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.passapply.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

How can an administrator configure the NGFW to automatically quarantine a device using GlobalProtect?

A. by adding the device\\'s Host ID to a quarantine list and configure GlobalProtect to prevent users from connecting to the GlobalProtect gateway from a quarantined device

B. by using security policies, log forwarding profiles, and log settings.

C. by exporting the list of quarantined devices to a pdf or csv file by selecting PDF/CSV at the bottom of the Device Quarantine page and leveraging the approbate XSOAR playbook

D. There is no native auto-quarantine feature so a custom script would need to be leveraged.

Correct Answer: B

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new- features/globalprotect-features/identification-and-quarantine-of-compromised-devices.html https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/hostinformation/quarantine-devices-using-host-information/automatically-quarantine-a-device.html#idb42b2b82-b253-4be7-9840-1efa49dba3da

QUESTION 2

YouTube videos are consuming too much bandwidth on the network, causing delays in mission-critical traffic. The administrator wants to throttle YouTube traffic. The following interfaces and zones are in use on the firewall:

*

ethernet1/1, Zone: Untrust (Internet-facing)

*

ethernet1/2, Zone: Trust (client-facing)

A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet1/1 has a QoS profile called Outbound, and interface Ethernet1/2 has a QoS

profile called Inbound.

Which setting for class 6 with throttle YouTube traffic?

A. Outbound profile with Guaranteed Ingress

B. Outbound profile with Maximum Ingress

C. Inbound profile with Guaranteed Egress

D. Inbound profile with Maximum Egress

Correct Answer: D

QUESTION 3

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

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

A. From the Monitor tab, click Traffic view and review the information in the detailed log view.

B. From the Monitor tab, click Traffic view, ensure that the Source or Destination NAT columns are included and review the information in the detailed log view.

C. From the Monitor tab, click App Scope > Network Monitor and filter the report for NAT rules.

D. From the Monitor tab, click Session Browser and review the session details.

Correct Answer: D

QUESTION 4

In an HA failover scenario what happens with sessions decrypted by a SSL Forward Proxy Decryption policy?

A. The existing session is transferred to the active firewall.

B. The firewall drops the session.

C. The session is sent to fastpath.

D. The firewall allows the session but does not decrypt the session.

Correct Answer: D

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-concepts/decryption-and-high-availability

QUESTION 5

SD-WAN is designed to support which two network topology types? (Choose two.)

A. ring

B. point-to-point

C. hub-and-spoke

D. full-mesh

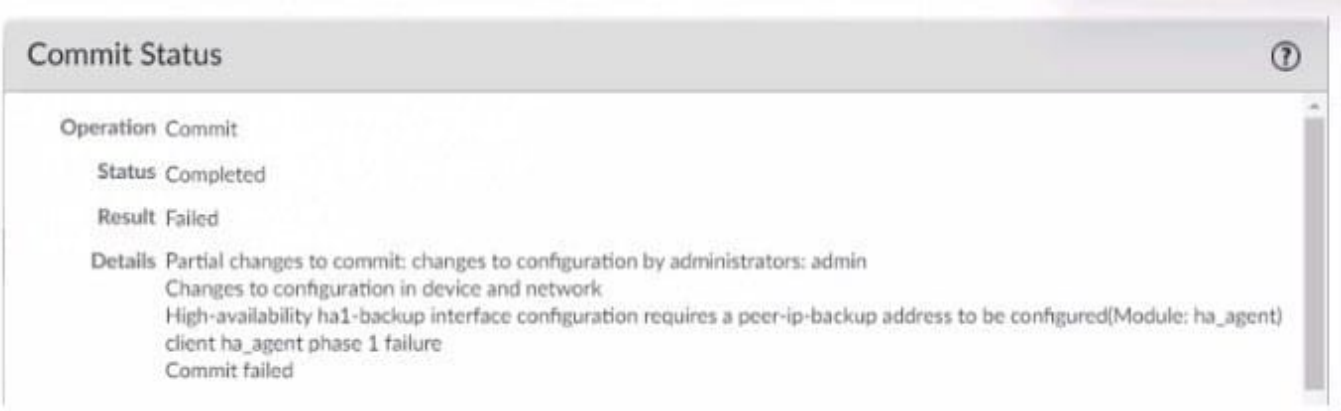
Correct Answer: CD

https://docs.paloaltonetworks.com/plugins/vm-series-and-panorama-plugins- release-notes/panorama-plugin-for-sd-

wan/sd-wan-plugin-200/features-introduced-in-sd- wan-2-0.html
https://www.paloaltonetworks.nl/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/guides/pan-os-secure-sd-wan-deployment-guide

QUESTION 6

After configuring HA in Active/Passive mode on a pair of firewalls the administrator gets a failed commit with the following details.



