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.pass4itsure.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

QUESTION 1

Engineer was tasked to simplify configuration of multiple firewalls with a specific set of configurations shared across all devices. Which two advantages would be gained by using multiple templates in a stack? (Choose two.)

A. inherits address-objects from the templates

B. standardizes server profiles and authentication configuration across all stacks

C. standardizes log-forwarding profiles for security policies across all stacks

D. defines a common standard template configuration for firewalls

Correct Answer: BD

QUESTION 2

Which three firewall states are valid? (Choose three)

A. Active

B. Functional

C. Pending

D. Passive

E. Suspended

Correct Answer: ADE

Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high- availability/ha-firewall-states

QUESTION 3

Which type of policy in Palo Alto Networks firewalls can use Device-ID as a match condition?

A. NAT

B. DOS protection

C. QoS

D. Tunnel inspection

Correct Answer: C

The type of policy in Palo Alto Networks firewalls that can use Device-ID as a match condition is QoS. This is because Device-ID is a feature that allows the firewall to identify and classify devices on the network based on their

characteristics, such as vendor, model, OS, and role1. QoS policies are used to allocate bandwidth and prioritize traffic based on various criteria, such as application, user, source, destination, and device2. By using Device-ID as a match condition in QoS policies, the firewall can apply different QoS actions to different types of devices, such as IoT devices, laptops, smartphones, etc3. This can help optimize the network performance and ensure the quality of service for critical applications and devices.

QUESTION 4

A firewall administrator needs to be able to inspect inbound HTTPS traffic on servers hosted in their DMZ to prevent the hosted service from being exploited. Which combination of features can allow PAN-OS to detect exploit traffic in a session with TLS encapsulation?

A. Decryption policy and a Data Filtering profile

B. a WildFire profile and a File Blocking profile

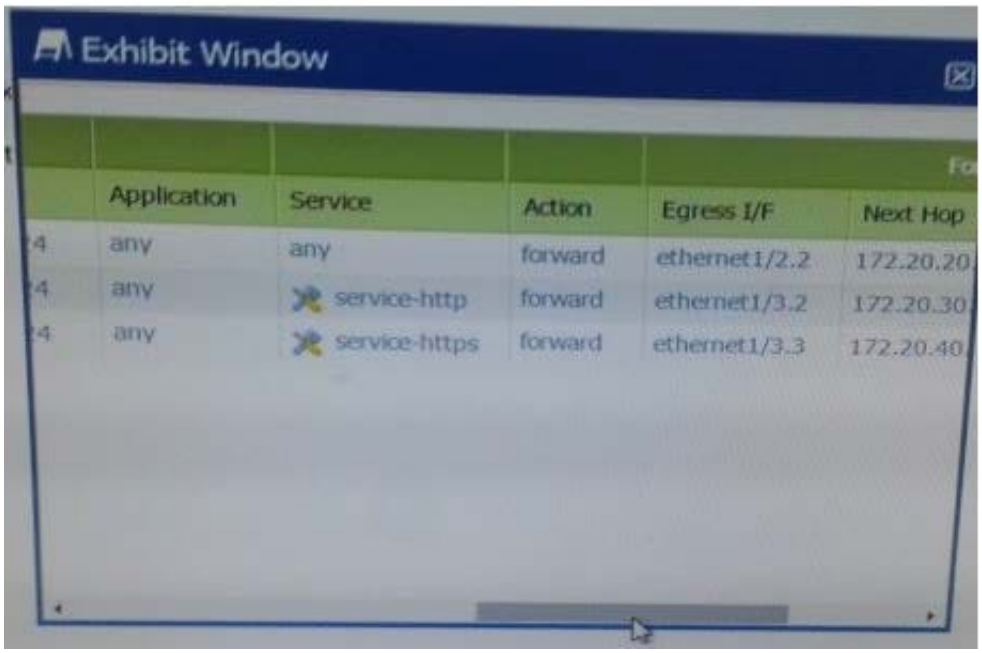
C. Vulnerability Protection profile and a Decryption policy

D. a Vulnerability Protection profile and a QoS policy

Correct Answer: C

QUESTION 5

Refer to Exhibit:



A firewall has three PDF rules and a default route with a next hop of 172.29.19.1 that is configured in the default VR. A user named XX-bes a PC with a 192.168.101.10 IP address.

He makes an HTTPS connection to 172.16.10.29.

What is the next hop IP address for the HTTPS traffic from Wills PC.

