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.leads4pass.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

A firewall administrator has been asked to configure a Palo Alto Networks NGFW to prevent against compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers. Which security Profile type will prevent these behaviors?

A. WildFire

B. Anti-Spyware

C. Vulnerability Protection

D. Antivirus

Correct Answer: B

https://www.paloaltonetworks.com/documentation/71/pan-os/pan- os/policy/anti-spyware-profiles Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients. You can apply various levels of protection between zones. For example, you may want to have custom Anti-Spyware profiles that minimize inspection between trusted zones, while maximizing inspection on traffic received from an untrusted zone, such as internet-facing zones.

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

QUESTION 2

An engineer troubleshoots an issue that causes packet drops.

Which command should the engineer run in the CLI to see if packet buffer protection is enabled and activated?

A. show session id

B. show system state | match packet-buffer-protection

C. show session packet-buffer- protection

D. show running resource-monitor

Correct Answer: C

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oNB7CAM

QUESTION 3

Which two statements are true about DoS Protection and Zone Protection Profiles? (Choose two).

A. Zone Protection Profiles protect ingress zones

B. Zone Protection Profiles protect egress zones

C. DoS Protection Profiles are packet-based, not signature-based

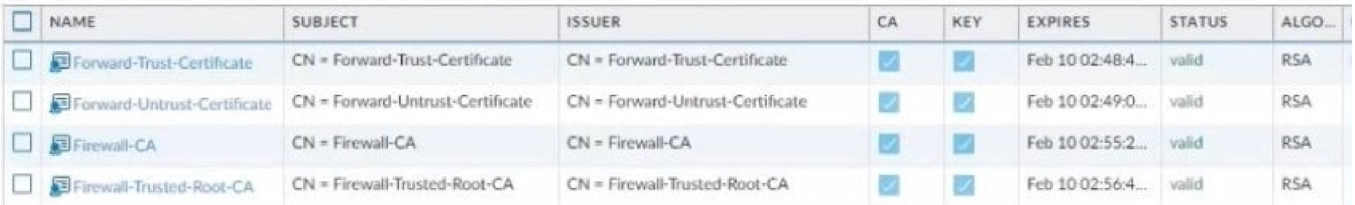
D. DoS Protection Profiles are linked to Security policy rules

Correct Answer: AD

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection- and-dos-protection/zone-defense/zone-protection-profiles

QUESTION 4

The SSL Forward Proxy decryption policy is configured. The following four certificate authority (CA) certificates are installed on the firewall.



□	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGO...
□	Forward-Trust-Certificate	CN = Forward-Trust-Certificate	CN = Forward-Trust-Certificate	☑	☑	Feb 10 02:48:4...	valid	RSA
□	Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	☑	☑	Feb 10 02:49:0...	valid	RSA
□	Firewall-CA	CN = Firewall-CA	CN = Firewall-CA	☑	☑	Feb 10 02:55:2...	valid	RSA
□	Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	☑	☑	Feb 10 02:56:4...	valid	RSA

An end-user visits the untrusted website https //www firewall-do-not-trust-website com.

Which certificate authority (CA) certificate will be used to sign the untrusted webserver certificate?

A. Forward-Untrust-Certificate

B. Forward-Trust-Certificate

C. Firewall-CA

D. Firewall-Trusted-Root-CA

Correct Answer: B

QUESTION 5

An engineer must configure the Decryption Broker feature.

Which Decryption Broker security chain supports bi-directional traffic flow?

A. Layer 2 security chain

B. Layer 3 security chain

C. Transparent Bridge security chain

D. Transparent Proxy security chain

Correct Answer: B

Together, the primary and secondary interfaces form a pair of decryption forwarding interfaces. Only interfaces that you have enabled to be Decrypt Forward interfaces are displayed here. Your security chain type (Layer 3 or Transparent Bridge) and the traffic flow direction (unidirectional or bidirectional) determine which of the two interfaces forwards allowed, clear text traffic to the security chain, and which interface receives the traffic back from the security chain after it has undergone additional enforcement.

QUESTION 6

Which three settings are defined within the Templates object of Panorama? (Choose three.)

