EXAMTOPICS

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



CERTIFICATION TEST

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

Question #1 *Topic 1*

What files are sent to FortiSandbox for inspection in flow-based inspection mode?

A. All suspicious files that do not have their hash value in the FortiGuard antivirus signature database.

B. All suspicious files that are above the defined oversize limit value in the protocol options.

C. All suspicious files that match patterns defined in the antivirus profile.

D. All suspicious files that are allowed to be submitted to FortiSandbox in the antivirus profile.

Suggested Answer: *C*

TBI Most Recent 5 years, 4 months ago
D is correct, answers allowed to be sent
upvoted 1 times

jm31 5 years, 7 months ago
D is correct!
upvoted 1 times

wassimtrabelsi 5 years, 8 months ago
D is the correct : FGT Security 6.2 Study Guide page 470
upvoted 1 times

sidd081 6 years, 2 months ago
D is the correct answer as per FGT Security 6.0 Study Guide page 438
upvoted 3 times

Levis 6 years, 3 months ago
D is answer
upvoted 2 times

montonearm 6 years, 5 months ago
for me is D
upvoted 4 times

Question #2 *Topic 1*

Which statements about a One-to-One IP pool are true? (Choose two.)

A. It is used for destination NAT.

B. It allows the fixed mapping of an internal address range to an external address range.

C. It does not use port address translation.

D. It allows the configuration of ARP replies.

Suggested Answer: *C, D*

TBI Most Recent 5 years, 4 months ago
C,D no mapping unlike Many to one
upvoted 1 times

wassimtrabelsi 5 years, 8 months ago
C,D is the correct answer : FGT Security 6.2 Study Guide page 155
upvoted 1 times

Vlad_R 5 years, 11 months ago
Guys, just clicked on a New dynamic IP Pool and, One-to-One Has: External Ip address/range and arp reply. So the correct answer is c&d.
upvoted 1 times

Edy_Crank 5 years, 11 months ago
Correct Answer is B & C : In the one-to-one pool type, an internal IP address is mapped with an external address on a first-come, first-served basis. PAT is not required
upvoted 2 times

guybrush06 5 years, 9 months ago
Mappings are NOT fixed. B is NOT correct.

Corrects are C and D
upvoted 1 times

manjikash 6 years ago
Its c and d
upvoted 3 times

KZM 6 years, 1 month ago
Actual answers are B and C I think.
upvoted 2 times

MrRobot2020 6 years, 2 months ago
B and C is correct. The IP pool type one-to one assocates an internal IP with a pool IP on a first come, first served basis. PAT disabled
upvoted 4 times

Addictioneer 6 years, 1 month ago
Correct. The answer is B & C
upvoted 2 times

georgianp 6 years, 1 month ago
Mapping is not FIXED. C and D are correct
upvoted 4 times

Levis 6 years, 2 months ago
C and D, mapping is not fixed.
upvoted 2 times

Fr4nx 6 years, 2 months ago
c & d are correct
upvoted 2 times

jbernard 6 years, 2 months ago

I think answer is B and C One to One NAT is NOT for destination, is for source... Is used to map internal to external addresses like 10.0.1.1 to 190.171.100.21. 10.0.1.2 to 190.171.100.22 and so on Doesn't use port translation, when you select one to one, doesn't appear the port option

upvoted 3 times

lol1000 6 years, 5 months ago

Think it's C,D From https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Objects/Configuring%20IP%20pools.htm

One-to-one Example for CLI config firewall ippool

edit Mail-Server

set comments "So the the correct IP address is resolved on reverse DNS look ups of the mail server."

set type one-to-one

set startip 10.23.56.21

set endip 10.23.56.21

set arp-reply enable

set arp-intf wan1

end

upvoted 3 times

Question #3 *Topic 1*

Which of the following FortiGate configuration tasks will create a route in the policy route table? (Choose two.)

A. Static route created with a Named Address object

B. Static route created with an Internet Services object

C. SD-WAN route created for individual member interfaces

D. SD-WAN rule created to route traffic based on link latency

Suggested Answer: *A, D*

Thisisatest Highly Voted 6 years, 5 months ago
B and D In support of B - "Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table." "Policy routes, and static routes created using ISDB addresses are not added to the routing table; they are added to the policy routing table." In support of D - "Static routes are simple and are often used in small networks. Policy-based routes, however, are more flexible. They can match more than just the destination IP address. For example, if you have two links - a slow one and a fast one - you can route packets from low-priority source IPs to the slow link."
upvoted 9 times

topicx Highly Voted 6 years, 10 months ago
i think should be B&D
upvoted 5 times

Cool_Guy Most Recent 5 years, 7 months ago
B,D is correct. Refer page 15 of Fortigate Infra study guide.
upvoted 1 times

ramiropalm 5 years, 8 months ago
B & D are correct: As such, "ISDB routes" are added to the policy routing table. Similar to ISDB routes, "SD-WAN rules" function as policy routes.
upvoted 3 times

Romulo 5 years, 11 months ago
I think taht it's C&D
upvoted 1 times

calibre 6 years, 1 month ago
B & D seems more accurate
upvoted 1 times

Leon2020 6 years, 2 months ago
Even though you must configure routes using the SD-WAN virtual interface, FortiGate installs individual routes for the member interfaces in the routing table. Information extracted from FortiGate_Infrastructure_6.2_Study_Guide-Online pag 72 Answer C,D
upvoted 1 times

guybrush06 5 years, 8 months ago
This is talking about "policy route table"
upvoted 1 times

Levis 6 years, 3 months ago
C and D.
upvoted 1 times

Washiedread 6 years, 5 months ago
Correct answer is B & D
upvoted 4 times

montonearm 6 years, 5 months ago
also for me is b & d
upvoted 3 times

psat 6 years, 5 months ago
Correct answer. " B. Static route created with an Internet Services object ". I was able to create a route using Internet Service Object and the route showed up under Monitor-->Routing Monitor --> Policy.

upvoted 3 times

Rim007 6 years, 8 months ago

Answer: C & D. I tried both options A & B and it does not create route in policy route table.

upvoted 2 times

jbernard 6 years, 2 months ago

how did you try B and didn't saw the policy route under Monitor - Routing Monitor - Policy???

upvoted 1 times

Question #4 *Topic 1*

A company needs to provide SSL VPN access to two user groups. The company also needs to display different welcome messages on the SSL VPN login screen for both user groups.
What is required in the SSL VPN configuration to meet these requirements?

A. Different SSL VPN realms for each group.

B. Two separate SSL VPNs in different interfaces mapping the same ssl.root.

C. Two firewall policies with different captive portals.

D. Different virtual SSL VPN IP addresses for each group.

Suggested Answer: *A*

Robin999 Most Recent 5 years, 5 months ago
To add flexibility to your SSL-VPN deployment, you may consider configuring SSL-VPN realms. The realms are custom login pages. They are usually for user groups, such as your accounting team and your sales team, but can be for individual users as well. With realms, users and user groups can access different portals based on the URL they enter. - A
upvoted 1 times

Robin999 5 years, 5 months ago
Study Guide 6.0 p. 568
upvoted 1 times

ipmaster 5 years, 9 months ago
Answer is A
upvoted 1 times

Question #5 *Topic 1*

An administrator is investigating a report of users having intermittent issues with browsing the web. The administrator ran diagnostics and received the output shown in the exhibit.
Examine the diagnostic output shown exhibit. Which of the following options is the most likely cause of this issue?



A. NAT port exhaustion

B. High CPU usage

C. High memory usage

D. High session timeout value

Suggested Answer: *C*

naguinix Highly Voted 6 years, 11 months ago
A is correct: https://kb.fortinet.com/kb/documentLink.do?externalID=FD33056
upvoted 13 times

Ronaldvb Most Recent 3 years, 5 months ago
Selected Answer: A
A, see clash value
upvoted 1 times

SebaAr22 5 years, 7 months ago
A is correct
upvoted 1 times

romartinedg 5 years, 11 months ago
A es correcta, pagina 188 Fortigate_Security_6.2
upvoted 2 times

gooz 5 years, 11 months ago
Gracias por la retro
upvoted 1 times

Basuso 6 years, 1 month ago
The value of clash is higher than 0, meaning it's experiencing NAT port exhaustion. Correct answer is A!
upvoted 1 times

chameleon_eh 6 years, 2 months ago
The correct answer is A. FortiGate_Security_6.2_Study_Guide-Online (page 188), it says: "NAT port exhaustion is also highlighted by a rise in the clash counter from the diagnose system session stat command."
upvoted 2 times

Levis 6 years, 3 months ago
A, Nat port exhaustion = clash counter.
upvoted 1 times

NetStef 6 years, 5 months ago

A is correct

upvoted 1 times

Washiedread 6 years, 5 months ago

Correct ANSWER is A

upvoted 1 times

montonearm 6 years, 5 months ago

also for me is A

upvoted 1 times

Question #6 *Topic 1*

An administrator has configured central DNAT and virtual IPs. Which of the following can be selected in the firewall policy Destination field?

A. A VIP group

B. The mapped IP address object of the VIP object

C. A VIP object

D. An IP pool

Suggested Answer: *C*

mohdnjb Highly Voted 6 years, 11 months ago
Correct Answer should be B
upvoted 12 times

mohdnjb Highly Voted 6 years, 11 months ago
https://kb.fortinet.com/kb/documentLink.do?externalID=FD38995
upvoted 7 times

marli Most Recent 3 years, 3 months ago
ANS IS B
upvoted 1 times

Ctnroger 5 years, 8 months ago
It is D. Because central Nat is enable. That's why you can choose a vip address for the destination field. If you disable central NAT it won't work
upvoted 1 times

farmez 5 years, 8 months ago
B is the correct answer. - when central NAT is enabled => put the mapped IP address of the VIP object - when central NAT is disabled => put the VIP object
upvoted 3 times

jbernard 6 years, 2 months ago
B is the one
upvoted 2 times

Levis 6 years, 2 months ago
B is correct
upvoted 2 times

psat 6 years, 5 months ago
Correct answer is " B. The mapped IP address object of the VIP object " , based on the sample Test taken on https://training.fortinet.com
upvoted 4 times

montonearm 6 years, 5 months ago
must be B
upvoted 1 times

Question #7 *Topic 1*

An administrator needs to strengthen the security for SSL VPN access. Which of the following statements are best practices to do so? (Choose three.)

