is ON.This page shows what is displayed when Intelligent Proxy has not been enabled yet. So, you can see that in our case, on the picture of the question, the Intelligent Proxy is already ON: https://docs.umbrella.com/deployment-umbrella/docs/enable-the-intelligent-proxy About Intelligent Proxy: https://docs.umbrella.com/deployment-umbrella/docs/enable-the-intelligent-proxy Umbrella's intelligent proxy intercepts and proxies requests for URLs, potentially malicious files, and domain names associated with certain uncategorized or unknown domains. About File Inspection: " File Inspection inspects files hosted on risky domains for DNS policies." https://docs.umbrella.com/umbrella-user-guide/docs/manage-file-analysisRisky domains: The intelligent proxy is the ability for Umbrella to intercept and proxy requests for malicious files embedded within certain so-called "grey" domains. ... The 'greylist' of risky domains is compromised of domains that host both malicious and safe content—we consider these “risky” domains. ... Umbrella’s intelligent proxy only routes the requests for risky domains for deeper inspection.More about File Inspection: https://docs.umbrella.com/deployment-umbrella/docs/file-inspection File inspection is an extension of the intelligent proxy’s scope and functionality. When enabled, you have the ability to scan files for malicious content hosted on risky domains before those files are downloaded. A risky domain is neither trusted ("known good") or known to be malicious, but one that could potentially pose a threat because little to no informatio

upvoted 3 times

Premium_Pils 1 year, 9 months ago

This page shows what is displayed when Intelligent Proxy has not been enabled yet. So, you can see that in our case, on the picture of the question, the Intelligent Proxy is already ON: https://docs.umbrella.com/deployment-umbrella/docs/enable-the-intelligent-proxy About Intelligent Proxy: https://docs.umbrella.com/deployment-umbrella/docs/enable-the-intelligent-proxy Umbrella's intelligent proxy intercepts and proxies requests for URLs, potentially malicious files, and domain names associated with certain uncategorized or unknown domains. About File Inspection: " File Inspection inspects files hosted on risky domains for DNS policies." https://docs.umbrella.com/umbrella-user-guide/docs/manage-file-analysisRisky domains: The intelligent proxy is the ability for Umbrella to intercept and proxy requests for malicious files embedded within certain so-called "grey" domains. ... The 'greylist' of risky domains is compromised of domains that host both malicious and safe content—we consider these “risky” domains. ... Umbrella’s intelligent proxy only routes the requests for risky domains for deeper inspection.More about File Inspection: https://docs.umbrella.com/deployment-umbrella/docs/file-inspection File inspection is an extension of the intelligent proxy’s scope and functionality. When enabled, you have the ability to scan files for malicious content hosted on risky domains before those files are downloaded. A risky domain is neither trusted ("known good") or known to be malicious, but one that could potentially pose a threat because little to no information is known about it.... File Inspection employs Umbrella’s intelligent proxy in order to have some domains proxied through our cloud but not others. ...Once a domain deemed 'risky’ is passed to the intelligent proxy....

upvoted 2 times

Premium_Pils 1 year, 9 months ago

Risky domains: The intelligent proxy is the ability for Umbrella to intercept and proxy requests for malicious files embedded within certain so-called "grey" domains. ... The 'greylist' of risky domains is compromised of domains that host both malicious and safe content—we consider these “risky” domains. ... Umbrella’s intelligent proxy only routes the requests for risky domains for deeper inspection.

upvoted 1 times

Premium_Pils 1 year, 9 months ago

More about File Inspection: https://docs.umbrella.com/deployment-umbrella/docs/file-inspection File inspection is an extension of the intelligent proxy’s scope and functionality. When enabled, you have the ability to scan files for malicious content hosted on risky domains before those files are downloaded. A risky domain is neither trusted ("known good") or known to be malicious, but one that could potentially pose a threat because little to no information is known about it.... File Inspection employs Umbrella’s intelligent proxy in order to have some domains proxied through our cloud but not others. ...Once a domain deemed 'risky’ is passed to the intelligent proxy....

upvoted 1 times

luismg 1 year, 11 months ago

The answer is B C is not because you can use umbrella just for dns security.

upvoted 1 times

RemiK 2 years, 2 months ago

File analysis enable = intelligent proxy Should be C

upvoted 2 times

mhd96far 2 years, 4 months ago

check out question 230

upvoted 1 times

XvidalX 2 years, 5 months ago

C is CORRECT - File analisys only is enabled when intelligent proxy is enable, even not seeing proxy configuration, we can assume that is enabled...

upvoted 3 times

LTLnetworker 2 years, 6 months ago

'Risky domain' is a term the documentation use for grey list / Intelligent Proxy. The IP cannot be seen but should be enabled in Advanced Settings.

upvoted 1 times

fdl543 3 years ago

"Refer to the Exhibit" We can not even see if Intelligent Proxy is enabled. So, it´s B.

upvoted 1 times

jku2cya 3 years, 1 month ago

Don't overthink it. The question first states "Refer to the exhibit".

upvoted 1 times

ffaiz 3 years, 1 month ago

https://docs.umbrella.com/deployment-umbrella/docs/manage-intelligent-proxy#:~:text=It%27s%20simple%3A%20Umbrella%20blocks%20those,again%2C%20no%20proxy%20is%20required. On this link Read this whole para: Which clearly states how Umberalla will handle "risky domains" Umbrella's intelligent proxy intercepts and proxies requests for URLs, potentially malicious files, and domain names associated with certain uncategorized or unknown domains. Some websites, especially those with large user communities or the ability to upload and share files, have content that most users want to access but also pose a risk because of the possibility of hosting malware. Administrators don't want to block access to an unknown domain for all users, but they also don't want your users to access files that could harm their computers or compromise company data.

upvoted 2 times

Jessie45785 3 years, 3 months ago

Selected Answer: B

Even though from logical point of view C makes more sense,... look at the Question 230

... hence against myself I am voting for B

230. When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

A. Application Control B. Security Category Blocking C. Content Category Blocking D. File Analysis

Correct Answer: B

upvoted 2 times

gc999 3 years, 2 months ago

After going through the document, I change to "C". It is because File Inspection is enabled, and it is an extension of the Intelligent Proxy. https://docs.umbrella.com/deployment-umbrella/docs/file-inspection#:~:text=File%20inspection%20is%20an%20extension%20of%20the%20intelligent%20proxy%E2%80%99s%20scope%20and%20functionality

upvoted 2 times

gc999 3 years, 2 months ago

The question is "Refer to the exhibit". Refer to the exhibit, we do not see any hints for Intelligent Proxy. So the answer should be "B", which the exhibit already mentioned it.

upvoted 1 times

gc999 3 years, 2 months ago

I got the same answer as you, but after reviewing the word clearly, question 230 said "when the domain host malware, command and control ...", those domains are already confirmed "bad", so it can use Security Category Blocking. But in here, the File Inspection is enabled AND the question said "risky", which is the grey list. So I believe answer here is C.

upvoted 3 times

Jessie45785 3 years, 3 months ago

Even though from logical point of view C makes more sense,... look at the Question 230 ... hence against myself I am voting for B 230. When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats? A. Application Control B. Security Category Blocking C. Content Category Blocking D. File Analysis Correct Answer: BI got the same answer as you, but after reviewing the word clearly, question 230 said "when the domain host malware, command and control ...", those domains are already confirmed "bad", so it can use Security Category Blocking. But in here, the File Inspection is enabled AND the question said "risky", which is the grey list. So I believe answer here is C.I agree with you that we are talking about the grey list so intelligent proxy is needed

upvoted 2 times

gc999 3 years, 2 months ago

I got the same answer as you, but after reviewing the word clearly, question 230 said "when the domain host malware, command and control ...", those domains are already confirmed "bad", so it can use Security Category Blocking. But in here, the File Inspection is enabled AND the question said "risky", which is the grey list. So I believe answer here is C.I agree with you that we are talking about the grey list so intelligent proxy is needed

upvoted 3 times

achille5 3 years, 6 months ago

C https://docs.umbrella.com/deployment-umbrella/docs/manage-intelligent-proxy

upvoted 1 times

cyberwhizzy0 3 years, 1 month ago

I agree with you that we are talking about the grey list so intelligent proxy is needed

upvoted 2 times

davezz 3 years, 6 months ago

C It seems the "File Analysis Enabled, File Inspection Enabled" indicates the Intelligent Proxy is enabled, as in order to do file inspection, web traffic needs to be pulled to the proxy server for inspection. Below link shows file inspection is a sub option after Intelligent Proxy is enabled: https://docs.umbrella.com/umbrella-user-guide/docs/enable-the-intelligent-proxy

upvoted 3 times

Question #227 *Topic 1*

An organization wants to improve its cybersecurity processes and to add intelligence to its data. The organization wants to utilize the most current intelligence data for URL filtering, reputations, and vulnerability information that can be integrated with the Cisco FTD and Cisco WSA. What must be done to accomplish these objectives?

A. Configure the integrations with Talos intelligence to take advantage of the threat intelligence that it provides.

B. Download the threat intelligence feed from the IETF and import it into the Cisco FTD and Cisco WSA databases.

C. Create an automated download of the Internet Storm Center intelligence feed into the Cisco FTD and Cisco WSA databases to tie to the dynamic access control policies.

D. Create a Cisco pxGrid connection to NIST to import this information into the security products for policy use.

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

Premium_Pils Most Recent 1 year, 9 months ago
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-sec-intel.html ->Read this!
upvoted 2 times

iluvmicrosoft 2 years, 4 months ago
I also agree its A I think the point here is current intelligence that can be ingested into FTD and WSA we know that FMC can use talos AND/OR 3rd party feeds.. (and then push the data to FTD) I found a post somewhere (wish i could find it) that stated FDM can only use talos also if you read up on how WSA gets its intelligence data, it states talos and i cannot find anything that says it can get 3rd party feeds - if these are both true then answer is not B NOR C as they can only use talos..
upvoted 3 times

Alizade 2 years, 10 months ago
Therefore, the answer is A.
upvoted 3 times

surforlife 4 years ago
Why not use pxGrid?pxGrid enables third party platforms to share threat intelligence , in another word ,pxGrid can be used for integration, it is not specifically related to importing information from NIST.
upvoted 1 times

surforlife 4 years ago
Why not use pxGrid?
upvoted 1 times

haiderzaid 3 years, 4 months ago
pxGrid enables third party platforms to share threat intelligence , in another word ,pxGrid can be used for integration, it is not specifically related to importing information from NIST.
upvoted 1 times

Question #228 *Topic 1*

An organization is implementing URL blocking using Cisco Umbrella. The users are able to go to some sites but other sites are not accessible due to an error.
Why is the error occurring?

A. Client computers do not have an SSL certificate deployed from an internal CA server.

B. Client computers do not have the Cisco Umbrella Root CA certificate installed.

C. IP-Layer Enforcement is not configured.

D. Intelligent proxy and SSL decryption is disabled in the policy.

Suggested Answer: *A*
Official Answer: A

Community vote distribution
B (100%)

screech Highly Voted 5 years, 3 months ago
Should be B. https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-Intelligent-Proxy

Requirements and Implementation Although only SSL sites on our 'grey' list will be proxied, it's required that the root certificate be installed on the computers that are using SSL Decryption for the Intelligent Proxy in their policy.