A. Setup

B. Virtual Routers

C. Interfaces

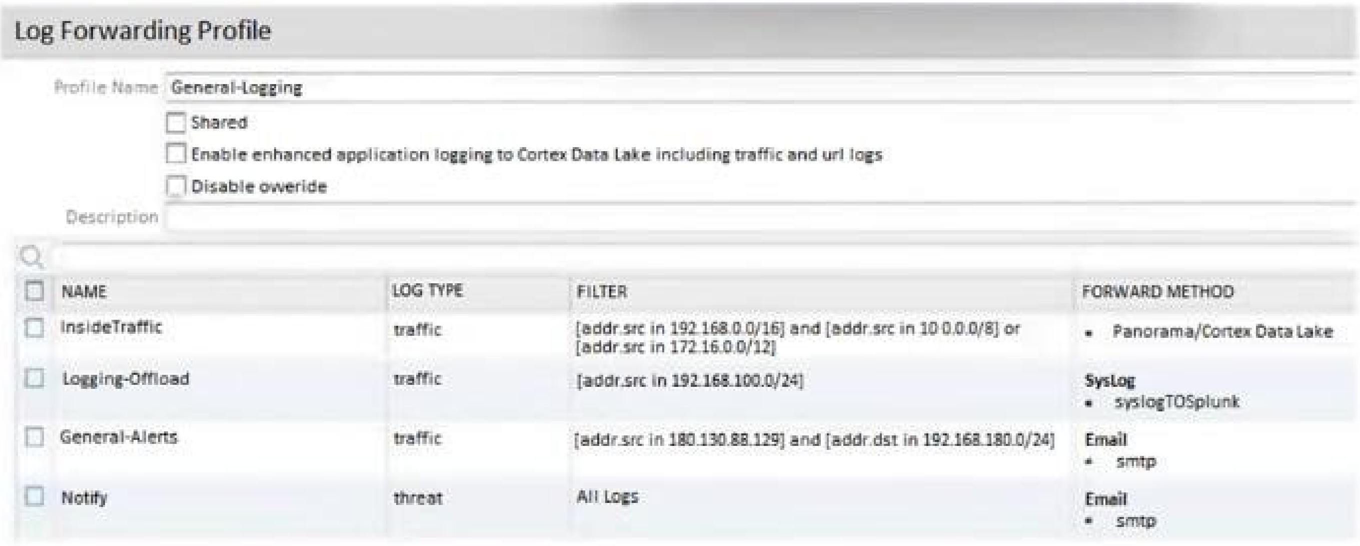
D. Security

E. Application Override

Correct Answer: ABC

QUESTION 7

Given the Sample Log Forwarding Profile shown, which two statements are true? (Choose two.)



Log Forwarding Profile

Profile Name: General-Logging

□ Shared

□ Enable enhanced application logging to Cortex Data Lake including traffic and url logs

□ Disable oweride

Description:

□	NAME	LOG TYPE	FILTER	FORWARD METHOD
□	InsideTraffic	traffic	[addr.src in 192.168.0.0/16] and [addr.src in 10.0.0.0/8] or [addr.src in 172.16.0.0/12]	• Panorama/Cortex Data Lake
□	Logging-Offload	traffic	[addr.src in 192.168.100.0/24]	Syslog • syslogTOSplunk
□	General-Alerts	traffic	[addr.src in 180.130.88.129] and [addr.dst in 192.168.180.0/24]	Email • smtp
□	Notify	threat	All Logs	Email • smtp

A. All traffic from source network 192.168.100.0/24 is sent to an external syslog target.

B. All threats are logged to Panorama.

C. All traffic logs from RFC 1918 subnets are logged to Panorama / Cortex Data Lake.

D. All traffic from source network 172.12.0.0/24 is sent to Panorama / Cortex Data Lake.

Correct Answer: AC

B is not correct as it is sent externally not to Panorama D is not correct as it is 172.12 (not 172.16)

QUESTION 8

A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.

Which two mandatory options are used to configure a VLAN interface? (Choose two.)

A. Virtual router

B. Security zone

C. ARP entries

D. Netflow Profile

Correct Answer: AB

Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface- help/network/network-interfaces/pa-7000-series- layer-2-interface#idd2bcaacc-54b9-4ec9- a1dd-8064499f5b9d

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRqCAK

VLAN interface is not necessary but in this scenario we assume it is. Create VLAN object, VLAN interface and VLAN Zone. Attach VLAN interface to VLAN object together with two L2 interfaces then attach VLAN interface to virtual router. Without VLAN interface you can pass traffic between interfaces on the same network and with VLAN interface you can route traffic to other networks.

QUESTION 9

An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab. Which profile is the cause of the missing Policies tab?

A. Admin Role

B. WebUI

C. Authentication

D. Authorization

Correct Answer: A

QUESTION 10

A network engineer troubleshoots a VPN Phase 2 mismatch and decides that PFS (Perfect Forward Secrecy) needs to be enabled.

What action should the engineer take?

