



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

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

Correct Answer: B

Community vote distribution

B (70%)

C (30%)

- 🗨️ **freepotatoes** Highly Voted 1 year, 9 months ago

Nonsense answers. C can't be right since PAN boxes contain multiple processors for multiple functions. Single pass means processing is done in parallel, it does not mean ALL functions are done with single processor...

upvoted 11 times
- 🗨️ **chenliang0301** Most Recent 5 months, 2 weeks ago

"Single Pass" >>> one processor

upvoted 1 times
- 🗨️ **ck19** 7 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times
- 🗨️ **GohanF2** 9 months, 2 weeks ago

The answer is C. Single pass parallel processing ensures the evaluation of app-ID , content-ID, user-ID per packet 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** 11 months, 3 weeks 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** 9 months, 1 week 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** 1 year, 4 months ago

Selected Answer: B

C is wrong because there is a cpu for each layer in SP3

upvoted 2 times
- 🗨️ **LostatSea** 1 year, 5 months ago

Selected Answer: B

B as C seems 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** 1 year, 7 months ago

Selected Answer: B

Commercially is the most used argument

upvoted 3 times

  **A0twoma** 2 years, 2 months ago

Selected Answer: C

correct

upvoted 3 times

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

Correct Answer: C

Community vote distribution

C (100%)



 **AOtwoma** 2 months ago

Selected Answer: C

Vulnerability Protection Profile

upvoted 3 times

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

Correct Answer: B

Reference:

https://media.paloaltonetworks.com/documents/Single_Pass_Parallel_Processing_Architecture.pdf

(page 6)

Community vote distribution

B (100%)

🗨️ 👤 **admripper** 1 month, 1 week 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

🗨️ 👤 **[Removed]** 7 months, 2 weeks ago

C. SIA (Scan It All) Processing Engine es la mejor respuesta porque este componente está diseñado para realizar una variedad de funciones de seguridad que incluyen: File proxy solution: Maneja la inspección y el control de archivos. Virus and spyware scanner: Escanea el tráfico en busca de malware. Vulnerability scanner: Detecta vulnerabilidades conocidas en el tráfico de red. HTTP decoder for URL filtering: Decodifica y analiza el tráfico HTTP para la aplicación de políticas de filtrado de URL.

upvoted 1 times

🗨️ 👤 **wsdeffwd** 9 months, 1 week ago

Selected Answer: B

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** 2 years, 1 month ago

Stream-based Signature Engine

upvoted 4 times

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

Correct 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%)

🗨️ 👤 **Majkiel** 6 months, 1 week 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** 9 months, 1 week ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/monitoring/use-the-automated-correlation-engine>

upvoted 1 times

🗨️ 👤 **nobody165456131354** 1 year, 2 months ago

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-the-automated-correlation-engine>

upvoted 1 times

🗨️ 👤 **freepotatoes** 1 year, 9 months ago

The Automated Correlation Engine

upvoted 1 times

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

Correct Answer: *BD*

  **onaicul** 4 weeks, 1 day 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

  **freepotatoes** 9 months, 4 weeks ago

HTTP/ HTTPS (BD)

upvoted 1 times

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

- A. Enterprise CA-signed certificates
- B. Self-Signed certificates
- C. Intermediate certificates
- D. Private key certificates

Correct Answer: AB

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** 3 months ago

Selected Answer: AB

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

upvoted 1 times

 **freepotatoes** 1 year, 3 months ago

It's AB following PAN KB... While in practice you don't use self signed in decryption, and often use Intermediate in the CA chain, thus making question misleading... So as usual - questions refer to what is written in their KB's, not what actually makes sense in real life.

upvoted 2 times

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


Correct Answer: AB

Reference:

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

Community vote distribution

AB (100%)

 **scanossa** 2 months, 3 weeks 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.](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** 4 months ago

Selected Answer: AB

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** 6 months, 2 weeks ago

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-broker>
upvoted 1 times

 **freepotatoes** 9 months, 4 weeks ago

AB is correct

upvoted 2 times

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

Correct Answer: A

Reference:

https://www.reddit.com/r/paloaltonetworks/comments/onz15y/what_is_the_result_if_a_panorama_administrator/

🗨️ 👤 **555b305** 2 weeks ago

Selected Answer: A

The answer is definitely A):

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=ka10g000000PNvrCAG>

upvoted 1 times

🗨️ 👤 **admripper** 3 weeks, 4 days ago

Selected Answer: B

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** 5 months, 2 weeks 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

🗨️ 👤 **freepotatoes** 1 year, 9 months ago

A is correct

upvoted 2 times

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

Correct Answer: D

Community vote distribution

D (100%)

413x122333444 **Highly Voted** 1 year, 9 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 month, 3 weeks ago

Selected Answer: D

Answer is D
upvoted 1 times

GohanF2 3 months, 2 weeks 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 7 months ago

D is correct
upvoted 2 times

onaicul 6 months, 3 weeks ago

<https://www.paloaltonetworks.com/services/bpa>
upvoted 1 times

ArangoTopics 11 months, 3 weeks ago

Selected Answer: D

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

ITime 1 year ago

Selected Answer: D

D is correct
upvoted 2 times

Jusecas 1 year, 1 month ago

Selected Answer: D

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 1 year, 4 months ago

Selected Answer: D

D is correct; BPA only checks your configurations against a baseline config
upvoted 4 times

gordonF 1 year, 4 months ago

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

upvoted 1 times

  **rmm1087** 1 year, 1 month 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

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

Correct Answer: A

Community vote distribution

A (56%)

