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

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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A. System Logs

B. Task Manager

C. Traffic Logs

D. Configuration Logs

Correct Answer: AB

A. System Logs: The system logs contain information about various events that occur on the firewall, including the commit process. The administrator can review the system logs to verify whether the commit completed successfully or whether there were any errors or warnings during the commit process. B. Task Manager: The task manager displays a list of all active tasks on the firewall, including the commit task. The administrator can use the task manager to check the status of the commit task, including whether it is in progress, completed successfully, or failed.

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/monitoring/view- and-manage-logs/log-types-and-severity-levels/config-logs https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/web-interface-basics/taskmanager.html

QUESTION 2

A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured.

What can be the cause of this problem?

A. No Zone has been configured on Ethernet 1/4.

B. Interface Ethernet 1/1 is in Virtual Wire Mode.

C. DNS has not been properly configured on the firewall.

D. DNS has not been properly configured on the host.

Correct Answer: A

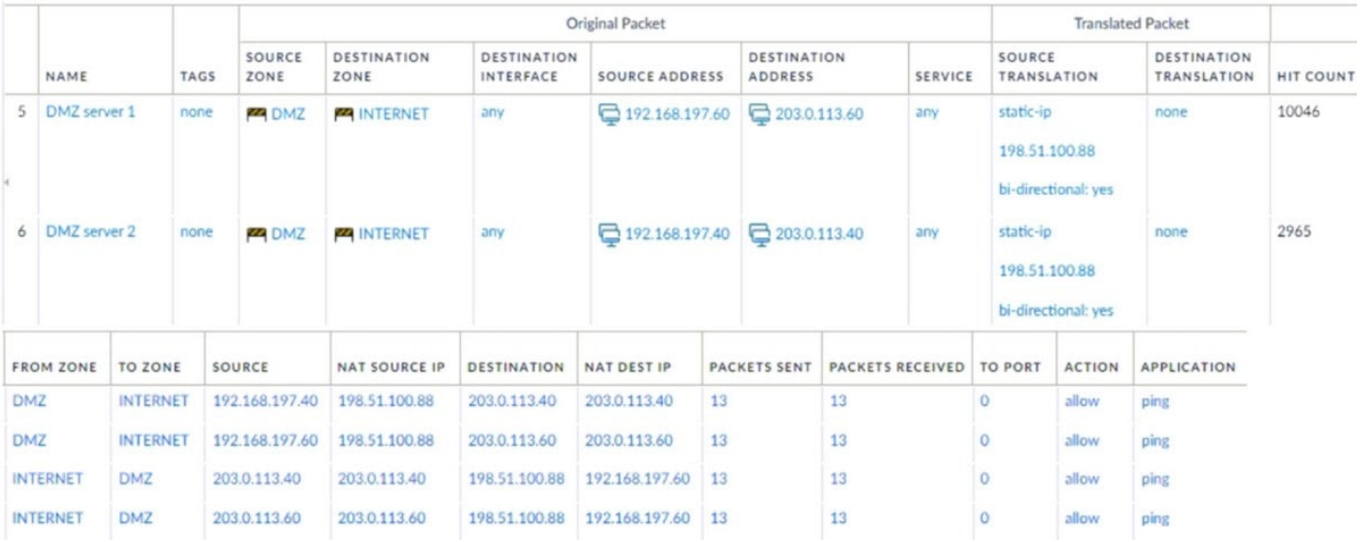
QUESTION 3

A new application server 192.168.197.40 has been deployed in the DMZ. There are no public IP addresses available, resulting in the server sharing NAT IP 198.51.100.88 with another DMZ serve that uses IP address 192.168.197.60.

Firewall security and NAT rules have been configured. The application team has confirmed that the new server is able to establish a secure connection to an external database with IP address 203.0.113.40.

The database team reports that they are unable to establish a secure connection to 198.51.100.88 from 203.0.113.40. However, it confirms a successful ping test to 198.51.100.88.

Referring to the NAT configuration and traffic logs provided how can the firewall engineer resolve the situation and ensure inbound and outbound connections work concurrently for both DMZ servers?



