Vendor: Palo Alto Networks

Exam Code:PCNSE

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

Version: Demo

QUESTION 1

An engineer is monitoring an active/passive high availability (HA) firewall pair. Which HA firewall state describes the firewall that is currently processing traffic?

A. Active-primary

B. Active

C. Active-secondary

D. Initial

Correct Answer: B

QUESTION 2

A firewall engineer creates a source NAT rule to allow the company\\'s internal private network 10.0.0.0/23 to access the internet. However, for security reasons, one server in that subnet (10.0.0.10/32) should not be allowed to access the internet, and therefore should not be translated with the NAT rule.

Which set of steps should the engineer take to accomplish this objective?

A. 1. Create a NAT rule (NAT-Rule-1) and set the source address in the original packet to 10.0.0.10/32.

2. Check the box for negate option to negate this IP from the NAT translation.

B. 1. Create a NAT rule (NAT-Rule-1) and set the source address in the original packet to 10.0.0.0/23.

2. Check the box for negate option to negate this IP subnet from NAT translation.

C. 1. Create a source NAT rule (NAT-Rule-1) to translate 10.0.0/23 with source address translation set to dynamic IP and port.

2.

Create another NAT rule (NAT-Rule-2) with source IP address in the original packet set to 10.0.0.10/32 and source translation set to none.

3.

Place (NAT-Rule-2) above (NAT-Rule-1).

D. 1. Create a source NAT rule (NAT-Rule-1) to translate 10.0.0/23 with source address translation set to dynamic IP and port.

2.

Create another NAT rule (NAT-Rule-2) with source IP address in the original packet set to 10.0.0.10/32 and source translation set to none.

3.

Place (NAT-Rule-1) above (NAT-Rule-2).

Correct Answer: C

NAT-Rule-2 needs to be above NAT-Rule-1 or else Rule 1 will shadow Rule 2 and Rule 2 will never get used.

QUESTION 3

A network security engineer configured IP multicast in the virtual router to support a new application. Users in different network segments are reporting that they are unable to access the application.

What must be enabled to allow an interface to forward multicast traffic?

A. IGMP

B. PIM

C. BFD

D. SSM

Correct Answer: B

A protocol that enables routers to forward multicast traffic efficiently based on the source and destination addresses. PIM can operate in two modes: sparse mode (PIM- SM) or dense mode (PIM-DM). PIM-SM uses a rendezvous point (RP) as a central point for distributing multicast traffic, while PIM-DM uses flooding and pruning techniques2. to enable PIM on the interface which allows routers to forward multicast traffic using either sparse mode or dense mode depending on your network topology and requirements.

QUESTION 4

An administrator notices that an interlace configuration has been overridden locally on a firewall. They require an configuration to be managed from Panorama and overrides are not allowed. What is one way the administrator can meet this requirement?

A. Perform a device-group commit push from Panorama using the "Include Device and Network Templates" option.

B. Reload the running configuration and perform a Firewall local commit.

C. Perform a template commit push from Panorama using the "Force Template Values\\'\\' option

D. Perform a commit force from the CLI of the firewall.

Correct Answer: C

The best way for the administrator to meet the requirement of managing all configuration from Panorama and preventing local overrides is B: Perform a template commit push from Panorama using the "Force Template Values" option. This option allows the administrator to overwrite any local configuration on the firewall with the values defined in the template1. This way, the administrator can ensure that the interface configuration and any other

---

QUESTION 5

The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

A. 6-tuple match: Source IP Address, Destination IP Address, Source port, Destination Port, Protocol, and Source Security Zone

B. 5-tuple match: Source IP Address, Destination IP Address, Source port, Destination Port, Protocol

C. 7-tuple match: Source IP Address, Destination IP Address, Source port, Destination Port, Source User, URL Category, and Source Security Zone

D. 9-tuple match: Source IP Address, Destination IP Address, Source port, Destination Port, Source User, Source Security Zone, Destination Security Zone, Application, and URL Category

Correct Answer: A

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVECA0 On a Palo Alto Networks firewall, a session is defined by two uni-directional flows each uniquely identified by a 6-tuple key: source-address, destination-address, source-port, destination-port, protocol, and security-zone.

QUESTION 6

An administrator wants to upgrade an NGFW from PAN-OS 9.0 to PAN-OS 10.0. The firewall is not a part of an HA pair. What needs to be updated first?