B (44%)

milkyway2000 5 months, 2 weeks ago

Selected Answer: A

A is correct, checked in lab, what VenomX51 is saying is true.
upvoted 2 times

VenomX51 5 months, 3 weeks ago

Selected Answer: A

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 6 months, 1 week ago

Selected Answer: B

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 7 months ago

Selected Answer: A

A is correct, see the link from nobody165456131354
upvoted 1 times

Jerar 7 months, 2 weeks ago

A is correct, see the link from nobody165456131354
upvoted 1 times

davidpm 7 months, 2 weeks ago

Selected Answer: B

Correct answer it's 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 1 year, 2 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

  **freepotatoes** 1 year, 9 months ago

A is corect

upvoted 4 times

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

Correct Answer: AD

Community vote distribution

AD (100%)

🗨️ 👤 **Majkiel** 6 months, 2 weeks ago

Selected Answer: AD

B and C are legacy
upvoted 2 times

🗨️ 👤 **fatehz** 1 year, 4 months ago

AD because B and C are the characteristics of legacy firewall
upvoted 4 times

🗨️ 👤 **freepotatoes** 1 year, 9 months ago

AD is correct
upvoted 4 times

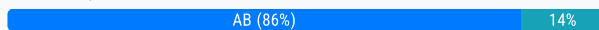
For customers with high bandwidth requirements for Service Connections, what two limitations exist when onboarding multiple Service Connections to the same

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

Correct Answer: AB

Community vote distribution



dschout 5 months, 2 weeks 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 1 year, 5 months ago

Selected Answer: AB

yet_another_user article correct as well as Faam13

upvoted 1 times

ArangoTopics 1 year, 5 months ago

Selected Answer: AB

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 1 year, 6 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 1 year, 7 months ago

Selected Answer: AB

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

upvoted 1 times

faam13 1 year, 8 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

freepotatoes 1 year, 9 months ago

It's AB... Check Prisma Access Administrator's Guide. These two are under prerequisites.

upvoted 2 times



  **gordonF** 1 year, 9 months ago

correct

Before you deploy multiple service connections from a single Prisma Access location to a single site, make sure that your network has the following prerequisites:

- You must divide the subnets in the headquarters or data center location and advertise a unique subnet on each service connection.
- Your customer premises equipment (CPE) must support, and you must be able to configure, the following networking features:
 - Policy-based forwarding (PBF) or policy-based routing—Your CPE must be able to selectively pick a specific path for a specific local source IP address and subnet.
 - Symmetric return—You must be able to configure your CPE to ensure symmetric traffic flows to and from a specific IP address and subnet, and configure symmetric return for failover tunnels if one of the tunnels goes down.

upvoted 1 times

  **cojotti** 1 year, 11 months ago

Selected Answer: AC

A & C are correct

upvoted 1 times


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

Correct Answer: ADE

Community vote distribution

ADE (100%)

 **mushi4ka** Highly Voted 1 year, 9 months ago

Selected Answer: ADE

I think that A is correct.

upvoted 9 times

 **ck19** Most Recent 1 month, 3 weeks ago

Selected Answer: ADE

ADE are correct

upvoted 1 times

 **LostatSea** 11 months, 2 weeks ago

Selected Answer: ADE

ADE correct

upvoted 1 times

 **ArangoTopics** 11 months, 3 weeks ago

Selected Answer: ADE

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

upvoted 2 times

 **yet_another_user** 1 year ago

Only A, D and E make sense

upvoted 1 times

 **TheMaster01** 1 year, 4 months ago

Selected Answer: ADE

A, D and E are correct

upvoted 3 times

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

Correct Answer: A

  **onaicul** 6 months, 3 weeks 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

  **freepotatoes** 1 year, 3 months ago

A is true
upvoted 3 times



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

Correct Answer: ABD

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 1 year, 9 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 10 times

  **onaicul** Most Recent 6 months, 3 weeks ago

ABD is true

upvoted 1 times

  **nobody165456131354** 8 months, 2 weeks ago

correct : <https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-features/credential-phishing-prevention/methods-to-check-for-corporate-credential-submissions>

upvoted 1 times

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

- A. GIF
- B. 7-Zip
- C. Flash
- D. RPM
- E. ISO
- F. DMG

Correct Answer: BCF

Community vote distribution

BCF (100%)

  **dnhan** Highly Voted 1 year ago

Selected Answer: BCF

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 2 months, 2 weeks ago

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



upvoted 3 times

  **LostatSea** 5 months, 1 week ago

Selected Answer: BCF

BCF correct



upvoted 1 times

  **yet_another_user** 6 months, 2 weeks ago

Selected Answer: BCF

See Link from dnhan


upvoted 1 times

  **Jusecas** 7 months, 2 weeks ago

Selected Answer: BCF

flash it's not a valid format

upvoted 1 times

  **gordonF** 10 months, 3 weeks ago

BCF correct

upvoted 2 times


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

Correct 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 1 year, 3 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 4 months ago

A and you will find the WF signature in the antivirus profile

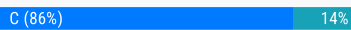
upvoted 1 times

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

- A. HA3
- B. HA1
- C. HA2
- D. HA4

Correct Answer: C

Community vote distribution



fatehz 1 year, 4 months ago

Selected Answer: C

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 1 year, 5 months 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

dschout 5 months, 2 weeks ago

the study guide is wrong...

upvoted 1 times

yet_another_user 1 year, 6 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 1 year, 8 months ago

Selected Answer: C

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

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

Correct Answer: A

Reference:

<https://www.paloguard.com/SP3-Architecture.asp>

Community vote distribution

A (100%)

🗨️ 👤 **fatehz** 4 months ago

Selected Answer: A

A is correct.

upvoted 3 times

🗨️ 👤 **madinaes** 8 months ago

A is correct. Thank you

upvoted 2 times

🗨️ 👤 **madinaes** 8 months ago

A is correct. Thank you

upvoted 1 times

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

Correct 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** 1 month, 1 week ago

Selected Answer: A

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

upvoted 1 times

🗉 **fatehz** 4 months ago

A tags of course for dag and dug

upvoted 1 times

🗉 **madinaes** 8 months ago

Tags is correct option.