Without the root certificate, when your users go to that service, they will receive errors in the browser and the site will not be accessible. The browser, correctly, will believe the traffic is being intercepted (and proxied!) by a 'man in the middle', which is our service in this case. The traffic won't be decrypted and inspected; instead, the entire website won't be available.
upvoted 20 times

samismayilov Highly Voted 5 years, 3 months ago
Answer is B
upvoted 16 times

RemiK Most Recent 2 years, 2 months ago
Selected Answer: B
https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information then https://docs.umbrella.com/deployment-umbrella/docs/install-cisco-umbrella-root-certificate all

No advice for pushing the Root CA Umbrella into an internal CA. Only via Windows GPO. Cisco wants you to answer B.
upvoted 1 times

Mohammad_h_tarawneh 2 years, 2 months ago
you can deploy certificate from internal CA server on cisco umbrella and users pc , so why answer A is wrong ?
upvoted 1 times

Jessie45785 3 years, 4 months ago
Selected Answer: B
Definitely B, was doing it myself https://docs.umbrella.com/deployment-umbrella/docs/install-cisco-umbrella-root-certificate
upvoted 1 times

Webster21 3 years, 9 months ago
Selected Answer: B
Should be B
upvoted 2 times

sis_net_sec 3 years, 10 months ago
Selected Answer: B
root certificate be installed on the computers that are using ssl Decryption for the intelligent proxy in their policy
https://docs.umbrella.com/deployment-umbrella/docs/manage-intelligent-proxy
upvoted 1 times

mrimmune 4 years, 2 months ago

Should be B

upvoted 2 times

jaciro11 4 years, 5 months ago

Selected Answer: B

Client computers do not have the Cisco Umbrella Root CA certificate installed.

upvoted 3 times

Minion2021 4 years, 5 months ago

Anwer is B

upvoted 2 times

MoII 4 years, 9 months ago

Answer should be B

upvoted 2 times

ZanaHiwa 4 years, 10 months ago

Answer is B:

B. Client computers do not have the Cisco Umbrella Root CA certificate installed.

upvoted 3 times

eazy99 4 years, 11 months ago

The answer is absolutely B, you will find it on the first paragraph in the link I included. https://support.opendns.com/hc/en-us/articles/227987007-Block-Page-Errors-Installing-the-Cisco-Umbrella-Root-CA

upvoted 2 times

trickbot 5 years, 3 months ago

Well it's a good thing I paid examtopics to see all the wrong answers on the rest of the questions. This is a missing certificate problem, but the missing certificate is a CA certificate. SSL certificates issued by internal CAs would prove the user's host machine's identity to the website, which is clearly not how web browsing works.

upvoted 6 times

Question #229 *Topic 1*

Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

A. File Analysis

B. SafeSearch

C. SSL Decryption

D. Destination Lists

Suggested Answer: *C*
Official Answer: C

idto Highly Voted 1 year, 8 months ago

Correct answer is C "As well, the intelligent proxy's SSL decryption feature is required in order to scan files on secure—HTTPS—sites." Source: https://docs.umbrella.com/umbrella-user-guide/docs/enable-file-analysis

upvoted 5 times

Question #230 *Topic 1*

When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

A. Application Control

B. Security Category Blocking

C. Content Category Blocking

D. File Analysis

Suggested Answer: *B*
Reference: https://support.umbrella.com/hc/en-us/articles/115004563666-Understanding-Security-Categories

abdulmalik_mail Highly Voted 3 years, 1 month ago
correct, Its B on reference "the security setting categories are, at a minimum, the ones listed below : 1. Malware 2. Command and Control Callbacks 3. Phishing Attack
upvoted 5 times

Arris9 Most Recent 2 years, 1 month ago
https://docs.umbrella.com/deployment-umbrella/docs/dns-security-categories
upvoted 3 times

ureis 2 years, 1 month ago
I have this options in the proper Umbrella Dashboard: "Add New Security Setting" Options: - Malware ****** - Newly Seen Domains - Command and Control Callbacks ****** - Phishing Attacks ******* - Dynamic DNS - Potentially Harmful Domains - DNS Tunneling VPN - Cryptomining
upvoted 3 times

Question #231 *Topic 1*

How is Cisco Umbrella configured to log only security events?

A. per policy

B. in the Reporting settings

C. in the Security Settings section

D. per network in the Deployments section

Suggested Answer: *A*

Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

Community vote distribution

A (100%)

Premium_Pils Most Recent 1 year, 9 months ago

It should be like this: Policies > Management > Add/Edit Policy > Edit Settings > Centralized Settings > Advanced Settings > Log Only Security Events https://docs.umbrella.com/deployment-msp/docs/customize-policies Create and Apply Policies https://docs.umbrella.com/deployment-umbrella/docs/configure-advanced-settings Configure Advanced Settings https://docs.umbrella.com/deployment-umbrella/docs/manage-logs Manage Logs

upvoted 2 times

abdulmalik_mail 4 years, 7 months ago

correct, It's A

upvoted 4 times

Question #232 *Topic 1*

Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

A. Cisco AMP

B. Cisco AnyConnect

C. Cisco Dynamic DNS

D. Cisco Talos

Suggested Answer: *D*
Official Answer: D

abdulmalik_mail Most Recent 2 years, 1 month ago

Correct, It's D https://www.insight.com/content/dam/insight-web/Canada/PDF/partner/cisco/cisco-umbrella-at-a-glance.pdf "The Umbrella proxy uses Cisco Talos web reputation and other third-party feeds to determine if a URL is malicious"

upvoted 1 times

Question #233 *Topic 1*

What are two list types within Cisco AMP for Endpoints Outbreak Control? (Choose two.)

A. blocked ports

B. simple custom detections

C. command and control

D. allowed applications

E. URL

Suggested Answer: *B, D*

Reference: https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf chapter 2

Community vote distribution

BD (100%)

nospampls Highly Voted 3 years, 6 months ago

B and D

https://docs.amp.cisco.com/AMPPrivateCloudConsoleUserGuide-latest.pdf

upvoted 12 times

aalnman 3 years, 4 months ago

B and D is CORRECT

upvoted 3 times

ITVI Most Recent 1 year, 4 months ago

Selected Answer: BD

Reference point:

https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf

upvoted 1 times

Tuxzinator 1 year, 12 months ago

Selected Answer: BD

bd correct

upvoted 1 times

MoII 3 years, 2 months ago

Voting for B and D here

upvoted 1 times

Question #234 *Topic 1*

For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two.)

A. computer identity

B. Windows service

C. user identity

D. Windows firewall

E. default browser

Suggested Answer: *B, D*

Official Answer: BD

Community vote distribution

BD (100%)

Vic25H Highly Voted 3 years, 8 months ago

Agree B&D https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.html

upvoted 29 times

Vic25H Highly Voted 3 years, 8 months ago

Agree B&D https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.htmlSpecifically: Table 2. Posture Assessment Options - Windows Service status/config can be assessed, Windows Firewall can be assessed by assessing the registry entry.

upvoted 29 times

bigdadzzz 3 years, 1 month ago

Specifically: Table 2. Posture Assessment Options - Windows Service status/config can be assessed, Windows Firewall can be assessed by assessing the registry entry.

upvoted 10 times

kudlaaaaty 3 years, 8 months ago

IMHO: B & D

upvoted 11 times

getafix Most Recent 1 year, 8 months ago

i have implemented this myself. Posture checks for firewall enablement and also checks for Windows updates enabled.

upvoted 2 times

larn 1 year, 9 months ago

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated to a posture requirement.

upvoted 2 times

MoII 2 years, 2 months ago

I agree with B and D

upvoted 2 times

pfunkylol 2 years, 2 months ago

b and c are correct

upvoted 1 times

itisfakemaillol 2 years, 7 months ago

B and D

upvoted 5 times

fr3dastik 3 years ago

Correct answer : B & D

upvoted 8 times

Question #235 *Topic 1*

Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

A. NGFW

B. AMP

C. WSA

D. ESA

Suggested Answer: *B*
Official Answer: B

CCNP21 Highly Voted 3 years ago

Now called Secure Endpoint.

upvoted 7 times

Ferdaush Most Recent 2 years, 1 month ago

Cisco Advanced Malware Protection (AMP) for Endpoints is a cloud-managed endpoint security solution that provides advanced protection against viruses, malware, and other cyber-threats by detecting, preventing, and responding to threats.

upvoted 2 times

Question #236 *Topic 1*

Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two.)

A. Patch for cross-site scripting.

B. Perform backups to the private cloud.

C. Protect against input validation and character escapes in the endpoint.

D. Install a spam and virus email filter.

E. Protect systems with an up-to-date antimalware program.

Suggested Answer: *D, E*

Official Answer: DE

Community vote distribution

DE (100%)

bigdadzzz Highly Voted 5 years, 1 month ago

https://us-cert.cisa.gov/ncas/tips/ST04-014

How do you avoid being a victim? "Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. (See Understanding Firewalls for Home and Small Office Use, Protecting Against Malicious Code, and Reducing Spam for more information.) "

"Less correct" answers than D/E A - Indirectly, yes. B - Defence against Ransomware C - Defence against SQLi

upvoted 15 times

bigdadzzz Highly Voted 5 years, 1 month ago

https://us-cert.cisa.gov/ncas/tips/ST04-014 How do you avoid being a victim? "Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. (See Understanding Firewalls for Home and Small Office Use, Protecting Against Malicious Code, and Reducing Spam for more information.) " "Less correct" answers than D/E A - Indirectly, yes. B - Defence against Ransomware C - Defence against SQLi...where: A. Patch for cross-site scripting & C. Protect against input validation and character escapes in the endpoint = BOTH ARE SERVER SIDE MEASURES, NOT ENDPOINT ("server side" in this case means WHO IS RESPONSIBLE for code security, NOT WHERE the code is running - XSS will run in user's browser at client side but responsible for that is vulnerable server) If some well known TRUSTED server (for example your own company's web) is vulnerable to XSS or another attack based on poor input validation, protection from user's side is mostly NOT possible - because you TRUST that server, you (and your security tools - for example NoScript) allow to run scripts from the server, you contentedly insert sensitive information to the page from the server, etc... Endpoint protection is anti-spam, anti-virus, anti-malware - i. e. options D & E

upvoted 15 times

NikoNiko 3 years, 7 months ago

...where: A. Patch for cross-site scripting & C. Protect against input validation and character escapes in the endpoint = BOTH ARE SERVER SIDE MEASURES, NOT ENDPOINT ("server side" in this case means WHO IS RESPONSIBLE for code security, NOT WHERE the code is running - XSS will run in user's browser at client side but responsible for that is vulnerable server) If some well known TRUSTED server (for example your own company's web) is vulnerable to XSS or another attack based on poor input validation, protection from user's side is mostly NOT possible - because you TRUST that server, you (and your security tools - for example NoScript) allow to run scripts from the server, you contentedly insert sensitive information to the page from the server, etc... Endpoint protection is anti-spam, anti-virus, anti-malware - i. e. options D & E

upvoted 3 times

Oz3006 5 years, 4 months ago

i think is D-E C is used for cross site scripting.

upvoted 6 times

Ferdaush Most Recent 2 years, 1 month ago

Cisco Advanced Malware Protection (AMP) for Endpoints is a cloud-managed endpoint security solution that provides advanced protection against viruses, malware, and other cyber-threats by detecting, preventing, and responding to threats.

upvoted 1 times

Mulema 2 years, 2 months ago

A and C are correct assuming the following question that I asked Bard AI: Can Cisco ISE install patches on an endpoint like a pc after identifying that the pc lacks up-to-date patches? Yes, Cisco ISE can install patches on an endpoint like a PC after identifying that the PC lacks up-to-date patches.

