EXAMTOPICS

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



CERTIFICATION TEST

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

Question #1 *Topic 1*

What is the key benefit of Palo Alto Networks Single Pass Parallel Processing design?

A. There are no benefits other than slight performance upgrades

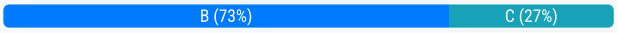
B. It allows Palo Alto Networks to add new functions to existing hardware

C. Only one processor is needed to complete all the functions within the box

D. It allows Palo Alto Networks to add new devices to existing hardware

Suggested Answer: *B*
Official Answer: B

Community vote distribution



pasan1986 Most Recent 1 year, 5 months ago
is this still valid? one comment says, its not valid?
upvoted 1 times

chenliang0301 2 years, 1 month ago
"Single Pass" >>> one processor
upvoted 1 times

ck19 2 years, 3 months ago
B is correct
upvoted 1 times

GohanF2 2 years, 5 months ago
The answer is C. Single pass parallel processing ensures the evualuation of app-ID , content-ID, user-ID per patcket in one single process. The hardware parallel processing which is divided in 3 platforms: data, control, and management is the one in charge to make the software process faster since each task is divided per platform. So, answer is still C.
upvoted 1 times

Majkiel 2 years, 7 months ago
https://www.paloaltonetworks.com/resources/whitepapers/single-pass-parallel-processing-architecture says: it enables high-throughput, low-latency network security, even while incorporating unprecedented features and technology "unprecedented features and technology" - so answer should be B."With our Single-Pass Architecture, Palo Alto Networks makes it possible to add a function to an NGFW instead of adding another security device"
upvoted 1 times

Majkiel 2 years, 7 months ago
https://www.paloaltonetworks.com/resources/whitepapers/single-pass-parallel-processing-architecture says: it enables high-throughput, low-latency network security, even while incorporating unprecedented features and technology

"unprecedented features and technology" - so answer should be B.
upvoted 1 times

wsdeffwd 2 years, 4 months ago
"With our Single-Pass Architecture, Palo Alto Networks makes it possible to add a function to an NGFW instead of adding another security device"
upvoted 1 times

fatehz 2 years, 11 months ago
C is wrong because their is a cpu for each layer in SP3
upvoted 2 times

LostatSea 3 years ago
B as C seams incorrect as there are multiple CPUs in every Firewall. If you read all functions as not just SP3 then you have the separate CPUs in Data & Control planes.
upvoted 1 times

Jusecas 3 years, 3 months ago
Commercialy is the most used argument

upvoted 3 times

AOtwoma 3 years, 9 months ago

correct

upvoted 3 times

Question #2 *Topic 1*

Which security profile on the NGFW includes signatures to protect you from brute force attacks?

A. Zone Protection Profile

B. URL Filtering Profile

C. Vulnerability Protection Profile

D. Anti-Spyware Profile

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

AOtwoma Most Recent 1 year, 9 months ago

Vulnerability Protection Profile

upvoted 3 times

Question #3 *Topic 1*

The need for a file proxy solution, virus and spyware scanner, a vulnerability scanner, and HTTP decoder for URL filtering is handled by which component in the
NGFW?

A. First Packet Processor

B. Stream-based Signature Engine

C. SIA (Scan It All) Processing Engine

D. Security Processing Engine

Suggested Answer: *B*
Reference: https://media.paloaltonetworks.com/documents/Single_Pass_Parallel_Processing_Architecture.pdfn (page 6)

Community vote distribution
B (100%)

admripper Most Recent 1 year, 9 months ago
C. The SIA (Scan It All) Processing Engine is the part of an NGFW that consolidates multiple security functionalities (e.g., antivirus, URL filtering, vulnerability scanning). It ensures comprehensive inspection to prevent threats while maintaining optimal performance.
upvoted 1 times

wsdeffwd 2 years, 4 months ago
The use of a stream-based engine replaces several components commonly used in other solutions: a file proxy for data, virus, and spyware; a signature engine for vulnerability exploits; and an HTTP decoder for URL filtering.
upvoted 1 times

mlj23 3 years, 9 months ago
Stream-based Signature Engine
upvoted 4 times

Question #4 *Topic 1*

A customer is looking for an analytics tool that uses the logs on the firewall to detect actionable events on the network. They require something to automatically process a series of related threat events that, when combined, indicate a likely compromised host on their network or some other higher level conclusion. They need to pinpoint the area of risk, such as compromised hosts on the network, allows you to assess the risk and take action to prevent exploitation of network resources.
Which feature of PAN-OS can you talk about to address their requirement to optimize their business outcomes?

A. The Automated Correlation Engine

B. Cortex XDR and Cortex Data Lake

C. WildFire with API calls for automation

D. 3rd Party SIEM which can ingest NGFW logs and perform event correlation

Suggested Answer: *A*
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/monitoring/use-the-automated-correlation-engine.html

Community vote distribution
A (100%)

jrugel Most Recent 1 year, 1 month ago
https://docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/monitor/monitor-automated-correlation-engine
upvoted 1 times

Majkiel 2 years, 1 month ago
why not cortex xdr? To address the customer's requirement for an analytics tool that uses firewall logs to detect actionable events on the network, automatically process a series of related threat events, and pinpoint areas of risk such as compromised hosts, you can talk about the Cortex XDR feature in PAN-OS.
upvoted 1 times

wsdeffwd 2 years, 4 months ago
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/monitoring/use-the-automated-correlation-engine
upvoted 1 times

nobody165456131354 2 years, 10 months ago
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-the-automated-correlation-engine
upvoted 1 times

Question #5 *Topic 1*

Which two email links, contained in SMTP and POP3, can be submitted from WildFire analysis with a WildFire subscription? (Choose two.)

A. FTP

B. HTTPS

C. RTP

D. HTTP

Suggested Answer: *B, D*
Official Answer: BD

onaicul Most Recent 1 year, 8 months ago

B and D are correct https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-concepts/email-link-analysis

upvoted 4 times

Question #6 *Topic 1*

What two types of certificates are used to configure SSL Forward Proxy? (I¡hoose two.)

A. Enterprise CA-signed certificates

B. Self-Signed certificates

C. Intermediate certificates

D. Private key certificates

Suggested Answer: *A, B*

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/configure-ssl-forward-proxy#:~:text=You%20can%20use%20an%20enterprise,as%20the%20forward%20trust%20certificate.&text=Certificate%20Name-,.,unique%20name%20for%20each%20firewall

Community vote distribution

AB (100%)

wsdeffwd Most Recent 1 year, 10 months ago

"You can use an enterprise CA-signed certificate or a self-signed certificate as the forward trust certificate."

upvoted 2 times

Question #7 *Topic 1*

Which two of the following does decryption broker provide on a NGFW? (Choose two.)

A. Decryption broker allows you to offload SSL decryption to the Palo Alto Networks next-generation firewall and decrypt traffic only once

B. Eliminates the need for a third party SSL decryption option which allows you to reduce the total number of third party devices performing analysis and enforcement

C. Provides a third party SSL decryption option which allows you to increase the total number of third party devices performing analysis and enforcement

D. Decryption broker allows you to offload SSL decryption to the Palo Alto Networks next-generation firewall and decrypt traffic multiple times

Suggested Answer: *A, B*

Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-broker.html

Community vote distribution

AB (100%)

scanossa Most Recent 1 year, 10 months ago

A & B https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-broker#:~:text=Decryption%20broker%20allows%20you%20to,party%20appliances)%20for%20additional%20enforcement.

upvoted 2 times

fatehz 1 year, 11 months ago

C is wrong because it's not a third party and D is wrong because it's done to avoid decryption multiple time

upvoted 1 times

yet_another_user 2 years, 1 month ago

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-broker

upvoted 1 times

Question #8 *Topic 1*

There are different Master Keys on Panorama and managed
firewalls.
What is the result if a Panorama Administrator pushes configuration to managed firewalls?

A. The push operation will fail regardless of an error or not within the configuration itself

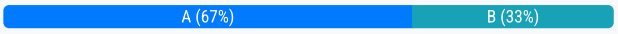
B. Provided there's no error within the configuration to be pushed, the push will succeed

C. The Master Key from the managed firewalls will be overwritten with the Master Key from Panorama

D. There will be a popup to ask if the Master Key from the Panorama should replace the Master Key from the managed firewalls

Suggested Answer: *A*
Reference: https://www.reddit.com/r/paloaltonetworks/comments/onz15y/what_is_the_result_if_a_panorama_administrator/

Community vote distribution



Rootinho Most Recent 1 year, 1 month ago
A is the right answer
upvoted 1 times

555b305 1 year, 8 months ago
The answer is definitely A): https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNvrCAG
upvoted 1 times

admripper 1 year, 8 months ago
The correct answer is: B. Provided there's no error within the configuration to be pushed, the push will succeed. Explanation: The Master Key on Panorama and managed firewalls does not affect the ability to push configuration changes. Panorama uses secure communication channels to manage firewalls, but the Master Key is specific to encrypting sensitive data (such as passwords and private keys) within a device. As long as there are no configuration errors, Panorama can push configurations successfully, even if the Master Key values differ between Panorama and the managed firewalls. However, the Master Key settings themselves are not pushed from Panorama to the managed firewalls during configuration pushes.
upvoted 1 times

44d0262 2 years ago
A is correct. No, this would not result in a commit error. The study guide mentions that "Administrators can commit or revert changes they make in a Panorama configuration independently of changes made by other administrators." This means that even if the master keys are not synced, the configuration push itself will not fail. The only issue would be that encrypted settings would not be updated. The commit would be successful, but the desired changes to the encrypted settings would not take effect on the managed firewalls until the master keys are synced.
upvoted 1 times

Question #9 *Topic 1*

Which task would be identified in Best Practice Assessment tool?