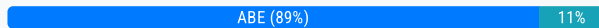
upvoted 2 times

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

Correct Answer: ABE

Community vote distribution



A0twoma Highly Voted 2 years, 2 months ago

Selected Answer: ABE

<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 month, 1 week 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 5 months, 2 weeks 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 7 months, 3 weeks ago

Selected Answer: ABE

ABE are correct
upvoted 1 times

Gabbranch 8 months ago

Selected Answer: ABC

Conflicted but the press release for PAN-OS 8.0 shows WF as a component to recognizing 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 1 year, 1 month ago

Selected Answer: ABE

Agreed, it's ABE
upvoted 1 times

fatehz 1 year, 4 months ago

Selected Answer: ABE

Agree with others ABE, C with wildfire is wrong WF is a sandbox
upvoted 1 times

Gabbranch 7 months, 4 weeks ago

WF scans email for http/https links to phishing sites.
upvoted 1 times

LostatSea 1 year, 5 months ago

Selected Answer: ABE

ABE, Agree with others

upvoted 1 times

  **yet_another_user** 1 year, 6 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** 2 years, 3 months ago

Selected Answer: ABE

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

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



Correct 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** 4 months ago

Selected Answer: A

A all other answer are wrong
upvoted 2 times

  **fatehz** 4 months ago

A all other answer are wrong
upvoted 1 times

  **yet_another_user** 6 months, 2 weeks ago

Answer A:

<https://docs.paloaltonetworks.com/network-security/security-policy/security-profiles/security-profile-file-blocking>
upvoted 2 times

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

Correct Answer: BCD

Community vote distribution

BCD (100%)

  **ck19** 1 month, 3 weeks ago

Selected Answer: BCD

BCD are correct

upvoted 1 times

  **bmarks** 8 months ago

Selected Answer: BCD

NEW LINK : <https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-features/credential-phishing-prevention/setup-credential-phishing-prevention>

PAN Doc explains why BCD is correct


upvoted 2 times

  **luismendes21** 9 months, 1 week ago

Selected Answer: BCD

Agree with others

upvoted 2 times

  **LostatSea** 11 months, 2 weeks ago

Selected Answer: BCD

BCD, Agree with others

upvoted 1 times

  **yet_another_user** 1 year ago

Selected Answer: BCD


<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/prevent-credential-phishing/setup-credential-phishing-prevention>

upvoted 1 times

  **JM1313** 1 year 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

  **A0twoma** 1 year, 8 months ago

Selected Answer: BCD

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/setup-credential-phishing-prevention#idc77030dc-6022-4458-8c50-1dc0fe7cffe4>

upvoted 4 times

  **mushi4ka** 1 year, 9 months ago

Selected Answer: BCD

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/setup-credential-phishing-prevention>

upvoted 4 times

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

Correct Answer: B

Community vote distribution

B (100%)

🗨️ **fatehz** 4 months ago

Selected Answer: B

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** 5 months, 1 week ago

Selected Answer: B

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** 6 months, 2 weeks 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** 8 months ago

B is correct as a best practice also

upvoted 2 times

🗨️ **madinaes** 8 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

🗨️ **scanossa** 2 months, 3 weeks ago

But Interzone ports are closed by default, so not all ports are open

upvoted 1 times

🗨️ **A0twoma** 1 year, 2 months ago

Selected Answer: B

Practically, B is correct

upvoted 3 times

🗨️ **mushi4ka** 1 year, 3 months ago

Selected Answer: B

B is better

upvoted 3 times

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

Correct Answer: ACDF

Community vote distribution

ACDF (100%)

🗳️ 👤 **ck19** 1 month, 2 weeks ago

Selected Answer: ACDF

ACDF are correct

upvoted 1 times

🗳️ 👤 **onaicul** 6 months, 3 weeks ago

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

upvoted 3 times

🗳️ 👤 **luismendes21** 9 months, 1 week ago

CORRECT

upvoted 1 times

🗳️ 👤 **DarioT** 1 year, 2 months ago

Selected Answer: ACDF

Correct

upvoted 3 times

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

Correct Answer: BDF

Community vote distribution

BDF (100%)

 **k3rnelpanicj** Highly Voted 1 year, 1 month 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 2 months, 1 week ago

Selected Answer: BDF

correct

upvoted 1 times

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

Correct 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** 6 months, 3 weeks ago

C is true

upvoted 1 times

🗨️ **Doobiedoo** 1 year, 1 month ago

Selected Answer: C

C is correct.

upvoted 2 times

🗨️ **mushi4ka** 1 year, 9 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


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

Correct Answer: BC

Reference:

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

  **onaicul** 5 months, 2 weeks 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

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

Correct Answer: B

Community vote distribution

B (100%)

🗨️ **Nomet** 4 months, 2 weeks ago

Selected Answer: B

<https://www.paloaltonetworks.com/resources/datasheets/autofocus-threat-intelligence>
upvoted 2 times

🗨️ **onaicul** 6 months, 3 weeks ago

B Autofocus - <https://docs.paloaltonetworks.com/autofocus>
upvoted 2 times

🗨️ **McMarius11** 8 months, 2 weeks ago

Selected Answer: B

Its B Boyz
upvoted 3 times

🗨️ **fatehz** 10 months, 1 week ago

I think its B because autofocus has information about threads
upvoted 1 times

🗨️ **yet_another_user** 1 year 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 2 times

🗨️ **rockyshenc** 1 year, 5 months ago

B shall be correct.
upvoted 2 times

🗨️ **gordonF** 1 year, 4 months ago

autofocus is no more.
upvoted 2 times

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

Correct Answer: ACD

Community vote distribution

ACD (100%)