This is done using the Cisco Endpoint Security Agent (ESA), which is a software agent that is installed on the endpoint. The ESA communicates with Cisco ISE to determine which patches are needed and then downloads and installs them on the endpoint.
https://bard.google.com/chat/24ec2765faf58266
upvoted 1 times

somaaoo 3 years, 11 months ago
D,E C for XSS
upvoted 3 times

MoII 4 years, 2 months ago
Voting for D and E here
upvoted 1 times

jaciro11 4 years, 3 months ago
D and E: Little cathedra: Okay many people put C " Protect against input validation and character escapes in the endpoint." well how you protect about that "E. Protect systems with an up-to-date antimalware program." So the answer is D and E
upvoted 5 times

Reece_S 4 years, 6 months ago
The question is specifically for mitigation on endpoints, so D&E.
upvoted 5 times

thegreek1 5 years, 4 months ago
phising is when someone tries to send you an email to lure you into a dummy website so D & E are both valid
upvoted 6 times

naddaf 5 years, 7 months ago
i believe C & E
upvoted 1 times

Alexis182b 5 years, 7 months ago
I think it is CD
upvoted 1 times

Question #237 *Topic 1*

An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware.
Which two solutions mitigate the risk of this ransomware infection? (Choose two.)

A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.

B. Set up a profiling policy in Cisco Identity Services Engine to check an endpoint patch level before allowing access on the network.

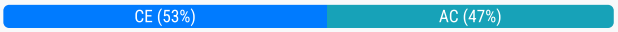
C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.

D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.

E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

Suggested Answer: *A, C*
Official Answer: AC

Community vote distribution



Sorel Highly Voted 5 years, 11 months ago
I'm struggling to find a good link on this, but seems to me that ISE will not patch an endpoint by himself, instead it relies on WSUS for this. So, A is probably incorect, and the right answer is CE. Anyone else?https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010110.html
upvoted 26 times

Sorel Highly Voted 5 years, 11 months ago
I'm struggling to find a good link on this, but seems to me that ISE will not patch an endpoint by himself, instead it relies on WSUS for this. So, A is probably incorect, and the right answer is CE. Anyone else?
upvoted 26 times

bigdadzzz 5 years, 7 months ago
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010110.html
upvoted 2 times

Monnezzo 5 years, 8 months ago
It's A and C source: https://community.cisco.com/t5/security-documents/how-to-integrate-cisco-ise-with-microsoft-sccm-for-patch/ta-p/3725035#toc-hId--2070782007
upvoted 10 times

Monnezzo 5 years, 8 months ago
It's A and C source: https://community.cisco.com/t5/security-documents/how-to-integrate-cisco-ise-with-microsoft-sccm-for-patch/ta-p/3725035#toc-hId--2070782007Disagree. Your link says that ISE only sees that SCCM shows that there are patches needed. It then uses AnyConnect to trigger SCCM to install the patch. Answer A specifically states that ISE installs the patch. There is nowhere in any guide that says ISE installs a patch. Further if you look at the posture policy section of the admin guide, it says nothing about pushing patches. Answer A mentions the configuring a posture policy.
upvoted 10 times

nep1019 3 years ago
Disagree. Your link says that ISE only sees that SCCM shows that there are patches needed. It then uses AnyConnect to trigger SCCM to install the patch. Answer A specifically states that ISE installs the patch. There is nowhere in any guide that says ISE installs a patch. Further if you look at the posture policy section of the admin guide, it says nothing about pushing patches. Answer A mentions the configuring a posture policy.
upvoted 1 times

Nian Most Recent 1 year, 5 months ago
I believe A is correct - A posture policy can be made with the remediation action that redirects the user to a remediation portal where they must install the MS17-010 patch before regaining full access.
upvoted 1 times

iluvmicrosoft 2 years, 4 months ago
anyone consider D? if your a client w tcp 445 open?? you could have been vulnerable.. file servers w tcp 445 ok.. but clients??

upvoted 1 times

XvidalX 2 years, 5 months ago

ISE does not intall patches , remediation policies does not install patches , Remediation policies does trigger installations by third party systems... A is malformed answer , C and E are totally correctE seems to be more logical

upvoted 4 times

XvidalX 2 years, 5 months ago

Selected Answer: CE

ISE does not intall patches , remediation policies does not install patches , Remediation policies does trigger installations by third party systems... A is malformed answer , C and E are totally correct

upvoted 4 times

Premium_Pils 2 years ago

E seems to be more logical

upvoted 1 times

nep1019 3 years ago

If you go look at the posture policy section of the admin guide (https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_client_posture_policies.html#task_DBFD37F536134843BC81C4DFEF34A8EC) you see that there is nothing in there that allows ISE to INSTALL a patch which is what it says for answer A). Can it be integrated with SCCM to invoke an action in SCCM to update with a patch? Yes. Can ISE itself install that patch? No. Answer is C and E.

upvoted 2 times

Tuxzinator 3 years, 6 months ago

Option C specifically addresses the vulnerability that was exploited by the WannaCry ransomware, which is the MS17-010 patch that was not installed on the endpoint. By configuring a posture policy to check that the endpoint patch level is met before allowing access to the network, the organization can ensure that all endpoints have the necessary patches installed to mitigate the risk of this ransomware. Option E is still a good solution in general to ensure that endpoints are patched in a timely fashion, but it does not specifically address the vulnerability that was exploited by the WannaCry ransomware.

upvoted 3 times

psuoh 3 years, 6 months ago

https://community.cisco.com/t5/network-access-control/ise-posture-windows-updates/td-p/3575621

upvoted 2 times

psuoh 3 years, 6 months ago

ISE wouldn't know how to patch an Windows OS. It needs integration with some patching system.

upvoted 1 times

Anonymous983475 3 years, 7 months ago

ICE can check for patches not install them in the end user's OS

upvoted 2 times

nomanlands 4 years, 1 month ago

A and C is correct. SCCM will integrate to do the patching as others mentioned and E is only not an option as it asks what can be done to mitigate THIS ransomware infection and not best practices overall.it asks what can be done to mitigate 'THE RISK' of this ransomware infection. Not to mitigate the ransomware itself. C and E mitigate the risk. ISE itself does not patch systems.

upvoted 1 times

nomanlands 4 years, 1 month ago

A and C is correct. SCCM will integrate to do the patching as others mentioned and E is only not an option as it asks what can be done to mitigate THIS ransomware infection and not best practices overall.

upvoted 1 times

west33637 3 years, 7 months ago

it asks what can be done to mitigate 'THE RISK' of this ransomware infection. Not to mitigate the ransomware itself. C and E mitigate the risk. ISE itself does not patch systems.

upvoted 1 times

larn 4 years, 3 months ago

People are saying patching isnt possible from ISE but the doco show it is configurable. https://community.cisco.com/t5/security-documents/how-to-integrate-cisco-ise-with-microsoft-sccm-for-patch/ta-p/3725035#toc-hId--2070782007 Step 1 Go to Workcentre-> Posture-> Policy Elements-> Condition-> Patch management. Add a patch management condition to check for up-to-date patch status. This conditions checks if there are any pending patches to be installed in the SCCM client.

upvoted 3 times

MoII 4 years, 9 months ago

I'd go with A and C here.

upvoted 2 times

jaciro11 4 years, 9 months ago

Hello TEAM, Well you want to check if a specified KB its patched in your system, okay nice the Answer is: A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network. but I think the appropriate answer for this is C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network. Well that's means A and C its the same but C its more completed answer. So the answer is C and E

upvoted 3 times

Steve122 4 years, 9 months ago

A: Patch will be installed by ISE NAC agent on endpoint C: ISE checks the endpoint first if that is compliant (NAC agent) B: Make no sense "profiling policy"

upvoted 2 times

beeker98106 4 years, 9 months ago

A+C is correct, just confirmedconfirmed by who?

upvoted 4 times

beeker98106 4 years, 9 months ago

A+C is correct, just confirmed

upvoted 4 times

stalkr3 3 years, 4 months ago

confirmed by who?

upvoted 4 times

jshow 5 years ago

A and C for me ....question states for THIS expolit

upvoted 2 times

Question #238 *Topic 1*

What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

A. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.

B. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.

C. EPP focuses on network security, and EDR focuses on device security.

D. EDR focuses on network security, and EPP focuses on device security.

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr.html

Community vote distribution

A (100%)

MPoels Most Recent 1 year, 11 months ago

Prevention capabilities provided by EPPs, and detection and response capabilities (if something evades preventative measures) provided by EDRs.
https://blogs.cisco.com/security/epp-edr-cisco-amp-for-endpoints-is-next-generation-endpoint-security

upvoted 4 times

NikoNiko 3 years, 7 months ago

A) is correct https://www.cynet.com/endpoint-protection-and-edr/epp-vs-edr-what-matters-more-prevention-or-response/

upvoted 2 times

Question #239 *Topic 1*

An engineer is configuring AMP for endpoints and wants to block certain files from executing.
Which outbreak control method is used to accomplish this task?

A. device flow correlation

B. simple detections

C. application blocking list

D. advanced custom detections

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

klu16 Highly Voted 3 years, 11 months ago
I thought it's B like some guys said, but it's C for sure...

From AMP for Endpoints User Guide, chapter 2: Outbreak Control: An application blocking list is composed of files that you do not want to allow users to execute but do not want to quarantine. You may want to use this for files you are not sure are malware, unauthorized applications, or you may want to use this to stop applications with vulnerabilities from executing until a patch has been released.

B also is incorrect, because it says "simple detections" but actually it's called simple custom detections (like in answer D, but it's another function which allows the customer to write his own antivirus definitions...).

I am 100% sure it's an answer C here :)
upvoted 17 times

aalnman 3 years, 10 months ago
C = Correct as Klu16 pointed out. Also "B" does not block, it quarantines. This is from same doc klu mentioned regarding "B": A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine. Not only will an entry in a Simple Custom Detection list quarantine future files, but through Retrospective it will quarantine instances of the file on any endpoints in your organization that the service has already seen it on.
upvoted 4 times

Alizade Most Recent 1 year, 10 months ago
Selected Answer: C
C. Application Blocking List
upvoted 2 times

Emlia1 2 years, 8 months ago
It's C
upvoted 2 times

denverfly 3 years, 5 months ago
C is good. Outbreak control: Achieve control over suspicious files or outbreaks and remediate an infection without waiting for a content update. Within the outbreak control feature: ◦ Simple custom detections can quickly block a specific file across all or selected systems ◦ Advanced custom signatures can block families of polymorphic malware ◦ Application blocking lists can enforce application policies or contain a compromised application being used as a malware gateway and stop the reinfection cycle ◦ Custom whitelists will help ensure that safe, custom, or mission-critical applications continue to run no matter what ◦ Device flow correlation will stop malware call-back communications at the source, especially for remote endpoints outside the corporate network
upvoted 2 times

MoII 3 years, 9 months ago
Would go with C here.
upvoted 2 times

Steve122 3 years, 9 months ago

Would go with C

Application Block Lists are only applicable to binaries. When the SHA-256 of a binary is added to the Application Block List, AMP will prevent that file from being executed.

upvoted 2 times

beeker98106 3 years, 9 months ago

C. it is

upvoted 3 times

ferari 4 years, 1 month ago

The correct answer is B. https://www.connection.com/~/media/pdfs/brands/c/cisco/cisco-security-amp-solution-overview.pdf?la=en

upvoted 2 times

itisfakemaillol 4 years, 1 month ago

For me the answer is B

A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine. Not only will an entry in a Simple Custom Detection list quarantine future files, but through Retrospective it will quarantine instances of the file on any endpoints in your organization that the service has already seen it on.

upvoted 3 times

Luc_10 4 years, 1 month ago

I would answer D in this case, as custom detection blocks specific files, while application control is used to block application

upvoted 1 times

Seawanderer 4 years, 1 month ago

It's tricky, as for example we don't execute an excel file but we run instead excel program that opens the excel file itself.

upvoted 2 times

Question #240 *Topic 1*

An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from
ISE.
Which CoA type achieves this goal?

A. Port Bounce

B. CoA Terminate

C. CoA Reauth

D. CoA Session Query

Suggested Answer: *C*
Official Answer: C

NikoNiko Most Recent 2 years, 1 month ago

C is correct:

"CoA Session Reauthenticate Command To initiate session authentication, the AAA server sends a standard CoA-Request message containing the following VSAs: Cisco:Avpair="subscriber:command=reauthenticate" ...