A. Add an authentication algorithm in the IPSec Crypto profile.

B. Enable PFS under the IPSec Tunnel advanced options.

C. Select the appropriate DH Group under the IPSec Crypto profile.

D. Enable PFS under the IKE gateway advanced options

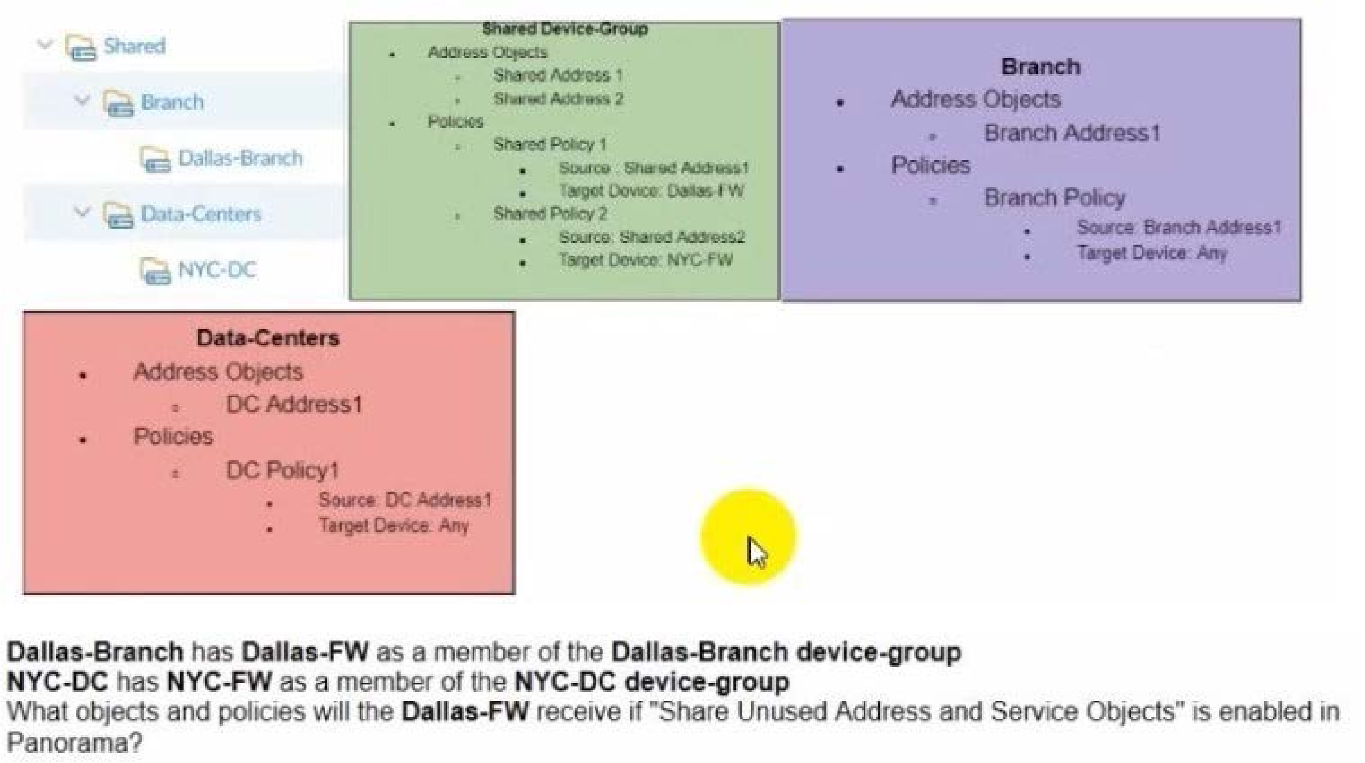
Correct Answer: C

PFS (Perfect Forward Secrecy) is a feature that ensures that the encryption keys used for each IPSec session are not derived from previous keys. This provides more security in case one key is compromised. To enable PFS, the administrator needs to select the appropriate DH (Diffie-Hellman) Group under the IPSec Crypto profile that is applied to the IPSec tunnel. The DH Group determines the strength of the key exchange and should match on both ends of the tunnel1. The other options do not enable PFS. The authentication algorithm in the IPSec Crypto profile is used to verify the integrity of the IPSec packets. The PFS option under the IPSec Tunnel advanced options or the IKE gateway advanced options does not exist in the WebUI.

References: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpn/site-to-site-vpn/configure-the-ipsec-crypto-profile

QUESTION 11

The following objects and policies are defined in a device group hierarchy A. Option A



Shared Device-Group

- Address Objects
  - Shared Address 1
  - Shared Address 2
- Policies
  - Shared Policy 1
    - Source : Shared Address1
    - Target Device: Dallas-FW
  - Shared Policy 2
    - Source: Shared Address2
    - Target Device: NYC-FW