🗨️ 👤 **fatehz** 4 months ago

Selected Answer: ACD

ACD are correct

upvoted 1 times

🗨️ 👤 **Xyn** 7 months, 4 weeks ago

Selected Answer: ACD

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



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

Correct Answer: ABF

Community vote distribution

ABF (100%)

  **dnhan** Highly Voted 2 years ago

Selected Answer: ABF

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 5 months, 3 weeks ago



Selected Answer: ABF

ABF looks correct.
upvoted 1 times

  **ck19** 7 months, 3 weeks ago

Selected Answer: ABF

ABF are correct
upvoted 1 times


  **JJ_512** 8 months, 1 week ago

Selected Answer: ABF

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** 1 year ago

acf
it should be acf
upvoted 1 times

  **luismendes21** 1 year, 3 months ago


Selected Answer: ABF

should be abf
upvoted 1 times

  **LostatSea** 1 year, 5 months ago

Selected Answer: ABF

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** 1 year, 5 months ago

Selected Answer: ABF

should be ABF
upvoted 1 times

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

Correct 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>

 **ironman_86** 1 month, 1 week ago

C is correct

upvoted 2 times


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

Correct Answer: A

Community vote distribution

A (100%)

  **kei_chige** 5 months, 1 week ago

Selected Answer: A

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

upvoted 3 times

DRAG DROP -

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

Select and Place:

Windows Executables

PowerShell Script 1

PowerShell Script 2

Answer Area

Machine Learning engine to dynamically detect malicious PowerShell scripts with known length

Machine Learning engine to dynamically identify malicious PE files

Machine Learning engine to dynamically detect malicious PowerShell scripts with unknown length

Correct Answer:

Answer Area

PowerShell Script 1

Machine Learning engine to dynamically detect malicious PowerShell scripts with known length

Windows Executables

Machine Learning engine to dynamically identify malicious PE files

PowerShell Script 2

Machine Learning engine to dynamically detect malicious PowerShell scripts with unknown length

Reference:

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

 **fatehz** 4 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 2 times

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

Correct Answer: B

Community vote distribution

B (100%)

ck19 1 month, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

kei_chige 5 months, 1 week ago

Selected Answer: B

I agree with madinaes

upvoted 1 times

ArangoTopics 11 months, 3 weeks ago

Selected Answer: B

Antivirus updates are released every 24 hours

upvoted 1 times

yet_another_user 1 year ago

Selected Answer: B

See madinaes link below

upvoted 2 times

yet_another_user 1 year ago

Selected Answer: B

Agree with madinaes, refer to the Link below

upvoted 2 times

madinaes 1 year, 2 months ago

B is correct: Antivirus updates are released every 24 hours which includes C2 (AntiSpyware)

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/dynamic-content-updates#:~:text=Antivirus%20updates%20are%20released%20every,signatures%20for%20newly%2Ddiscovered%20malware.>

upvoted 4 times

gordonF 1 year, 4 months 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](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)

B is correct

upvoted 3 times

23casper23 1 year, 8 months ago

One day should be correct

upvoted 3 times

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

Correct Answer: AB

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%)

🗨️ 👤 **ck19** 1 month, 2 weeks ago

Selected Answer: AB

AB are correct

upvoted 1 times

🗨️ 👤 **kei_chige** 5 months, 1 week ago

Selected Answer: AB

The split-brain conditions can be prevented by configuring the "HA1" backup-link and enabling heartbeat backup.

upvoted 1 times

🗨️ 👤 **onaicul** 5 months, 2 weeks ago

yes, A and B : <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CISuCAK>

upvoted 2 times


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

- A. JScript
- B. PythonScript
- C. PowerShell Script
- D. VBScript
- E. MonoScript

Correct Answer: ACD

Community vote distribution

ACD (100%)

 **mushi4ka** Highly Voted 1 year, 9 months ago

Selected Answer: ACD

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


upvoted 14 times

 **ck19** Most Recent 1 month, 3 weeks ago

Selected Answer: ACD

ACD are correct


upvoted 1 times

 **JJ_512** 2 months, 1 week ago

Selected Answer: ACD

ACD is correct.


upvoted 1 times

 **Erle1988** 6 months, 2 weeks ago

Selected Answer: ACD

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

upvoted 1 times

 **luismendes21** 9 months, 1 week ago

Selected Answer: ACD

acd i guess

upvoted 1 times

 **zerox7305** 11 months, 1 week ago

Selected Answer: ACD

upvoted 1 times

 **ArangoTopics** 11 months, 3 weeks ago

Selected Answer: ACD

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

upvoted 1 times

 **gordonF** 1 year, 4 months ago

ACD correct

upvoted 4 times

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

Correct 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** 5 months, 2 weeks ago

ok C : https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u00000040PJCA2&lang=en_US%E2%80%A9
upvoted 1 times

🗨️ **cheatface** 7 months, 2 weeks ago

Selected Answer: C

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

DRAG DROP -

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

Select and Place:

App-ID User-ID SSL.IPSec		
Virus Spyware Credit Card Number		
NAT QoS route lookup		

Answer Area

	Network Processing
	Security Processing
	Signature Matching

Correct Answer:

Answer Area

NAT QoS route lookup	Network Processing
App-ID User-ID SSL.IPSec	Security Processing
Virus Spyware Credit Card Number	Signature Matching

onaicul 5 months, 2 weeks ago

yes, correct: <https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-single-pass-parallel-processing-hardware-architecture.html>
upvoted 3 times

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

Correct Answer: ABC

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVPCA0>

Community vote distribution

ABC (100%)

 **wsdeffwd** 3 months ago

Selected Answer: ABC

Agreed

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVPCA0>

upvoted 2 times

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

Correct Answer: BCE

Community vote distribution

BCE (83%)

BCD (17%)