A. identify the visibility and presence of command-and-control sessions

B. identify sanctioned and unsanctioned SaaS applications

C. identify the threats associated with each application

D. identify and provide recommendations for device management access

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

4l3x122333444 Highly Voted 3 years, 5 months ago
I think this is D, https://www.paloaltonetworks.com/content/dam/pan/en_US/partners/nextwave/bpa/best-practice-assessment.pdf
upvoted 7 times

ck19 Most Recent 1 year, 9 months ago
Answer is D
upvoted 1 times

GohanF2 1 year, 11 months ago
Answer A is wrong. Correct answer is : B. BPA only works as a guidance in the current security industry standard regulations , it will provide recommendations on areas where we can improve the security on different zones, interfaces, policy rules and finally give us a total of percent that represents the level of compliance with the market standards.
upvoted 2 times

onaicul 2 years, 2 months ago
D is correcthttps://www.paloaltonetworks.com/services/bpa
upvoted 2 times

onaicul 2 years, 2 months ago
D is correct
upvoted 2 times

onaicul 2 years, 2 months ago
https://www.paloaltonetworks.com/services/bpa
upvoted 1 times

ArangoTopics 2 years, 7 months ago
https://docs.paloaltonetworks.com/best-practices/10-2/bpa-getting-started/evaluate-security-policy-capability-adoption
upvoted 2 times

ITime 2 years, 7 months ago
D is correct
upvoted 2 times

Jusecas 2 years, 9 months ago
D is correct, the main funtion of BPA is checking how the configuration works compared with best configuration practice lines of PA networks, and with this, formulate recommendations
upvoted 3 times

TheMaster01 2 years, 11 months ago
D is corrrect; BPA only checks your configurations against a baseline config
upvoted 4 times

gordonF 3 years ago
B is correct https://www.youtube.com/watch?v=LwElz1Hgu_MThe answer is D, I saw the video that you share but at no time do they talk about BPA, BPA is attached to showing improvements in the configuration, it has nothing to do with application identification, application identification is part of APP ID no from BPA
upvoted 1 times

gordonF 3 years ago

B is correct https://www.youtube.com/watch?v=LwElz1Hgu_M

upvoted 1 times

rmm1087 2 years, 9 months ago

The answer is D, I saw the video that you share but at no time do they talk about BPA, BPA is attached to showing improvements in the configuration, it has nothing to do with application identification, application identification is part of APP ID no from BPA

upvoted 3 times

Question #10 *Topic 1*

A customer requests that a known spyware threat signature be triggered based on a rate of occurrence, for example, 10 hits in 5 seconds.
How is this goal accomplished?

A. Create a custom spyware signature matching the known signature with the time attribute

B. Add a correlation object that tracks the occurrences and triggers above the desired threshold

C. Submit a request to Palo Alto Networks to change the behavior at the next update

D. Configure the Anti-Spyware profile with the number of rule counts to match the occurrence frequency

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (55%) B (45%)

Jazzadub Most Recent 1 year ago
This is definitely A - I have just confirmed on Panorama that it is NOT possible to add custom Correlation Objects.
upvoted 1 times

jrugel 1 year, 1 month ago
Las firmas personalizadas se centran más en el patrón de la amenaza en sí, no en su frecuencia. La correlación de eventos (Correlation Objects) es precisamente la característica en los firewalls de Palo Alto Networks que te permite definir reglas basadas en la ocurrencia de múltiples eventos o un solo evento repetido dentro de un marco de tiempo específico.
upvoted 1 times

milkyway2000 2 years, 1 month ago
A is correct, checked in lab, what VenomX51 is saying is true.
upvoted 2 times

VenomX51 2 years, 1 month ago
The answer is A This is exactly how brute force threat ID is triggered. It watches a separate threat ID (failed auth attempt, which is an alert by default), and has a time event that if that monitored threat ID is triggered x times in y seconds by the same source IP, then the brute force threat is triggered, and can then take a different action such as block IP. You would create a custom spyware profile to do the same; trigger when x has occurred y times in z seconds. A correlation object does not trigger anything. It pulls data from multiple sources and can create a log entry when it's defined conditions are met.
upvoted 2 times

MaxG 2 years, 1 month ago
To trigger a known spyware threat signature based on a rate of occurrence (e.g., 10 hits in 5 seconds), you need to add a correlation object that tracks the occurrences and triggers an alert or action when the specified threshold is met. This correlation object monitors the frequency of the spyware signatures and ensures that action is taken only when the threshold is exceeded, providing more granular control over threat detection and response. References: Palo Alto Networks Threat Prevention and Correlation Objects documentation.
upvoted 2 times

Jerar 2 years, 2 months ago
A is correct, see the link from nobody165456131354
upvoted 1 times

davidpm 2 years, 3 months ago
Correct answer it´s b B. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-the-automated-correlation-engine/automated-correlation-engine-concepts/correlation-object
upvoted 2 times

nobody165456131354 2 years, 10 months ago
https://docs.paloaltonetworks.com/pan-os/u-v/custom-app-id-and-threat-signatures/custom-application-and-threat-signatures/create-a-custom-threat-signature/create-a-combination-signature
upvoted 4 times

Question #11 *Topic 1*

Which two features are found in Palo Alto Networks NGFW but are absent in a legacy firewall product? (Choose two.)

A. Policy match is based on application

B. Traffic control is based on IP, port, and protocol

C. Traffic is separated by zones

D. Identification of application is possible on any port

Suggested Answer: *A, D*

Official Answer: AD

Community vote distribution

AD (100%)

Majkiel Most Recent 2 years, 2 months ago

B and C are legacy

upvoted 2 times

fatehz 2 years, 11 months ago

AD because B and C are the characteristics of legacy firewall

upvoted 4 times

Question #12 *Topic 1*

For customers with high bandwidth requirements for Service Connections, what two limitations exist when onboarding multiple Service Connections to the same Prisma Access location servicing a single Datacenter? (Choose two.)

A. Network segments in the Datacenter need to be advertised to only one Service Connection

B. The customer edge device needs to support policy-based routing with symmetric return functionality

C. The resources in the Datacenter will only be able to reach remote network resources that share the same region

D. A maximum of four service connections per Datacenter are supported with this topology

Suggested Answer: *A, B*

Official Answer: AB

Community vote distribution



dschout Most Recent 2 years, 1 month ago

It is A & B D is incorrect it is specifically stated that: "Prisma Access does not limit the maximum number of service connections you can onboard to a single headquarters or data center remote network location." https://docs.paloaltonetworks.com/prisma/prisma-access/3-2/prisma-access-panorama-admin/prisma-access-advanced-deployments/service-connection-advanced-deployments/create-a-high-bandwidth-network-using-multiple-service-connections

upvoted 2 times

LostatSea 3 years ago

yet_another_user article correct as well as Faam13

upvoted 1 times

ArangoTopics 3 years, 1 month ago

Correct AB. Refer to step 2: https://docs.paloaltonetworks.com/prisma/prisma-access/3-2/prisma-access-panorama-admin/prisma-access-advanced-deployments/service-connection-advanced-deployments/create-a-high-bandwidth-network-using-multiple-service-connections/create-a-high-bandwidth-connection-to-a-headquarters-or-data-center-location

upvoted 4 times

yet_another_user 3 years, 2 months ago

Refer to step 5, PBR: https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-advanced-deployments/service-connection-advanced-deployments/create-a-high-bandwidth-network-using-multiple-service-connections/configure-more-than-two-service-connections-to-a-headquarters-or-data-center-location So A and B are correct, see also Link from faam13

upvoted 1 times

Jusecas 3 years, 3 months ago

A and B are correct, you must guarantee correct routing adversiment between dc and the sc

upvoted 1 times

faam13 3 years, 4 months ago

answer is A & B. https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/create-a-high-bandwidth-network-using-multiple-service-connections.html

upvoted 2 times

cojotti 3 years, 7 months ago

A & C are correct

upvoted 1 times

Question #13 *Topic 1*

Which three categories are identified as best practices in the Best Practice Assessment tool? (Choose three.)