A. XML Agent

B. Applications and Threats

C. WildFire

D. PAN-OS Upgrade Agent

Correct Answer: B

https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to- pan-os-80/upgrade-the-firewall-to-pan-os-80/upgrade-a-firewall-to-pan-os-80

QUESTION 7

A network engineer is troubleshooting a VPN and wants to verify whether the decapsulation/encapsulation counters are increasing. Which CLI command should the engineer run?

A. Show vpn tunnel name | match encap

B. Show vpn flow name

C. Show running tunnel flow lookup

D. Show vpn ipsec-sa tunnel

Correct Answer: B

QUESTION 8

An administrator needs to implement an NGFW between their DMZ and Core network. EIGRP Routing between the two environments is required. Which interface type would support this business requirement?

A. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ

B. Layer 3 or Aggregate Ethernet interfaces, but configuring EIGRP on subinterfaces only

C. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel (with the GlobalProtect License to support LSVPN and EIGRPprotocols)

D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

Correct Answer: A

EIGRP is a Cisco proprietary protocol. The dynamic routing protocols supported on the PAN are RIPv2, OSPF and BGP.

QUESTION 9

A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation. Which two formats are correct for naming aggregate interfaces? (Choose two.)

A. ae.8

B. aggregate.1

C. ae.1

D. aggregate.8

Correct Answer: AC

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface- help/network/network-interfaces/aggregate-ethernet-ae-interface-group.html

---

QUESTION 10

DRAG DROP

Please match the terms to their corresponding definitions.

Select and Place:

management plane	security processing
signature matching	network processing

	provides configuration, logging, and reporting separate processor, RAM, and hard drive
	stream-based, uniform signature matching in exploits (IPS), virus, spyware, CC#, and SSN
	high-density parallel processing for flexible standardized complex functions
	network processing hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Correct Answer:

management plane	provides configuration, logging, and reporting separate processor, RAM, and hard drive
signature matching	stream-based, uniform signature matching in exploits (IPS), virus, spyware, CC#, and SSN
security processing	high-density parallel processing for flexible standardized complex functions
network processing	network processing hardware-accelerated per-packet route lookup, MAC lookup, and NAT

QUESTION 11

After implementing a new NGFW, a firewall engineer sees a VoIP traffic issue going through the firewall After troubleshooting the engineer finds that the firewall performs NAT on the voice packets payload and opens dynamic pinholes for media ports

What can the engineer do to solve the VoIP traffic issue?

A. Disable ALG under H.323 application

B. Increase the TCP timeout under H.323 application

C. Increase the TCP timeout under SIP application

D. Disable ALG under SIP application

Correct Answer: D

According to the Palo Alto Networks documentation1, application-level gateway (ALG) is a feature that allows the firewall to inspect and modify the payload of some protocols, such as SIP, to enable NAT traversal and firewall policy enforcement. However, ALG can also cause issues with some VoIP implementations, such as modifying the SIP headers incorrectly or opening unnecessary pinholes for media ports. Therefore, disabling ALG under SIP application can help solve the VoIP traffic issue by preventing the firewall from altering the voice packets payload and opening dynamic pinholes2. Therefore, the correct answer is D. The other options are not relevant or helpful for solving the VoIP

traffic issue: Disable ALG under H.323 application: This option would disable ALG for H.323 protocol, which is another VoIP protocol, but not the one used in this scenario. The scenario mentions SIP as the signaling protocol, so disabling ALG under

H.323 application would have no effect on the VoIP traffic issue. Increase the TCP timeout under H.323 application: This option would increase the TCP timeout for H.323 protocol, which is another VoIP protocol, but not the one used in this scenario. The scenario mentions SIP as the signaling protocol, which uses UDP by default, so increasing the TCP timeout under H.323 application would have no effect on the VoIP traffic issue. Increase the TCP timeout under SIP application: This option would increase the TCP timeout for SIP protocol, which is the signaling protocol used in this scenario. However, SIP uses UDP by default, so increasing the TCP timeout would have no effect on the VoIP traffic issue. Moreover, increasing the TCP timeout would not address the problem of NAT on the voice packets payload and dynamic pinholes for media ports.

References:

1: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/disable-the-sip-application-level-gateway-alg

2: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEsCAK

QUESTION 12

What is the purpose of the firewall decryption broker?

A. Decrypt SSL traffic a then send it as cleartext to a security chain of inspection tools

B. Force decryption of previously unknown cipher suites

C. Inspection traffic within IPsec tunnel

D. Reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools

Correct Answer: A

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new- features/decryption-features/decryption-broker