 **rockyshenc** Highly Voted 1 year, 5 months 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 month, 3 weeks ago

Selected Answer: BCE

BCE are correct


upvoted 1 times

 **McMarius11** 8 months, 2 weeks ago

Selected Answer: BCE

BCE is the answer

upvoted 1 times

 **zerox7305** 11 months, 1 week ago

Selected Answer: BCE

MUST BE B , C , E

upvoted 1 times

 **LostatSea** 11 months, 1 week ago

Selected Answer: BCD

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

upvoted 1 times

 **yet_another_user** 1 year ago

Selected Answer: BCE

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

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

Correct Answer: ADE

Community vote distribution

ADE (100%)

🗨️ 👤 **MaxG** 5 months, 3 weeks ago

Selected Answer: ADE

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 3 times

🗨️ 👤 **ck19** 7 months, 3 weeks ago

Selected Answer: ADE

ADE are correct

upvoted 1 times

🗨️ 👤 **gordonF** 1 year, 10 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%20](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%20)

upvoted 2 times

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

Correct Answer: B

Community vote distribution

B (86%)

14%

 **samir111** 3 months, 3 weeks ago

Selected Answer: B

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** 5 months, 2 weeks ago

Selected Answer: B

<https://docs.paloaltonetworks.com/sd-wan/3-2/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-tasks>

upvoted 2 times

 **Erle1988** 6 months, 2 weeks ago

Selected Answer: B

B is right

upvoted 1 times

 **gtricky** 7 months ago

Selected Answer: B

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** 7 months, 2 weeks ago

Selected Answer: C

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

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

Correct Answer: BCE

Community vote distribution

BCE (80%)

ABD (20%)

🗨️ 👤 **MaxG** 5 months, 3 weeks ago

Selected Answer: BCE

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** 7 months, 3 weeks 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** 7 months, 3 weeks ago

Selected Answer: BCE

BCE are correct

upvoted 1 times

🗨️ 👤 **Gabbranch** 8 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** 10 months ago

Selected Answer: ABD

Agree with scanossa, ABD is correct

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

upvoted 1 times

🗨️ 👤 **scanossa** 1 year, 2 months ago

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

upvoted 2 times

🗨️ 👤 **fatehz** 1 year, 4 months ago

Selected Answer: BCE

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** 1 year, 6 months ago

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

upvoted 1 times

🗨️ 👤 **Xyn** 1 year, 7 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

🗨️ 👤 **madinaes** 1 year, 8 months ago

BCE are OK

upvoted 3 times

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

Correct 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!

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

- A. Prisma Cloud Compute
- B. Panorama
- C. NGFW
- D. Prisma Cloud Enterprise


Correct Answer: AD

Reference:

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

Community vote distribution

AD (100%)

 **fatehz** 4 months ago

Selected Answer: AD

A and D are correct Panorama and NGFW are part of Strata
upvoted 2 times

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

Correct Answer: ABC

Community vote distribution

ABC (100%)

  **mushi4ka** Highly Voted 1 year, 9 months ago

Selected Answer: ABC

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=ka10g000000Cm3ACAS>

upvoted 8 times

  **ck19** Most Recent 1 month, 3 weeks ago

Selected Answer: ABC

ABC are correct



upvoted 1 times

  **50f5b7d** 3 months ago

Selected Answer: ABC

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



upvoted 1 times

  **Erle1988** 6 months, 2 weeks ago

Selected Answer: ABC

A,B,C are right



upvoted 1 times

  **cheatface** 7 months, 2 weeks ago

Selected Answer: ABC

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

upvoted 1 times

  **fatehz** 10 months, 1 week ago

Selected Answer: ABC

ABC are correct, panorama can do nothing again Email link



upvoted 1 times

  **ArangoTopics** 11 months, 3 weeks ago

Selected Answer: ABC

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

upvoted 1 times

  **madinaes** 1 year, 2 months ago

A and C seems same so have to select one. so BCD are Correct

upvoted 1 times


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 such as malware, phishing, and C2 are updated every five minutes 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

Correct Answer: A

Community vote distribution

A (100%)

 **cb4251b** 5 months, 3 weeks ago

Selected Answer: A

As a Presales Architect I would hate for the answer to be B. I choose A
upvoted 1 times

 **cheatface** 1 year, 1 month ago

Selected Answer: A

The correct answer is A
upvoted 2 times

 **McMarius11** 1 year, 2 months ago


Selected Answer: A

A as it should be
upvoted 1 times

 **luismendes21** 1 year, 3 months ago

Selected Answer: A

i should be answer is A
upvoted 1 times

 **zerox7305** 1 year, 5 months ago

Selected Answer: A

Agree with A
upvoted 1 times

 **zerox7305** 1 year, 5 months ago

Selected Answer: A
upvoted 1 times

 **ArangoTopics** 1 year, 5 months ago



Selected Answer: A

The NGFW is more than the URL-F capabilities and A mention all
upvoted 1 times

 **yet_another_user** 1 year, 6 months ago

Agree with A

upvoted 1 times

  **faam13** 1 year, 8 months ago

answer should be A

upvoted 2 times

  **sguerouate** 1 year, 6 months ago

i do agree

upvoted 2 times

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

Correct 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** 4 months, 1 week ago