A. Configure split tunneling for content inspection.

B. Configure host restrictions by IP or MAC address.

C. Configure two-factor authentication using security certificates.

D. Configure SSL offloading to a content processor (FortiASIC).

E. Configure a client integrity check (host-check).

Suggested Answer: *C, D, E*

mohdnjb Highly Voted 6 years, 11 months ago
Correct Answers BCE
upvoted 10 times

romartinedg Highly Voted 5 years, 11 months ago
B,C,E correctas, pag. 607, 608, 609 Fortigate_Security_6.2
upvoted 6 times

SebaAr22 Most Recent 5 years, 7 months ago
B - C - E
upvoted 1 times

farmez 5 years, 8 months ago
BCE correct answers checked on FGT > SSL VPN Settings: - Restrict Access -> Limit access to specific hosts - Requie Client Certificate > SSL VPN Portals - Host Check
upvoted 1 times

Levis 6 years, 3 months ago
BCE as per fortinet guide
upvoted 5 times

NetStef 6 years, 5 months ago
Correct answers are B,C,E
upvoted 5 times

montonearm 6 years, 5 months ago
must be BCE
upvoted 5 times

psat 6 years, 5 months ago
D is not the rigth option. what D does is " Hardware acceleration overview " Most FortiGate models have specialized acceleration hardware that can offload resource intensive processing from main processing (CPU) resources. Most FortiGate units include specialized content processors (CPs) that accelerate a wide range of important security processes such as virus scanning, attack detection, encryption and decryption. (Only selected entry-level FortiGate models do not include a CP processor.) Many FortiGate models also contain security processors (SPs) that accelerate processing for specific security features such as IPS and network processors (NPs) that offload processing of high volume network traffic.
upvoted 2 times

Question #8 *Topic 1*

Which statement about FortiGuard services for FortiGate is true?

A. The web filtering database is downloaded locally on FortiGate.

B. Antivirus signatures are downloaded locally on FortiGate.

C. FortiGate downloads IPS updates using UDP port 53 or 8888.

D. FortiAnalyzer can be configured as a local FDN to provide antivirus and IPS updates.

Suggested Answer: *B*

Ctnroger Most Recent 5 years, 8 months ago

B is correct. C it wrong because it use TCP no UDP

upvoted 1 times

sim_cybersecurityspecialist 5 years, 10 months ago

Correct answer is B Page 19 6.2 security guide. You're welcome.

upvoted 3 times

romartinedg 5 years, 11 months ago

B es correcta, C es incorrecta ya que el IPS actualiza Fortiguard a través del puerto TCP 443

upvoted 4 times

HazemBadr 6 years, 1 month ago

I think answer should be C

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ports-and-protocols-54/FortiGuard.htm

upvoted 1 times

calibre 6 years, 1 month ago

IPS uses 443/8890 https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ports-and-protocols-54/FortiGuard.htm so C is wrong

upvoted 3 times

Question #9 *Topic 1*

Which of the following route attributes must be equal for static routes to be eligible for equal cost multipath (ECMP) routing? (Choose two.)

A. Priority

B. Metric

C. Distance

D. Cost

Suggested Answer: *A, C*

sethjam Highly Voted 6 years, 1 month ago

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40730

upvoted 5 times

stressed_ereck Highly Voted 6 years ago

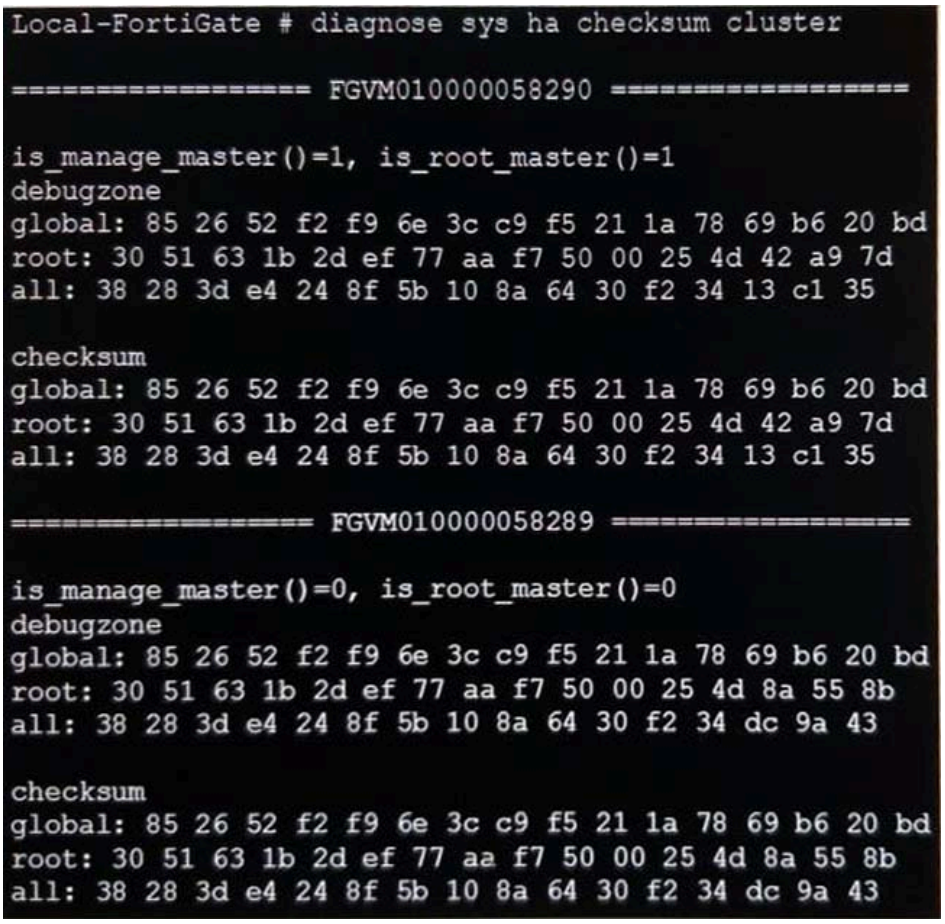
static routes use the Distance and Priority route attributes so A and C.

upvoted 5 times

Question #10 *Topic 1*

View the exhibit.

Based on this output, which statements are correct? (Choose two.)



A. The all VDOM is not synchronized between the primary and secondary FortiGate devices.

B. The root VDOM is not synchronized between the primary and secondary FortiGate devices.

C. The global configuration is synchronized between the primary and secondary FortiGate devices.

D. The FortiGate devices have three VDOMs.

Suggested Answer: *B, C*

farmez Most Recent 5 years, 8 months ago

B and C global checksum is the same for both FGTs root checksum of the 1st FGT is different from the root checksum of the 2nd FGT

upvoted 1 times

henzoo 5 years, 8 months ago

B and C. Fortigate_Infrastructure_6.2_Study_Guide-Online p.324

upvoted 2 times

Ctnroger 5 years, 8 months ago

B is correct, the all vdom dosen't exit and it is not Syn

upvoted 1 times

QuangLNH 5 years, 10 months ago

A is correct too, right ? I see all VDOM not the same?

upvoted 1 times

guybrush06 5 years, 10 months ago

No. All VDOMs are NOT sync' ed because root VDOM isn´t. All is not a VDOM name.

Correct B C

upvoted 2 times

mark05 6 years, 1 month ago

see https://kb.fortinet.com/kb/documentLink.do?externalID=FD40284

upvoted 4 times

Question #11 *Topic 1*

Which statement is true regarding the policy ID number of a firewall policy?

A. Defines the order in which rules are processed.

B. Represents the number of objects used in the firewall policy.

C. Required to modify a firewall policy using the CLI.

D. Changes when firewall policies are reordered.

Suggested Answer: *C*

sethjam Highly Voted 6 years, 1 month ago

https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-firewall-52/Security%20Policies/Policy%20identification.htm

upvoted 5 times

kpnalin Most Recent 5 years, 10 months ago

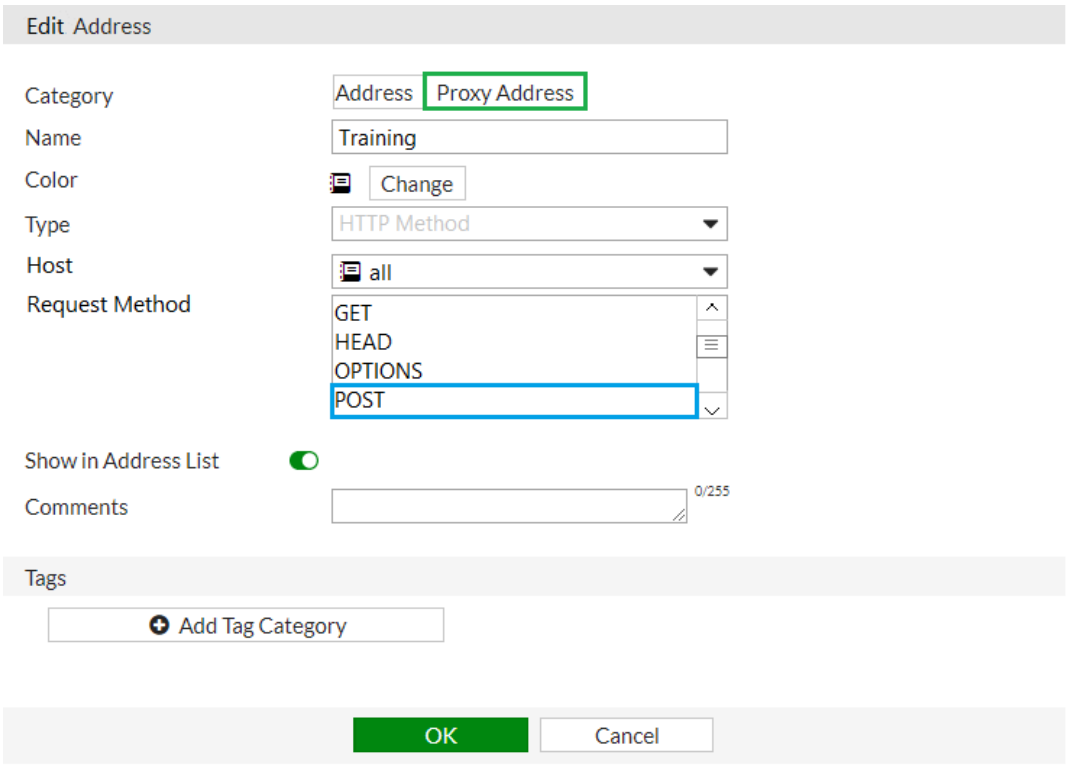
When looking at the policy listing it can appear as if the policies are identified by the sequence number in the far left column. The problem is that this number changes as the position of the policy in the sequence changes. The column that correctly identifies the policy, and the value sticks with the policy is the "ID" column. This column is not shown by default in the listing but can be added to the displayed columns by right clicking on the column heading bar and selecting it from the list of possible columns.

