PCNSE Q&As

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 11.x

Pass Palo Alto Networks PCNSE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/pcnse.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Users have reported an issue when they are trying to access a server on your network. The requests aren\\'t taking the expected route. You discover that there are two different static routes on the firewall for the server. What is used to determine which route has priority?

A. The first route installed

B. Bidirectional Forwarding Detection

C. The route with the lowest administrative distance

D. The route with the highest administrative distance

Correct Answer: C

QUESTION 2

An engines must configure the Decryption Broker feature. To which router must the engineer assign the decryption forwarding interfaces that are used m the Decryption Broker security Chain?

A. a virtual router that has no additional interfaces for passing data-plane traffic and no other configured routes than those used in for the security chain

B. the virtual router that routes the traffic that the Decryption Broker security chain inspects

C. a virtual router that is configured with at least one dynamic routing protocol and has at least one entry in the RIB

D. the default virtual router (If there is no default virtual router the engineer must create one during setup)

Correct Answer: B

Decryption Broker is a feature that allows you to use a Palo Alto Networks firewall as a decryption broker for other security devices in your network1. It works by decrypting traffic on one interface and forwarding it to another interface where it can be inspected by other devices before being re-encrypted and sent to its destination2. The firewall acts as a transparent bridge between the two interfaces and does not change the source or destination IP addresses of the traffic2. To configure Decryption Broker, you need to assign decryption forwarding interfaces (DFIs) to the virtual router that routes the traffic that you want to inspect. The DFIs are used to forward decrypted traffic from one interface to another in a security chain3. A security chain is a set of devices that perform different security functions on the same traffic flow3. You can have multiple security chains for different types of traffic or different segments of your network3. The reason why you need to assign DFIs to the virtual router that routes the traffic is because Decryption Broker uses routing tables to determine which DFI belongs to which security chain and how to forward traffic between them2. If you assign DFIs to a different virtual router than the one that routes the traffic, Decryption Broker will not be able to find them or forward traffic correctly2.

QUESTION 3

An administrator needs to identify which NAT policy is being used for internet traffic.

From the Monitor tab of the firewall GUI, how can the administrator identify which NAT policy is in use for a traffic flow?

A. Click Session Browser and review the session details.

B. Click Traffic view and review the information in the detailed log view.

C. Click Traffic view; ensure that the Source or Destination NAT columns are included and review the information in the detailed log view.

D. Click App Scope > Network Monitor and filter the report for NAT rules.

Correct Answer: C

Traffic view in the Monitor tab of the firewall GUI can display the information about the NAT policy that is in use for a traffic flow, if the Source or Destination NAT columns are included and reviewed in the detailed log view1. The Source NAT column shows the translated source IP address and port, and the Destination NAT column shows the translated destination IP address and port2. These columns can help the administrator identify which NAT policy is applied to the traffic flow based on the pre-NAT and post-NAT addresses and ports.

QUESTION 4

Which CLI command enables an administrator to check the CPU utilization of the dataplane?

A. show running resource-monitor

B. debug data-plane dp-cpu

C. show system resources

D. debug running resources

Correct Answer: A

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXwCAK
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CluDCAS

QUESTION 5

Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

A. Dynamic

B. Custom Panorama Admin

C. Role Based

D. Device Group

E. Template Admin

Correct Answer: DE

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClETCA0

QUESTION 6

Which three external authentication services can the firewall use to authenticate admins into the Palo Alto Networks NGFW without creating administrator account on the firewall? (Choose three.)

A. RADIUS

B. TACACS+

C. Kerberos

D. LDAP

E. SAML

Correct Answer: ABE

According to the Palo Alto Networks documentation1, the firewall can use three external authentication services to authenticate admins into the Palo Alto Networks NGFW without creating administrator accounts on the firewall: RADIUS,

TACACS+, and SAML. These services allow the firewall to verify the credentials of admins against an external server and grant them access based on their assigned roles and permissions.

Therefore, the correct answer is A, B, and E.

The other options are not external authentication services that the firewall can use to authenticate admins:

Kerberos: This option is not an external authentication service that the firewall can use to authenticate admins. Kerberos is a protocol that allows users to access network resources using a single sign-on mechanism. The firewall can use

Kerberos to authenticate users for GlobalProtect VPN or Captive Portal, but not for admin access.

LDAP: This option is not an external authentication service that the firewall can use to authenticate admins. LDAP is a protocol that allows querying and modifying directory services over a network. The firewall can use LDAP to retrieve user

and group information from an external server, but not to authenticate admins.

References:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-types/external-authentication-services

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-types/kerberos-authentication

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-users-using-an-ldap-server

QUESTION 7

Which event will happen if an administrator uses an Application Override Policy?

A. Threat-ID processing time is decreased.

B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.

C. The application name assigned to the traffic by the security rule is written to the Traffic log.

D. App-ID processing time is increased.

Correct Answer: B

Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to- Create-an-Application-Override/ta-p/65513

https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/manage-custom-or- unknown- applications#

"If you define an application override, the firewall stops processing at Layer-4. The custom application name is assigned to the session to help identify it in the logs, and the traffic is not scanned for threats."