A. use of device management access and settings

B. identify sanctioned and unsanctioned SaaS applications

C. expose the visibility and presence of command-and-control sessions

D. measure the adoption of URL filters, App-ID, User-ID

E. use of decryption policies

Suggested Answer: *A, D, E*

Official Answer: ADE

Community vote distribution

ADE (100%)

mushi4ka Highly Voted 3 years, 4 months ago

I think that A is correct.

upvoted 9 times

ck19 Most Recent 1 year, 9 months ago

ADE are correct

upvoted 1 times

LostatSea 2 years, 6 months ago

ADE correct

upvoted 1 times

ArangoTopics 2 years, 7 months ago

https://docs.paloaltonetworks.com/best-practices/10-2/bpa-getting-started/evaluate-security-policy-capability-adoption

upvoted 2 times

yet_another_user 2 years, 8 months ago

Only A, D and E make sense

upvoted 1 times

TheMaster01 2 years, 11 months ago

A, D and E are correct

upvoted 3 times

Question #14 *Topic 1*

You have a prospective customer that is looking for a way to provide secure temporary access to contractors for a designated period of time. They currently add contractors to existing user groups and create ad hoc policies to provide network access. They admit that once the contractor no longer needs access to the network, administrators are usually too busy to manually delete policies that provided access to the contractor. This has resulted in over-provisioned access that has allowed unauthorized access to their systems.
They are looking for a solution to automatically remove access for contractors once access is no longer required.
You address their concern by describing which feature in the NGFW?

A. Dynamic User Groups

B. Dynamic Address Groups

C. Multi-factor Authentication

D. External Dynamic Lists

Suggested Answer: *A*
Official Answer: A

onaicul Most Recent 2 years, 2 months ago

A is true - https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups

upvoted 3 times

Question #15 *Topic 1*

Which methods are used to check for Corporate Credential Submissions? (Choose three.)

A. Group Mapping

B. IP User Mapping

C. LDAP query

D. Domain Credential Filter

E. User ID Credential Check

Suggested Answer: *A, B, D*
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/methods-to-check-for-corporate-credential- submissions.html#id29eff481-13de-45b9-b73c-83e2e932ba20

mushi4ka Highly Voted 3 years, 4 months ago
Correct: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/methods-to-check-for-corporate-credential-submissions
upvoted 11 times

onaicul Most Recent 2 years, 2 months ago
ABD is true
upvoted 2 times

nobody165456131354 2 years, 4 months ago
correct : https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-features/credential-phishing-prevention/methods-to-check-for-corporate-credential-submissions
upvoted 2 times

Question #16 *Topic 1*

WildFire subscription supports analysis of which three types? (Choose three.)

A. GIF

B. 7-Zip

C. Flash

D. RPM

E. ISO

F. DMG

Suggested Answer: *B, C, F*

Official Answer: BCF

Community vote distribution

BCF (100%)

dnhan Highly Voted 2 years, 8 months ago

BCF for sure, refer to: https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-concepts/file-analysis

upvoted 10 times

nobody165456131354 Most Recent 1 year, 10 months ago

BCF new link : https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-concepts/file-analysis

upvoted 3 times

LostatSea 2 years ago

BCF correct

upvoted 1 times

yet_another_user 2 years, 1 month ago

See Link from dnhan

upvoted 1 times

Jusecas 2 years, 3 months ago

flash it's not a valid format

upvoted 1 times

gordonF 2 years, 6 months ago

BCF correct

upvoted 2 times

Question #17 *Topic 1*

The WildFire Inline Machine Learning is configured using which Content-ID profiles?

A. Antivirus Profile

B. WildFire Analysis Profile

C. Threat Prevention Profile

D. File Blocking Profile

Suggested Answer: *A*
Reference: https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/wildfire-features/configure-wildfire-inline-ml.html

mushi4ka Highly Voted 2 years, 10 months ago
Correct: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/wildfire-inline-ml/configure-wildfire-inline-ml
upvoted 6 times

fatehz Most Recent 1 year, 11 months ago
A and you will find the WF signature in the antivirus profile
upvoted 1 times

Question #18 *Topic 1*

In an HA pair running Active/Passive mode, over which interface do the dataplanes communicate?

A. HA3

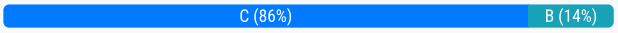
B. HA1

C. HA2

D. HA4

Suggested Answer: *C*
Official Answer: C

Community vote distribution



fatehz 2 years, 11 months ago

C is correct. The firewalls in an HA pair use HA links to synchronize data and maintain state information. Some models of the firewall have dedicated HA ports—Control link (HA1) and Data link (HA2), while others require you to use the in-band ports as HA links.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links

upvoted 3 times

renanshenrique 3 years ago

Selected Answer: B

From Palo Alto 48. Which dedicated HA port is used for which plane in HA pairs? a. HA1 for the data plane, and HA2 for the management plane (V) b. HA1 for the management plane, and HA2 for the data plane c. MGT for the management plane and HA2 as a backup d. HA1 for the management plane and HA2 for the data plane in the PA-7000 Series

upvoted 1 times

renanshenrique 3 years ago

From Palo Alto 48. Which dedicated HA port is used for which plane in HA pairs? a. HA1 for the data plane, and HA2 for the management plane (V) b. HA1 for the management plane, and HA2 for the data plane c. MGT for the management plane and HA2 as a backup d. HA1 for the management plane and HA2 for the data plane in the PA-7000 Seriesthe study guide is wrong...

upvoted 1 times

dschout Most Recent 2 years, 1 month ago

the study guide is wrong...

upvoted 1 times

yet_another_user 3 years, 2 months ago

Answer C is correct, see also: https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/device/device-high-availability/ha-communications

upvoted 2 times

DarioT 3 years, 4 months ago

From: https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/network/network-interfaces/ha-interface Each high availability (HA) interface has a specific function: one interface is for configuration synchronization and heartbeats, and the other interface is for state synchronization. That means that HA2 is the correct answer.

upvoted 3 times

Question #19 *Topic 1*

A potential customer requires an NGFW solution which enables high-throughput, low-latency network security, all while incorporating unprecedented features and technology. They need a solution that solves the performance problems that plague today's security infrastructure.
Which aspect of the Palo Alto Networks NGFW capabilities can you highlight to help them address the requirements?

A. SP3 (Single Pass Parallel Processing)

B. GlobalProtect

C. Threat Prevention

D. Elastic Load Balancers

Suggested Answer: *A*
Reference: https://www.paloguard.com/SP3-Architecture.asp

Community vote distribution
A (100%)

fatehz Most Recent 1 year, 11 months ago
A is correct.
upvoted 3 times

Question #20 *Topic 1*

What filtering criteria is used to determine what users to include as members of a dynamic user group?

A. Tags

B. Login IDs

C. Security Policy Rules

D. IP Addresses

Suggested Answer: *A*

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups

Community vote distribution

A (100%)

nobody165456131354 Most Recent 1 year, 9 months ago

https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-web-interface-help/objects/objects-dynamic-user-groups

upvoted 1 times

fatehz 1 year, 11 months ago

A tags of course for dag and dug

upvoted 1 times

Question #21 *Topic 1*

Which three features are used to prevent abuse of stolen credentials? (Choose three.)

A. multi-factor authentication

B. URL Filtering Profiles

C. WildFire Profiles

D. Prisma Access

E. SSL decryption rules

Suggested Answer: *A, B, E*
Official Answer: ABE

Community vote distribution
ABE (90%)

AOtwoma Highly Voted 3 years, 9 months ago
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up-credential-phishing-prevention#idc77030dc-6022-4458-8c50-1dc0fe7cffe4
upvoted 10 times

Hikmat Most Recent 1 year, 9 months ago
SSL decryption is used for to decrypt the traffic and check whether there is credential inside it or not. So, A, B and E are correct answers.
upvoted 1 times

dthensley 2 years, 1 month ago
ABC are the correct answers. https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-delivers-industry-first-capabilities-to-prevent-credential-theft-and-abuse
upvoted 2 times

ck19 2 years, 3 months ago
ABE are correct
upvoted 1 times

Gabranch 2 years, 3 months ago
Conflicted but the press release for PAN-OS 8.0 shows WF as a component to recofnizing and blocking phishing sites, preventing credential abuse: https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-delivers-industry-first-capabilities-to-prevent-credential-theft-and-abuse
upvoted 2 times

cheatface 2 years, 9 months ago
Agreed, it's ABE
upvoted 1 times

fatehz 2 years, 11 months ago
Selected Answer: ABE
Agree with others ABE, C with wildfire is wrong WF is a sandbox
upvoted 1 times

fatehz 2 years, 11 months ago
Agree with others ABE, C with wildfire is wrong WF is a sandboxWF scans email for http/https links to phishing sites.
upvoted 1 times

Gabranch 2 years, 3 months ago
WF scans email for http/https links to phishing sites.
upvoted 1 times

LostatSea 3 years ago
ABE, Agree with others
upvoted 1 times

yet_another_user 3 years, 2 months ago
Agree with A, B and E. Wildfire delivers input for PAN-DB which feeds the URL catalog, but see the steps in links below.

upvoted 2 times

mushi4ka 3 years, 10 months ago

Multi Factor Authentication, URL filter, SSL Decryption https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing

upvoted 4 times

Question #22 *Topic 1*

A customer has business-critical applications that rely on the general web-browsing application. Which security profile can help prevent drive-by-downloads while still allowing web-browsing traffic?