The following rules apply: • "subscriber:command=reauthenticate" must be present to trigger a reauthentication. • If "subscriber:reauthenticate-type" is not specified, the default behavior is to rerun the last successful authentication method for the session. If the method reauthenticates successfully, all old authorization data is replaced with the new reauthenticated authorization data"

A - Bounce = session disrupted by disabling & enabling port B - Terminate = session discarded D - Session Query = ISE getting info about auth. session

"CoA Session Query Command The CoA session query command requests service information about a subscriber session"

Source: https://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-coa-supp.pdf
upvoted 3 times

Question #241 *Topic 1*

Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two.)

A. malware

B. denial-of-service attacks

C. ARP spoofing

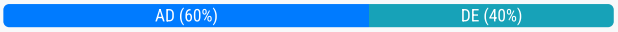
D. exploits

E. eavesdropping

Suggested Answer: *A, D*

Official Answer: AD

Community vote distribution



dr4gn00t Highly Voted 2 years, 7 months ago

D (Exploits) for sure. B (DDoS) would be suitable if the questions was about servers but since it is about endpoints, I would go with A&D.Even with current patches a DDoS attack could not really be prevented on servers or clients. You could just bomb them with illegitimate traffic and they could not do anything. It is for sure A & D.

upvoted 7 times

dr4gn00t Highly Voted 2 years, 7 months ago

D (Exploits) for sure. B (DDoS) would be suitable if the questions was about servers but since it is about endpoints, I would go with A&D.

upvoted 7 times

FortiSherlock 2 years ago

Even with current patches a DDoS attack could not really be prevented on servers or clients. You could just bomb them with illegitimate traffic and they could not do anything. It is for sure A & D.

upvoted 4 times

SomKeat Most Recent 2 months, 3 weeks ago

A and D is the correct answer

upvoted 1 times

Pages 4 months, 1 week ago

Why malware isn't selected here (in the Cisco context): Your comment is correct: Cisco focuses more on which specific risk is mitigated by patching. Malware is often viewed as something that is also addressed by other solutions, such as AMP (Advanced Malware Protection). While patching does help indirectly against malware, Cisco does not consider it the primary risk in this question. Key insight: Exam/logic answer (Cisco): exploits + eavesdropping General security practice: malware + exploits is also a valid answer So for your Cisco exam: choose D and E.

upvoted 1 times

Pages 6 months ago

CramQuiz: Organizations without a patching stategy will be vulnerable to exploits and eavesdropping. Protection againts malwere is considering Cisco done with e.g. Cisco AMP.

upvoted 1 times

CyberGhost666 1 year, 1 month ago

A and D) A lack of endpoint patching leaves systems exposed to malware and exploits, which are among the most common and dangerous cybersecurity threa

upvoted 2 times

Question #242 *Topic 1*

Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?

A. It adds endpoints to identity groups dynamically

B. It allows the endpoint to authenticate with 802.1x or MAB

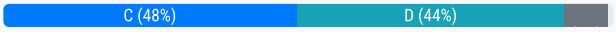
C. It allows CoA to be applied if the endpoint status is compliant

D. It verifies that the endpoint has the latest Microsoft security patches installed

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Jeeves69 Highly Voted 5 years, 5 months ago

Correct answer should be D

upvoted 28 times

Jeeves69 Highly Voted 5 years, 5 months ago

Correct answer should be DDepends what the policy requirements are, if the requirements on the policy don't include the latest patches, then D is incorrect.But "by ensuring that the endpoint is compliant", then you can authenticate afterwards. So might be a B also... I agree that with posture policy you verify the latest patches are installed, but when you ensure that, you can then authenticate. Or is my interpretation incorrect? ;)

upvoted 28 times

Smileebloke 4 years, 4 months ago

Depends what the policy requirements are, if the requirements on the policy don't include the latest patches, then D is incorrect.

upvoted 3 times

klu16 4 years, 11 months ago

But "by ensuring that the endpoint is compliant", then you can authenticate afterwards. So might be a B also... I agree that with posture policy you verify the latest patches are installed, but when you ensure that, you can then authenticate. Or is my interpretation incorrect? ;)

upvoted 3 times

MoII 4 years, 9 months ago

Answer should be C https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215419-ise-session-management-and-posture.html step 3. Posture assessment happens. step 4. Session marked as Compliant. step 5. Change of Authorization (COA) triggered by posture status change leads to re-authentication of the endpoint to apply the next access level.

upvoted 22 times

tal10 Most Recent 4 months, 1 week ago

d is correct

upvoted 1 times

Pages 6 months ago

Answer should be C facilitates endpoint re-authentication based on posture assessment
https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8300/software_config/cat8300swcfg-xe-17-book/m-chng-of-auth.pdf

upvoted 1 times

CyberGhost666 1 year, 1 month ago

Posture checks: AV, firewall, patch level, etc. • If compliant → ISE sends CoA → Endpoint gets full network access • □ Correct answer: C

upvoted 2 times

Diegosuarezb 1 year, 4 months ago

C is the "benefit "

upvoted 2 times

madboy2 1 year, 4 months ago

Cisco Identity Services Engine (ISE) Posture Policy is used to verify that endpoints comply with security policies before granting them network access. When an endpoint is compliant with the posture policy, ISE can apply a Change of Authorization (CoA). CoA dynamically updates the endpoint's access privileges without requiring the user to reconnect. If the endpoint is non-compliant, ISE can restrict access to a remediation VLAN or apply a quarantine policy. Why not the other options? A. It adds endpoints to identity groups dynamically. While ISE can dynamically categorize

endpoints, this is not a direct function of posture compliance. B. It allows the endpoint to authenticate with 802.1X or MAB 802.1X and MAB (MAC Authentication Bypass) occur before posture assessment, meaning compliance does not impact authentication. D. It verifies that the endpoint has the latest Microsoft security patches installed Posture policies can check for security patches, but ensuring compliance does not guarantee the latest patches are installed.

upvoted 1 times

kloug 1 year, 9 months ago

Answer c

upvoted 1 times

MomoBill 1 year, 10 months ago

We need to answer based on the question, the question asked for benefit. Should be D. Since CoA is mechanism, not benefit, authentication with dot1x and MAB also not a benefit.

upvoted 2 times

klu16 2 years, 1 month ago

Option C remains the most appropriate answer because it directly addresses the capability of applying CoA based on endpoint compliance status, which is a key benefit of posture assessment and enforcement in Cisco ISE. Therefore, while option D is a valuable functionality, option C offers a more comprehensive and overarching benefit of posture compliance in Cisco ISE. It highlights the dynamic access control and policy enforcement capabilities enabled by CoA based on the endpoint's security posture. In conclusion, while option D reflects a significant aspect of posture policies, option C provides a more encompassing benefit by emphasizing the dynamic access control and policy enforcement possibilities through CoA based on the endpoint's overall security posture.

upvoted 1 times

Rododendron2 2 years, 2 months ago

Selected Answer: D

CoA is not a benefit, it is mechanism

upvoted 1 times

Rododendron2 2 years, 2 months ago

CoA is not a benefit, it is mechanismmechanism that brings desired result = benefit

upvoted 1 times

Rododendron2 2 years, 1 month ago

mechanism that brings desired result = benefit

upvoted 1 times

abdul9621 2 years, 6 months ago

D is correct

upvoted 1 times

Mulema 2 years, 8 months ago

C is the correct answer for me. An endpoint (PC) having the latest Microsoft security patches installed, is part of the compliant posture policy defined in ISE. So, an and point cannot be said to be compliant without this Microsoft patch and the other necessary patches for the other applications running on that pc. The patches are determined by the company in function of its business applications.

upvoted 1 times

Edy79 2 years, 9 months ago

It must be D. It cannot be C because CoA also happens if the endpoint is not compliant. " Validating a Posture Requirement Request Once the client (an endpoint) is authenticated on the network, the client can be granted limited access on the network. For example, the client can access remediation-only resources on the network. The NAC Agent that is installed on the client validates the requirements for an endpoint and the endpoint is moved to a compliant state upon successful validation of the requirements. If the endpoint satisfies the requirement, a compliance report will be sent to the Cisco ISE node that assumes the Policy Service persona and the run-time services triggers a Change of Authorization (CoA) for the posture compliant status. If the endpoint fails to satisfy the requirement, a noncompliance report will be sent to the Cisco ISE node that assumes the Policy Service persona and the run-time services triggers a CoA for the posture noncompliant status." source: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_pos_pol.html#wp1496783

upvoted 2 times

cyberwhizzy0 3 years, 1 month ago

This is what I have been thinking about too but I am not sure...I'm tilting towards "C" 5. Change of Authorization (COA) triggered by posture status change leads to re-authentication of the endpoint to apply the next access level. https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215419-ise-session-management-and-posture.html

upvoted 3 times

SegaMasterSystemAdmin 3 years, 2 months ago

Please stop voting for C, it is not the right answer. CoA is not a benefit, it's just the action as result of the compliance status whether it is compliant, noncompliant, or unknown. If you read the question carefully "Which benefit is provided by ensuring that an endpoint is compliant.." if checking for the latest MS security patches is what the posture policy is looking for, then that would be the benefit, answer is D.

upvoted 4 times

stalkr3 3 years, 4 months ago

The key here, is allowing COA is not a "benefit", rather the expected behaviour once the endpoint is compliant, to grant full access.

upvoted 2 times

Question #243 *Topic 1*

An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group. Which probe must be enabled for this type of profiling to work?

A. SNMP

B. NMAP

C. DHCP

D. NetFlow

Suggested Answer: *C*

Official Answer: C

Community vote distribution



Jeeves69 Highly Voted 5 years, 5 months ago

The answer is C, through DHCP Profiling. The OUI is part of the MAC address, which can be learned from the dhcp-client-identifier option 61.And check Nmap probe to access mac ...it is done on manual scanhttps://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/Workflow/b_endpoint_profiling_2_4.html#reference_FD15BD65A25A4390B2A865450F938ADFI agree. NMAP scan is based on IP, any information collected during scan will be discarded if MAC-IP binding doesn't exist According to ISE profile design guide, "The dhcp-client-identifier typically provides the MAC address, which in turn provides the vendor OUI information through correlation from the MAC Address-OUI mapping table." under Procedure 25 Verify DHCP Probe Data https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456#toc-hld-2096149162in addition to Jeeves69, It is option 60, not 61 https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKSEC-2725.pdf Vendor / OS information can be gathered from dhcp-class-identifier (60) DHCP parameter request list and DHCP class ID can be used for platform and model.The dhcp-client-identifier typically provides the MAC address, which in turn provides the vendor OUI information through correlation from the MAC Address-OUI mapping table. The dhcp-class-identifier often provides a unique platform-specific attribute and in some cases provides a detailed description of the connected endpoint - in this example, MSFT 5.0 which is the value assigned to Microsoft Windows workstations. https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456

upvoted 35 times

Jeeves69 Highly Voted 5 years, 5 months ago

The answer is C, through DHCP Profiling. The OUI is part of the MAC address, which can be learned from the dhcp-client-identifier option 61.