			Original Packet						Translated Packet		
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION	HIT COUNT
5	DMZ server 1	none	DMZ	INTERNET	any	192.168.197.60	203.0.113.60	any	static-ip 198.51.100.88 bi-directional: yes	none	10046
6	DMZ server 2	none	DMZ	INTERNET	any	192.168.197.40	203.0.113.40	any	static-ip 198.51.100.88 bi-directional: yes	none	2965

FROM ZONE	TO ZONE	SOURCE	NAT SOURCE IP	DESTINATION	NAT DEST IP	PACKETS SENT	PACKETS RECEIVED	TO PORT	ACTION	APPLICATION
DMZ	INTERNET	192.168.197.40	198.51.100.88	203.0.113.40	203.0.113.40	13	13	0	allow	ping
DMZ	INTERNET	192.168.197.60	198.51.100.88	203.0.113.60	203.0.113.60	13	13	0	allow	ping
INTERNET	DMZ	203.0.113.40	203.0.113.40	198.51.100.88	192.168.197.60	13	13	0	allow	ping
INTERNET	DMZ	203.0.113.60	203.0.113.60	198.51.100.88	192.168.197.60	13	13	0	allow	ping

A. Move the NAT rule 6 DMZ server 2 above NAT rule 5 DMZ server 1.

B. Replace the two NAT rules with a single rule that has both DMZ servers as "Source Address" both external servers as "Destination Address," and Source Translation remaining as is with bidirectional option enabled.

C. Configure separate source NAT and destination NAT rules for the two DMZ servers without using the bidirectional option.

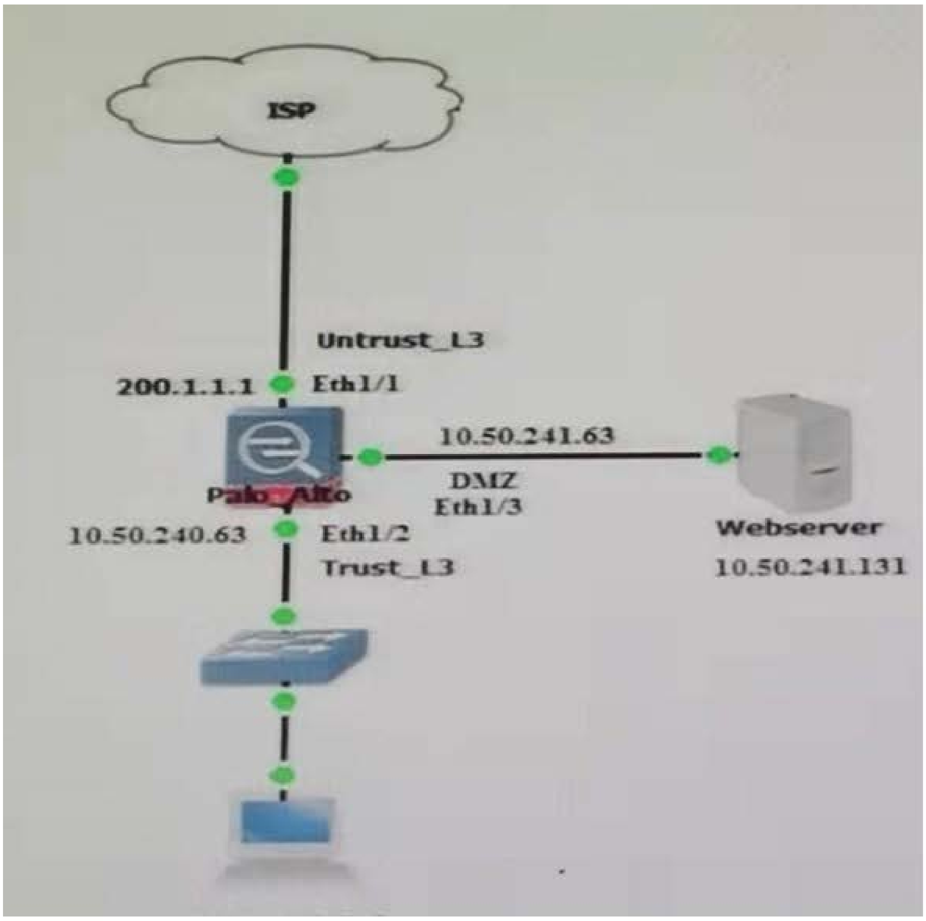
D. Sharing a single NAT IP is possible for outbound connectivity not for inbound therefore a new public IP address must be obtained for the new DMZ server and used in the NAT rule 6 DMZ server 2.