A. File Blocking Profile

B. DoS Protection Profile

C. URL Filtering Profile

D. Vulnerability Protection Profile

Suggested Answer: *A*

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjaw53CvdHyAhUPy4UKHXT5D-MQFnoECAMQAQ&url=https%3A%2F%2Fknowledgebase.paloaltonetworks.com%2Fservlet%2FfileField%3FentityId%3Dka10g000000U0roAAC%26field%3DAttachment_1__Body__s&usg=AOvVaw3DCBM7-FwWInkWYANLrzUt (32)

Community vote distribution

A (100%)

fatehz Most Recent 1 year, 11 months ago

A all other answer are wrong

upvoted 2 times

yet_another_user 2 years, 1 month ago

Answer A: https://docs.paloaltonetworks.com/network-security/security-policy/security-profiles/security-profile-file-blocking

upvoted 2 times

Question #23 *Topic 1*

Which three settings must be configured to enable Credential Phishing Prevention?
(Choose three.)

A. validate credential submission detection

B. enable User-ID

C. define an SSL decryption rulebase

D. define URL Filtering Profile

E. Enable App-ID

Suggested Answer: *B, C, D*
Official Answer: BCD

Community vote distribution
BCD (100%)

ck19 Most Recent 1 year, 9 months ago
BCD are correct
upvoted 1 times

bmarks 2 years, 3 months ago
NEW LINK : https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-features/credential-phishing-prevention/set-up-credential-phishing-prevention PAN Doc explains why BCD is correct
upvoted 2 times

luismendes21 2 years, 4 months ago
Agree with others
upvoted 2 times

LostatSea 2 years, 6 months ago
BCD, Agree with others
upvoted 1 times

yet_another_user 2 years, 8 months ago
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/prevent-credential-phishing/set-up-credential-phishing-prevention
upvoted 1 times

JM1313 2 years, 8 months ago
PAN-OS Administrator's Guide—Prevent Credential Phishing, https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/prevent-credential -phishing.html
upvoted 2 times

AOtwoma 3 years, 3 months ago
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up-credential-phishing-prevention#idc77030dc-6022-4458-8c50-1dc0fe7cffe4
upvoted 4 times

mushi4ka 3 years, 4 months ago
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up-credential-phishing-prevention
upvoted 4 times

Question #24 *Topic 1*

A customer with a legacy firewall architecture is focused on port and protocol level security, and has heard that next generation firewalls open all ports by default.
What is the appropriate rebuttal that positions the value of a NGFW over a legacy firewall?

A. Palo Alto Networks does not consider port information, instead relying on App-ID signatures that do not reference ports

B. Default policies block all interzone traffic. Palo Alto Networks empowers you to control applications by default ports or a configurable list of approved ports on a per-policy basis

C. Palo Alto Networks keep ports closed by default, only opening ports after understanding the application request, and then opening only the application- specified ports

D. Palo Alto Networks NGFW protects all applications on all ports while leaving all ports opened by default

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

LabDan123 Most Recent 1 year, 1 month ago
B is Correct
upvoted 1 times

fatehz 1 year, 11 months ago
B is true, C is wrong because it's say that he open the app ports only and it's wrong i can run an application on another not default port and it ll work.
upvoted 2 times

LostatSea 2 years ago
B and not C as "only opening ports after understanding the application request", the Palo Alto's can function as a layer 3 firewall based solely on port and no need to understand the application e.g unknown-tcp
upvoted 1 times

yet_another_user 2 years, 1 month ago
Read the answers a few times, B and C is valid, can't distinguished. Each firewall blocks interzone traffic, not specific to PA.
upvoted 1 times

madinaes 2 years, 3 months ago
B is correct as a best practice also
upvoted 2 times

madinaes 2 years, 3 months ago
B is correct as a best practice alsoBut the question is about Ports, that PA keeps all ports open by default so C is correct as an answer to this specific question.But Interzone ports are closed by default, so not all ports are open
upvoted 2 times

madinaes 2 years, 3 months ago
But the question is about Ports, that PA keeps all ports open by default so C is correct as an answer to this specific question.
upvoted 1 times

madinaes 2 years, 3 months ago
But the question is about Ports, that PA keeps all ports open by default so C is correct as an answer to this specific question.But Interzone ports are closed by default, so not all ports are open
upvoted 1 times

scanossa 1 year, 10 months ago
But Interzone ports are closed by default, so not all ports are open
upvoted 1 times

AOtwoma 2 years, 9 months ago
Practically, B is correct
upvoted 3 times

mushi4ka 2 years, 10 months ago

B is better

upvoted 3 times

Question #25 *Topic 1*

Which four actions can be configured in an Anti-Spyware profile to address command-and-control traffic from compromised hosts? (Choose four.)

A. Reset

B. Quarantine

C. Drop

D. Allow

E. Redirect

F. Alert

Suggested Answer: *A, C, D, F*

Official Answer: ACDF

Community vote distribution

ACDF (100%)

ck19 Most Recent 1 year, 9 months ago

ACDF are correct

upvoted 1 times

onaicul 2 years, 2 months ago

ACDF is true - https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-anti-spyware

upvoted 3 times

luismendes21 2 years, 4 months ago

CORRECT

upvoted 1 times

DarioT 2 years, 10 months ago

Correct

upvoted 3 times

Question #26 *Topic 1*

What are three valid sources that are supported for user IP address mapping in Palo Alto Networks NGFW? (Choose three.)

A. RADIUS

B. Client Probing

C. Lotus Domino

D. Active Directory monitoring

E. TACACS

F. eDirectory monitoring

Suggested Answer: *B, D, F*
Official Answer: BDF

Community vote distribution
BDF (100%)

k3rnelpanicpj Highly Voted 2 years, 9 months ago
Correct BDF: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-overview
upvoted 8 times

Eiffelsturm Most Recent 1 year, 10 months ago
correct
upvoted 1 times

Question #27 *Topic 1*

Which CLI allows you to view the names of SD-WAN policy rules that send traffic to the specified virtual SD-WAN interface, along with the performance metrics?

A. >show sdwan connection all |

B. >show sdwan path-monitor stats vif

C. >show sdwan rule vif sdwan.x

D. >show sdwan session distribution policy-name

Suggested Answer: *C*

Reference: https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-tasks.html

Community vote distribution

C (100%)

onaicul Most Recent 2 years, 2 months ago

C is true

upvoted 1 times

Doobiedoo 2 years, 9 months ago

C is correct.

upvoted 2 times

mushi4ka 3 years, 4 months ago

Correct: https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-tasks

upvoted 1 times

Question #28 *Topic 1*

Which two actions can be taken to enforce protection from brute force attacks in the security policy? (Choose two.)

A. Create a log forwarding object to send logs to Panorama and a third-party syslog server event correlation

B. Install content updates that include new signatures to protect against emerging threats

C. Attach the vulnerability profile to a security rule

D. Add the URL filtering profile to a security rule

Suggested Answer: *B, C*

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-brute-force-attacks.html

Community vote distribution

BC (100%)

KeppraXR Most Recent 1 year, 1 month ago

https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/configure-threat-prevention/prevent-brute-force-attacks

upvoted 1 times

onaicul 2 years ago

Yes, B and C : https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-brute-force-attacks

upvoted 4 times

Question #29 *Topic 1*

A customer is concerned about zero-day targeted attacks against its intellectual property.
Which solution informs a customer whether an attack is specifically targeted at them?

A. Cortex XDR Prevent

B. AutoFocus

C. Cortex XSOAR Community edition

D. Panorama Correlation Report

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

Nomet 1 year, 12 months ago
https://www.paloaltonetworks.com/resources/datasheets/autofocus-threat-intelligence
upvoted 2 times

onaicul 2 years, 2 months ago
B Autofocus - https://docs.paloaltonetworks.com/autofocus
upvoted 2 times

McMarius11 2 years, 4 months ago
Its B Boyz
upvoted 3 times

fatehz 2 years, 5 months ago
I think its B bacause autofocus has information about threads
upvoted 1 times

yet_another_user 2 years, 8 months ago
Assume B. Autofocus is EoS but not EoL, see: https://live.paloaltonetworks.com/t5/blogs/autofocus-end-of-sale-faq-and-alternatives/ba-p/516051
upvoted 3 times

yet_another_user 2 years, 8 months ago
Assume B. Autofocus is EoS but not EoL, see: https://live.paloaltonetworks.com/t5/blogs/autofocus-end-of-sale-faq-and-alternatives/ba-p/516051EOL that's September 30, 2025.
upvoted 3 times

KeppraXR Most Recent 1 year, 1 month ago
EOL that's September 30, 2025.
upvoted 1 times

rockyshenc 3 years ago
B shall be correct.
upvoted 2 times

rockyshenc 3 years ago
B shall be correct.autofocus is no more.
upvoted 2 times

gordonF 3 years ago
autofocus is no more.
upvoted 2 times

Question #30 *Topic 1*

Which three actions should be taken before deploying a firewall evaluation unit in the customer's environment? (Choose three.)