When looking in the configuration file the sequence is based upon the order of the policies as they are in the file just as they are in the list in the GUI. However, if you need to edit the policy in the CLI you must use the ID number.

upvoted 3 times

Question #12 *Topic 1*

An administrator wants to block HTTP uploads. Examine the exhibit, which contains the proxy address created for that purpose.
Where must the proxy address be used?



A. As the source in a firewall policy.

B. As the source in a proxy policy.

C. As the destination in a firewall policy.

D. As the destination in a proxy policy.

Suggested Answer: *B*

kpnalin Highly Voted 5 years, 10 months ago
proxy addresses are used only in proxy policies, in proxy addresses , HTTP methods are used as source addresses in proxy polices.
upvoted 5 times

ramiropalm Most Recent 5 years, 9 months ago
According to the guide in the Proxy Address Types the HTTP Methods are used in Proxy Policies. So, "B" is right.
upvoted 2 times

kunjimon 5 years, 10 months ago
B is right
upvoted 2 times

sim_cybersecurityspecialist 5 years, 10 months ago
any clue which one is the right answer?
upvoted 1 times

sethjam 6 years, 1 month ago
https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-firewall/Configuration%20-%20Web%20Proxy/General%20explicit%20web%20proxy%20configuration%20steps.htm
upvoted 2 times

Question #13 *Topic 1*

Which statement is true regarding SSL VPN timers? (Choose two.)

A. Allow to mitigate DoS attacks from partial HTTP requests.

B. SSL VPN settings do not have customizable timers.

C. Disconnect idle SSL VPN users when a firewall policy authentication timeout occurs.

D. Prevent SSL VPN users from being logged out because of high network latency.

Suggested Answer: *A, D*

romartinedg Highly Voted 5 years, 11 months ago
A y D son correctas, pag. 617 Fortigate_Security_6.2
upvoted 8 times

sim_cybersecurityspecialist Most Recent 5 years, 10 months ago
CORRECT ANSWER!
upvoted 2 times

montonearm Highly Voted 6 years, 5 months ago
sorry correct are A &D
upvoted 5 times

[Removed] 6 years, 2 months ago
A&C https://help.fortinet.com/cli/fos60hlp/60/Content/FortiOS/fortiOS-cli-ref/config/vpn/ssl%20settings.htm
upvoted 2 times

trawa05 6 years, 1 month ago
A - http-request-header-timeout D - idle-timeout
upvoted 5 times

Levis 6 years, 2 months ago
definately A and D
upvoted 5 times

montonearm 6 years, 5 months ago
should be A AND C
upvoted 2 times

Question #14 *Topic 1*

Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

A. The public key of the web server certificate must be installed on the browser.

B. The web-server certificate must be installed on the browser.

C. The CA certificate that signed the web-server certificate must be installed on the browser.

D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Suggested Answer: *C*

montoro Highly Voted 6 years, 1 month ago

C is the correct answer. Otherwise, a browser will display a warning.

upvoted 10 times

trawa05 6 years, 1 month ago

agree - C

upvoted 3 times

kunjimon 5 years, 10 months ago

C is right

upvoted 2 times

ericnesh 5 years, 10 months ago

C Third party CA in this case FortiGate as a CA, its certificate should be installed in the web browser pg344

upvoted 4 times

Levis 6 years, 2 months ago

ACtually A should be answer. browser only has public keys of all CAs, it doesn't store all CA certs.

upvoted 1 times

Ctnroger Most Recent 5 years, 8 months ago

It store the full certificate. Remember it looks revocation list, date, public key...after all it can trust the certificate

upvoted 2 times

Question #15 *Topic 1*

When using SD-WAN, how do you configure the next-hop gateway address for a member interface so that FortiGate can forward Internet traffic?

A. It must be configured in a static route using the sdwan virtual interface.

B. It must be provided in the SD-WAN member interface configuration.

C. It must be configured in a policy-route using the sdwan virtual interface.

D. It must be learned automatically through a dynamic routing protocol.

Suggested Answer: *A*

ni Highly Voted 6 years, 9 months ago
Answer is B
upvoted 10 times

Levis Highly Voted 6 years, 2 months ago
BbBBBBBBBBBBBBBBBBBB
upvoted 7 times

Deens Most Recent 5 years, 7 months ago
B is correct- Check SD-WAN Member interface configuration. there you have gateway configuration option.
upvoted 2 times

SebaAr22 5 years, 7 months ago
B es correcta
upvoted 1 times

kunjimon 5 years, 10 months ago
Ans is B. Based on experience.
upvoted 4 times

Vlad_R 5 years, 11 months ago
The correct answer is B, when selecting sd-wan from static routes the gateway option dissapear.The only option to select gateway for sd-wan is from sd-wan create new and add members(interfaces)
upvoted 3 times

Basuso 6 years, 1 month ago
The correct answer is B. When you configure SD-WAN and have to choose its member interfaces, you have to also specify their gateway individually. After this when you create a Static Route and select SD-WAN you won't even have the "Gateway" field available to be filled.
upvoted 3 times

georgianp 6 years, 1 month ago
B

Fortigate Insfrastructure 6.2 guide page 71
upvoted 3 times

Levis 6 years, 2 months ago
sorry correction, C is right
upvoted 1 times

Levis 6 years, 2 months ago
bcoz there is no option, so A is correct
upvoted 1 times

NetStef 6 years, 5 months ago
Correct is B
upvoted 3 times

montonearm 6 years, 5 months ago
the correct is B
upvoted 3 times

psat 6 years, 5 months ago

B is the correct answer, I tried testing option A and C, but do not see to an option to specify the gateway address.

upvoted 4 times

Question #16 *Topic 1*

Which of the following services can be inspected by the DLP profile? (Choose three.)

A. NFS

B. FTP

C. IMAP

D. CIFS

E. HTTP-POST

Suggested Answer: *B, C, E*

Ctnroger Most Recent 5 years, 8 months ago

I watched the full videos of NSE training 6.2 twice. And i am sure DLP profile dosen't apper. So it shouldn't be in the exam

upvoted 2 times

JesseJames 5 years, 11 months ago

B,C,E according to Creating/editing a DLP sensor

upvoted 2 times

sethjam 6 years, 1 month ago

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/DLP/Creating%20or%20editing%20a%20DLP%20sensor.htm

upvoted 4 times

Question #17 *Topic 1*

Which of the following statements describe WMI polling mode for the FSSO collector agent? (Choose two.)

A. The NetSessionEnum function is used to track user logoffs.

B. WMI polling can increase bandwidth usage in large networks.

C. The collector agent uses a Windows API to query DCs for user logins.

D. The collector agent do not need to search any security event logs.

Suggested Answer: *B, C*

topicx Highly Voted 6 years, 10 months ago
i think is C&D
upvoted 10 times

t12345 6 years, 7 months ago
I thought agent-based and polling but rely on security event logs from the DC's
upvoted 1 times

intaqto Highly Voted 6 years, 5 months ago
C and D. Page 239, Infrastructure 6.0 Study Guide v2
upvoted 8 times

rkchandra Most Recent 4 years, 4 months ago
C&D is correct
upvoted 1 times

albato239 4 years, 9 months ago
Selected Answer: CD
Page 265, Infrastructure 6.4 Study Guide
upvoted 1 times

meli_ssa 5 years, 8 months ago
las respuestas son C y D, la explicación aqui: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732
upvoted 2 times

Ctnroger 5 years, 8 months ago
B&D. C is a true statment, but is not what they are asking.
upvoted 1 times

Edy_Crank 5 years, 11 months ago
C&D is correct answer : This is from Fortinet 6.2 Training: WMI: A Windows API that gets system information from a Windows server. The DC returns all requested logon events. The collector agent is a WMI client and sends WMI queries for user logon events to the DC, which, in this case, is a WMI server. The collector agent doesn't need to search security event logs on the DC for user logon events; instead, the DC returns all requested logon events. This reduces network load between the collector agent and DC.
upvoted 1 times

ipam 5 years, 11 months ago
, DC returns all requested logon events via WMI. This also reduces network load between CA and DC. it means WMI decrease bandwidth usage instead of increasing it.... so B is not correct. C & D is
upvoted 1 times

carroyoc 6 years, 2 months ago
3) Event log using WMI polling: WMI is a Windows API to get system information from a Windows server, CA is a WMI client and sends WMI queries for user logon events to DC, which in this case is a WMI server. Main advantage in this mode is that CA does not need to search security event logs on DC for user logon events, instead, DC returns all requested logon events via WMI. This also reduces network load between CA and DC.

https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732
upvoted 5 times

georgianp 6 years, 1 month ago
+B(This also reduces network load between CA and DC.) In this case, BCD are correct :)

upvoted 1 times

montonearm 6 years, 5 months ago

should be C and D

upvoted 6 times

Question #18 *Topic 1*

Which statements about DNS filter profiles are true? (Choose two.)

A. They can inspect HTTP traffic.

B. They can redirect blocked requests to a specific portal.

C. They can block DNS requests to known botnet command and control servers.

D. They must be applied in firewall policies with SSL inspection enabled.

Suggested Answer: *B, C*

romartinedg Most Recent 5 years, 11 months ago

B & C son correctas, pag. 404 FortiGate_Security_6.2

upvoted 3 times

sethjam 6 years, 1 month ago

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_DNSInspectionProfile.htm

upvoted 1 times

Question #19 *Topic 1*

An administrator has configured a dialup IPsec VPN with XAuth. Which statement best describes what occurs during this scenario?