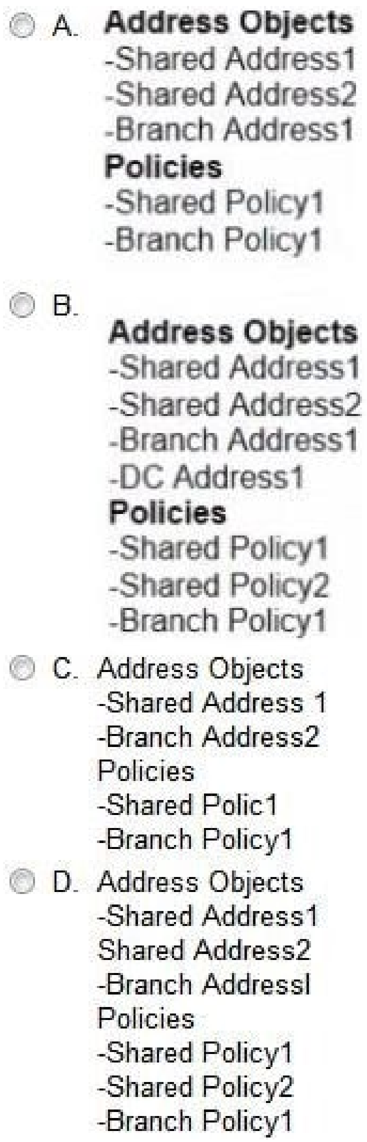
Branch

- Address Objects
  - Branch Address1
- Policies
  - Branch Policy
    - Source: Branch Address1
    - Target Device: Any

Data-Centers

- Address Objects
  - DC Address1
- Policies
  - DC Policy1
    - Source: DC Address1
    - Target Device: Any

Dallas-Branch has **Dallas-FW** as a member of the **Dallas-Branch device-group**
NYC-DC has **NYC-FW** as a member of the **NYC-DC device-group**
What objects and policies will the **Dallas-FW** receive if "Share Unused Address and Service Objects" is enabled in Panorama?



○ A. **Address Objects**
-Shared Address1
-Shared Address2
-Branch Address1
Policies
-Shared Policy1
-Branch Policy1

○ B. **Address Objects**
-Shared Address1
-Shared Address2
-Branch Address1
-DC Address1
Policies
-Shared Policy1
-Shared Policy2
-Branch Policy1

○ C. Address Objects
-Shared Address 1
-Branch Address2
Policies
-Shared Polic1
-Branch Policy1

○ D. Address Objects
-Shared Address1
Shared Address2
-Branch Addressl
Policies
-Shared Policy1
-Shared Policy2
-Branch Policy1

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 12

Which four NGFW multi-factor authentication factors are supported by PAN-OS? (Choose four.)

A. Short message service

B. Push

C. User logon

D. Voice

E. SSH key

F. One-Time Password

Correct Answer: ABDF

https://docs.paloaltonetworks.com/pan-os/8-0/pan-os- admin/authentication/authentication-types/multi-factor-authentication Push - An endpoint device (such as a phone or tablet) prompts the user to allow or deny authentication. Short

message service (SMS) - An SMS message on the endpoint device prompts the user to allow or deny authentication. In some cases, the endpoint device provides a code that the user must enter in the MFA login page.

Voice - An automated phone call prompts the user to authenticate by pressing a key on the phone or entering a code in the MFA login page.

One-time password (OTP) - An endpoint device provides an automatically generated alphanumeric string, which the user enters in the MFA login page to enable authentication for a single transaction or session.

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication- types/multi-factor-authentication.html#idbc927952-a47e-4bec-ab80-0605a47b4873

QUESTION 13

In a template, which two objects can be configured? (Choose two.)

A. SD-WAN path quality profile

B. Monitor profile

C. IPsec tunnel

D. Application group

Correct Answer: BC

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-monitor.html

QUESTION 14

An engineer is pushing configuration from Panorama lo a managed firewall.

What happens when the pushed Panorama configuration has Address Object names that duplicate the Address Objects already configured on the firewall?

A. The firewall rejects the pushed configuration, and the commit fails.

B. The firewall renames the duplicate local objects with "-1" at the end signifying they are clones; it will update the references to the objects accordingly and fully commit the pushed configuration.

C. The firewall fully commits all of the pushed configuration and overwrites its locally configured objects

D. The firewall ignores only the pushed objects that have the same name as the locally configured objects, and it will commit the rest of the pushed configuration.

Correct Answer: A

QUESTION 15

How can Panorama help with troubleshooting problems such as high CPU or resource exhaustion on a managed firewall?

A. Firewalls send SNMP traps to Panorama when resource exhaustion is detected Panorama generates a system log and can send email alerts

B. Panorama provides visibility into all the system and traffic logs received from firewalls it does not offer any ability to see or monitor resource utilization on managed firewalls

C. Panorama monitors all firewalls using SNMP It generates a system log and can send email alerts when resource exhaustion is detected on a managed firewall

D. Panorama provides information about system resources of the managed devices in the Managed Devices > Health menu

Correct Answer: D

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