A. Reset the evaluation unit to factory default to ensure that data from any previous customer evaluation is removed

B. Request that the customer make port 3978 available to allow the evaluation unit to communicate with Panorama

C. Upgrade the evaluation unit to the most current recommended firmware, unless a demo of the upgrade process is planned

D. Inform the customer that they will need to provide a SPAN port for the evaluation unit assuming a TAP mode deployment

E. Set expectations around which information will be presented in the Security Lifecycle Review because sensitive information may be made visible

Suggested Answer: *A, C, D*
Official Answer: ACD

Community vote distribution
ACD (100%)

fatehz Most Recent 1 year, 11 months ago
ACD are correct
upvoted 1 times

Xyn 2 years, 3 months ago
Panorama is not required for evaluation so B is out. There is no confidential data on SLR result since it's all just summarized metadata so E is also out
upvoted 2 times

Question #31 *Topic 1*

Which three activities can the botnet report track? (Choose three.)

A. Accessing domains registered in the last 30 days

B. Visiting a malicious URL

C. Launching a P2P application

D. Detecting malware within a one-hour period

E. Initiating API calls to other applications

F. Using dynamic DNS domain providers

Suggested Answer: *A, B, F*

Official Answer: ABF

Community vote distribution

ABF (100%)

dnhan Highly Voted 3 years, 8 months ago

ABF, refer to the link: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage-reports/generate-botnet-reports

upvoted 7 times

cb4251b Most Recent 2 years, 1 month ago

ABF looks correct.

upvoted 1 times

ck19 2 years, 3 months ago

ABF are correct

upvoted 1 times

JJ_512 2 years, 3 months ago

The botnet report enables you to use heuristic and behavior-based mechanisms to identify potential malware- or botnet-infected hosts in your network. To evaluate botnet activity and infected hosts, the firewall correlates user and network activity data in Threat, URL, and Data Filtering logs with the list of malware URLs in PAN-DB, known dynamic DNS domain providers, and domains registered within the last 30 days.

upvoted 2 times

Mohamad_Seifeldine 2 years, 7 months ago

acf it should be acf

upvoted 1 times

luismendes21 2 years, 10 months ago

should be abf

upvoted 1 times

LostatSea 3 years ago

ABF, To evaluate botnet activity and infected hosts, the firewall correlates user and network activity data in Threat, URL, and Data Filtering logs with the list of malware URLs in PAN-DB, known dynamic DNS domain providers, and domains registered within the last 30 days

upvoted 1 times

f143c37 3 years, 1 month ago

should be ABF

upvoted 1 times

Question #32 *Topic 1*

A customer requires protections and verdicts for PE (portable executable) and ELF (executable and linkable format) as well as integration with products and services can also access the immediate verdicts to coordinate enforcement to prevent successful attacks.
What competitive feature does Palo Alto Networks provide that will address this requirement?

A. File Blocking Profile

B. Dynamic Unpacking

C. WildFire

D. DNS Security

Suggested Answer: *C*
Reference: https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud-features/real-time-wildfire-verdicts-and-signatures-for-pe-and-elf- files.html

Community vote distribution
C (100%)

KeppraXR Most Recent 1 year, 1 month ago
https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud-features/real-time-wildfire-verdicts-and-signatures-for-pe-and-elf-files
upvoted 1 times

ironman_86 1 year, 9 months ago
C is correct
upvoted 2 times

Question #33 *Topic 1*

Which statement is true about Deviating Devices and metrics?

A. A metric health baseline is determined by averaging the health performance for a given metric over seven days plus the standard deviation

B. Deviating Device Tab is only available with a SD-WAN Subscription

C. An Administrator can set the metric health baseline along with a valid standard deviation

D. Deviating Device Tab is only available for hardware-based firewalls

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

kei_chige Most Recent 2 years ago

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PN4TCAW

upvoted 3 times

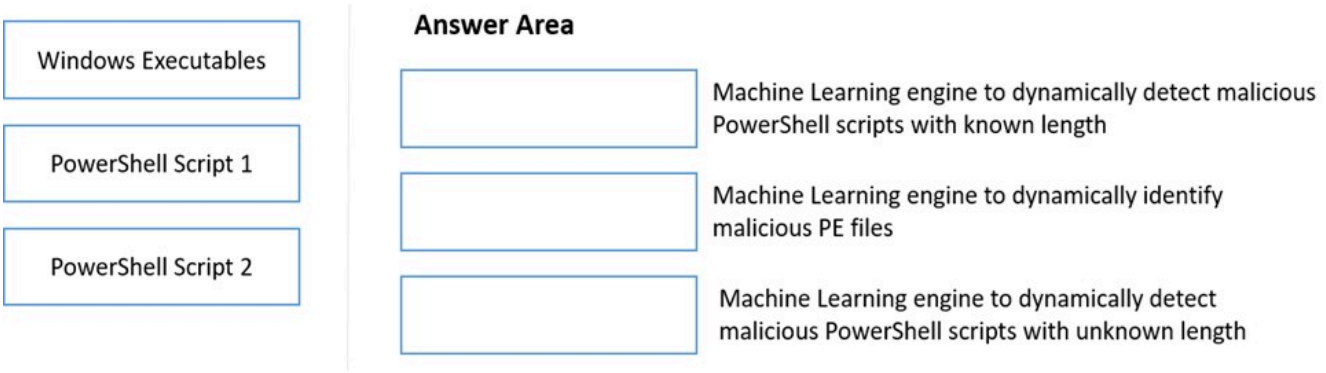
Question #34 *Topic 1*

DRAG DROP

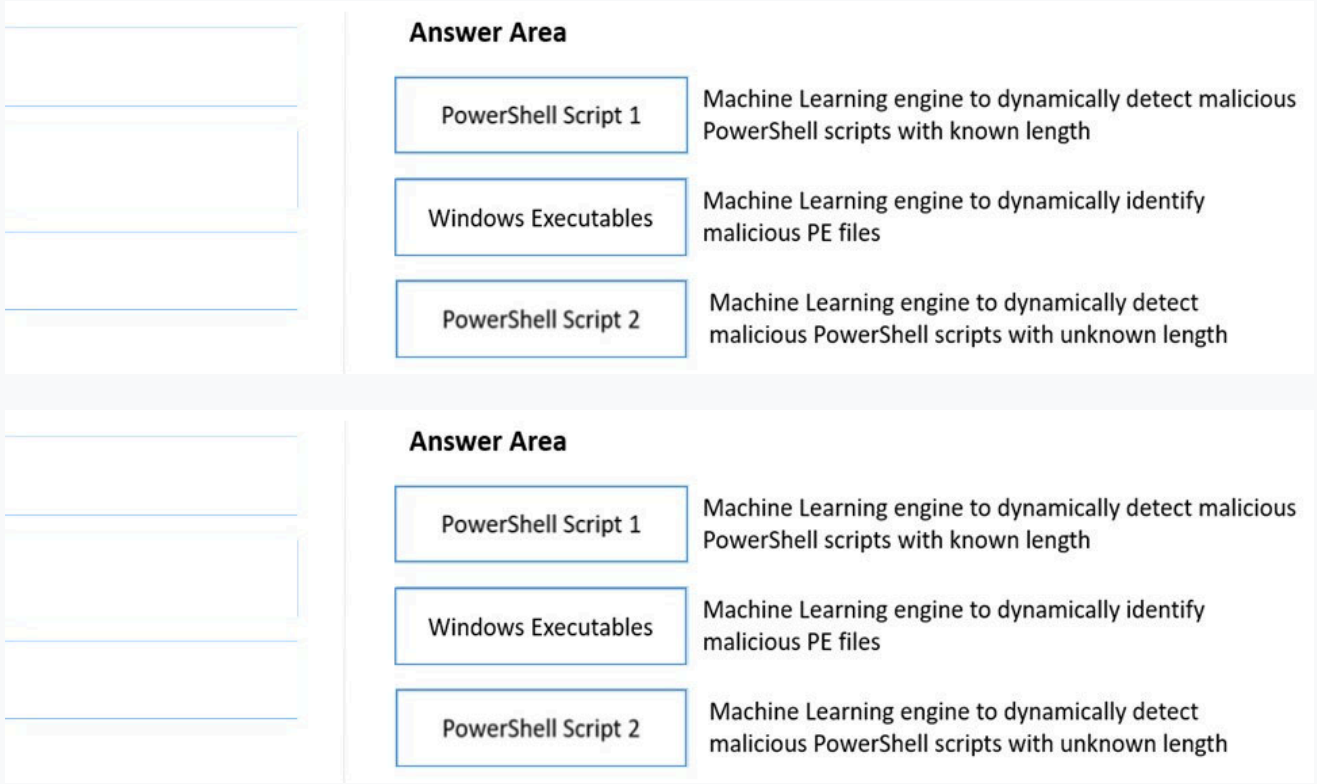
-

Match the WildFire Inline Machine Learning Model to the correct description for that model.