A. Phase 1 negotiations will skip preshared key exchange.

B. Only digital certificates will be accepted as an authentication method in phase 1.C

C. Dialup clients must provide a username and password for authentication.

D. Dialup clients must provide their local ID during phase 2 negotiations.

Suggested Answer: *C*

rkchandra Most Recent 4 years, 4 months ago

Selected Answer: C

Ans is C

upvoted 1 times

sethjam 6 years, 1 month ago

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/Phase_1/Using_XAuth.htm

upvoted 3 times

Question #20 *Topic 1*

An administrator has configured two VLAN interfaces:
A DHCP server is connected to the VLAN10 interface. A DHCP client is connected to the VLAN5 interface. However, the DHCP client cannot get a dynamic IP address from the DHCP server. What is the cause of the problem?

```
config system interface
  edit "VLAN10"
        set vdom "VDOM1"
        set forward-domain 100
        set role lan
        set interface "port9"
        set vlanid 10
     next
     edit "VLAN5"
        set vdom "VDOM1"
        set forward-domain 50
        set role lan
        set interface "port10"
        set vlanid 5
     next
end
```

A. Both interfaces must belong to the same forward domain.

B. The role of the VLAN10 interface must be set to server.

C. Both interfaces must have the same VLAN ID.

D. Both interfaces must be in different VDOMs.

Suggested Answer: *A*

Levis Highly Voted 6 years, 2 months ago
must be same forward domains, becasue with same forward domain, even different VLANs can do dhcp, but with vlans and different forward domains, DHCP will fail
upvoted 5 times

rahav 6 years ago
Correct. The answer here is not valid.
upvoted 1 times

meli_ssa Most Recent 5 years, 8 months ago
i think A is correct, it is explained in: https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/183521/checking-the-bridging-information-in-transparent-mode
upvoted 1 times

SantaScotty 6 years ago
The answer is A, which Levis states and the answer key states.
upvoted 2 times

Question #21 *Topic 1*

Which of the following statements about virtual domains (VDOMs) are true? (Choose two.)

A. The root VDOM is the management VDOM by default.

B. A FortiGate device has 64 VDOMs, created by default.

C. Each VDOM maintains its own system time.

D. Each VDOM maintains its own routing table.

Suggested Answer: *A, D*

sethjam Highly Voted 6 years, 1 month ago

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-virtual-domains-54/1-VDOM-overview/1-Introduction.htm

upvoted 6 times

JesseJames 5 years, 11 months ago

Thanks for sharing these, it really helps explain more on how the answers are correct.

upvoted 1 times

jm31 Most Recent 5 years, 7 months ago

C and D! You can set transparent and NAT mode in VDOM below is my reference. :) So A is incorrect! B I think you can set a name for new VDOM but not system hostname, its configure globally the system hostname. VDOM NAT and Transparent mode!

https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/986787/nat-and-transparent-mode

upvoted 1 times

meli_ssa 5 years, 8 months ago

A y D https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/109991/virtual-domains

upvoted 1 times

kunjimon 5 years, 10 months ago

A n D is right

upvoted 1 times

sim_cybersecurityspecialist 5 years, 10 months ago

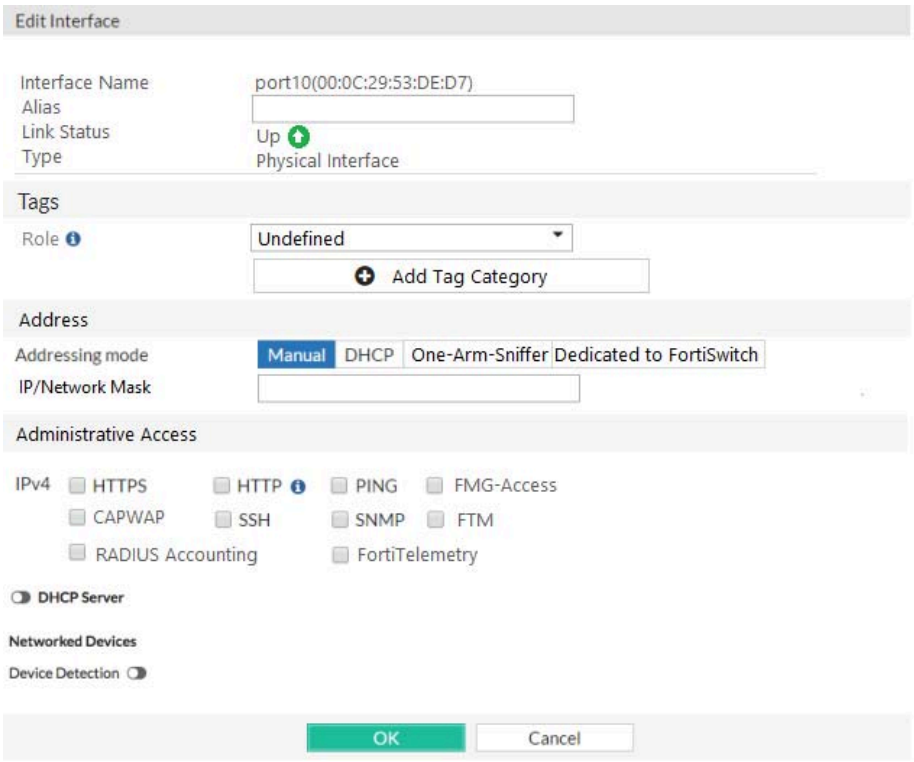
A and D

https://kb.fortinet.com/kb/documentLink.do?externalID=FD38863

upvoted 2 times

Question #22 *Topic 1*

You are configuring the root FortiGate to implement the security fabric. You are configuring port10 to communicate with a downstream FortiGate.
View the default
Edit Interface in the exhibit below:
When configuring the root FortiGate to communicate with a downstream FortiGate, which settings are required to be configured? (Choose two.)



A. Device detection enabled.

B. Administrative Access: FortiTelemetry.

C. IP/Network Mask.

D. Role: Security Fabric.

Suggested Answer: *B, C*

Thisisatest Highly Voted 6 years, 4 months ago
I think A and B From https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/788897/configuring-the-root-fortigate-and-downstream-fortigates In support of A: "Under Network, turn on Device Detection." In support of B: "Enable FortiGate Telemetry."
upvoted 5 times

Levis Highly Voted 6 years, 3 months ago
B and c
upvoted 5 times

wainse Most Recent 5 years, 8 months ago
if look into 6.2.3 links mentioned above, it seems AB, where as 6.0.0 has also mentioned about ip/network,,,,,,, so I would say AB
upvoted 1 times

Ryansiao 5 years, 9 months ago
https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/179964/configuring-edge
upvoted 1 times

rpena072 5 years, 9 months ago
the answer is b and c https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/724439/fortinet-security-fabric-installation you dont need to enable device detection to configure the security fabric for fortigates, like EvanABS said, that would be for field equipment
upvoted 4 times

khaganiabbasov 6 years ago

B and C (In root FG Telemetry and IP)

Device detection must be enable during downstream fortigate configuration.

Fortigate Security Study Guide page 68/69

upvoted 4 times

sim_cybersecurityspecialist 5 years, 10 months ago

This is wrong sir. please recheck. I have read page 68 and 69 , nowhere is shows, you need to have IP / subnet mask configured.

upvoted 1 times

belly123 6 years, 2 months ago

A & B Fortigate Security 6.0 page 61

upvoted 1 times

EvanABS 6 years, 4 months ago

Device Detection is only for field equipment

upvoted 2 times

Question #23 *Topic 1*

What FortiGate components are tested during the hardware test? (Choose three.)

A. Administrative access

B. HA heartbeat

C. CPU

D. Hard disk

E. Network interfaces

Suggested Answer: *C, D, E*

sethjam Most Recent 6 years, 1 month ago

https://kb.fortinet.com/kb/documentLink.do?externalID=FD39581

upvoted 3 times

belly123 6 years, 2 months ago

CDE Fortigate Infrastructure 6.0 page 401

upvoted 4 times

Question #24 *Topic 1*

Which statements correctly describe transparent mode operation? (Choose three.)

A. All interfaces of the transparent mode FortiGate device must be on different IP subnets.

B. Ethernet packets are forwarded based on destination MAC addresses, not IP addresses.

C. The transparent FortiGate is visible to network hosts in an IP traceroute.

D. It permits inline traffic inspection and firewalling without changing the IP scheme of the network.

E. FortiGate acts as transparent bridge and forwards traffic at Layer 2.

Suggested Answer: *B, D, E*

Makalanguzu Most Recent 6 years ago

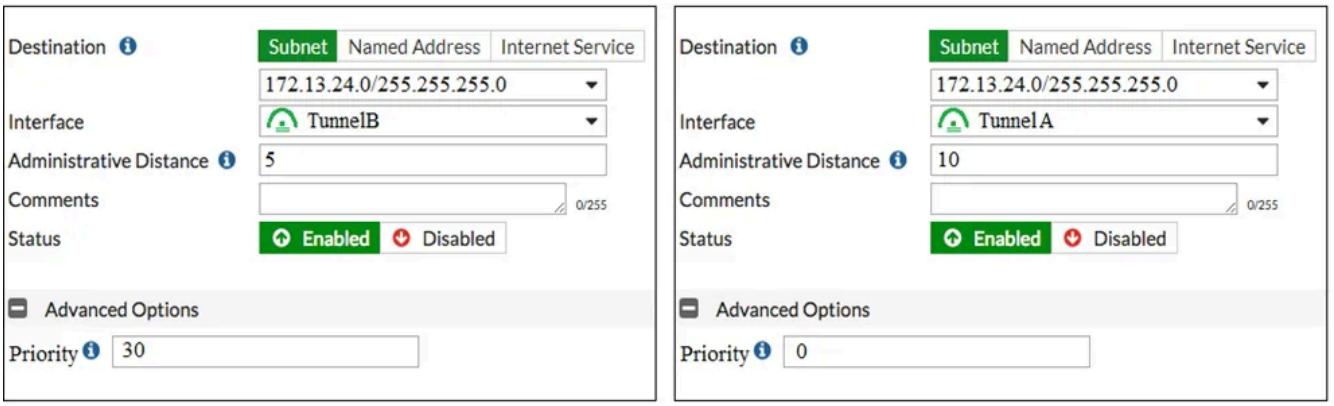
BDE is correct

upvoted 3 times

Question #25 *Topic 1*

View the exhibit.

Which of the following statements are correct? (Choose two.)



A. This setup requires at least two firewall policies with the action set to IPsec.

B. Dead peer detection must be disabled to support this type of IPsec setup.

C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.

D. This is a redundant IPsec setup.

Suggested Answer: *C, D*

Makalanguzu Most Recent 6 years ago

CD is correct

upvoted 4 times

Question #26 *Topic 1*

Which one of the following processes is involved in updating IPS from FortiGuard?

A. FortiGate IPS update requests are sent using UDP port 443.

B. Protocol decoder update requests are sent to service.fortiguard.net.

C. IPS signature update requests are sent to update.fortiguard.net.

D. IPS engine updates can only be obtained using push updates.

Suggested Answer: *C*

sethjam Highly Voted 6 years, 1 month ago

https://docs.fortinet.com/document/fortigate/6.0.0/fortinet-communication-ports-and-protocols/649403/fortiguard

upvoted 6 times

Question #27 *Topic 1*

How does FortiGate select the central SNAT policy that is applied to a TCP session?