Selected Answer: C

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

🗨️ **pherminus** 1 year, 2 months ago

best answer in the world
upvoted 1 times

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

Correct Answer: A

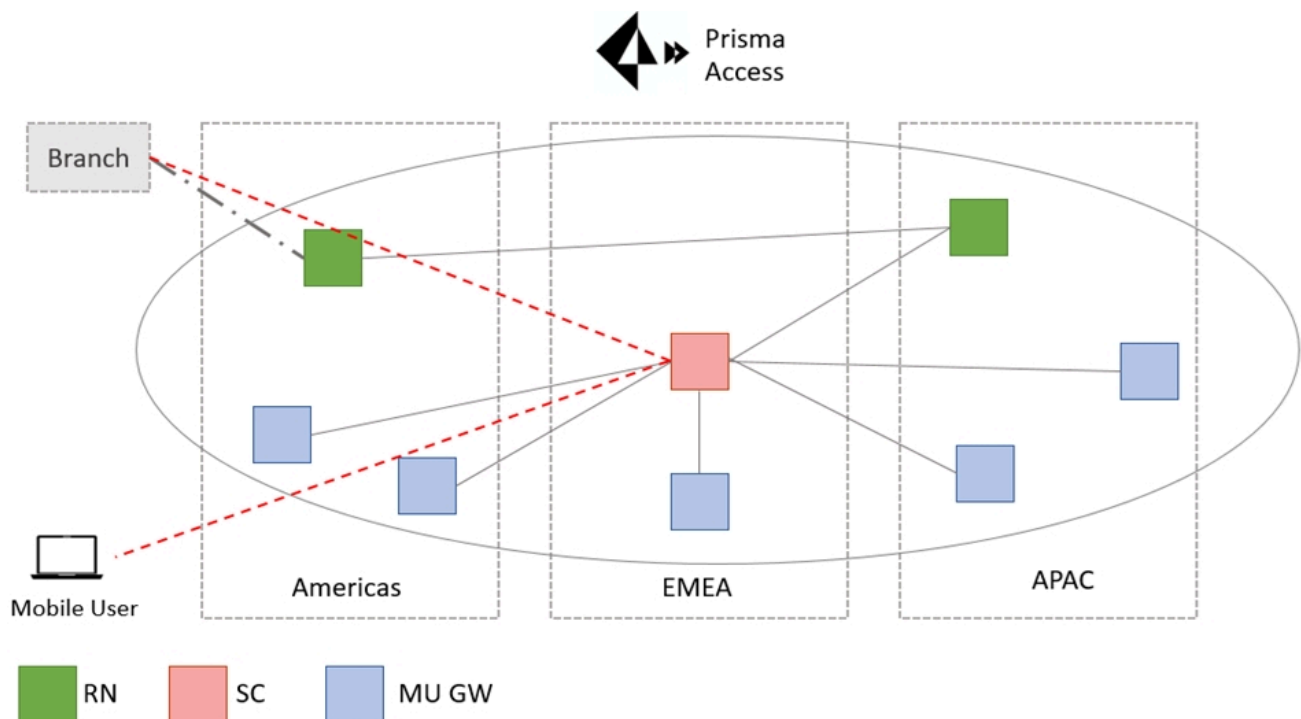
Community vote distribution

A (100%)

 **blockface** 4 months, 1 week ago

Selected Answer: A

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



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

Correct Answer: A

Community vote distribution

A (100%)

mushi4ka Highly Voted 1 year, 9 months ago

Selected Answer: A

I think that A is the correct answer.

upvoted 8 times

5dbdd34 Most Recent 1 month, 3 weeks ago

Selected Answer: A

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



gtricky 7 months ago

Selected Answer: A

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** 7 months, 2 weeks ago

The best answer seems to be either A or D, depending on the actual geographic location of the "Branch" and where the majority of its traffic needs to go. If the "Branch" is in the Americas and most of its traffic needs to go there, then A would be the best solution. If the "Branch" has a significant amount of traffic that needs to go directly to EMEA, then D would be the optimal solution.

upvoted 2 times

  **pherminus** 1 year, 2 months ago

I think it's D

upvoted 3 times

What are the three possible verdicts in WildFire Submissions log entries for a submitted sample? (Choose four.)

- A. Benign
- B. Spyware
- C. Malicious
- D. Phishing
- E. Grayware

Correct Answer: ACDE

Community vote distribution

ACDE (100%)

  **ck19** 1 month, 2 weeks ago

Selected Answer: ACDE

ACDE are correct
upvoted 1 times

  **utahman3431** 2 months, 3 weeks ago

Selected Answer: ACDE

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/wildfire-submissions-logs#:~:text=WildFire%20Submissions%20log%20entries%20include,severity%20level%20of%20the%20sample.&text=Indicates%20that%20the%20entry%2>
upvoted 1 times

  **kei_chige** 5 months ago

Selected Answer: ACDE

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/wildfire-submissions-logs#:~:text=WildFire%20Submissions%20log%20entries%20include,severity%20level%20of%20the%20sample.&text=Indicates%20that%20the%20entry%2>
upvoted 1 times

  **yet_another_user** 1 year ago

Selected Answer: ACDE

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/wildfire-submissions-logs>
upvoted 3 times

What two types of traffic should you exclude from a decryption policy? (Choose two.)

- A. All Business and regulatory traffic
- B. All outbound traffic
- C. All Mutual Authentication traffic
- D. All SSL/TLS 1.3 traffic

Correct Answer: AC

Community vote distribution

AC (94%) 6%

 **mushi4ka** Highly Voted 2 years, 3 months ago


Selected Answer: AC

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-exclusions>
upvoted 9 times

 **redmldad** Most Recent 6 months, 2 weeks ago

Selected Answer: AC

AC - from the referenced link
upvoted 1 times

 **redmldad** 6 months, 2 weeks ago

Selected Answer: AB

AB - from the referenced link
upvoted 1 times

 **ck19** 7 months, 3 weeks ago

Selected Answer: AC

AC are correct
upvoted 1 times

 **zerox7305** 1 year, 5 months ago

Selected Answer: AC

Agree with A,C
upvoted 1 times

 **LostatSea** 1 year, 5 months ago

Selected Answer: AC


Traffic that breaks decryption for technical reasons, such as using a pinned certificate, an incomplete certificate chain, unsupported ciphers, or mutual authentication

Traffic that you choose not to decrypt because of business, regulatory, personal, or other reasons
upvoted 2 times

 **ArangoTopics** 1 year, 5 months ago

Selected Answer: AC

Agree with mushi4ka, refer to the link
upvoted 1 times

 **faam13** 1 year, 8 months ago

Answer A and C
upvoted 3 times

Which functionality is available to firewall users with an active Threat Prevention subscription, but no WildFire license?