A. 172.20.30.1

B. 172.20.20.1

C. 172.20.10.1

D. 172.20.40.1

Correct Answer: B

QUESTION 6

What are three valid method of user mapping? (Choose three)

A. Syslog

B. XML API

C. 802.1X

D. WildFire

E. Server Monitoring

Correct Answer: ABE

QUESTION 7

An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS?software, the administrator enables log forwarding from the firewalls to PanoramA. Pre-existing logs from the firewalls are not appearing in PanoramA.

Which action would enable the firewalls to send their pre-existing logs to Panorama?

A. Use the import option to pull logs.

B. Export the log database

C. Use the scp logdb export command

D. Use the ACC to consolidate the logs

Correct Answer: B

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/use-the-cli/use-secure-copy-to-import-and-export-files/export-and-import-a-complete-log-database-logdb

QUESTION 8

A firewall engineer creates a new App-ID report under Monitor > Reports > Application Reports > New Applications to monitor new applications on the network and better assess any Security policy updates the engineer might want to make. How does the firewall identify the New App-ID characteristic?

A. It matches to the New App-IDs downloaded in the last 90 days.

B. It matches to the New App-IDs in the most recently installed content releases.

C. It matches to the New App-IDs downloaded in the last 30 days.

D. It matches to the New App-IDs installed since the last time the firewall was rebooted.

Correct Answer: B

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/monitor-new-app-ids

QUESTION 9

An existing NGFW customer requires direct interne! access offload locally at each site and iPSec connectivity to all branches over public internet. One requirement is mat no new SD- WAN hardware be introduced to the environment. What is the best solution for the customer?

A. Configure a remote network on PAN-OS

B. Upgrade to a PAN-OS SD-WAN subscription

C. Deploy Prisma SD-WAN with Prisma Access

D. Configure policy-based forwarding

Correct Answer: B

QUESTION 10

When you configure an active/active high availability pair which two links can you use? (Choose two)