A. It selects the SNAT policy specified in the configuration of the outgoing interface.

B. It selects the first matching central SNAT policy, reviewing from top to bottom.

C. It selects the central SNAT policy with the lowest priority.

D. It selects the SNAT policy specified in the configuration of the firewall policy that matches the traffic.

Suggested Answer: *B*

kunjimon Most Recent 5 years, 10 months ago

B is right

upvoted 2 times

JesseJames 5 years, 10 months ago

B is correct

upvoted 4 times

georgianp 6 years, 1 month ago

It could be B: A central SNAT policy is processed from top to bottom and if a match is found, src address and src port are translated based on the central SNAT policy OR it could be D: SNAT policy is selected according to the configuration of the firewall policy that matches the traffic. FOrtigate security 6.2 study guide page 165

upvoted 4 times

mninty 6 years, 1 month ago

The question mentions Central SNAT, so there is no SNAT on a firewall policy level.

upvoted 3 times

sethjam 6 years, 1 month ago

https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/1000_Managing%20policies/1600_Central%20SNAT.htm

upvoted 1 times

Question #28 *Topic 1*

Which of the following conditions are required for establishing an IPSec VPN between two FortiGate devices? (Choose two.)

A. If XAuth is enabled as a server in one peer, it must be enabled as a client in the other peer.

B. If the VPN is configured as route-based, there must be at least one firewall policy with the action set to IPSec.

C. If the VPN is configured as DialUp User in one peer, it must be configured as either Static IP Address or Dynamic DNS in the other peer.

D. If the VPN is configured as a policy-based in one peer, it must also be configured as policy-based in the other peer.

Suggested Answer: *B, C*

rogue7 Highly Voted 7 years ago

B is incorrect. https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-ipsecvpn/Defining_VPN_Policies/Defining_Policies_for_Policy_and_Route.htm?Highlight=route%20based%20vpn

upvoted 5 times

SebaAr22 Most Recent 5 years, 7 months ago

A - C are correct

upvoted 1 times

farmez 5 years, 8 months ago

A and C B incorrect => IPSEC ACTION in a firewall policy is used with policy-based VPN and not route-based VPN

upvoted 1 times

Vlad_R 5 years, 11 months ago

B- action can be set to Accept,Deny and learn so is wrong.A is correct : Adding XAuth authentication Extended Authentication (XAuth) increases security by requiring additional user authentication in a separate exchange at the end of the VPN Phase 1 negotiation. The FortiGate unit challenges the user for a user name and password. It then forwards the user's credentials to an external RADIUS or LDAP server for verification.

Implementation of XAuth requires configuration at both the FortiGate unit and the FortiClient application. For information about configuring a FortiGate unit as an XAuth server, see Phase 1 parameters. The following procedure explains how to configure the FortiClient application. So the correct answers are A&C.

upvoted 4 times

NETeng01 5 years, 8 months ago

for me correct are C and D

upvoted 1 times

Levis 6 years, 3 months ago

A and c

upvoted 4 times

montonearm 6 years, 5 months ago

i think A & C

upvoted 3 times

Ctnroger 5 years, 8 months ago

But Xauth is use for dialup vpn no site to site vpn

upvoted 1 times

ni 6 years, 9 months ago

Answer is AC

upvoted 4 times

Question #29 *Topic 1*

Which of the following statements about converse mode are true? (Choose two.)

A. FortiGate stops sending files to FortiSandbox for inspection.

B. FortiGate stops doing RPF checks over incoming packets.

C. Administrators cannot change the configuration.

D. Administrators can access the FortiGate only through the console port.

Suggested Answer: *A, B*

myutran Highly Voted 6 years, 11 months ago

Correct answer : A & C

upvoted 12 times

PoBratsky Most Recent 3 years, 7 months ago

Selected Answer: AC

Correct answer : A & C

upvoted 1 times

Ctnroger 5 years, 8 months ago

A&C is correct

upvoted 1 times

mmelo 5 years, 10 months ago

Correct: A and C

upvoted 1 times

Makalanguzu 6 years ago

Typo in question:Conserve mode Correct Answer is:A & C

upvoted 2 times

Fr4nx 6 years, 2 months ago

A & C, Reverse Path Filter configuration will drop based on source Ip, conserve mode block AV

upvoted 3 times

Levis 6 years, 3 months ago

A and b actually.

upvoted 1 times

montonearm 6 years, 5 months ago

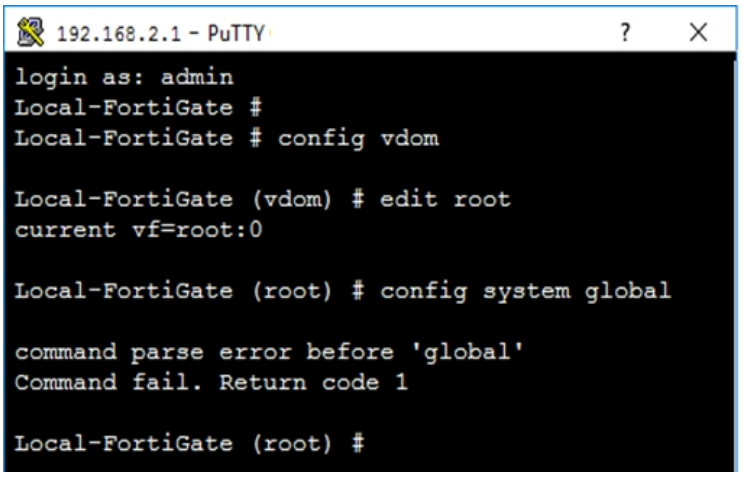
also for me is A & C

upvoted 3 times

Question #30 *Topic 1*

View the exhibit.

Why is the administrator getting the error shown in the exhibit?



A. The administrator must first enter the command edit global.

B. The administrator admin does not have the privileges required to configure global settings.

C. The global settings cannot be configured from the root VDOM context.

D. The command config system global does not exist in FortiGate.

Suggested Answer: *C*

nabilzay Most Recent 5 years, 12 months ago

C is correct

upvoted 4 times

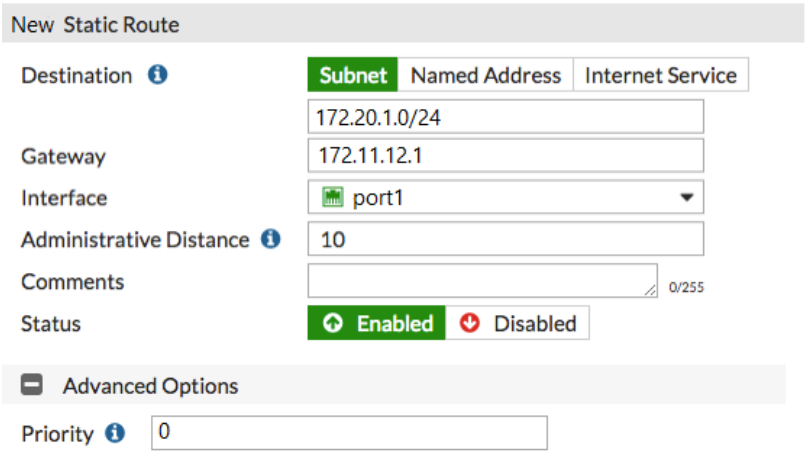
Question #31 *Topic 1*

Examine the network diagram and the existing FGTI routing table shown in the exhibit, and then answer the following question:
An administrator has added the following static route on FGTI.
Since the change, the new static route is not showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?




```
FGT1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1,  N2 - OSPF external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default;

S      172.20.0.0/16 [10/0] via 172.21.1.2, port2
C      172.21.0.0/16 is directly connected, port2
C      172.11.11.0/24 is directly connected, port1
```



A. The new route's destination subnet overlaps an existing route.

B. The new route's Distance value should be higher than 10.

C. The Gateway IP address is not in the same subnet as port1.

D. The Priority is 0, which means that this route will remain inactive.

Suggested Answer: *C*

rahav 6 years ago

The question is not valid- look at the drawing- port2 have connected subnet - 172.20.1.1/24 and it's not appearing in the routing table - which not making any sense. Also the answer is not correct because if you have connected subnet it's will always be preferred over static route- also - you can configure static route to subnet that is not same subnet of your port.

upvoted 1 times

freakydummy Highly Voted 6 years ago

The output is from FGT1, C is correct.

upvoted 7 times

Question #32 *Topic 1*

Which configuration objects can be selected for the Source field of a firewall policy? (Choose two.)

A. Firewall service

B. User or user group

C. IP Pool

D. FQDN address

Suggested Answer: *B, C*

SebaAr22 Most Recent 5 years, 7 months ago
B y D - IP pool cant be selected
upvoted 2 times

kunjimon 5 years, 10 months ago
Just tested, FQDN & User/User Group can be added as source in policy. IP Pool is not possible to be added.
upvoted 4 times

Vlad_R 5 years, 11 months ago
On the source u can select from address , user and device no ip pool.Don't missunderstand the address configured with ip range. So the correct answer is B&D
upvoted 4 times

Mahbubul 6 years, 2 months ago
B & D is correct
upvoted 2 times

NetStef 6 years, 5 months ago
B and D
upvoted 2 times

montonearm 6 years, 5 months ago
also for me B & D
upvoted 2 times

ni 6 years, 9 months ago
Answer is BD
upvoted 4 times

fireman17 6 years, 10 months ago
Answer D, cloud be a valid response? On the Student Guide is mentioned as a must source and the user - user group as optional.
upvoted 1 times

Question #33 *Topic 1*

View the exhibit.

Which users and user groups are allowed access to the network through captive portal?