Select and Place:



Suggested Answer:



Reference: https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos-100/configure-wildfire-inline-ml.html

fatehz Most Recent 1 year, 11 months ago

correct and the source : https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos-100/configure-wildfire-inline-ml

upvoted 3 times

Question #35 *Topic 1*

Palo Alto Networks publishes updated Command-and-Control signatures.
How frequently should the related signatures schedule be set?

A. Once an hour

B. Once a day

C. Once a week

D. Once every minute

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

ck19 Most Recent 1 year, 9 months ago
B is correct
upvoted 1 times

kei_chige 2 years ago
I agree with madinaes
upvoted 1 times

ArangoTopics 2 years, 7 months ago
Antivirus updates are released every 24 hours
upvoted 1 times

yet_another_user 2 years, 7 months ago
See madinaes link below
upvoted 2 times

yet_another_user 2 years, 8 months ago
Agree with madinaes, refer to the Link below
upvoted 2 times

gordonF 3 years ago
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/software-and-content-updates/dynamic-content-updates#:~:text=(Requires%20Threat%20Prevention)%20Automatically%2Dgenerated%20command%2Dand%2Dcontrol%20(C2)%20signatures%20that%20detect%20certain%20patterns%20in%20C2%20traffic.%20These%20signatures%20enable%20the%20firewall%20to%20detect%20C2%20activity%20even%20when%20the%20C2%20host%20is%20unknown%20or%20changes%20rapidly. B is correct
upvoted 3 times

23casper23 3 years, 3 months ago
One day should be correct
upvoted 3 times

Question #36 *Topic 1*

Which two methods will help avoid Split Brain when running HA in Active/Active mode?
(Choose two.)

A. Configure a Backup HA1 Interface

B. Configure a Heartbeat Backup

C. Create a loopback IP address and use that as a Source Interface

D. Place your management interface in an Aggregate Interface Group configuration

Suggested Answer: *A, B*
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/set-up-activeactive-ha/configure-activeactive-ha.html

Community vote distribution
AB (100%)

KeppraXR Most Recent 1 year, 1 month ago
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/high-availability/set-up-activeactive-ha/configure-activeactive-ha
upvoted 1 times

ck19 1 year, 9 months ago
AB are correct
upvoted 1 times

kei_chige 2 years ago
The split-brain conditions can be prevented by configuring the "HA1" backup-link and enabling heartbeat backup.
upvoted 1 times

onaicul 2 years ago
yes, A and B : https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSuCAK
upvoted 2 times

Question #37 *Topic 1*

Which three script types can be analyzed in WildFire? (Choose three.)

A. JScript

B. PythonScript

C. PowerShell Script

D. VBScript

E. MonoScript

Suggested Answer: *A, C, D*

Official Answer: ACD

Community vote distribution

ACD (100%)

mushi4ka Highly Voted 3 years, 4 months ago

Selected Answer: ACD

https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud-features/script-sample-support

upvoted 15 times

mushi4ka Highly Voted 3 years, 4 months ago

https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud-features/script-sample-supportThe WildFire cloud is capable of analyzing the following script types: JScript (.js) VBScript (.vbs) PowerShell Script (.ps1)

upvoted 15 times

KeppraXR Most Recent 1 year, 1 month ago

The WildFire cloud is capable of analyzing the following script types: JScript (.js) VBScript (.vbs) PowerShell Script (.ps1)

upvoted 1 times

ck19 1 year, 9 months ago

ACD are correct

upvoted 1 times

JJ_512 1 year, 9 months ago

ACD is correct.

upvoted 1 times

Erle1988 2 years, 2 months ago

https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos-90/wildfire-appliance-script-support

upvoted 1 times

luismendes21 2 years, 4 months ago

acd i guess

upvoted 1 times

zerox7305 2 years, 6 months ago

Selected Answer: ACD

upvoted 1 times

ArangoTopics 2 years, 7 months ago

https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-subscription

upvoted 1 times

gordonF 3 years ago

ACD correct

upvoted 4 times

Question #38 *Topic 1*

What helps avoid split brain in active/passive HA pair deployment?

A. Use a standard traffic interface as the HA2 backup

B. Enable preemption on both firewalls in the HA pair

C. Use the management interface as the HA1 backup link

D. Use a standard traffic interface as the HA3 link

Suggested Answer: *C*

Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/high-availability/set-up-activepassive-ha/configure-activepassive-ha.html

Community vote distribution

C (100%)

onaicul Most Recent 2 years ago

ok C : https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000004OPJCA2&lang=en_US%E2%80%A9

upvoted 1 times

cheatface 2 years, 2 months ago

C: ref https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/high-availability/set-up-activepassive-ha/configuration-guidelines-for-activepassive-ha#id04060941-71c5-4dd3-9f4e-ff55c4bfe0ab

upvoted 2 times

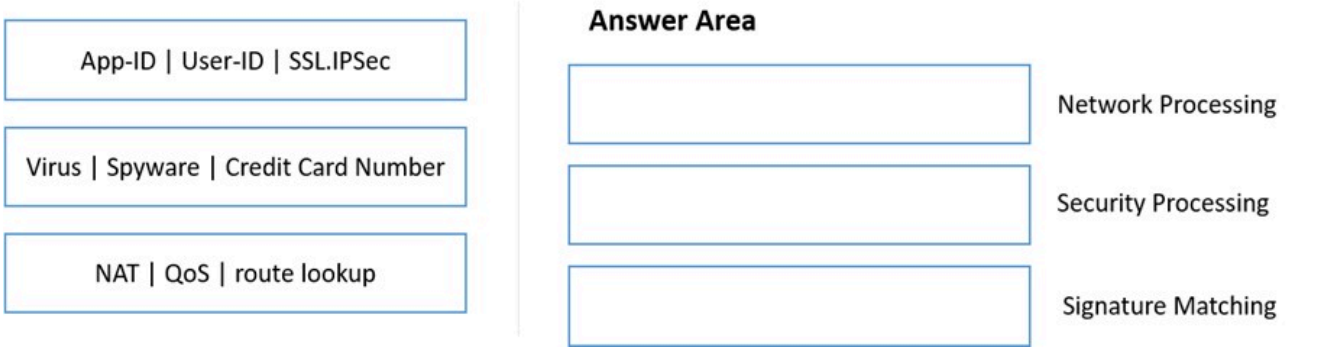
Question #39 *Topic 1*

DRAG DROP

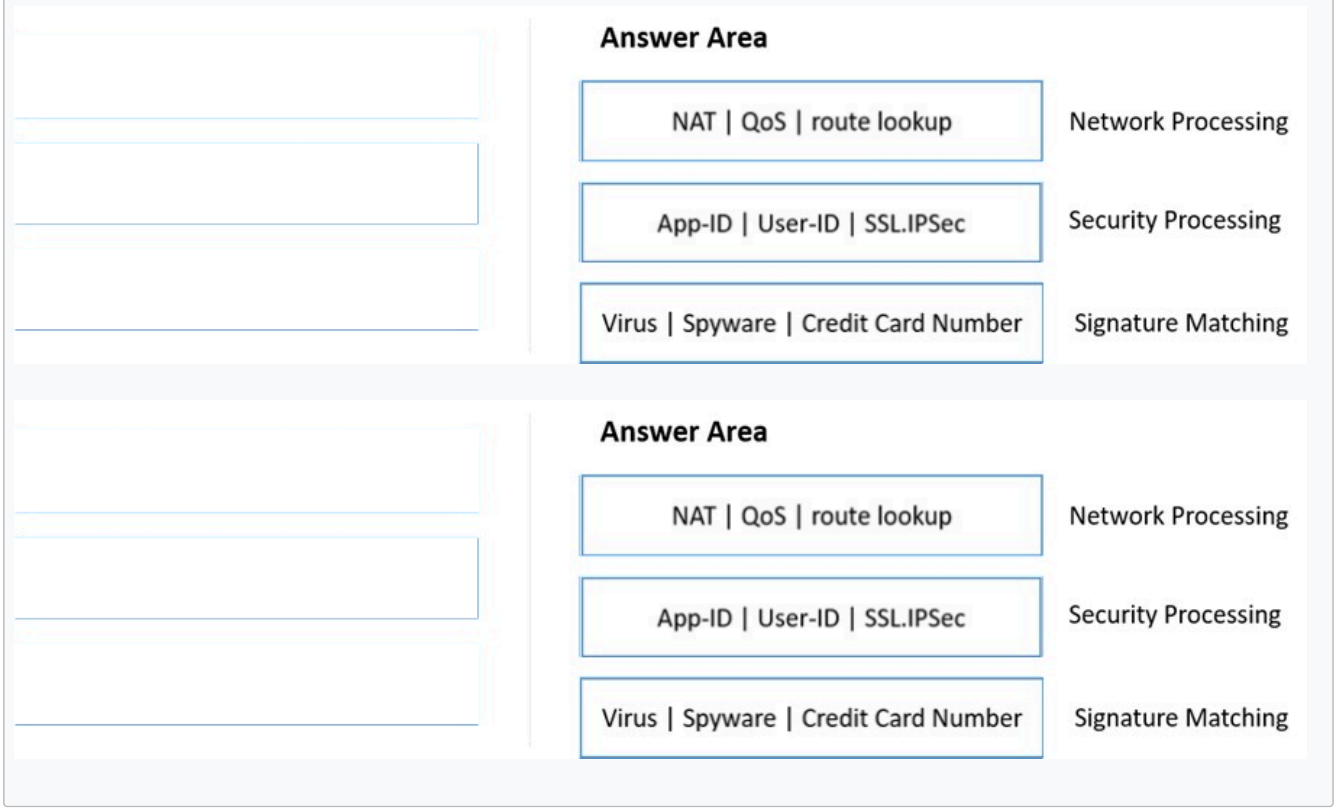
-

Match the functions to the appropriate processing engine within the dataplane.