A. HA2 backup

B. HA3

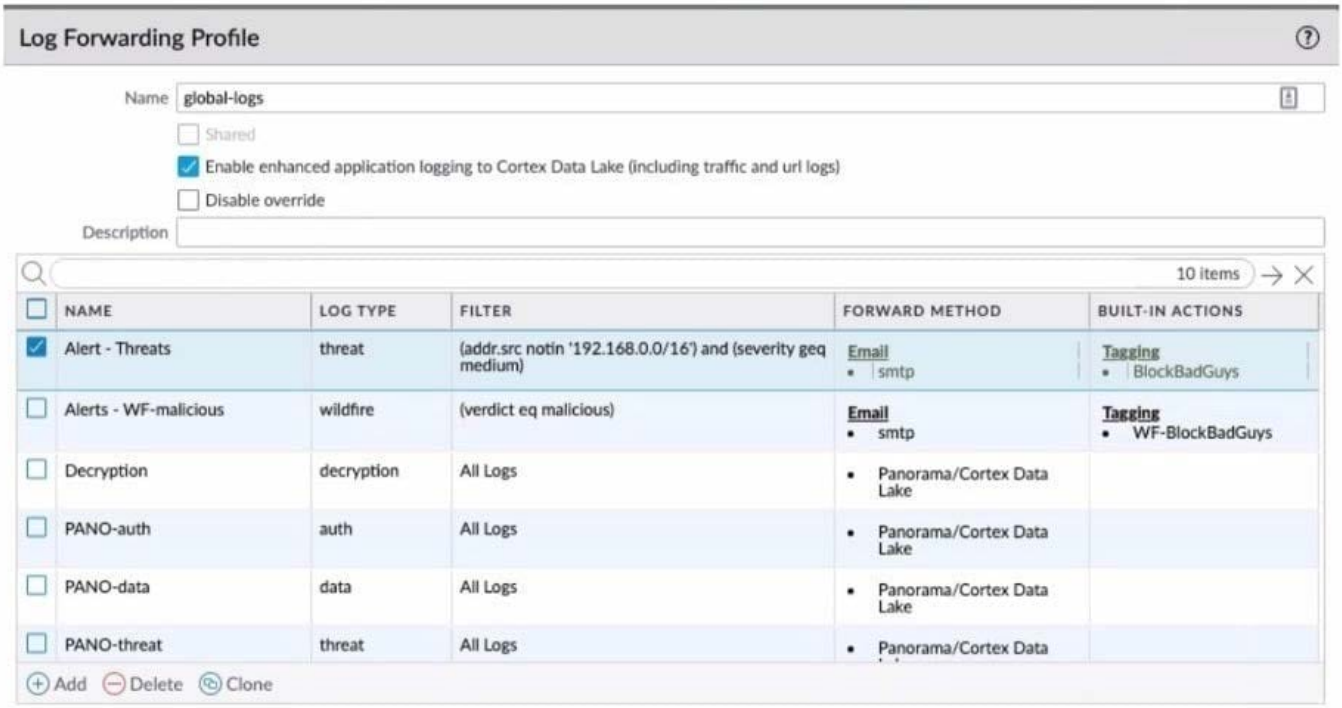
C. Console Backup

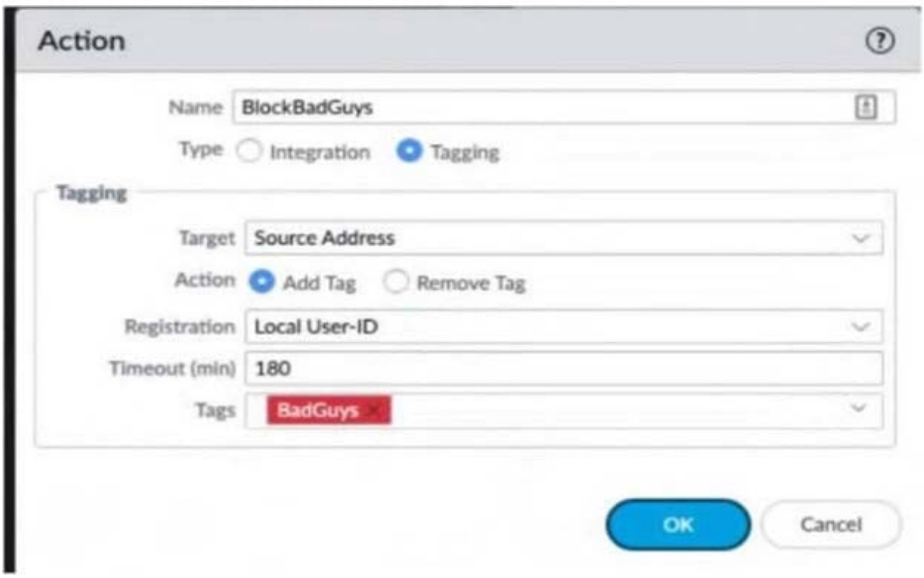
D. HSCI-C

Correct Answer: AB

QUESTION 11

Review the images. A firewall policy that permits web traffic includes the global-logs policy as depicted.





What is the result of traffic that matches the "Alert - Threats" Profile Match List?

A. The source address of SMTP traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.

B. The source address of traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.

C. The source address of traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.

D. The source address of SMTP traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.

Correct Answer: C

QUESTION 12

Which type of interface does a firewall use to forward decrypted traffic to a security chain for inspection?

A. Layer 2

B. Tap

C. Layer 3

D. Decryption Mirror

Correct Answer: C

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking- admin/network-packet-broker/configure-routed-layer-3-security-chains Configure security chain devices with Layer 3 interfaces to connect to the security chain network. These Layer 3 interfaces must have an assigned IP address and subnet mask. https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption- broker/security-chain-layer-3-guidelines.html

QUESTION 13

The firewall identifies a popular application as an unknown-tcp.

Which two options are available to identify the application? (Choose two.)

A. Create a custom application.

B. Create a custom object for the custom application server to identify the custom application.

C. Submit an App-ID request to Palo Alto Networks.

D. Create a Security policy to identify the custom application.

Correct Answer: AC

https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/use- application-objects-in-policy/create-a-custom-application https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/manage-custom-or-unknownapplications.html

QUESTION 14

In an HA failover scenario what occurs when sessions match an SSL Forward Proxy Decryption policy?

A. HA Sync does not occur the existing session is transferred to the active firewall.

B. HA Sync does not occur the firewall drops the session.

C. HA Sync occurs the session is sent to testpath

D. HA Sync occurs the firewall allows the session Put does not decrypt the session.

Correct Answer: D

QUESTION 15

A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours.

Which two steps are likely to mitigate the issue? (Choose TWO)

A. Exclude video traffic

B. Enable decryption

C. Block traffic that is not work-related

D. Create a Tunnel Inspection policy

Correct Answer: AC

This is because excluding video traffic from being sent over the VPN will reduce the amount of bandwidth being used during peak hours, allowing more bandwidth to be available for other types of traffic. Blocking non-work related traffic will also reduce the amount of bandwidth being used, further freeing up bandwidth for work-related traffic. Enabling decryption and creating a Tunnel Inspection policy are not likely to mitigate the issue of decreased performance during peak-use hours, as they do not directly address the issue of limited bandwidth availability during these times.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PP3ICAW