A. Users and groups defined in the firewall policy.

B. Only individual users "" not groups "" defined in the captive portal configuration

C. Groups defined in the captive portal configuration

D. All users

Suggested Answer: *C*

myutran Highly Voted 6 years, 11 months ago

Correct answer : A

upvoted 9 times

bltmayo 5 years, 7 months ago

I think C because Allow All is referring to All groups configured not all users. Page 239 Security 6.2 study guide.

upvoted 1 times

Vlad_R 5 years, 10 months ago

Omg , i did a mistake by confusing ssid with interface.From interface settings upon security mode , captive portal next to user acces says : all users can login but access will be defined by relevant policies.So the corect answer is A

upvoted 2 times

Vlad_R 5 years, 11 months ago

Guys in 6.2 and newer firmware there is no allow all option, only user groups to add.So in the correct answer is C for 6.2 remember.

upvoted 1 times

SebaAr22 Most Recent 5 years, 7 months ago

Allow all exists in 6.2 and 6.4

upvoted 1 times

chameleon_eh 6 years, 2 months ago

FortiGate_Security_6.2_Study_Guide-Online (page 239). The correct answer is "A" because the Allow All option was selected.

upvoted 2 times

fugiyama 6 years, 2 months ago

Also think its A

upvoted 1 times

Mahbubul 6 years, 2 months ago

A is correct

upvoted 1 times

jbernard 6 years, 2 months ago

Correct is A, Users and Groups defined in the firewall policy configuration

upvoted 2 times

NetStef 6 years, 5 months ago

It's A

upvoted 2 times

montonearm 6 years, 5 months ago

also for me A

upvoted 2 times

Question #34 *Topic 1*

NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

A. Web filtering

B. Antivirus

C. Web proxy

D. Application control

Suggested Answer: *C*

Mahbubul Most Recent 6 years, 2 months ago

B is the right answer

upvoted 2 times

jbernard 6 years, 2 months ago

Antivirus and IPS is enhanced by the IPS Engine, so that is why B is the right answer

upvoted 3 times

montonearm 6 years, 5 months ago

antivirus so right should B

upvoted 2 times

myutran 6 years, 11 months ago

Correct answer : B

upvoted 4 times

Question #35 *Topic 1*

During the digital verification process, comparing the original and fresh hash results satisfies which security requirement?

A. Authentication.

B. Data integrity.

C. Non-repudiation.

D. Signature verification.

Suggested Answer: *D*

JOY099 Most Recent 5 years, 2 months ago

B is the answer, since the request is from original hash to fresh hash based on the security requirement.

If the request was from the fresh hash to the original hash then it will be signature verification

upvoted 1 times

JOY099 5 years, 2 months ago

B since its from original to the fresh based on the security requirement.

It the request was from the fresh to the original then it will be signature verification.

upvoted 1 times

Cyril_the_Squirl 5 years, 3 months ago

B is correct

upvoted 1 times

Null0 5 years, 10 months ago

B is correct.

upvoted 1 times

Levis 6 years, 1 month ago

D, page 318 of 6.2 guide.

upvoted 1 times

Humungus 6 years ago

The digital signature is the result of a encrypted hash. The Hash is to verify data integrity.

upvoted 3 times

georgianp 6 years, 1 month ago

Yes, it is describing the process, which is indeed signature verification. But it asks which SECURITY requirement satisfy and it is data integrity.

upvoted 4 times

Mahbubul 6 years, 2 months ago

B is correct as per the Study guide.

upvoted 2 times

Levis 6 years, 3 months ago

hash match is to make sure data is integral. B

upvoted 1 times

intaqto 6 years, 5 months ago

B FortiGate_Security_6.0_Study_Guide_v2-Online page 288

upvoted 2 times

ni 6 years, 9 months ago

Answer is B

upvoted 2 times

Question #36 *Topic 1*

An administration wants to throttle the total volume of SMTP sessions to their email server. Which of the following DoS sensors can be used to achieve this?

A. tcp_port_scan

B. ip_dst_session

C. udp_flood

D. ip_src_session

Suggested Answer: *A*

Samanosuke Highly Voted 6 years, 10 months ago

The correct answer is B. The A is only to detect probing.

upvoted 8 times

Cyril_the_Squirl Most Recent 5 years, 4 months ago

The question says..."To throttle...Volume of SMTP SESSIONS...TO their Server" Answer is B.

upvoted 1 times

wassimtrabelsi 5 years, 8 months ago

Answer B is correct : Fortigate Security 6.2 Study Guide page 541

upvoted 1 times

Levis 6 years, 1 month ago

Flooding If the number of sessions targeting a single destination in one second is over a threshold, the destination is experiencing flooding. Scan If the number of sessions from a single source in one second is over a threshold, the source is scanning. Source session limit If the number of concurrent sessions from a single source is over a threshold, the source session limit is reached. Destination session limit If the number of concurrent sessions to a single destination is over a threshold, the destination session limit is reached.

upvoted 1 times

Fr4nx 6 years, 2 months ago

B. ip_dst_session

upvoted 1 times

rjalburq 6 years, 5 months ago

I think D https://kb.fortinet.com/kb/viewContent.do?externalId=FD35259 "If you want to protect your own servers from DoS attacks from the Internet:

- Be sure to configure only your own servers as destination of the traffic. You have to use 'Address' objects, not VIPs. - Set the services you provide in your server. This is HTTP, HTTPS, SMTP, etc. - Configure only the anomalies which will match the services of your server(s). For example, if your server provides SMTP access only, use the following anomalies:

+ tcp_syn_flood, or + tcp_src_session, or + ip_src_session"

upvoted 2 times

Addictioneer 6 years, 1 month ago

Be careful. Continue reading your shared link “If you use (in this case) tcp_dst_session or ip_dst_session, you would be limiting the number of concurrent sessions your server will handle (purpose of Denial of Service).“

If u use “ip_src_session” and let say set the threshold to 100. “Each source IP” will be allowed unless they pass 100

The question asks to protect the volume of traffic to the server. So if we use “ip_dst_session” and set it to 100, the total volume of traffic will be allowed unless it passes the 100 threshold.

Perspective!

The answer is B

upvoted 3 times

montonearm 6 years, 5 months ago

i think B

upvoted 2 times

[Removed] 6 years, 8 months ago

The Correct answer 100% A If addmin want to all traffic reduce answer b or d. snmp packet l4 so tcp_port_scan is correct check
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Policies/IPv4%20DoS%20Policy.htm
https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-firewall-52/Security%20Policies/DoS%20Protection.htm

upvoted 1 times

naicoram Highly Voted 6 years, 4 months ago

So, based on the second link "DoS Protection", the answer "B ip_dst_session" is the correct !

it said : ip_dst_session : If the number of concurrent IP connections to one destination IP address exceeds the configured threshold value, the action is executed tcp_port_scan : If the SYN packet rate of new TCP connections, including retransmission, from one source IP address exceeds the configured threshold value, the action is executed.

for ip_dst_session : " ...connections to one destination IP..." For tcp_port_scan : "... from one source IP address..."

So the ip_dst_session is more approriate in this case of "throttle the total volume of SMTP sessions to their email server" !!

upvoted 13 times

ni 6 years, 9 months ago

Correct answer is C

upvoted 1 times

Question #37 *Topic 1*

Why must you use aggressive mode when a local FortiGate IPSec gateway hosts multiple dialup tunnels?

A. In aggressive mode, the remote peers are able to provide their peer IDs in the first message.

B. FortiGate is able to handle NATed connections only in aggressive mode.

C. FortiClient only supports aggressive mode.

D. Main mode does not support XAuth for user authentication.

Suggested Answer: *A*

Arc543 Most Recent 5 years, 8 months ago

A. In aggressive mode, the remote peers are able to provide their peer IDs in the first message.

upvoted 1 times

Question #38 *Topic 1*

Examine this output from a debug flow:

Why did the FortiGate drop the packet?

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

A. The next-hop IP address is unreachable.

B. It failed the RPF check.

C. It matched an explicitly configured firewall policy with the action DENY.

D. It matched the default implicit firewall policy.

Suggested Answer: *D*

sethjam Most Recent 6 years, 1 month ago

The (default) drop rule that is the last rule in the policy and that is automatically added has a policy ID number of 0.

https://kb.fortinet.com/kb/documentLink.do?externalID=13900

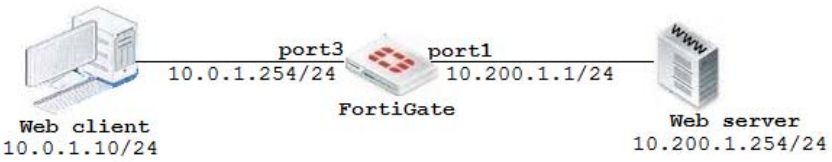
upvoted 4 times

Question #39 *Topic 1*

View the exhibit:

The client cannot connect to the HTTP web server. The administrator ran the FortiGate built-in sniffer and got the following output:

What should be done next to troubleshoot the problem?




```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.755510 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
```

A. Run a sniffer in the web server.

B. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10".

C. Capture the traffic using an external sniffer connected to port1.

D. Execute a debug flow.

Suggested Answer: *C*

myutran Highly Voted 6 years, 11 months ago

Correct answer : D

upvoted 7 times

Penn 6 years, 10 months ago

kindly explain

upvoted 1 times

Bluey 6 years, 9 months ago

Traffic is entering FG on port 3 but isnt leaving it on port 1, so problem lies on fortigate. External sniffer is a bogus answer and gives you no information. Only correct option is a debug flow (or simply check logs) to see why traffic is failing

upvoted 4 times

notarussianagent 6 years, 8 months ago

It is not confirmed if traffic is egressing port1, all we see in the flow debug is inbound traffic from the host on port3 that wants to go to the web server out port1. Personally, I would sniff the web host to see if they are getting in. But I feel the answer Fortinet is looking for is what myutran and bluey say it is; D. the flow debug will confirm the traffic inbound on port3 and if it is egressing port1. the flow debug will also show us if the web server traffic is even entering the FG or being denied. Sniffers do not show deny traffic, only debugs do that.

upvoted 1 times

carroyoc 6 years, 2 months ago

It is simple , if you see the filters it says interface any, so this means that if the packet is leaving the Fortigate, we would be able to see it, but we are not. So this means the packet is getting drop in the Fortigate, so we need the debug.

upvoted 3 times

jbernard Most Recent 6 years, 2 months ago

Debug flow will show why the Syn packet is not creating a new session

https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/054688/debugging-the-packet-flow

upvoted 2 times

Levis 6 years, 3 months ago

D is answer

upvoted 1 times

montonearm 6 years, 5 months ago

also for me is D

upvoted 1 times

Question #40 *Topic 1*

Which of the following statements about policy-based IPsec tunnels are true? (Choose two.)