Correct Answer: D

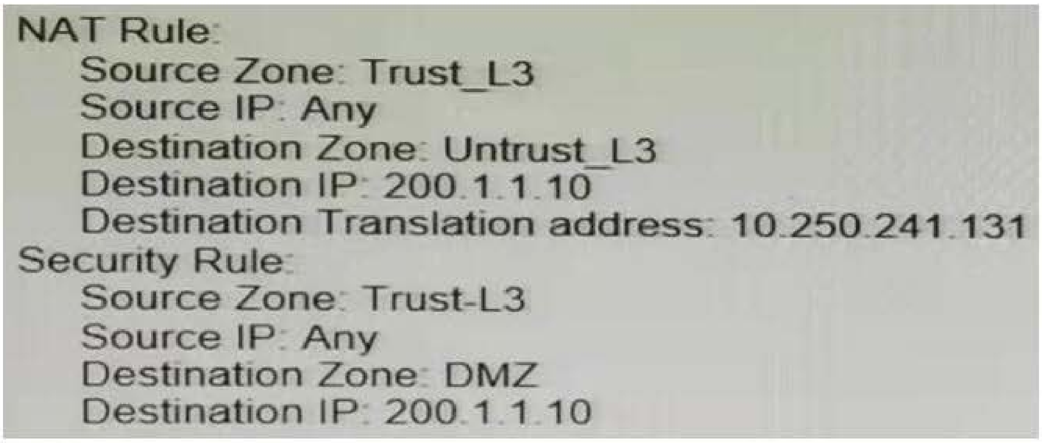
QUESTION 4

A user at an internal system queries the DNS server for their web server with a private IP of 10 250 241 131 in the. The DNS server returns an address of the web server\\'s public address, 200.1.1.10.

In order to reach the web server, which security rule and U-Turn NAT rule must be configured on the firewall?



○ A.



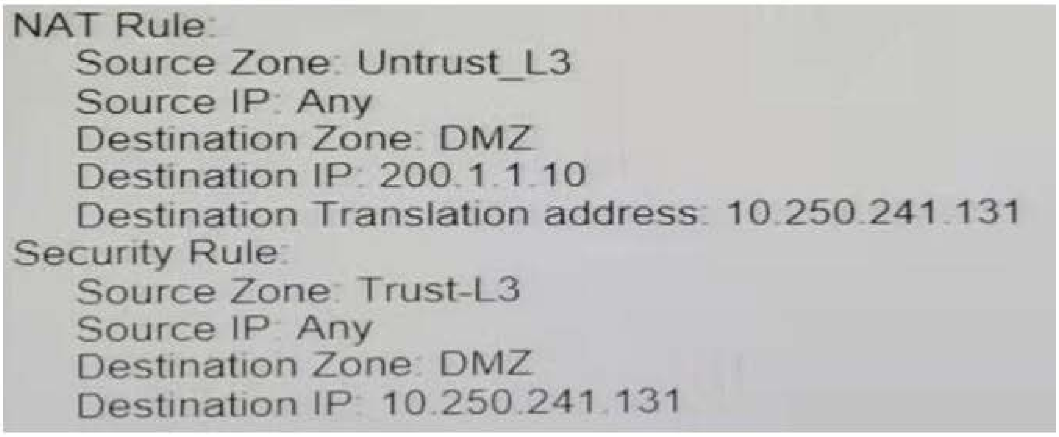
NAT Rule:

Source Zone: Trust_L3
Source IP: Any
Destination Zone: Untrust_L3
Destination IP: 200.1.1.10
Destination Translation address: 10.250.241.131

Security Rule:

Source Zone: Trust-L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 200.1.1.10

○ B.