Select and Place:



Suggested Answer:



onaicul Most Recent 2 years ago

yes, correct: https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-single-pass-parallel-processing-hardware-architecture.html

upvoted 4 times

Question #40 *Topic 1*

What are three considerations when deploying User-ID? (Choose three.)

A. Specify included and excluded networks when configuring User-ID

B. Only enable User-ID on trusted zones

C. Use a dedicated service account for User-ID services with the minimal permissions necessary

D. User-ID can support a maximum of 15 hops

E. Enable WMI probing in high security networks

Suggested Answer: *A, B, C*

Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVPCA0

Community vote distribution

ABC (100%)

wsdeffwd Most Recent 1 year, 10 months ago

Agreed https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVPCA0

upvoted 2 times

Question #41 *Topic 1*

Which three considerations should be made prior to installing a decryption policy on the NGFW? (Choose three.)

A. Include all traffic types in decryption policy

B. Inability to access websites

C. Exclude certain types of traffic in decryption policy

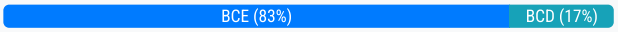
D. Deploy decryption setting all at one time

E. Ensure throughput is not an issue

Suggested Answer: *B, C, E*

Official Answer: BCE

Community vote distribution



rockyshenc Highly Voted 3 years ago

may BCE https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/prepare-to-deploy-decryption

upvoted 10 times

ck19 Most Recent 1 year, 9 months ago

BCE are correct

upvoted 1 times

McMarius11 2 years, 4 months ago

BCE is the answer

upvoted 1 times

zerox7305 2 years, 6 months ago

MUST BE B , C , E

upvoted 1 times

LostatSea 2 years, 6 months ago

BCE, C negates A and not all traffic should be decrypted

upvoted 1 times

yet_another_user 2 years, 7 months ago

Must be B, C and E. Please refer to: https://docs.paloaltonetworks.com/best-practices/9-1/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment

upvoted 2 times

Question #42 *Topic 1*

Which three components are specific to the Query Builder found in the Custom Report creation dialog of the firewall? (Choose three.)

A. Connector

B. Database

C. Recipient

D. Operator

E. Attribute

F. Schedule

Suggested Answer: *A, D, E*

Official Answer: ADE

Community vote distribution

ADE (100%)

MaxG Most Recent 2 years, 1 month ago

The Query Builder found in the Custom Report creation dialog of the firewall specifically includes the following components: - Connector: This is used to connect different parts of the query, allowing the user to specify how data elements are linked. - Operator: Operators are used to define the conditions for the query, such as equals, not equals, greater than, etc. - Attribute: Attributes represent the fields or data points that can be queried. These components are essential for building effective and precise queries within the custom report creation functionality of the firewall, ensuring that users can extract relevant data based on specific conditions.

upvoted 4 times

ck19 2 years, 3 months ago

ADE are correct

upvoted 1 times

gordonF 3 years, 6 months ago

correct https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports/generate-custom-reports#:~:text=(Optional)%20Select%20the%20Query%20Builder%20attributes%20if%20you%20want%20to%20further%20refine%20the%20selection%20criteria.%20To%20build%20a%20report%20query%2C%20specify%20the%20following%20and%20click%20Add.%20Repeat%20as%20needed%20to%20construct%20the%20full%20query.

upvoted 3 times

Question #43 *Topic 1*

Which CLI commands allows you to view SD-WAN events such as path selection and path quality measurements?

A. >show sdwan connection all

B. >show sdwan event

C. >show sdwan path-monitor stats vif

D. >show sdwan session distribution policy-name

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (88%) C (12%)

samir111 Most Recent 1 year, 11 months ago
View SD-WAN events such as path selection and path quality measurements. When you make an SD-WAN configuration change (such as a Path Quality profile change) that results in a different SD-WAN path being selected, the traffic log does not count or log the path change. > show sdwan event https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-tasks
upvoted 1 times

svcks 2 years, 1 month ago
https://docs.paloaltonetworks.com/sd-wan/3-2/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-tasks
upvoted 2 times

Erle1988 2 years, 2 months ago
B is right
upvoted 1 times

gtrickty 2 years, 2 months ago
B is right. Looking at the CLI TS sheet, " View SD-WAN events such as path selection and path quality measurements. show sdwan event " https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-tasks.html
upvoted 3 times

cheatface 2 years, 2 months ago
I thinks it's C: show sdwan path-monitor stats vif This command allows you to view latency, jitter, and packet loss on a virtual SD-WAN interface, which are key components of path quality measurements.
upvoted 1 times

Question #44 *Topic 1*

Which three steps in the cyberattack lifecycle does Palo Alto Networks Security Operating Platform prevent? (Choose three.)

A. recon the target

B. deliver the malware

C. exfiltrate data

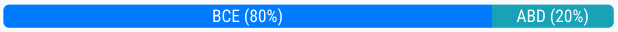
D. weaponize vulnerabilities

E. lateral movement

Suggested Answer: *B, C, E*

Official Answer: BCE

Community vote distribution



MaxG Most Recent 2 years, 1 month ago

The Palo Alto Networks Security Operating Platform is designed to prevent various stages of the cyberattack lifecycle. Specifically, it effectively prevents the following four stages: - Breach the Perimeter: By using advanced threat prevention mechanisms, the platform can stop initial attempts to penetrate the network perimeter. - Lateral Movement: Once inside the network, attackers often try to move laterally to access more systems. The platform uses network segmentation and advanced monitoring to detect and prevent such movements. - Exfiltrate Data: Data exfiltration is the process of unauthorized data transfer out of the network. The platform employs data loss prevention (DLP) technologies to detect and block such attempts. - Deliver the Malware: The platform can prevent malware delivery through its threat prevention capabilities, including anti-malware, anti-spyware, and sandboxing technologies. These steps cover critical phases where the platform can intervene to stop attacks before they cause significant damage.

upvoted 1 times

ck19 2 years, 3 months ago

Disagree with scanossa. Cyber attack can be prevented by breaking any one of the five cyber attack lifecycle stages. Recon and weaponize occur outside of your network. So the answer is BCE

upvoted 2 times

ck19 2 years, 3 months ago

BCE are correct

upvoted 1 times

Gabranch 2 years, 3 months ago

NOT Weaponization "You cannot defend against this stage of attack because all activity occurs outside of the org's network" https://www.youtube.com/watch?v=GTkHQ-HQbjQ @ 1:42

upvoted 1 times

blockface 2 years, 5 months ago

Agree with scanossa, ABD is correct https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

upvoted 1 times

scanossa 2 years, 10 months ago

ABD, the question says "prevent". C & E occurs after the threat has control

upvoted 2 times

fatehz 2 years, 11 months ago

D is not correct because generally the weaponization of the malware is not at the hacker level so we can't prevent it and A is also wrong because we can't prevent from passive recon so BCE are true

upvoted 2 times

karksark 3 years, 2 months ago

ACD: https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

upvoted 1 times

Xyn 3 years, 3 months ago

I think BCD is better. Recon, especially passive one cannot be prevented by network security. lateral movement also difficult to stop with firewall since not all traffic will go through firewall (for example, traffic from same network segment). Vulnerability protection is literally the function of IPS

upvoted 1 times

Question #45 *Topic 1*

Which profile or policy should be applied to protect against port scans from the internet?

A. An App-ID security policy rule to block traffic sourcing from the untrust zone

B. Zone protection profile on the zone of the ingress interface

C. Security profiles to security policy rules for traffic sourcing from the untrust zone

D. Interface management profile on the zone of the ingress interface

Suggested Answer: *B*
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/network/network-network-profiles-zone-protection/reconnaissance- protection.html

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

Which two products are included in the Prisma Brand? (Choose two.)

A. Prisma Cloud Compute

B. Panorama

C. NGFW

D. Prisma Cloud Enterprise

Suggested Answer: *A, D*

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/welcome/pcee_vs_pcce.html

Community vote distribution

AD (100%)

fatehz Most Recent 1 year, 11 months ago

A and D are correct Panorama and NGFW are part of Strata

upvoted 2 times

Question #47 *Topic 1*

Which three platform components can identify and protect against malicious email links? (Choose three.)