upvoted 35 times

044f2fc 2 years, 4 months ago

And check Nmap probe to access mac ...it is done on manual scanhttps://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/Workflow/b_endpoint_profiling_2_4.html#reference_FD15BD65A25A4390B2A865450F938ADF

upvoted 1 times

044f2fc 2 years, 4 months ago

And check Nmap probe to access mac ...it is done on manual scan

upvoted 1 times

044f2fc 2 years, 4 months ago

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/Workflow/b_endpoint_profiling_2_4.html#reference_FD15BD65A25A4390B2A865450F938ADF

upvoted 1 times

semi1750 4 years, 5 months ago

I agree. NMAP scan is based on IP, any information collected during scan will be discarded if MAC-IP binding doesn't exist According to ISE profile design guide, "The dhcp-client-identifier typically provides the MAC address, which in turn provides the vendor OUI information through correlation from the MAC Address-OUI mapping table." under Procedure 25 Verify DHCP Probe Data https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456#toc-hld-2096149162in addition to Jeeves69, It is option 60, not 61 https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKSEC-2725.pdf Vendor / OS information can be gathered from dhcp-class-identifier (60) DHCP parameter request list and DHCP class ID can be used for platform and model.The dhcp-client-identifier typically provides the MAC address, which in turn provides the vendor OUI information through correlation from the MAC Address-OUI mapping table. The dhcp-class-identifier often provides a unique platform-specific attribute and in some cases provides a detailed description of the connected endpoint - in this

example, MSFT 5.0 which is the value assigned to Microsoft Windows workstations. https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456

upvoted 8 times

semi1750 4 years, 5 months ago

I agree. NMAP scan is based on IP, any information collected during scan will be discarded if MAC-IP binding doesn't exist According to ISE profile design guide, "The dhcp-client-identifier typically provides the MAC address, which in turn provides the vendor OUI information through correlation from the MAC Address-OUI mapping table." under Procedure 25 Verify DHCP Probe Data https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456#toc-hId-2096149162

upvoted 8 times

semi1750 4 years, 3 months ago

in addition to Jeeves69, It is option 60, not 61 https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKSEC-2725.pdf Vendor / OS information can be gathered from dhcp-class-identifier (60) DHCP parameter request list and DHCP class ID can be used for platform and model.The dhcp-client-identifier typically provides the MAC address, which in turn provides the vendor OUI information through correlation from the MAC Address-OUI mapping table. The dhcp-class-identifier often provides a unique platform-specific attribute and in some cases provides a detailed description of the connected endpoint - in this example, MSFT 5.0 which is the value assigned to Microsoft Windows workstations. https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456

upvoted 4 times

semi1750 4 years, 3 months ago

in addition to Jeeves69, It is option 60, not 61 https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKSEC-2725.pdf Vendor / OS information can be gathered from dhcp-class-identifier (60) DHCP parameter request list and DHCP class ID can be used for platform and model.

upvoted 4 times

Premium_Pils 2 years ago

The dhcp-client-identifier typically provides the MAC address, which in turn provides the vendor OUI information through correlation from the MAC Address-OUI mapping table. The dhcp-class-identifier often provides a unique platform-specific attribute and in some cases provides a detailed description of the connected endpoint - in this example, MSFT 5.0 which is the value assigned to Microsoft Windows workstations. https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456

upvoted 2 times

nomanlands 4 years, 1 month ago

The answer is SNMP. It will work and can pull ARP tables from the network devices. In fact, page 28 in the ISE Profiling guide recommends it if Radius or DHCP probes can't be effective. An NMAP scan cannot get a MAC address. If it is on the same subnet, then it would pull the MAC from the ARP table which would then be effective. That's a big IF DHCP would missing static devices as mentioned. A Netflow probe with additional attributes of SRC_MAC and DST_MAC should also be able to work for this situation if placed properly within the networks but I'm going with SNMP as that is what is recommended in the guide.

upvoted 6 times

madboy2 Most Recent 1 year, 4 months ago

Explanation: To automatically assign endpoints with a specific Organizationally Unique Identifier (OUI) into a new endpoint group, Cisco ISE needs to identify the MAC addresses of those endpoints. The DHCP probe extracts MAC addresses from DHCP request packets, allowing Cisco ISE to determine the OUI (first 24 bits of the MAC address) and categorize devices accordingly. Why not the other options? A. SNMP – Used for network device discovery, but not effective for identifying endpoint MAC addresses dynamically. B. NMAP – Performs active scanning but does not focus on OUI-based profiling. D. NetFlow – Provides traffic flow analysis, but does not extract MAC addresses from endpoint traffic.

upvoted 2 times

Basuso 1 year, 9 months ago

Correcting myself from my answer below. According to "Probe Selection Best Practices" in the ISE Profiling Designing Guide, from the official Cisco documentation, it's SNMP.

upvoted 1 times

Basuso 1 year, 9 months ago

I vote for C. As many before have said, the DHCP probe in Cisco ISE can capture information from DHCP requests, including the MAC address of the endpoint. The OUI is part of the MAC address and can be used to profile and categorize endpoints into specific groups based on this information.

upvoted 2 times

kloug 1 year, 9 months ago

Answer c

upvoted 2 times

luismg 1 year, 11 months ago

OUI is know from the MAC address witch is located through the DHCP "DORA" process.

upvoted 2 times

Premium_Pils 2 years ago

https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456

upvoted 2 times

Korndal 2 years, 1 month ago

DHCP. This is the most used function for ISE to learn about endpoints. Since it can learn about them even if the endpoints are not in a 802.1x enabled port. NMAP is a manually/triggered. Its teoretic that some clients use static IP. Most devices use dhcp

upvoted 2 times

RemiK 2 years, 2 months ago

More relevant about OUI stil "probe DHCP". Answer C.

upvoted 2 times

Rododendron2 2 years, 2 months ago

A and C will work, C for dynamic only. I just like it more. NMAP looks to me as and absolute nonsense , would work only scanning on same subnet

upvoted 2 times

c66bc39 2 years, 2 months ago

SNMP https://community.cisco.com/t5/tkb/articleprintpage/tkb-id/4561-docs-security/article-id/6096 Procedure 11

upvoted 1 times

044f2fc 2 years, 4 months ago

Why not D? Check profiling probe using net flow v9 ... also dhcp on security perspective uses ip to mac binding doesn't mean it is used as a probe to get mac details..And check Nmap probe to access mac ...it is done on manual scanhttps://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/Workflow/b_endpoint_profiling_2_4.html#reference_FD15BD65A25A4390B2A865450F938ADF

upvoted 1 times

044f2fc 2 years, 4 months ago

Selected Answer: D

Why not D? Check profiling probe using net flow v9 ... also dhcp on security perspective uses ip to mac binding doesn't mean it is used as a probe to get mac details..

upvoted 1 times

squirrelzzz 2 years, 5 months ago

OUI is part of MAC Address

upvoted 1 times

nekkrokvlt 2 years, 10 months ago

I vote for C As well, NMAP is layer 3.

upvoted 1 times

GoldFree 2 years, 11 months ago

Probe SNMP: Key profiling attributes: · MAC Address/OUI - CDP/LLDP - ARP tables Common Endpoint Profiling Use Cases See RADIUS probe for MAC info. Valuable for any vendor that uses CDP/LLDP. For example, Cisco IP phones, cameras, access points, appliances. Polling of device ARP tables populates ISE MAC-to-IP bindings. https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456 CTRL + F to the setion: "Probe Selection Best Practices"

upvoted 2 times

F0rtyx40 3 years, 1 month ago

NMAP scans for open ports and OS detection, how do you get MAC address in NMAP scans over L3? you can configure SNMP probes to start profiling and populating endpoints before enforcing MAB/802.1X IN ISE. I have done this a few times.

upvoted 2 times

Question #244 *Topic 1*

What is the benefit of installing Cisco AMP for Endpoints on a network?

A. It enables behavioral analysis to be used for the endpoints

B. It provides flow-based visibility for the endpoints' network connections.

C. It protects endpoint systems through application control and real-time scanning.

D. It provides operating system patches on the endpoints for security.

Suggested Answer: *C*
Official Answer: C

Community vote distribution
A (50%) C (36%) B (14%)

jaciro11 Highly Voted 4 years, 8 months ago
I use AMP for many years Like partner. But now I have this questions Obviously its A Or C. A Behavioral analysis its an amazing plus which this EDR doing. C Real time and App block : This is something which all the antivirus or EPP use. Im confused here because AMP can do the both but which answer is the more accurate answer. How I hate this CISCO EXAMS, never have a good sense to make a real question and not a stupid tricky question like this... let me know guys what you think about itim convinced they ask to choose one but have 2 correct answers and if you choose either they will mark it as correct.As they are asking about AMP BENEFITS, it will be probably A - behavioral analysis - because it is greater benefit than real-time scanning, which can be also done by standard AV solution. "Behavioral protection: Secure Endpoint's enhanced behavioral analysis continually monitors all user and endpoint activity to protect against malicious behavior in real-time by matching a stream of activity records against a set of attack activity patterns which are dynamically updated as threats evolve. For example, this enables granular control and protection from the malicious use of living-off-the-land tools." https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.htmlMoreover, traditional AV scanning in AMP - TETRA engine - is disabled by default (but there is still real-time protection "through application control and real-time scanning", so this is just for info): "There are three detection and protection "engines" in AMP for Endpoints: • TETRA: A full client-side antivirus solution. Do not enable the use of TETRA if there is an existing antivirus product in place. The default AMP setting is to leave TETRA disabled, as it changes the nature of the AMP connector from being a very lightweight agent to being a "thicker" software client that consumes more disk space for signature storage + BW for updates. • Spero: A machine learning–based t
upvoted 20 times

jaciro11 Highly Voted 4 years, 8 months ago
I use AMP for many years Like partner. But now I have this questions Obviously its A Or C. A Behavioral analysis its an amazing plus which this EDR doing. C Real time and App block : This is something which all the antivirus or EPP use.

Im confused here because AMP can do the both but which answer is the more accurate answer.

How I hate this CISCO EXAMS, never have a good sense to make a real question and not a stupid tricky question like this... let me know guys what you think about it
upvoted 19 times

bob511 4 years, 5 months ago
im convinced they ask to choose one but have 2 correct answers and if you choose either they will mark it as correct.
upvoted 2 times

NikoNiko 4 years, 1 month ago
As they are asking about AMP BENEFITS, it will be probably A - behavioral analysis - because it is greater benefit than real-time scanning, which can be also done by standard AV solution.

"Behavioral protection: Secure Endpoint's enhanced behavioral analysis continually monitors all user and endpoint activity to protect against malicious behavior in real-time by matching a stream of activity records against a set of attack activity patterns which are dynamically updated as threats evolve. For example, this enables granular control and protection from the malicious use of living-off-the-land tools."

https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html
upvoted 4 times

NikoNiko 4 years, 1 month ago

As they are asking about AMP BENEFITS, it will be probably A - behavioral analysis - because it is greater benefit than real-time scanning, which can be also done by standard AV solution. "Behavioral protection: Secure Endpoint's enhanced behavioral analysis continually monitors all user and endpoint activity to protect against malicious behavior in real-time by matching a stream of activity records against a set of attack activity patterns which are dynamically updated as threats evolve. For example, this enables granular control and protection from the malicious use of living-off-the-land tools." https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.htmlMoreover, traditional AV scanning in AMP - TETRA engine - is disabled by default (but there is still real-time protection "through application control and real-time scanning", so this is just for info): "There are three detection and protection "engines" in AMP for Endpoints: • TETRA: A full client-side antivirus solution. Do not enable the use of TETRA if there is an existing antivirus product in place. The default AMP setting is to leave TETRA disabled, as it changes the nature of the AMP connector from being a very lightweight agent to being a "thicker" software client that consumes more disk space for signature storage + BW for updates. • Spero: A machine learning–based technology that proactively identifies threats that were previously unknown. It uses active heuristics to gather execution attributes, and because the underlying algorithms come up with generic models, they can identify malicious software based on its general appearance rather than basing identity on specific patterns or signatures. • Ethos: A "fuzzy fingerprinting" engine that uses static or passive heuristics." Source: CCNP / CCIE SCOR official cert guide by Omar Santos

upvoted 4 times

NikoNiko 4 years, 1 month ago

Moreover, traditional AV scanning in AMP - TETRA engine - is disabled by default (but there is still real-time protection "through application control and real-time scanning", so this is just for info): "There are three detection and protection "engines" in AMP for Endpoints: • TETRA: A full client-side antivirus solution. Do not enable the use of TETRA if there is an existing antivirus product in place. The default AMP setting is to leave TETRA disabled, as it changes the nature of the AMP connector from being a very lightweight agent to being a "thicker" software client that consumes more disk space for signature storage + BW for updates. • Spero: A machine learning–based technology that proactively identifies threats that were previously unknown. It uses active heuristics to gather execution attributes, and because the underlying algorithms come up with generic models, they can identify malicious software based on its general appearance rather than basing identity on specific patterns or signatures. • Ethos: A "fuzzy fingerprinting" engine that uses static or passive heuristics." Source: CCNP / CCIE SCOR official cert guide by Omar Santos

upvoted 2 times

SomKeat Most Recent 2 months, 3 weeks ago

Answer is 100% C

upvoted 1 times

kloug 1 year, 9 months ago

Answer c

upvoted 1 times

madboy2 1 year, 4 months ago

Cisco AMP (Advanced Malware Protection) for Endpoints is a security solution that uses behavioral analysis to detect and prevent threats on endpoints. It continuously monitors and records endpoint activities, leveraging machine learning, threat intelligence, and retrospective security to identify malicious behaviors and respond to threats in real time.