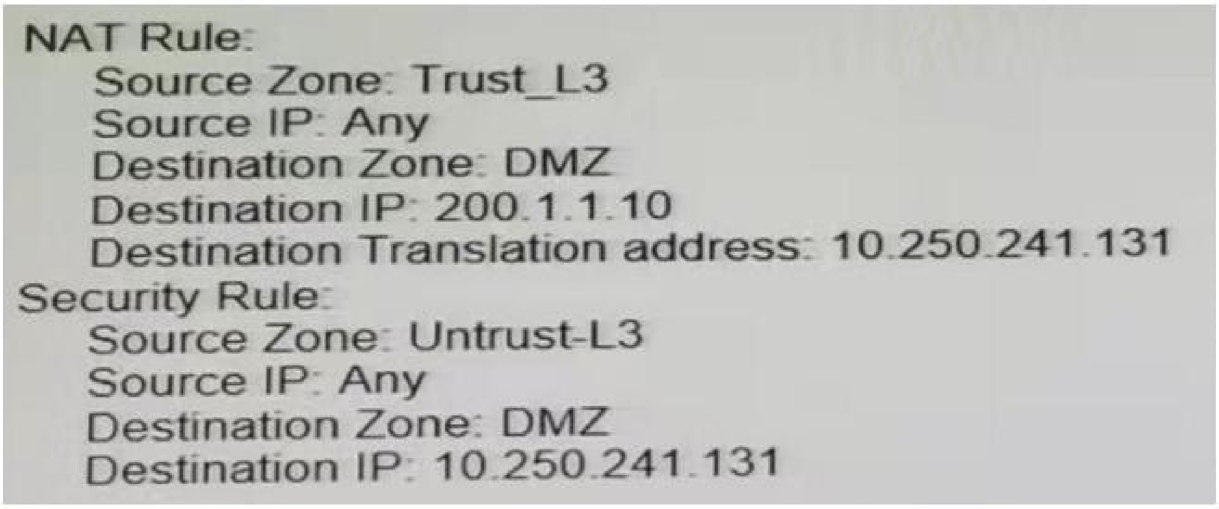
NAT Rule:

Source Zone: Untrust_L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 200.1.1.10
Destination Translation address: 10.250.241.131

Security Rule:

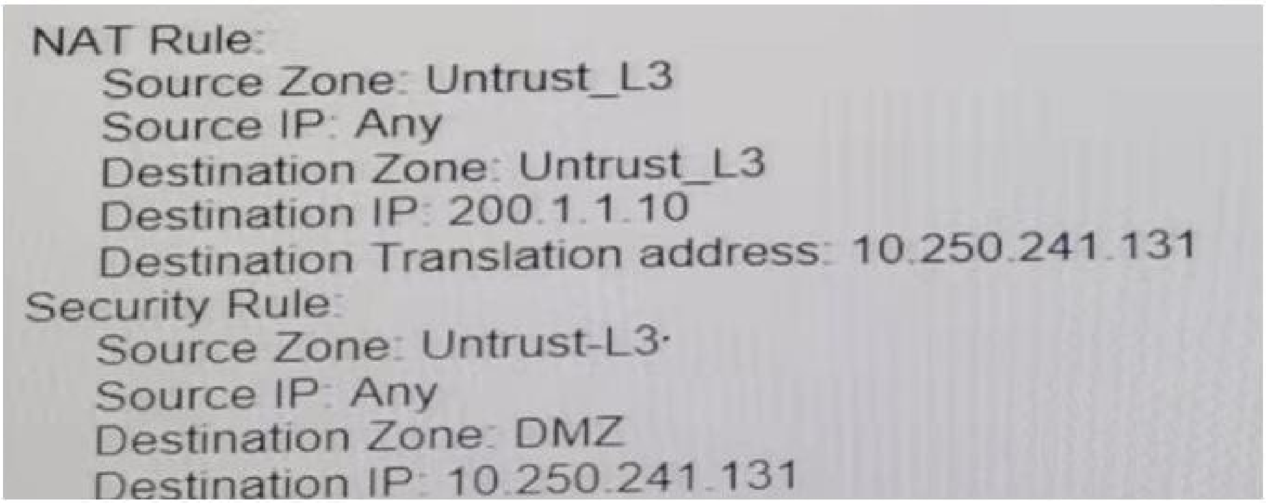
Source Zone: Trust-L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 10.250.241.131

○ C.



NAT Rule:
Source Zone: Trust_L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 200.1.1.10
Destination Translation address: 10.250.241.131
Security Rule:
Source Zone: Untrust-L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 10.250.241.131

○ D.



NAT Rule:
Source Zone: Untrust_L3
Source IP: Any
Destination Zone: Untrust_L3
Destination IP: 200.1.1.10
Destination Translation address: 10.250.241.131
Security Rule:
Source Zone: Untrust-L3·
Source IP: Any
Destination Zone: DMZ
Destination IP: 10.250.241.131

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 5

After pushing a security policy from Panorama to a PA-3020 firwall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama\\'s traffic logs. What could be the problem?