A. WildFire hybrid cloud solution

B. WildFire public cloud

C. WF-500

D. M-200

E. M-600

Suggested Answer: *A, B, C*

Official Answer: ABC

Community vote distribution

ABC (100%)

mushi4ka Highly Voted 3 years, 4 months ago

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm3ACAS

upvoted 8 times

ck19 Most Recent 1 year, 9 months ago

ABC are correct

upvoted 1 times

50f5b7d 1 year, 10 months ago

D & E are panorama devices which do nothing to protect.

upvoted 1 times

Erle1988 2 years, 2 months ago

A,B,C are right

upvoted 1 times

cheatface 2 years, 2 months ago

As the other guys said, D: m-200 is a panorama appliance.

upvoted 1 times

fatehz 2 years, 5 months ago

ABC are correct, panorama can do nothing again Email link

upvoted 1 times

ArangoTopics 2 years, 7 months ago

Correct are ABC, D is incorrect because M-200 is a Panorama apppliance and the email links are checkd by WildFire.

upvoted 1 times

Question #48 *Topic 1*

When having a customer pre-sales call, which aspects of the NGFW should be covered?

A. The NGFW simplifies your operations through analytics and automation while giving you consistent protection through exceptional visibility and control across the data center, perimeter, branch, mobile and cloud networks

B. The Palo Alto Networks-developed URL filtering database, PAN-DB provides high-performance local caching for maximum inline performance on URL lookups, and offers coverage against malicious URLs and IP addresses. As WildFire identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs), the PAN-DB database is updated with information on malicious URLs so that you can block malware downloads and disable Command and Control (C2) communications to protect your network from cyberthreats. URL categories that identify confirmed malicious content ع€" malware, phishing, and C2 are updated every five minutes ع€" to ensure that you can manage access to these sites within minutes of categorization

C. The NGFW creates tunnels that allow users/systems to connect securely over a public network, as if they were connecting over a local area network (LAN). To set up a VPN tunnel you need a pair of devices that can authenticate each other and encrypt the flow of information between them The devices can be a pair of Palo Alto Networks firewalls, or a Palo Alto Networks firewall along with a VPN-capable device from another vendor

D. Palo Alto Networks URL Filtering allows you to monitor and control the sites users can access, to prevent phishing attacks by controlling the sites to which users can submit valid corporate credentials, and to enforce safe search for search engines like Google and Bing

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

KeppraXR Most Recent 1 year, 1 month ago
I selected A
upvoted 1 times

cb4251b 2 years, 1 month ago
As a Presales Architect I would hate for the answer to be B. I choose A
upvoted 1 times

cheatface 2 years, 9 months ago
The correct answer is A
upvoted 2 times

McMarius11 2 years, 10 months ago
A as it should be
upvoted 1 times

luismendes21 2 years, 10 months ago
i should be answer is A
upvoted 1 times

zerox7305 3 years ago
Agree with A
upvoted 1 times

zerox7305 3 years ago
Selected Answer: A
upvoted 1 times

ArangoTopics 3 years, 1 month ago
The NGFW is more than the URL-F capabilities and A mention all
upvoted 1 times

yet_another_user 3 years, 1 month ago
Agree with A
upvoted 1 times

faam13 3 years, 4 months ago

answer should be A

upvoted 2 times

faam13 3 years, 4 months ago

answer should be Ai do agree

upvoted 2 times

sguerouate 3 years, 2 months ago

i do agree

upvoted 2 times

Question #49 *Topic 1*

What aspect of PAN-OS allows for the NGFW admin to create a policy that provides auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility?

A. Remote Device UserID Agent

B. user-to-tag mapping

C. Dynamic User Groups

D. Dynamic Address Groups

Suggested Answer: *C*

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups

Community vote distribution

C (100%)

blockface Most Recent 1 year, 11 months ago

C is correct. Read the 1st line: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups

upvoted 2 times

phermenious 2 years, 10 months ago

best answer in the world

upvoted 1 times

Question #50 *Topic 1*

You have enabled the WildFire ML for PE files in the antivirus profile and have added the profile to the appropriate firewall rules. When you go to Palo Alto Networks WildFire test av file and attempt to download the test file it is allowed through. In order to verify that the machine learning is working from the command line, which command returns a valid result?

A. show mlav cloud-status

B. show wfml cloud-status

C. show ml cloud-status

D. show wfav cloud-status

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

blockface Most Recent 1 year, 11 months ago

A is correct. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/configuring-url-filtering/configure-inline-categorization#tabs-configure-inline-categorization-pan-os

upvoted 1 times

Question #51 *Topic 1*

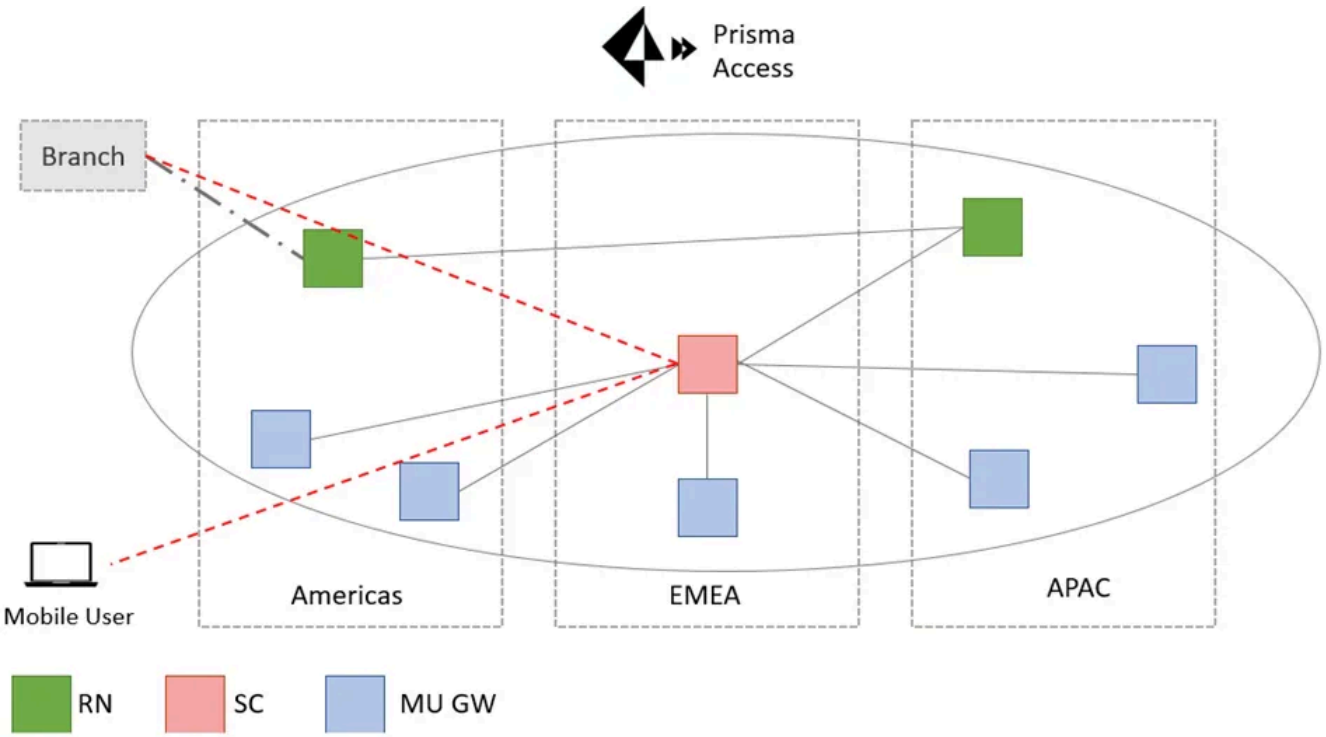
What action would address the sub-optimal traffic path shown in the figure?

Key:

RN - Remote Network -

SC - Service Connection -

MU GW - Mobile User Gateway -



A. Onboard a Service Connection in the Americas region

B. Remove the Service Connection in the EMEA region

C. Onboard a Service Connection in the APAC region

D. Onboard a Remote Network location in the EMEA region

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

mushi4ka Highly Voted 3 years, 4 months ago

I think that A is the correct answer.

upvoted 8 times

5dbdd34 Most Recent 1 year, 9 months ago

Correct Answers is A. Beacuse, mobile user connect with service connection to Branch Office. So, the diagram show us that the mobile user use an app, services, proxy, etc. to connect remote office.

upvoted 1 times

gtrickty 2 years, 2 months ago

I feel that A is the right one, but we also are not told where the user is. If the user is in APAC, then having a SC there would speed up the connection to the remote office. Is part of the question missing? Such as "this mobile user is in APAC and trying to get to that remote network, but closest and only service connector is in EMEA, what action would address the sub-optimal traffic path shown in the figure?" Without that information, this seems like a silly question.

upvoted 2 times

cheatface 2 years, 2 months ago