upvoted 1 times

kloug 1 year, 9 months ago

Answer cAnswer b

upvoted 1 times

kloug 1 year, 9 months ago

Answer b

upvoted 1 times

Premium_Pils 2 years ago

"Behavior-based malware detection, which builds a full context around every process execution path in real time"
https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

upvoted 1 times

4pelos 2 years, 5 months ago

Correct answer C Checked with securitytut

upvoted 1 times

gc999 3 years, 3 months ago

For A and C, I will choose C. For A, it said "It enables behavioral analysis to be used for the endpoints", it didn't tell the benefit, how to use and what does it use for? Does it mean the endpoint use it? For C, it can help for the protection.

upvoted 2 times

loser4fun 3 years, 5 months ago

The correct answer is C: It protects endpoint systems through application control and real-time scanning. Cisco AMP for Endpoints is an advanced endpoint security solution that provides protection for endpoints such as desktops, laptops, servers, and mobile devices. It provides multiple layers of protection against various types of cyber threats, such as malware, viruses, spyware, and ransomware. Option A, behavioral analysis, is a feature of Cisco AMP for Endpoints that enables the detection of malicious activity on an endpoint by analyzing its behavior. It is a part of the real-time scanning and advanced threat intelligence capabilities of the solution. Option B, flow-based visibility, is a feature of Cisco Firepower that provides visibility into the network connections of endpoints, but it is not a feature of Cisco AMP for Endpoints. Option D, operating system patches, is not a feature of Cisco AMP for Endpoints. However, it is important to keep endpoint systems updated with the latest security patches to protect against vulnerabilities.

upvoted 2 times

achille5 3 years, 6 months ago

Both are A C are important benefits, however to protects endpoint systems through application control and real-time scanning," as it is the primary benefit of using Cisco AMP for Endpoints.

upvoted 1 times

psuoh 3 years, 6 months ago

i think the best Cisco answer is A. IT makes there app standout from other AV apps.

upvoted 1 times

Emlia1 3 years, 8 months ago

it should be C

upvoted 1 times

minous123 4 years ago

Question is tricky.. but it is asking about BENEFIT of installing AMP for endpoints on a NETWORK. Based on that I choose B because it can monitor network connection and block malicious. A and C seems also valid but B seems to be the best option based on question. Explanation: You can enable Device Flow Correlation. It allows you to monitor network activity and determine which action the connector should take when connections to malicious hosts are detected. https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf

upvoted 2 times

semi1750 4 years, 3 months ago

Vote for A AMP for Endpoints Malicious Activity Protection (MAP) engine included in the AMP Connector Version 6.1.5 for Windows defends your endpoints by monitoring the system and identifying processes that exhibit malicious activities when they execute and stops them from running. Because the MAP engine detects threats by observing the behavior of the process at run time, it can generically determine if a system is under attack by a new variant of ransomware or malware that may have eluded other security products and detection technology, such as legacy signature-based malware detection. The first release of the MAP engine targets identification, blocking, and quarantine of ransomware attacks on the endpoint.

upvoted 1 times

dr4gn00t 4 years, 6 months ago

C is not wrong but it is something that every AV does. A is better answer for AMP.

upvoted 1 times

Jetnor 4 years, 7 months ago

Voying for C https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html check section: Benefits In the rapidly evolving world of malware, threats are becoming harder and harder to detect. The most advanced 1% of these threats, those that will eventually enter and wreak havoc in your network, could potentially go undetected. However, Secure Endpoint provides comprehensive protection against that 1%. This security software prevents breaches, blocks malware at the point of entry, and continuously monitors and analyzes file and process activity to rapidly detect, contain, and remediate threats that can evade front-line defenses.

upvoted 2 times

MoII 4 years, 8 months ago

Voting for C here

upvoted 2 times

jaciro11 4 years, 8 months ago

The answer is A https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html Behavioral protection: Secure Endpoint's enhanced behavioral analysis continually monitors all user and endpoint activity to protect against malicious behavior in real-time by matching a stream of activity records against a set of attack activity patterns which are dynamically updated as threats evolve. For example, this enables granular control and protection from the malicious use of living-off-the-land tools.

upvoted 4 times

Question #245 *Topic 1*

Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?

A. because defense-in-depth stops at the network

B. because human error or insider threats will still exist

C. to prevent theft of the endpoints

D. to expose the endpoint to more threats

Suggested Answer: *B*
Official Answer: B

Currently there are no comments in this discussion, be the first to comment!

Question #246 *Topic 1*

What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?

A. SNMP probe

B. CoA

C. external identity source

D. posture assessment

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

entitty Highly Voted 3 years, 8 months ago
b - COA See -https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html - search for Endpoint deleted: When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network
upvoted 20 times

Minipaf Highly Voted 3 years, 9 months ago
Answer is B CoA.
upvoted 10 times

sull3y Most Recent 2 years ago
B. CoA (Change of Authorization) Cisco ISE (Identity Services Engine) is a policy control platform that provides secure access control and BYOD (Bring Your Own Device) support. To enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group, a Change of Authorization (CoA) must be configured in ISE. CoA allows for dynamic changes to the authorization level of an endpoint, and can be used to trigger reauthentication when an endpoint is deleted from an identity group. This helps to ensure that the endpoint remains compliant with security policies and that any potential security risks are addressed in real-time.
upvoted 2 times

nomanlands 2 years, 7 months ago
B, deleting causes a CoA to occur
upvoted 1 times

MoII 3 years, 2 months ago
Would go with Answer: A here
upvoted 1 times

MoII 3 years, 2 months ago
Would go with Answer: A herehttps://community.cisco.com/t5/network-access-control/do-i-really-need-the-snmp-query-probe/td-p/2915326
upvoted 1 times

MoII 3 years, 2 months ago
https://community.cisco.com/t5/network-access-control/do-i-really-need-the-snmp-query-probe/td-p/2915326
upvoted 1 times

Steve122 3 years, 3 months ago
C

The profiling service issues the change of authorization in the following cases: - Endpoint deleted: When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network.
upvoted 1 times

Steve122 3 years, 3 months ago
C The profiling service issues the change of authorization in the following cases: - Endpoint deleted: When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network.not C, B
upvoted 1 times

Steve122 3 years, 3 months ago

not C, B

upvoted 1 times

MoII 3 years, 3 months ago

Answer: A makes sense https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html Cisco ISE does not issue a CoA for the following reasons: An Endpoint disconnected from the network

upvoted 2 times

MoII 3 years, 3 months ago

Answer: A makes sense https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html Cisco ISE does not issue a CoA for the following reasons: An Endpoint disconnected from the networkits not disconnecting. its being deleted from the policy. 2 different things. Its a definite B.

upvoted 2 times

killbots 2 years, 10 months ago

its not disconnecting. its being deleted from the policy. 2 different things. Its a definite B.

upvoted 1 times

klu16 3 years, 6 months ago

Yeah, B...

upvoted 4 times

acc2326 3 years, 9 months ago

CoA for sure

upvoted 5 times

kakakayayaya 3 years, 9 months ago

SNMP probe - no use for CoA

upvoted 4 times

Question #247 *Topic 1*

In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?

A. when there is a need to have more advanced detection capabilities

B. when there is no firewall on the network

C. when there is a need for traditional anti-malware detection

D. when there is no need to have the solution centrally managed

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

jccastiyo Highly Voted 2 years, 9 months ago

It's so obvious if you know the difference between EDR and EPP.

upvoted 10 times

kakakayayaya Highly Voted 3 years, 3 months ago

Traditional EPP Advanced EDR So A fits better

upvoted 6 times

sis_net_sec Most Recent 2 years ago

Selected Answer:A What is the difference between an endpoint protection platform (EPP) and endpoint detection and response (EDR)? EDR focuses primarily on advanced threats that are designed to evade front-line defenses and have successfully entered into the environment. An EPP focuses solely on prevention at the perimeter. It is difficult, if not impossible, for an EPP to block 100 percent of threats. So in the ideal case, an endpoint security solution deploys both EPP and EDR capabilities. https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection- response- edr.html#:~:text=What%20is%20the%20difference%20between,on%20prevention%20at%20the %20perimeter.

upvoted 2 times

killbots 2 years, 3 months ago

Its A. EDR provide advanced capabilities as EPP provide your traditional protections.

upvoted 3 times

MoII 2 years, 9 months ago

Answer should be A

upvoted 5 times

Steve122 2 years, 9 months ago

A EDR focuses primarily on advanced threats that are designed to evade front-line defenses and have successfully entered into the environment. An EPP focuses solely on prevention at the perimeter.

upvoted 5 times

itisfakemaillol 3 years, 1 month ago

A. when there is a need to have more advanced detection capabilities

upvoted 6 times

trickbot 3 years, 3 months ago

Endpoint Detection and Response (EDR)is the next gen replacement of traditional anti-malware which was primarily signature based. EDR is centrally managed because it is practically run by crowd sourced AI. Having a firewall on the network wouldnt influence a decision between the two. Signature based Anti-malware is going bye-bye.

upvoted 6 times

Minipaf 3 years, 3 months ago

Correct answer is A: when there is a need to have more advanced detection capabilities. https://www.esecurityplanet.com/endpoint/antivirus-vs-epp-vs-edr/#:~:text=Endpoint%20detection%20and%20response%20(EDR)%20represents%20the%20newest%20and%20most,advanced%20layer%20of%20endpoint%20protection.&text=Whereas%20EPP%20is%20a%20first,they%20can%20cause%20significant%20damage.

upvoted 5 times

Question #248 *Topic 1*

Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two.)

A. RADIUS

B. TACACS+

C. DHCP

D. sFlow

E. SMTP

Suggested Answer: *A, C*

Reference: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

Community vote distribution

AC (100%)

loser4fun Most Recent 1 year, 11 months ago

The correct answers are A. RADIUS and C. DHCP.

Cisco Identity Services Engine (ISE) uses different probes to gather information about network endpoints for device profiling and authentication. Two of the probes used to gather attributes of connected endpoints are:

A. RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides centralized authentication, authorization, and accounting (AAA) management for devices that connect and use a network service. ISE can use RADIUS probes to gather endpoint attributes such as device type, operating system, and installed applications.

C. DHCP: Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables devices to automatically obtain an IP address and network configuration settings from a DHCP server. ISE can use DHCP probes to gather endpoint attributes such as MAC address, hostname, and IP address.

upvoted 2 times

killbots 2 years, 10 months ago

Selected Answer: AC

The selected answer is correct.

upvoted 1 times

Question #249 *Topic 1*

What are two reasons for implementing a multifactor authentication solution such as Cisco Duo Security provide to an organization? (Choose two.)