A. A Server Profile has not been configured for logging to this Panorama device.

B. Panorama is not licensed to receive logs from this particular firewall.

C. The firewall is not licensed for logging to this Panorama device.

D. None of the firwwall\\'s policies have been assigned a Log Forwarding profile

Correct Answer: D

QUESTION 6

The same route appears in the routing table three times using three different protocols. Which mechanism determines how the firewall chooses which route to use?

A. Administrative distance

B. Round Robin load balancing

C. Order in the routing table

D. Metric

Correct Answer: A

Administrative distance is the measure of trustworthiness of a routing protocol. It is used to determine the best path when multiple routes to the same destination exist. The route with the lowest administrative distance is chosen as the best route.

QUESTION 7

Users within an enterprise have been given laptops that are joined to the corporate domain. In some cases, IT has also deployed Linux-based OS systems with a graphical desktop. Information Security needs IP-to-user mapping, which it will use in group-based policies that will limit internet access for the Linux desktop users.

Which method can capture IP-to-user mapping information for users on the Linux machines?

A. You can configure Captive Portal with an authentication policy.

B. IP-to-user mapping for Linux users can only be learned if the machine is joined to the domain.

C. You can set up a group-based security policy to restrict internet access based on group membership

D. You can deploy the User-ID agent on the Linux desktop machines

Correct Answer: D

QUESTION 8

Palo Alto Networks maintains a dynamic database of malicious domains.

Which two Security Platform components use this database to prevent threats? (Choose two)

A. Brute-force signatures

B. BrightCloud Url Filtering

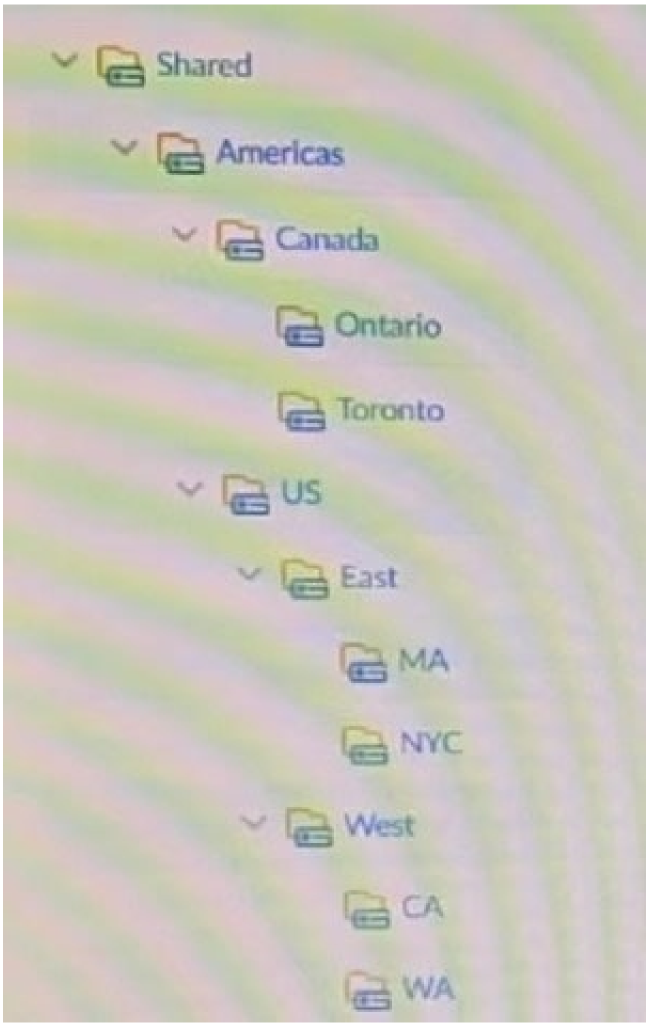
C. PAN-DB URL Filtering

D. DNS-based command-and-control signatures

Correct Answer: CD

QUESTION 9

Refer to the diagram.



- Shared
  - Americas
    - Canada
      - Ontario
      - Toronto
    - US
      - East
        - MA
        - NYC
      - West
        - CA
        - WA

An administrator needs to create an address object that will be useable by the NYC. MA, CA and WA device groups.

Where will the object need to be created within the device-group hierarchy?

A. Americas

B. US

C. East

D. West

Correct Answer: A

QUESTION 10

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

A. Layer 1

B. Layer 3

C. Tap

D. Decryption Mirror

Correct Answer: B

QUESTION 11

An administrator is using Panorama to manage me and suspects an IKE Crypto mismatch between peers, from the firewalls to Panorama. However, pre-existing logs from the firewalls are not appearing in Panorama. Which action should be taken to enable the firewalls to send their pre-existing logs to Panorama?