QUESTION 8

Which administrative authentication method supports authorization by an external service?

A. Certificates

B. LDAP

C. RADIUS

D. SSH keys

Correct Answer: C

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall- administration/manage-firewall-administrators/administrative-authentication

QUESTION 9

An organization has recently migrated its infrastructure and configuration to NGFWs, for which Panorama manages the devices The organization is coming from a L2-L4 firewall vendor, but wants to use App-ID while identifying policies that are no longer needed.

Which Panorama tool can help this organization?

A. Config Audit

B. Policy Optimizer

C. Application Groups

D. Test Policy Match

Correct Answer: B

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id- features/policy-optimizer his new feature identifies port-based rules so you can convert them to application-based rules that allow the traffic or add applications to existing rules without compromising application availability. https://docs.paloaltonetworks.com/pan-os/90/pan-os-new-features/app-id-features/policy-optimizer.html

QUESTION 10

An administrator is considering upgrading the Palo Alto Networks NGFW and central management Panorama version.

What is considered best practice for this scenario?

A. Perform the Panorama and firewall upgrades simultaneously

B. Upgrade the firewall first wait at least 24 hours and then upgrade the Panorama version

C. Upgrade Panorama to a version at or above the target firewall version

D. Export the device state perform the update, and then import the device state

Correct Answer: C

QUESTION 11

Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)

A. Red Hat Enterprise Virtualization (RHEV)

B. Kernel Virtualization Module (KVM)

C. Boot Strap Virtualization Module (BSVM)

D. Microsoft Hyper-V

Correct Answer: BD

Reference: https://www.paloaltonetworks.com/products/secure-the-network/virtualized- next-generation-firewall/vm-series docs.paloaltonetworks.com/vm-series/8-0/vm-series-deployment/about-the-vm-series- firewall/vm-series-deployments

QUESTION 12

A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

A. Application Override policy.

B. Security policy to identify the custom application.

C. Custom application.

D. Custom Service object.

Correct Answer: AC

Unlike the App-ID engine, which inspects application packet contents for unique signature elements, the Application Override policy\\'s matching conditions are limited to header-based data only. Traffic matched by an Application Override policy is identified by the App-ID entered in the Application entry box.Choices are limited to applications currently in the App-ID database.Because this traffic bypasses all Layer 7 inspection, the resulting security is that of a Layer-4 firewall. Thus, this traffic should be trusted without the need for Content-ID inspection. The resulting application assignment can be used in other firewall functions such as Security policy and QoS.Use CasesThree primary uses cases for Application Override Policy are: To identify "Unknown" App-IDs with a different or custom application signature To re-identify an existing application signature To bypass the Signature Match Engine (within the SP3 architecture) to improve processing timesA discussion of typical uses of application override and specific implementation examples is here:https://live.paloaltonetworks.com/t5/LearningArticles/Tips-amp-Tricks- How-to-Create-an-Application- Override/ta-p/65513

QUESTION 13

What happens when an A P firewall cluster synchronies IPsec tunnel security associations (SAs)?

A. Phase 2 SAs are synchronized over HA2 finks

B. Phase 1 and Phase 2 SAs are synchronized over HA2 links

C. Phase 1 SAs are synchronized over HA1 links

D. Phase 1 and Phase 2 SAs are synchronized over HA3 links

Correct Answer: A

From the Palo Alto documentation below, "when a VPN is terminated on a Palo Alto firewall HA pair, not all IPSEC related information is synchronized between the firewalls... This is an expected behavior. IKE phase 1 SA information is NOT

synchronized between the HA firewalls."

And from the second link, "Data link (HA2) is used to sync sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in the HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-

alive). It flows from the active firewall to the passive firewall."

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCA
Wandlang=en_US%E2%80%A9andrefURL=http%3A%2F%2Fknowledgebase.paloaltonetworks
.com%2FKCSArticleDetail https://help.aryaka.com/display/public/KNOW/Palo+Alto+Networks+NFV+Technical+Brief

QUESTION 14

What is exchanged through the HA2 link?

A. hello heartbeats

B. User-ID information

C. session synchronization

D. HA state information

Correct Answer: C

Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high- availability/ha-links-and-backup-links

"Data Link--The HA2 link is used to synchronize sessions, forwarding tables, IPSec security associations and ARP tables between devices in an HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive); it flows from the active device to the passive device." https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/high-availability-for-vm-series-firewall-on-aws/halinks#:~:text=%E2%80%94The%20HA1%20link%20is%20used,port%20is%20used%20for %20HA1

QUESTION 15

What are three tasks that cannot be configured from Panorama by using a template stack? (Choose three)

A. Change the firewall management IP address

B. Configure a device block list

C. Add administrator accounts

D. Rename a vsys on a multi-vsys firewall

E. Enable operational modes such as normal mode, multi-vsys mode, or FIPS-CC mode

Correct Answer: BDE

https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/template-capabilities-and-exceptions