A. They can be configured in both NAT/Route and transparent operation modes.

B. They support L2TP-over-IPsec.

C. They require two firewall policies: one for each directions of traffic flow.

D. They support GRE-over-IPsec.

Suggested Answer: *A, B*

rjalburq Highly Voted 6 years, 5 months ago

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Overview/Types_of_VPNs.htm

upvoted 5 times

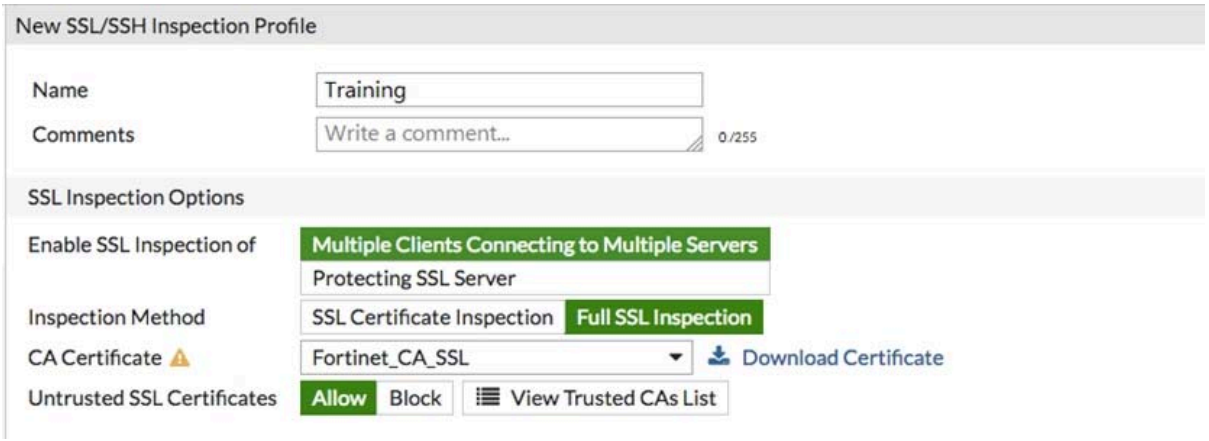
Nostradagus Most Recent 6 years, 1 month ago

So A & B are correct.

upvoted 4 times

Question #41 *Topic 1*

An employee connects to the https://example.com on the Internet using a web browser. The web server's certificate was signed by a private internal CA. The
FortiGate that is inspecting this traffic is configured for full SSL inspection.
This exhibit shows the configuration settings for the SSL/SSH inspection profile that is applied to the policy that is invoked in this instance. All other settings are set to defaults. No certificates have been imported into FortiGate. View the exhibit and answer the question that follows.
Which certificate is presented to the employee's web browser?



A. The web server's certificate.

B. The user's personal certificate signed by a private internal CA.

C. A certificate signed by Fortinet_CA_SSL.

D. A certificate signed by Fortinet_CA_Untrusted.

Suggested Answer: *A*

myutran Highly Voted 6 years, 11 months ago
Correct answer : D
upvoted 7 times

ericnesh Most Recent 5 years, 10 months ago
D. FortiGate Security 6.2 Study Guide, page 336
upvoted 2 times

jlaspalas 6 years, 1 month ago
It's D :D the questions says the web server is a PRIVATE ca cert, so you won't have it on trusted CAs ;D
upvoted 1 times

Levis 6 years, 2 months ago
D, because fortinet will present similar (if trusted, then trusted, if untrsuted, then untrusted) cert to browser, what it sees on website.
upvoted 2 times

montonearm 6 years, 5 months ago
also for me is D
upvoted 1 times

intaqto 6 years, 5 months ago
D. FortiGate Security 6.0 Study Guide, P.304,
upvoted 2 times

rogue7 7 years ago
wrong answer.
upvoted 1 times

Question #42 *Topic 1*

Examine this FortiGate configuration:

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

```
config authentication setting
     set active-auth-scheme SCHEME1
end
config authentication rule
     edit WebProxyRule
       set srcaddr 10.0.1.0/24
       set active-auth-method SCHEME2
     next
end
```

A. It always authorizes the traffic without requiring authentication.

B. It drops the traffic.

C. It authenticates the traffic using the authentication scheme SCHEME2.

D. It authenticates the traffic using the authentication scheme SCHEME1.

Suggested Answer: *C*

myutran Highly Voted 6 years, 11 months ago

Correct Answer : D

upvoted 9 times

Penn 6 years, 10 months ago

CORRECT. srcadr 10.0.1.0/24 uses SCHEME2

upvoted 2 times

Diego_Farani Most Recent 2 years, 9 months ago

Selected Answer: D

The answer is D.

upvoted 1 times

hkhan049 3 years, 8 months ago

Found this question also for preparing to NSE4 7.0. But answer "D" is not clear to me.

"Authentication rules are used to receive user-identity, based on the values set for protocol and source address. Having said this, if a rule fails to match based on source address, there will be no other attempt to match the rule, however the next policy will be attempted. "
https://www.fortinetguru.com/2019/05/authentication-in-security-policies/

There is only "one" authentication rule, that does not match on 10.2.1.200. I can't see another rule that do match on 10.2.1.200. Schouldn't traffic be blocked in this case?

upvoted 1 times

Sergio3000 5 years, 8 months ago

Correcta es D

upvoted 1 times

jbernard 6 years, 2 months ago

D is correct, not C cause 10.2.1.200 is part of 10.2.1.0/24 subnet, doesn't applies 10.0.1.0/24 subnet's rule

upvoted 3 times

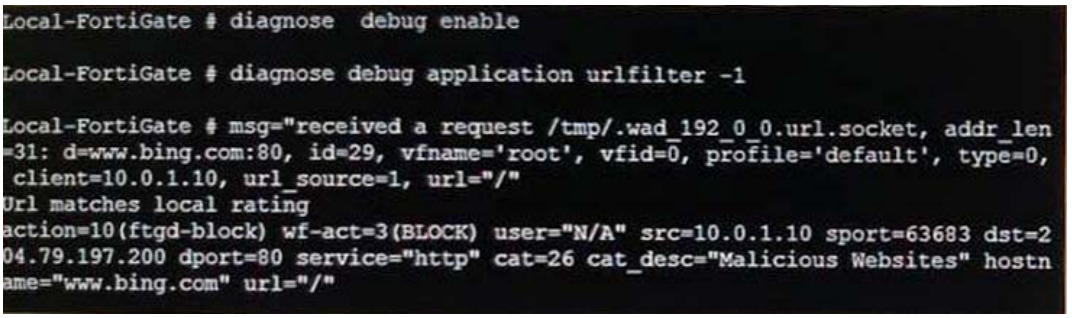
montonearm 6 years, 5 months ago

also for me is D

upvoted 1 times

Question #43 *Topic 1*

Examine the exhibit, which shows the output of a web filtering real time debug.
Why is the site www.bing.com being blocked?



A. The web site www.bing.com is categorized by FortiGuard as Malicious Websites.

B. The user has not authenticated with the FortiGate yet.

C. The web server IP address 204.79.197.200 is categorized by FortiGuard as Malicious Websites.

D. The rating for the web site www.bing.com has been locally overridden to a category that is being blocked.

Suggested Answer: *D*

Arc543 Most Recent 5 years, 8 months ago

D. The rating for the web site www.bing.com has been locally overridden to a category that is being blocked
upvoted 1 times

Question #44 *Topic 1*

Which of the following statements are best practices for troubleshooting FSSO? (Choose two.)

A. Include the group of guest users in a policy.

B. Extend timeout timers.

C. Guarantee at least 34 Kbps bandwidth between FortiGate and domain controllers.

D. Ensure all firewalls allow the FSSO required ports.

Suggested Answer: *A, D*

wassimtrabelsi Most Recent 5 years, 8 months ago

Correct Answer A&D : Fortigate Infrastructure 6.2 Study Guide page : 276

upvoted 2 times

JesseJames 5 years, 10 months ago

c & d, Ensure the Collector agent has at least 64kbps bandwidth to the FortiGate unit. If not, information FSSO information may not reach the FortiGate unit resulting in outages. The best solution is to configure traffic shaping between the FortiGate unit and the Collector agent to ensure that minimum bandwidth is always available. Ensure the Collector agent has at least 64kbps bandwidth to the FortiGate unit. If not, information FSSO information may not reach the FortiGate unit resulting in outages. The best solution is to configure traffic shaping between the FortiGate unit and the Collector agent to ensure that minimum bandwidth is always available.

upvoted 2 times

admins 5 years, 10 months ago

But C is stating that we're going to ensure a minimum of 32kbps which is less than the required minimum. As JesseJames has stated above.

upvoted 2 times

sethjam 6 years, 1 month ago

https://help.fortinet.com/fos40hlp/43/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=FSAE.69.55.html

upvoted 3 times

jlaspalas 6 years ago

So C and D?

upvoted 3 times

JesseJames 5 years, 10 months ago

I can't edit my comment, but I would say A&D is correct. C is stating 34kbs when the article that @sethjam listed says at least 64kbps bandwidth to the FortiGate unit

upvoted 2 times

Question #45 *Topic 1*

When override is enabled, which of the following shows the process and selection criteria that are used to elect the primary FortiGate in an HA cluster?

A. Connected monitored ports > HA uptime > priority > serial number

B. Priority > Connected monitored ports > HA uptime > serial number

C. Connected monitored ports > priority > HA uptime > serial number

D. HA uptime > priority > Connected monitored ports > serial number

Suggested Answer: *C*

ni Highly Voted 6 years, 9 months ago
ANswer is C when overide is enable
upvoted 7 times

ericnesh Most Recent 5 years, 10 months ago
C. Connected monitored ports > priority > HA uptime > serial number - override enabled Connected monitored ports > HA uptime> priority > serial number - override disabled(deafult) FortiGate Infrastructure study guide 6.2 pg.293
upvoted 5 times

Anzelimo 5 years, 11 months ago
With override enabled, C

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_override.htm
upvoted 3 times

DUMLKY 5 years, 11 months ago
The correcto answer is C
upvoted 2 times

hmzx 6 years, 2 months ago
when override „c
upvoted 3 times

chameleon_eh 6 years, 2 months ago
The answer is C https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_override.htm

Note that the question says the override option is enabled...
upvoted 3 times

Levis 6 years, 2 months ago
C for sure
upvoted 2 times

toru 6 years, 3 months ago
answer C
upvoted 3 times

toru 6 years, 3 months ago
answer A
upvoted 1 times

NetStef 6 years, 5 months ago
answer is C
upvoted 3 times

montonearm 6 years, 5 months ago
correct is C
upvoted 3 times

galactas 6 years, 5 months ago
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_primary_selection.htm

upvoted 2 times

Nico242 6 years, 12 months ago

answer A

upvoted 1 times

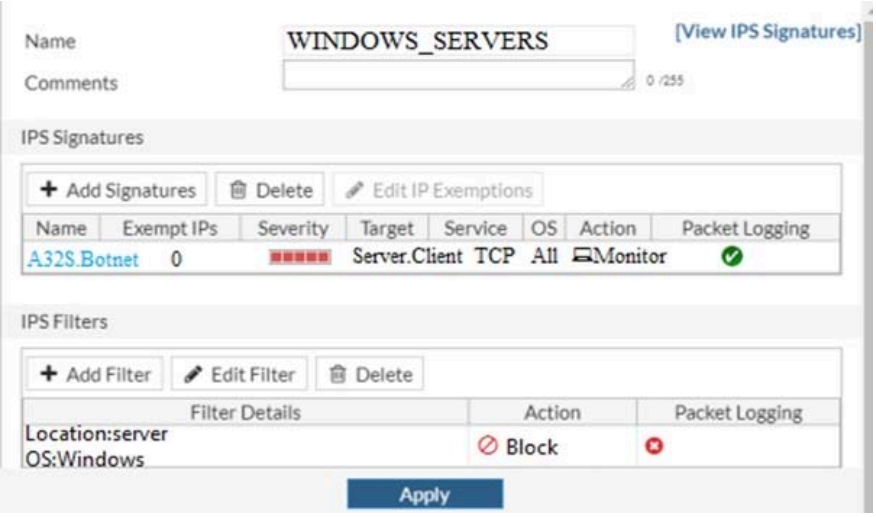
myutran Highly Voted 6 years, 11 months ago

Correct answer C

upvoted 11 times

Question #46 *Topic 1*

Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.
What are the expected actions if traffic matches this IPS sensor? (Choose two.)