- A. Access to the WildFire API
- B. WildFire hybrid deployment
- C. PE file upload to WildFire
- D. 5 minute WildFire updates to threat signatures

Correct Answer: C

Community vote distribution

C (78%)

D (22%)

 **ck19** 1 month, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

 **wsdeffwd** 3 months ago

Selected Answer: C

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/9-0/pan-os-admin/pan-os-admin.pdf


upvoted 2 times

 **svcks** 5 months, 2 weeks ago

Selected Answer: C

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

upvoted 3 times

 **Jestrada** 5 months, 3 weeks ago

Selected Answer: C

Because Five-Minute Updates is for The standard WildFire subscription, so, can't be D

upvoted 1 times

 **YazanOmar** 7 months, 2 weeks ago

c IS CORRECT

Basic WildFire support is included as part of the Threat Prevention license. Anyone with or without a Threat Prevention license can forward PE files to WildFire for analysis. The WildFire subscription service provides enhanced services for organizations that require immediate coverage for threats, frequent WildFire signature updates, advanced file type forwarding (APK, PDF, Microsoft Office, and Java Applet), and the ability to upload files using the WildFire API. A WildFire subscription is also required if your firewalls will be forwarding files to an on-premises WF-500 appliance.

upvoted 1 times

 **nobody165456131354** 7 months, 2 weeks ago

Selected Answer: D

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

upvoted 2 times

 **clmt** 7 months, 4 weeks ago

B is correct

upvoted 1 times

 **clmt** 7 months, 4 weeks ago

SORRY D is correct

upvoted 1 times

What is the recommended way to ensure that firewalls have the most current set of signatures for up-to-date protection?

- A. Run a Perl script to regularly check for updates and alert when one is released
- B. Store updates on an intermediary server and point all the firewalls to it
- C. Utilize dynamic updates with an aggressive update schedule
- D. Monitor update announcement and manually push updates to firewalls

Correct Answer: *C*

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


What three Tabs are available in the Detailed Device Health on Panorama for hardware-based firewalls? (Choose three.)

- A. Errors
- B. Environments
- C. Interfaces
- D. Mounts
- E. Throughput
- F. Sessions
- G. Status

Correct Answer: BCF

Community vote distribution

BCF (100%)

 **yet_another_user** Highly Voted 1 year, 6 months ago

Selected Answer: BCF

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-managed-devices-summary/detailed-device-health-in-panorama>

upvoted 5 times

 **dfdc27a** Most Recent 6 months, 1 week ago

BCEF: Environments, interfaces, Throughput and sessions

but if we have to choose just 3 (Environments is wrong since its correctly mentioned on panorama as "Environnementals")

-> I vote for CEF


upvoted 1 times

 **482aa95** 1 year, 8 months ago

Answer is correct. Environments, interfaces, sessions

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/panorama-web-interface/panorama-managed-devices-summary/detailed-device-health-in-panorama>

upvoted 4 times

 **faam13** 1 year, 8 months ago

Throughput, interfaces, sessions.

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/device-monitoring-on-panorama/monitor-device-health.html>

upvoted 1 times

What component is needed if there is a large scale deployment of Next Generation Firewalls with multiple Panorama Management Servers?

- A. M-600 Appliance
- B. Panorama Large Scale VPN Plugin
- C. Panorama Interconnect Plugin
- D. Palo Alto Networks Cluster License

Correct Answer: C

Community vote distribution

C (100%)



 **yet_another_user** 6 months, 1 week ago

Selected Answer: C

<https://docs.paloaltonetworks.com/plugins/vm-series-and-panorama-plugins-release-notes/panorama-interconnect-plugin>

upvoted 3 times

Which is the smallest Panorama solution that can be used to manage up to 2500 Palo Alto Networks Next Generation firewalls?

- A. M-200
- B. M-600
- C. M-100
- D. Panorama VM-Series

Correct Answer: D

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000boF1CAI>

Community vote distribution

D (100%)

 **Xyn** Highly Voted 1 year, 1 month ago

M200 support 1000 gateway, M600 support 5000 GW. to manage 2500 GW with most cost efficiency, a VM panorama can be used
upvoted 5 times

 **wsdeffwd** Most Recent 3 months ago

Selected Answer: D

If you are activating a new device management license on a Panorama, you can manage up to 5,000 firewalls with an M-600, M-700 appliance, or Panorama virtual appliance on ESXi, or up to 2,500 firewalls with a Panorama virtual appliance, but the Description still displays Device management license to manage up to 1000 devices or more.

upvoted 2 times

XYZ Corporation has a legacy environment with asymmetric routing. The customer understands that Palo Alto Networks firewalls can support asymmetric routing with redundancy.

Which two features must be enabled to meet the customer's requirements? (Choose two.)

- A. Virtual systems
- B. HA active/active
- C. HA active/passive
- D. Policy-based forwarding

Correct Answer: *BD*

Community vote distribution

BD (100%)

🗨️ 👤 **ck19** 1 month, 2 weeks ago

Selected Answer: BD

BD are correct

upvoted 2 times

🗨️ 👤 **kei_chige** 5 months, 1 week ago

Selected Answer: BD

B and D

upvoted 1 times

What is the correct behavior when a Palo Alto Networks next-generation firewall (NGFW) is unable to retrieve a DNS verdict from DNS service cloud in the configured lookup time?

- A. NGFW discard a response from the DNS server.
- B. NGFW temporarily disable DNS Security function.
- C. NGFW permit a response from the DNS server.
- D. NGFW resend a verdict challenge to DNS service cloud.