A. single sign-on access to on-premises and cloud applications

B. identification and correction of application vulnerabilities before allowing access to resources

C. secure access to on-premises and cloud applications

D. integration with 802.1x security using native Microsoft Windows supplicant

E. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes, and push notifications

Suggested Answer: *C, E*
Official Answer: CE

aalnman Highly Voted 4 years, 10 months ago
C & E - I agree with. BUT this is also on DUOs page: Simple, Secure Single Sign-On Single sign-on (SSO) from Duo provides users with an easy and consistent login experience for any and every application, whether it's on-premises or cloud-based. Cloud-based and hosted by Duo, it's easy to set up and manage. https://duo.com/product/single-sign-on-sso
upvoted 11 times

west33637 Highly Voted 3 years, 7 months ago
Selected Answer: AC
A,C are the correct answers. The question is what are the reasons? In other words, why would you deploy DUO? for single sign on access to apps and for secure access to apps, whether onprem or cloud. I have never heard a CISO say we want to buy a DUO solution because it has many different authentication methods.
upvoted 8 times

kloug Most Recent 1 year, 9 months ago
Answer c,e
upvoted 1 times

Premium_Pils 2 years ago
Selected Answer: AC
AC based on these articles: https://www.cisco.com/c/en/us/products/security/duo/what-is-duo.html
https://www.cisco.com/c/en/us/products/security/what-is-two-factor-authentication.html#~related-solutions
upvoted 1 times

XvidalX 2 years, 5 months ago
Selected Answer: CE
DUO support SSO, but not provide, SAML or AD provide SSO. A is incorrect
upvoted 2 times

mikexian 2 years, 7 months ago
Selected Answer: AC
A C focus on why we should choose Multifactor authentication
upvoted 1 times

Przemol 2 years, 11 months ago
I go for C and E

Cisco Duo as MFA solution provides Duo Push, Call me and passcode:
https://guide.duo.com/prompt#:~:text=Authenticate%20via%20phone%20callback.&text=Log%20in%20using%20a%20passcode,%2Dtouch%20hardware%2Dbacked%20authentication.

Also provides secure access to on-premises and cloud applications.

I am not going for A, because SSO is one of the features Cisco Duo provides besides MFA. And in this question they ask for reasons for implementing a multifactor authentication solution such as Cisco Duo.

upvoted 2 times

gc999 3 years, 4 months ago

I don't think "C" is the reason.

upvoted 1 times

gc999 3 years, 4 months ago

Sorry for the typo. I wanted to say "E" is not a reason.

upvoted 1 times

stalkr3 3 years, 4 months ago

Thee is a Cisco reason. This is also a marketing question

upvoted 1 times

Toni_Su91 3 years, 5 months ago

https://duo.com/product/multi-factor-authentication-mfa/authentication-methods

I don't see voice call-backs in the guide. Is this the clue? :)

upvoted 1 times

achille5 3 years, 5 months ago

Why i can't access this exam? I paid for 1 yr contributor access.

upvoted 2 times

jerac58653 3 years, 5 months ago

Selected Answer: CE

C+E Read Carefully, they are asking about the reason to implement MFA (DUO is just an example), not to implement DUO specifically. SSO is another separate feature that is not asked about here.

upvoted 5 times

zimmer54 3 years, 6 months ago

CE https://duo.com/docs/sso

upvoted 1 times

Emlia1 3 years, 8 months ago

Selected Answer: AE

finally I prefer A, E

upvoted 1 times

Emlia1 3 years, 8 months ago

AE or CE

upvoted 1 times

4000000 3 years, 9 months ago

I think, A, c and e seems to be all correct combinations..... Just to be smart enough to have the choices 😂😁

upvoted 1 times

sis_net_sec 3 years, 10 months ago

Selected Answer: AE

Trust Every User With Single Sign-On and 2FA Verify the identity of your users with two-factor authentication and give them easy access to work applications with single sign- on. Customized policies and controls on a per-application basis will secure your organization from risky users and devices.

upvoted 1 times

Question #250 *Topic 1*

What are the two most commonly used authentication factors in multifactor authentication? (Choose two.)

A. biometric factor

B. time factor

C. confidentiality factor

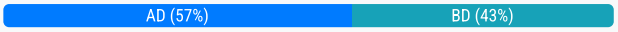
D. knowledge factor

E. encryption factor

Suggested Answer: *A, D*

Official Answer: AD

Community vote distribution



NikoNiko Highly Voted 4 years, 1 month ago

"Authentication credentials are called factors. There are three categories of factors:

• Knowledge (something the user knows) --> authentication by knowledge would be a user providing a password, a personal identification number (PIN) code, or answering security questions.

• Possession (something a user has) --> authentication by ownership or possession include the following: a one-time passcode, memory card, smartcard, and out-of-band communication. The most common of the four is the one-time passcode sent to a device in the user's possession.

• Inherence (something the user is)" --> authentication by characteristic authenticates the user based on some physical or behavioral characteristic, sometimes referred to as a biometric attribute. The most used physical or physiological characteristics are as follows: • Fingerprints • Face recognition • Retina and iris • Palm and hand geometry • Blood and vascular information • Voice recognition

CCNP / CCIE SCOR official cert guide by Omar Santos

upvoted 10 times

RemiK Most Recent 2 years, 2 months ago

Selected Answer: AD

agree with A & D

upvoted 1 times

SegaMasterSystemAdmin 3 years, 2 months ago

Selected Answer: AD

A and D are correct. B is not correct, time is not a factor in MFA

upvoted 1 times

bobie 3 years, 3 months ago

Selected Answer: AD

I'll go for biometric and knowledge factor : Something you know - (Knowledge - password) Something you have - (No choices) Something you are - (Biometric - fingerprint scanning or facial recognition or voice biometry)

upvoted 1 times

stalkr3 3 years, 4 months ago

people please stop voting for answer A - how many times have you used 2FA that relies on biometric data?

upvoted 1 times

Jessie45785 3 years, 3 months ago

Daily, and not only biometric but live GPS position as well - time based tokens are so outdated

upvoted 1 times

SegaMasterSystemAdmin 3 years, 2 months ago

Go hit the books kiddo

upvoted 2 times

nep1019 3 years ago

Every. Single. Day.

upvoted 2 times

Jessie45785 3 years, 4 months ago

Selected Answer: AD

B- is not a factor - we can have time based hashed function but it is not a factor - in this case it would be possession factor which is not listed

upvoted 1 times

stalkr3 3 years, 4 months ago

it IS a factor, hence the inherent security of using OTPs that expire after a very short time. And it is used very frequently, so B should be correct

upvoted 2 times

Emlia1 3 years, 8 months ago

Selected Answer: BD

BD - should be the correct answer

upvoted 1 times

Jessie45785 3 years, 4 months ago

B- is not a factor - you can have time based hashed function but it is not a factor - in this case it would be possession factor listed not time

upvoted 1 times

NikoNiko 4 years, 1 month ago

Currently: "Duo Push is our most commonly-used second factor of authentication, thanks to its simplicity and reliability. Users just download the Duo Mobile app and are automatically prompted to confirm each login attempt " --> Questio: Push is knowledge-based or time-based or both? - I think both. https://duo.com/product/multi-factor-authentication-mfa/authentication-methods/tokens-and-passcodes

2019 DUO: "Passcodes. Passcodes are the most common form of 2FA, and usually consist of a short string of numbers sent to a smartphone. Passcodes definitely count as 2FA. Since they rely on phone lines, however — which can be compromised — they represent the least secure method. Passcodes aren't a real hit with users, either: each code must be manually entered, which can be a nuisance"

https://duo.com/blog/two-factor-authentication-the-basics

upvoted 1 times

NikoNiko 4 years, 1 month ago

UPDATE: Push / one-time passcode is POSSESSION BASED (something a user has), but also time-based according to Cisco DUO:

" Time-Based One-Time Passcodes

Some websites and online services let users protect their accounts with a mobile-generated passcode that must be manually entered and only works for a certain amount of time — typically 30-60 seconds. Duo Mobile can generate these time-based one-time passcodes (TOTP) for all third-party sites, letting users keep all of their accounts in one app."

https://duo.com/product/multi-factor-authentication-mfa/authentication-methods/tokens-and-passcodes

upvoted 1 times

nomanlands 4 years, 1 month ago

Selected Answer: BD

D is a given.

This page mentions Time-based is currently widely used while biometric is still up and coming.
https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html#~methods

upvoted 1 times

Thusi26 4 years, 2 months ago

A, B and D all are good according to Cisco.

From Cisco Site:

Knowledge Knowledge--usually a password--is the most commonly used tool in MFA solutions. However, despite their simplicity, passwords have become a security problem and slow down productivity.

Inherent This category includes biometrics like fingerprint, face, and retina scans.

And.....

Location-based and time-based Authentication systems can use GPS coordinates, network parameters, and metadata for the network in use, and device recognition for MFA. Adaptive authentication combines these data points with historical or contextual user data.

Cisco needs to get their stuff together...

upvoted 1 times

pohqinan 4 years, 4 months ago

Reference: https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html The two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint, face, and retina scans. Biometrics is used commonly in mobile devices).

A and D is correct

upvoted 1 times

Sun2sun 4 years, 6 months ago

Selected Answer: BD

Its B and D. time factor , knowledge factor

upvoted 1 times

lurker8000 4 years, 7 months ago

I'd go with AD here, here's a reference where "Biometric Factor" is mentioned on a cisco documentation: https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html#~how-mfa-works.

D is a no brainer in my mind, that's the most common, although not the most secure...

upvoted 4 times

coentror 4 years, 9 months ago

There not much here. A and D are the correct one. Do no complicate what is easy.

:)

upvoted 1 times

coentror 4 years, 8 months ago

Sorry B and D are correct.

upvoted 1 times

MoII 4 years, 9 months ago

Agree with B and D

upvoted 1 times

jaciro11 4 years, 9 months ago

Ey people stop discuss it Its B and D. https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html

upvoted 2 times

abdulmalik_mail 4 years, 7 months ago

AD, on that URL writted, inherent... This category includes biometrics like fingerprint, face, and retina scans.

upvoted 1 times

eazy99 4 years, 10 months ago

Something you are. Something you know. Correct, A and D.

upvoted 3 times

NullNull88 4 years, 8 months ago

Uh em, .."something you "have" something you "know".

upvoted 2 times

Question #251 *Topic 1*

An MDM provides which two advantages to an organization with regards to device management? (Choose two.)