What are two explanations for this type of issue? (Choose two)

A. The peer IP is not included in the permit list on Management Interface Settings

B. The Backup Peer HA1 IP Address was not configured when the commit was issued

C. Either management or a data-plane interface is used as HA1-backup

D. One of the firewalls has gone into the suspended state

Correct Answer: BC

Cause The issue is seen when the HA1-backup is configured with either management (MGT) or an in-band interface. The "Backup Peer HA1 IP Address" is not configured :
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UmPCAUandlang=en_US%E2%80%A9

QUESTION 7

Which item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

A. ACC

B. System Logs

C. App Scope

D. Session Browser

Correct Answer: D

QUESTION 8

Which profile generates a packet threat type found in threat logs?

A. Zone Protection

B. WildFire

C. Anti-Spyware

D. Antivirus

Correct Answer: A

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/threat-log-fields

packet--Packet-based attack protection triggered by a Zone Protection profile.

QUESTION 9

A network administrator configured a site-to-site VPN tunnel where the peer device will act as initiator None of the peer addresses are known. What can the administrator configure to establish the VPN connection1?

A. Set up certificate authentication

B. Enable Passive Mode

C. Use the Dynamic IP address type

D. Configure the peer address as an FQDN

Correct Answer: C

When the peer device will act as the initiator and none of the peer addresses are known, the administrator can enable Passive Mode to establish the VPN connection. Passive Mode tells the firewall to wait for the peer device to initiate the VPN connection. The other options are incorrect. Option A, setting up certificate authentication, would require the administrator to know the peer device\\'s certificate. Option C, using the Dynamic IP address type, would require the administrator to know the peer device\\'s dynamic IP address. Option D, configuring the peer address as an FQDN, would require the administrator to know the peer device\\'s fully qualified domain name.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClIGCA0

QUESTION 10

Before an administrator of a VM-500 can enable DoS and zone protection, what actions need to be taken?

A. Measure and monitor the CPU consumption of the firewall data plane to ensure that each firewall is properly sized to support DoS and zone protection

B. Create a zone protection profile with flood protection configured to defend an entire egress zone against SYN. ICMP ICMPv6, UDP. and other IP flood attacks

C. Add a WildFire subscription to activate DoS and zone protection features

D. Replace the hardware firewall because DoS and zone protection are not available with VM-Series systems

Correct Answer: A

1 - https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone- protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone- protection-using-bestpractices.html#:~:text=DoS%20and%20Zone%20Protection%20help,device%20at%20the%20internet%20perimeter.

2 - https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos- protection/zone-defense/take-baseline-cps-measurements-for-setting-flood- thresholds/how-to-measure-cps.html https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos- protection.html

QUESTION 11

An engineer needs to collect User-ID mappings from the company\\'s existing proxies. What two methods can be used to pull this data from third party proxies? (Choose two.)