A. Export the log database.

B. Use the import option to pull logs.

C. Use the ACC to consolidate the logs.

D. Use the scp logdb export command.

Correct Answer: A

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 12

What is a correct statement regarding administrative authentication using external services with a local authorization method?

A. Prior to PAN-OS 10.2. an administrator used the firewall to manage role assignments, but access domains have not been supported by this method.

B. Starting with PAN-OS 10.2. an administrator needs to configure Cloud Identity Engine to use external authentication services for administrative authentication.

C. The administrative accounts you define locally on the firewall serve as references to the accounts defined on an external authentication server.

D. The administrative accounts you define on an external authentication server serve as references to the accounts defined locally on the firewall.

Correct Answer: C

The administrative accounts you define locally on the firewall serve as references to the accounts defined on an external Multi-Factor Authentication, SAML, Kerberos, TACACS+, RADIUS, or LDAP server. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication

QUESTION 13

If an administrator wants to decrypt SMTP traffic and possesses the server\\'s certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

A. TLS Bidirectional Inspection

B. SSL Inbound Inspection

C. SSH Forward Proxy

D. SMTP Inbound Decryption

Correct Answer: B

Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan- os/decryption/configure-ssl-inbound-inspection

1.

SSL Forward Proxy - Inside to Outside (To the the internet)

2.

SSL Inbound Proxy - Outside to Inside (usually towards a hosted webserver in your net)

3.

SSH Forward Proxy - As is states, for SSH traffic. The important one to remember for this type of decryption is that no certs are required.

QUESTION 14

Which three multi-factor authentication methods can be used to authenticate access to the firewall? (Choose three.)

A. One-time password

B. User certificate

C. Voice

D. SMS

E. Fingerprint

Correct Answer: ABD

The firewall can use three multi-factor authentication methods to authenticate access to the firewall: SMS, user certificate, and one-time password. These methods can be used in combination with other authentication factors, such as username and password, to provide stronger security for accessing the firewall web interface or CLI. The firewall can integrate with various MFA vendors that support these methods through RADIUS or SAML protocols. Voice and fingerprint are not supported by the firewall as MFA methods. References: MFA Vendor Support, PCNSE Study Guide (page 48)

QUESTION 15

A firewall engineer is configuring quality of service (QoS) policy for the IP address of a specific server in an effort to limit the bandwidth consumed by frequent downloads of large files from the internet.

Which combination of pre-NAT and/or post-NAT information should be used in the QoS rule?

A. Pre-NAT source IP address Pre-NAT source zone

B. Post-NAT source IP address Pre-NAT source zone

C. Pre-NAT source IP address Post-NAT source zone

D. Post-NAT source IP address Post-NAT source zone

Correct Answer: B

When configuring Quality of Service (QoS) policies, particularly for traffic going to or from specific IP addresses and involving NAT, it\\'s important to base the rule on how the firewall processes the traffic. For QoS, the firewall evaluates traffic using pre-NAT IP addresses and zones because QoS policies typically need to be applied before the NAT action occurs. This is especially true for inbound traffic, where the goal is to limit bandwidth before the destination IP is translated.

The correct combination for a QoS rule in this scenario, where the aim is to limit bandwidth for downloads from a specific server (implying inbound traffic to the server), would be:

Pre-NAT source IP address

Pre-NAT source zone:

Pre-NAT source IP address: This refers to the original IP address of the client or source device before any NAT rules are applied. Since QoS policies are evaluated before NAT, using the pre-NAT IP address ensures that the policy applies to

the correct traffic.

Pre-NAT source zone: This is the zone associated with the source interface before NAT takes place. Using the pre-NAT zone ensures that the QoS policy is applied to traffic as it enters the firewall, before any translations or routing decisions are made.

By configuring the QoS rule with pre-NAT information, the firewall can accurately apply bandwidth limitations to the intended traffic, ensuring efficient use of network resources and mitigating the impact of large file downloads from the specified server.

For detailed guidelines on configuring QoS policies, refer to the Palo Alto Networks documentation, which provides comprehensive instructions and best practices for managing bandwidth and traffic priorities on the network.

PCNSE VCE Dumps PCNSE Study Guide PCNSE Exam Questions