A. asset inventory management

B. allowed application management

C. AD group policy management

D. network device management

E. critical device management

Suggested Answer: *A, B*

Official Answer: AB

Community vote distribution

AB (100%)

bigdadzzz Highly Voted 4 years, 1 month ago

I'm going to chime in with A&B as correct answers. I've administered Mobile Device Management systems for several years, and never managed a network device or critical device (ie server) with them. While I suppose it's technically POSSIBLE, it's just not the purpose of the solution. MDMs will use the term groups/policies/Group Policy, but it's never going to allow you to manage ADDS GPOs. What I HAVE done though, is use it to remotely manage a fleet of mobile devices and add/remove/monitor those assets, and control the applications on the device.

upvoted 26 times

j0ej0e Highly Voted 4 years, 2 months ago

A an B are correct.

upvoted 12 times

CyberGhost666 Most Recent 1 year, 1 month ago

A Mobile Device Management (MDM) solution provides centralized control over mobile devices (phones, tablets, laptops) within an organization. Two of its main benefits include: • A. Asset inventory management: MDM tracks and maintains a detailed inventory of all enrolled devices, including hardware details, OS versions, and ownership (corporate vs. personal). • B. Allowed application management: MDM allows organizations to whitelist or blacklist apps, enforce app installation/removal, and control access to corporate resources based on installed applications.

upvoted 1 times

sull3y 2 years ago

A. Asset inventory management: A Mobile Device Management (MDM) solution provides an organization with the ability to maintain an inventory of all the mobile devices that are being used within the organization. This includes tracking information such as device type, operating system, serial number, and other relevant details. This information helps organizations to manage their mobile device fleet effectively, keep track of devices and ensure they are properly configured and secure. B. Allowed application management: An MDM solution also enables organizations to control and manage the applications that are installed on the mobile devices being used within the organization. This includes the ability to allow or disallow specific applications, manage updates and upgrades, and enforce security policies around application usage. This helps organizations to maintain a secure and controlled environment for mobile devices and ensure that only approved applications are being used within the network.

upvoted 6 times

MoII 3 years, 2 months ago

Agree with A and B

upvoted 1 times

thegreek1 4 years, 4 months ago

I would not call a mobile phone to be a 'critical device management' https://en.wikipedia.org/wiki/Mobile_device_management Some of the core functions of MDM include: Ensuring that diverse user equipment is configured to a consistent standard / supported set of applications, functions, or corporate policies Updating equipment, applications, functions, or policies in a scalable manner Ensuring that users use applications in a consistent and supportable manner Ensuring that equipment performs consistently Monitoring and tracking equipment (e.g. location, status, ownership, activity) Being able to efficiently diagnose and troubleshoot equipment remotelyCompletely agree with A/B, however, have you dealt with a sales bod / A/B/C level exec whos mobile isn't working - Their world has come to an end.....

upvoted 3 times

thegreek1 4 years, 4 months ago

I would not call a mobile phone to be a 'critical device management' https://en.wikipedia.org/wiki/Mobile_device_management

Some of the core functions of MDM include:

Ensuring that diverse user equipment is configured to a consistent standard / supported set of applications, functions, or corporate policies Updating equipment, applications, functions, or policies in a scalable manner Ensuring that users use applications in a consistent and supportable manner Ensuring that equipment performs consistently Monitoring and tracking equipment (e.g. location, status, ownership, activity) Being able to efficiently diagnose and troubleshoot equipment remotely

upvoted 3 times

Smileebloke 2 years, 10 months ago

Completely agree with A/B, however, have you dealt with a sales bod / A/B/C level exec whos mobile isn't working - Their world has come to an end.....

upvoted 1 times

FilipNel 4 years, 5 months ago

The answer is B, E

upvoted 2 times

naddaf 4 years, 7 months ago

i think the correct Answer is B & E

upvoted 2 times

Question #252 *Topic 1*

What is the purpose of the My Devices Portal in a Cisco ISE environment?

A. to register new laptops and mobile devices

B. to manage and deploy antivirus definitions and patches on systems owned by the end user

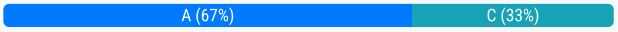
C. to provision userless and agentless systems

D. to request a newly provisioned mobile device

Suggested Answer: *A*

Official Answer: A

Community vote distribution



karmaomar Highly Voted 4 years, 2 months ago

A is a correct answer My Devices Portal Q. Why do I need to use the My Devices Portal? A. Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network. When you use a laptop computer, mobile phone, or tablet to access the Internet, you typically use a web browser on the device itself.

upvoted 19 times

sull3y 2 years, 6 months ago

A. to register new laptops and mobile devices. The My Devices Portal in a Cisco ISE environment is a self-service portal that allows end users to register and manage their personal devices, such as laptops and mobile devices, within the ISE network. This portal enables users to enroll their devices, update device information, and manage device settings, such as certificates and Wi-Fi profiles. This can help streamline the process of onboarding new devices and improve the overall security posture of the network by ensuring that all devices are properly registered and managed.

upvoted 3 times

Emlia1 2 years, 8 months ago

Employees can use MDP to register and manage their personal devices.

upvoted 2 times

Webster21 2 years, 9 months ago

Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network. When you use a laptop computer, mobile phone, or tablet to access the Internet, you typically use a web browser on the device itself. The first time you try to do so using your company's network, the system will automatically guide you through registering and installing the required software. You may not need to use the My Devices Portal to register those types of devices. However, once you register them, you can use the My Devices Portal to perform operations such as remove them, mark them as lost, or reinstate devices that were marked as lost, once they are found. Other network devices do not have web browsers on them because they need access to the network only to allow you to perform activities such as listen to music, print documents, and watch videos. If you want to add these types of devices to your company's network, you need to use the My Devices portal.

upvoted 1 times

beeker98106 3 years, 9 months ago

It should be C. The FAQ section explains the use of the portal for radios or other funny devices that don't have users or even browsers https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.htmlKEY WORD is register not provision

upvoted 3 times

beeker98106 3 years, 9 months ago

It should be C.

The FAQ section explains the use of the portal for radios or other funny devices that don't have users or even browsers https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html

upvoted 3 times

PeterHasse Most Recent 2 years, 1 month ago

KEY WORD is register not provision

upvoted 1 times

Darealis 4 years, 2 months ago

Answer is D

upvoted 1 times

Darealis 4 years, 2 months ago

Answer is DSo when I need a new phone, I can go to My Devices Portal and get a new one? :-)I wish so :D Good one! :D

upvoted 1 times

Seawanderer Highly Voted 4 years, 1 month ago

So when I need a new phone, I can go to My Devices Portal and get a new one? :-)

upvoted 8 times

Seawanderer 4 years, 1 month ago

So when I need a new phone, I can go to My Devices Portal and get a new one? :-)I wish so :D Good one! :D

upvoted 8 times

NikoNiko 3 years, 1 month ago

I wish so :D Good one! :D

upvoted 3 times

Question #253 *Topic 1*

Which Cisco platform ensures that machines that connect to organizational networks have the recommended antivirus definitions and patches to help prevent an organizational malware outbreak?

A. Cisco Prime Infrastructure

B. Cisco ESA

C. Cisco WiSM

D. Cisco ISE

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Felice44 Most Recent 1 year, 11 months ago

Posture Assessment with ISE

upvoted 1 times

Question #254 *Topic 1*

In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two.)

A. It integrates with third-party products to provide better visibility throughout the network.

B. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.

C. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.

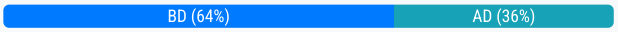
D. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).

E. It allows multiple security products to share information and work together to enhance security posture in the network.

Suggested Answer: *B, D*

Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-with-easy-connect-configuration-guide.pdf

Community vote distribution



Sarbi Highly Voted 4 years, 11 months ago

Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity. Active Directory logins are used to map user information onto network connections, which are then used for authorizing users on the network even when the Identity Services Engine (ISE) is not involved in the authentication process. Consequently, this authorization method only supports devices that authenticate with a Domain Controller. Easy Connect can also be used as a backup authentication method to 802.1X, to ensure that managed assets are classified even when an 802.1X supplicant is not correctly configured. This can dramatically reduce help desk calls

upvoted 13 times

ITVI Most Recent 1 year, 4 months ago

B & D is my choice based on the links folks here have provided, do your research.

upvoted 1 times

madboy2 1 year, 4 months ago

Cisco Easy Connect is a feature in Cisco TrustSec that simplifies network access control by automatically assigning Security Group Tags (SGTs) without requiring 802.1X authentication on switches or endpoints. Why these answers? B. Easy Connect allows for the assignment of Security Group Tags and does not require 802.1X to be configured on the switch or the endpoint. Removes the need for complex 802.1X configurations while still enforcing TrustSec policies. Uses PassiveID (Passive Identity Mapping) to automatically assign SGTs based on Active Directory authentication without requiring endpoint authentication via 802.1X. D. Easy Connect allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID). When a user logs into a domain-joined device, Easy Connect captures login events from Active Directory and assigns an SGT to the endpoint dynamically. This simplifies access control while ensuring TrustSec policies are still enforced.

upvoted 4 times

Demon_Queen_Velverosa 1 year, 10 months ago

BD as i made a comment as 802.1x may not be avalible

upvoted 1 times

Rododendron2 2 years, 3 months ago

switch needs to have dot1x setup, end point does notAfter I again reviewed documentation, BD is right, Easyconnect does not required dot1x on switch and integrates with TrustSec on ISE as Passive IDYes the answer is B and D

upvoted 2 times

Rododendron2 2 years, 3 months ago

Selected Answer: AD

switch needs to have dot1x setup, end point does not

upvoted 2 times

Rododendron2 2 years, 2 months ago

After I again reviewed documentation, BD is right, Easyconnect does not required dot1x on switch and integrates with TrustSec on ISE as Passive IDYes the answer is B and D

upvoted 1 times

Rododendron2 2 years, 2 months ago

After I again reviewed documentation, BD is right, Easyconnect does not required dot1x on switch and integrates with TrustSec on ISE as Passive ID

upvoted 1 times

Demon_Queen_Velverosa 1 year, 10 months ago

Yes the answer is B and D

upvoted 1 times

iluvmicrosoft 2 years, 4 months ago

https://community.cisco.com/t5/security-knowledge-base/ise-easy-connect/ta-p/3638861 MAB or 802.1X (required for ISE to stitch RADIUS session with PassiveID info) You can configure NAD w MAB, so technically 802.1x is not a requirement??

upvoted 2 times

XvidalX 2 years, 5 months ago

A CORRECT - EASYconenct integrate with AD to gaing visibility B- incorrect - SWITCHES NEED 802.1x configuration , Endpoints DOES not C- Does not create dashboards D - its correct - it is the main purpose E - incorrect - it is not about posture needsNo it's for when 802.1x is not available as AD don't need 802.1x as it can be used as an alternate.

upvoted 2 times

XvidalX 2 years, 5 months ago

Selected Answer: AD

A CORRECT - EASYconenct integrate with AD to gaing visibility B- incorrect - SWITCHES NEED 802.1x configuration , Endpoints DOES not C- Does not create dashboards D - its correct - it is the main purpose E - incorrect - it is not about posture needs

upvoted 2 times

Demon_Queen_Velverosa 1 year, 10 months ago

No it's for when 802.1x is not available as AD don't need 802.1x as it can be used as an alternate.

upvoted 1 times

haiderzaid 3 years, 4 months ago

why not B C since PassiveID can be used independently without easy connect feature??im wrong C does not describe the way in which Easy Connect helps control network access so I will go for BD802.1x may not be avalible and can be used as an alternate as it uses Active Directory instead and f 802.1x We don't care about a dashboard Answer BD

upvoted 1 times

haiderzaid 3 years, 4 months ago

why not B C since PassiveID can be used independently without easy connect feature??

upvoted 1 times

haiderzaid 3 years, 4 months ago

im wrong C does not describe the way in which Easy Connect helps control network access so I will go for BD

upvoted 2 times

Demon_Queen_Velverosa 1 year, 10 months ago

802.1x may not be avalible and can be used as an alternate as it uses Active Directory instead and f 802.1x We don't care about a dashboard Answer BD

upvoted 1 times

sull3y 3 years, 6 months ago

B. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint. D. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID). Easy Connect helps control network access by allowing for the assignment of Security Group Tags (SGTs) and mapping managed endpoints that authenticate to AD to Security Groups (PassiveID). This enables organizations to enforce granular access policies based on the endpoint's identity and role, rather than just its IP address or MAC address. The use of SGTs and PassiveID helps simplify the deployment of TrustSec and reduces the complexity of network access control, as it does not require the configuration of 802.1x on the switch or endpoint.

upvoted 4 times

Emlia1 3 years, 7 months ago

I prefer B, D asy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity. Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsecwith-easy- connect-configuration-guide.p

upvoted 1 times

Jamesy 3 years, 11 months ago

D & E in my opinion. Cheers

upvoted 1 times