A. Syslog

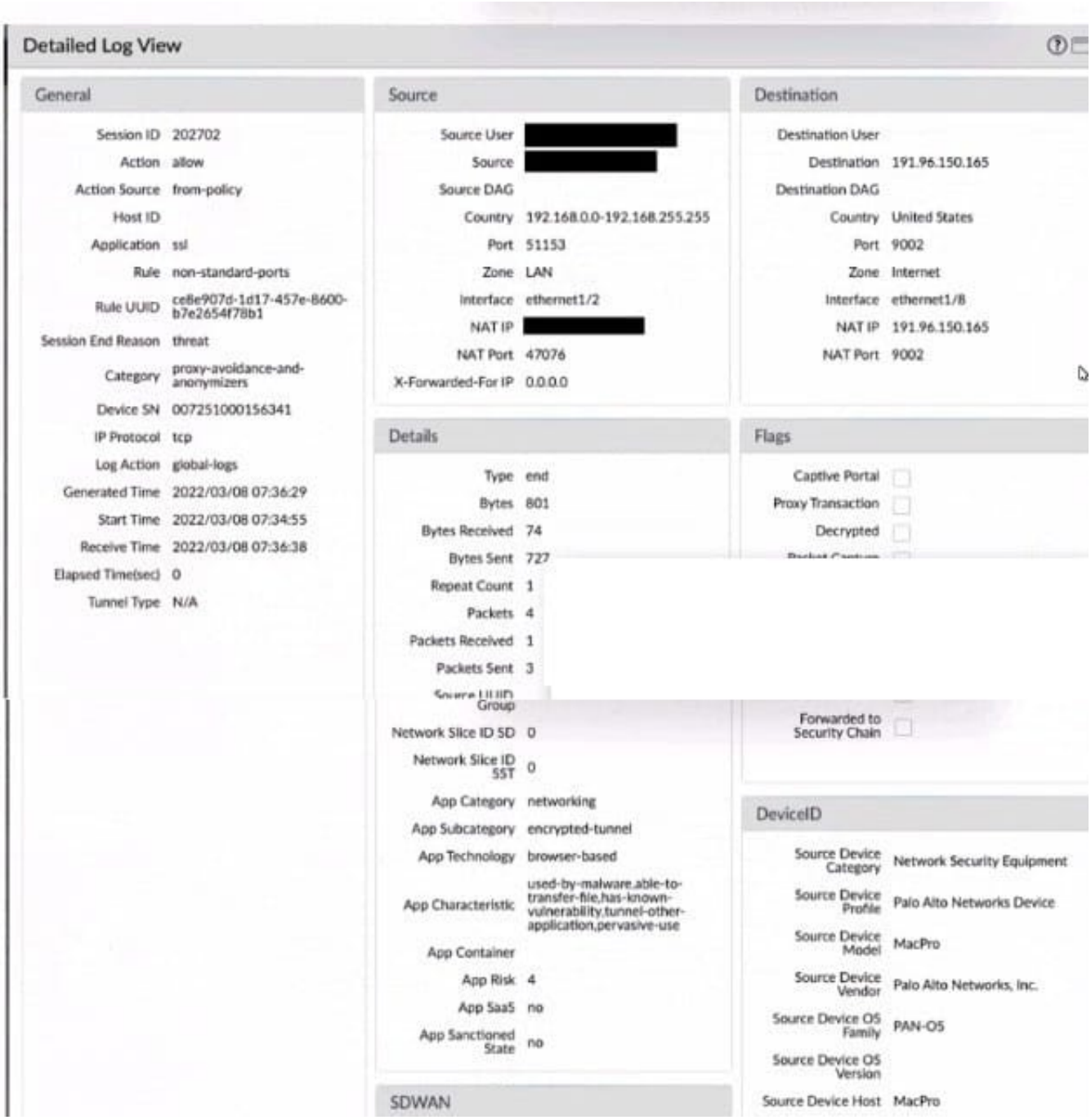
B. XFF Headers

C. Client probing

D. Server Monitoring

Correct Answer: AB

QUESTION 12



Given the screenshot, how did the firewall handle the traffic?

A. Traffic was allowed by policy but denied by profile as encrypted.

B. Traffic was allowed by policy but denied by profile as a threat.

C. Traffic was allowed by profile but denied by policy as a threat.

D. Traffic was allowed by policy but denied by profile as a nonstandard port.

Correct Answer: B

QUESTION 13

An engineer creates a set of rules in a Device Group (Panorama) to permit traffic to various services for a specific LDAP user group. What needs to be configured to ensure Panorama can retrieve user and group information for use in these rules?

A. A service route to the LDAP server

B. A Master Device

C. Authentication Portal

D. A User-ID agent on the LDAP server

Correct Answer: B

https://live.paloaltonetworks.com/t5/general-topics/what-is-a-master-device-in-device-groups/td-p/15032

QUESTION 14

Which statement accurately describes service routes and virtual systems?

A. Virtual systems can only use one interface for all global service and service routes of the firewall

B. The interface must be used for traffic to the required external services

C. Virtual systems that do not have specific service routes configured inherit the global service and service route settings for the firewall

D. Virtual systems cannot have dedicated service routes configured: and virtual systems always use the global service and service route settings for the firewall

Correct Answer: C

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/virtual-systems/customize-service-routes-for-a-virtual-system "When a firewall is enabled for multiple virtual systems, the virtual systems inherit the global service and service route settings. For example, the firewall can use a shared email server to originate email alerts to all virtual systems. In some scenarios, you\\'d want to create different service routes for each virtual system."

QUESTION 15

What are three reasons for excluding a site from SSL decryption? (Choose three.)

A. the website is not present in English

B. unsupported ciphers

C. certificate pinning

D. unsupported browser version

E. mutual authentication

Correct Answer: BCE

Reasons that sites break decryption technically include pinned certificates, client authentication, incomplete certificate chains, and unsupported ciphers. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryptionexclusions/exclude-a-server-from-decryption.html