Correct Answer: C

Community vote distribution

C (100%)

wsdeffwd 3 months ago

Selected Answer: C

"If the firewall is unable to retrieve a signature verdict in the allotted time due to connectivity issues, the request, including all subsequent DNS responses, are passed through."

upvoted 1 times

JP_I 7 months, 3 weeks ago

Selected Answer: C

Updated link here: <https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/configure-lookup-timeout>

upvoted 1 times

yet_another_user 1 year ago

Selected Answer: C

C is right, refer to Step 11

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns-security/enable-dns-security>

upvoted 1 times

Xyn 1 year, 1 month ago

Result is still C on newer OS config guide

upvoted 1 times

Which statement best describes the business value of Palo Alto Networks' Zero Touch Provisioning (ZTP)?

- A. When it is in place, it removes the need for an onsite firewall.
- B. When purchasing the service, Palo Alto Networks will send an engineer to physically deploy the firewall to the customer environment.
- C. It allows a firewall to be automatically connected to the local network wirelessly.
- D. It is designed to simplify and automate the onboarding of new firewalls to the Panorama management server.

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning/ztp-overview/about-ztp>

 **admripper** 3 weeks, 3 days ago

Selected Answer: A

When HTTP header logging is enabled on a URL Filtering profile, the attribute-value that can be logged is the HTTP method.

Correct Answer: A. HTTP method

Explanation:

HTTP header logging allows specific parts of the HTTP request or response headers to be captured for analysis. The HTTP method (e.g., GET, POST, PUT) is one of the attributes typically logged to provide context about the type of request being made.

Other attributes, like response status codes (B) or content type (C), are usually part of the response, not directly related to the URL Filtering HTTP header logging feature. Similarly, while X-Forwarded-For (D) is a header, it's more relevant in logging configurations specific to proxy or client IP tracking, not URL Filtering's HTTP header logging.

upvoted 1 times

When HTTP header logging is enabled on a URL Filtering profile, which attribute-value can be logged?

- A. HTTP method
- B. HTTP response status code
- C. Content type
- D. X-Forwarded-For

Correct Answer: D

Community vote distribution

D (100%)

 **admripper** 3 weeks, 3 days ago

Selected Answer: A

When HTTP header logging is enabled on a URL Filtering profile, the attribute-value that can be logged is the HTTP method.

Correct Answer: A. HTTP method

Explanation:

HTTP header logging allows specific parts of the HTTP request or response headers to be captured for analysis. The HTTP method (e.g., GET, POST, PUT) is one of the attributes typically logged to provide context about the type of request being made.

Other attributes, like response status codes (B) or content type (C), are usually part of the response, not directly related to the URL Filtering HTTP header logging feature. Similarly, while X-Forwarded-For (D) is a header, it's more relevant in logging configurations specific to proxy or client IP tracking, not URL Filtering's HTTP header logging.

upvoted 1 times

 **yet_another_user** 6 months, 1 week ago

Selected Answer: D

Also with 10.1

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/http-header-logging>

upvoted 3 times


In PAN-OS 10.0 and later, DNS Security allows policy actions to be applied based on which three domains? (Choose three.)

- A. benign
- B. government
- C. command and control (C2)
- D. malware
- E. grayware

Correct Answer: CDE

Community vote distribution

CDE (100%)

 **confusion** 5 months, 1 week ago

Selected Answer: CDE

CDE, comment answers and links provided are correct.

upvoted 1 times

 **ArangoTopics** 5 months, 3 weeks ago

Selected Answer: CDE

CDE are correct

<https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/dns-security-test-domains#id4c731690-c824-4990-8a63-fc0c873c5c25>

upvoted 4 times

 **yet_another_user** 6 months, 1 week ago

Answers are correct, see step 5

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns-security/enable-dns-security>

upvoted 2 times

 **gspot** 10 months ago

Correct:

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/http-header-logging>

upvoted 1 times


Which two features are key in preventing unknown targeted attacks? (Choose two.)

- A. Single Pass Parallel Processing (SP3)
- B. nightly botnet report
- C. App-ID with the Zero Trust model
- D. WildFire Cloud threat analysis

Correct Answer: CD

Community vote distribution

CD (100%)

  **mushi4ka** Highly Voted 1 year, 9 months ago

Selected Answer: CD

C and D as they make more sense.
upvoted 7 times

  **ck19** Most Recent 1 month, 3 weeks ago

Selected Answer: CD

CD are correct
upvoted 1 times

  **ArangoTopics** 11 months, 3 weeks ago

Selected Answer: CD

<https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>
upvoted 2 times

  **yet_another_user** 1 year ago

Selected Answer: CD

Only C and D make sense
upvoted 1 times

Which of the following statements is valid with regard to Domain Name System (DNS) sinkholing?

- A. It requires the Vulnerability Protection profile to be enabled.
- B. It requires a Sinkhole license in order to activate.
- C. DNS sinkholing signatures are packaged and delivered through Vulnerability Protection updates.
- D. Infected hosts connecting to the Sinkhole Internet Protocol (IP) address can be identified in the traffic logs.

Correct Answer: D

Community vote distribution

D (100%)

  **mushi4ka** Highly Voted 1 year, 9 months ago

Selected Answer: D

The purpose of the feature is to be able to identify infected hosts:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=ka10g000000CIGECA0>

upvoted 7 times

  **ck19** Most Recent 1 month, 3 weeks ago

Selected Answer: D

D is correct



upvoted 1 times

  **zerox7305** 11 months, 1 week ago

Selected Answer: D

Agree with D

upvoted 1 times

  **nosaj_** 11 months, 1 week ago

Selected Answer: D

This feature is not configured in a VP profile.

upvoted 1 times

  **ArangoTopics** 11 months, 3 weeks ago

Selected Answer: D

A is incorrect, DNS sinkholing is embedded in Anti-Spyware rprofile. Correct is D.

upvoted 1 times

  **homersimpson** 1 year, 4 months ago

Selected Answer: D

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=ka10g000000CIGECA0>

upvoted 3 times