A. The sensor will gather a packet log for all matched traffic.

B. The sensor will not block attackers matching the A32S.Botnet signature.

C. The sensor will block all attacks for Windows servers.

D. The sensor will reset all connections that match these signatures.

Suggested Answer: *A, C*

petrus28 Most Recent 5 years, 5 months ago
B&C - IPS Filter is set to not generate any packer log, so A is not correct.
upvoted 1 times

Sergio3000 5 years, 8 months ago
B and C correcto
upvoted 1 times

SantaScotty 6 years ago
A & B are correct. Individual signature actions override filter actions. So Monitor and Log actions will take place.
upvoted 1 times

ndlgd 6 years ago
B&C Each IPS sensor consists of two parts: filters and overrides. Overrides are always checked before filters.
upvoted 3 times

Fr4nx 6 years, 2 months ago
A & C correct, but B can be correct, action - monitor
upvoted 1 times

Addictioneer 6 years, 1 month ago
B cannot be correct. The A32S.Botnet attacker will be blocked if they target windows OS
upvoted 2 times

guybrush06 5 years, 9 months ago
The signature overrides the Filter, so it will be allowed as "Monitor".

A can´t be correct since all the traffic matching IPS filter (blocked traffic) will NOT generate log.
upvoted 1 times

Levis 6 years, 2 months ago
B and C final
upvoted 1 times

NetStef 6 years, 5 months ago

A and B

upvoted 2 times

montonearm 6 years, 5 months ago

A & C are correct

upvoted 1 times

Samanosuke 6 years, 10 months ago

A&B correct

upvoted 2 times

Samanosuke Highly Voted 6 years, 10 months ago

Sorry, B&C are correct

upvoted 16 times

EvanABS 6 years, 4 months ago

The block log will not be recorded

upvoted 2 times

Question #47 *Topic 1*

How can you block or allow to Twitter using a firewall policy?

A. Configure the Destination field as Internet Service objects for Twitter.

B. Configure the Action field as Learn and select Twitter.

C. Configure the Service field as Internet Service objects for Twitter.

D. Configure the Source field as Internet Service objects for Twitter.

Suggested Answer: *A*

Arc543 Most Recent 5 years, 8 months ago

A. Configure the Destination field as Internet Service objects for Twitter.

upvoted 1 times

Question #48 *Topic 1*

Which statements about HA for FortiGate devices are true? (Choose two.)

A. Sessions handled by proxy-based security profiles cannot be synchronized.

B. Virtual clustering can be configured between two FortiGate devices that have multiple VDOMs.

C. HA management interface settings are synchronized between cluster members.

D. Heartbeat interfaces are not required on the primary device.

Suggested Answer: *B, C*

onururas Highly Voted 6 years, 9 months ago
A&B correct
upvoted 9 times

hkhan049 Most Recent 5 years, 7 months ago
I also would choose A & B. C were not bad, if you configure a cluster management IP, but otherwise, the mgmt is dedicated per member. A: "Session-pickup has some limitations. For example, the FGCP does not support session failover for sessions being scanned by proxy-based security profiles. Session" I assume, this is valid not only for the 6000 https://docs.fortinet.com/document/fortigate-6000/6.0.4/fortigate-6000-handbook/686471/session-failover-session-pickup
upvoted 1 times

bull01 5 years, 8 months ago
A & B regarding FG Infrastructure Study Guide 6.4 (page 327)
upvoted 1 times

theazlan 5 years, 9 months ago
Why A & B?
upvoted 1 times

ronnycix 5 years, 8 months ago
Fortigate Study Guide 6.0 pages: 301 and 312: ONLY sessions not being handled by proxy based sec profile can be syncronized Virtual Clustering: You can use virtual clustering to manually distribute traffic between two cluster devices.
upvoted 1 times

Aps123 5 years, 9 months ago
A & C is correct
upvoted 1 times

Aps123 5 years, 9 months ago
Sorry B & C is correct after reading below, it takes out A https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/869218/fgsp-session-synchronization-peer-setup
upvoted 1 times

Vlad_R 5 years, 11 months ago
C is correct :) HA management interface will be enabled automatically on slave unit and interface will be configured same as Master.
upvoted 3 times

Mohamed_M 5 years, 11 months ago
A&B correct
upvoted 1 times

ndlgd 6 years ago
A&B is correct
upvoted 1 times

chameleon_eh 6 years, 2 months ago
The FortiGate_Infrastructure_6.2_Stude_Guide-Online (Pages 304, 315).
upvoted 2 times

chameleon_eh 6 years, 2 months ago
A & B are correct
upvoted 2 times

Levis 6 years, 2 months ago

A and B

upvoted 2 times

joeytrib 6 years, 3 months ago

Correct answer : A&B

upvoted 2 times

NetStef 6 years, 5 months ago

A and B

upvoted 3 times

montonearm 6 years, 5 months ago

A & B are right

upvoted 3 times

Question #49 *Topic 1*

An administrator is configuring an antivirus profiles on FortiGate and notices that Proxy Options is not listed under Security Profiles on the GUI. What can cause this issue?

A. FortiGate needs to be switched to NGFW mode.

B. Proxy options section is hidden by default and needs to be enabled from the Feature Visibility menu.

C. Proxy options are no longer available starting in FortiOS 5.6.

D. FortiGate is in flow-based inspection mode.

Suggested Answer: *D*

hkhan049 Most Recent 5 years, 7 months ago

D might be correct if they mean the proxy feature support for MAPI and CDR, which are actual only available, if the AV profile is set to proxy-based mode

upvoted 1 times

Arc543 5 years, 8 months ago

D. FortiGate is in flow-based inspection mode.

upvoted 1 times

sethjam 6 years, 1 month ago

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Inspection%20Modes/individ_security_profile_considerations.htm

upvoted 2 times

Question #50 *Topic 1*

An administrator has configured a route-based IPsec VPN between two FortiGate devices. Which statement about this IPsec VPN configuration is true?

A. A phase 2 configuration is not required.

B. This VPN cannot be used as part of a hub-and-spoke topology.

C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.

D. The IPsec firewall policies must be placed at the top of the list.

Suggested Answer: *C*

EvanABS Highly Voted 6 years, 4 months ago

C is correct, refer: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Overview/Types_of_VPNs.htm

upvoted 5 times

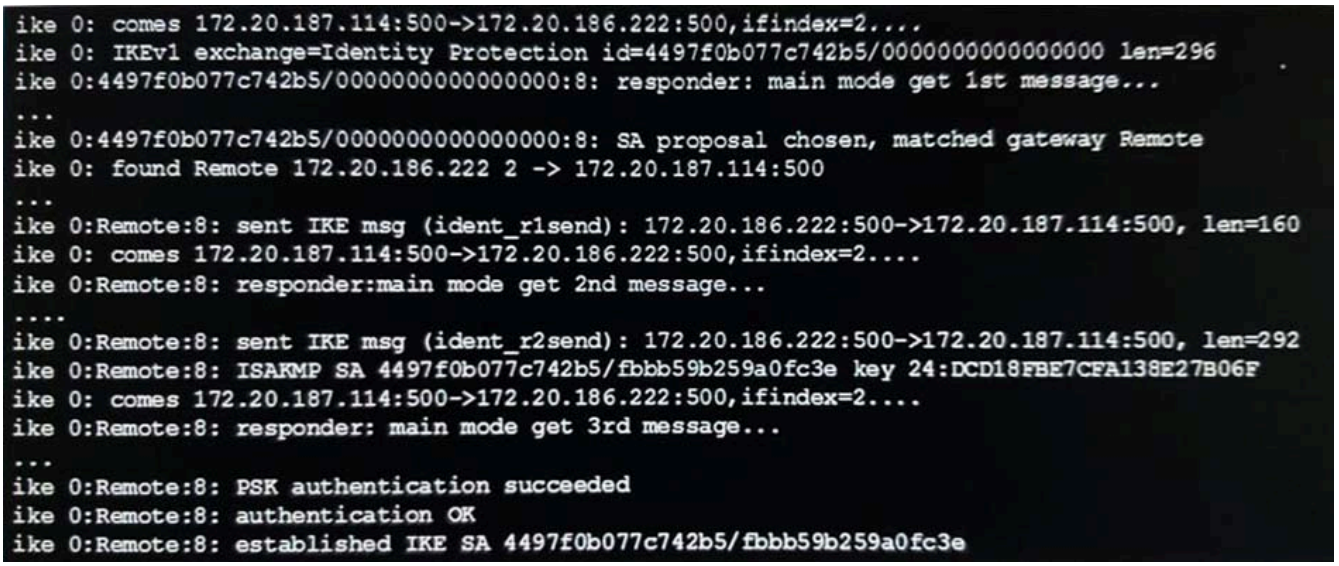
Ibrahimadwan Most Recent 3 years, 2 months ago

C is correct

upvoted 1 times

Question #51 *Topic 1*

Examine the exhibit, which shows the partial output of an IKE real-time debug.
Which of the following statement about the output is true?



A. The VPN is configured to use pre-shared key authentication.

B. Extended authentication (XAuth) was successful.

C. Remote is the host name of the remote IPsec peer.

D. Phase 1 went down.

Suggested Answer: *A*

Arc543 Most Recent 5 years, 8 months ago

Answer:A

upvoted 2 times