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

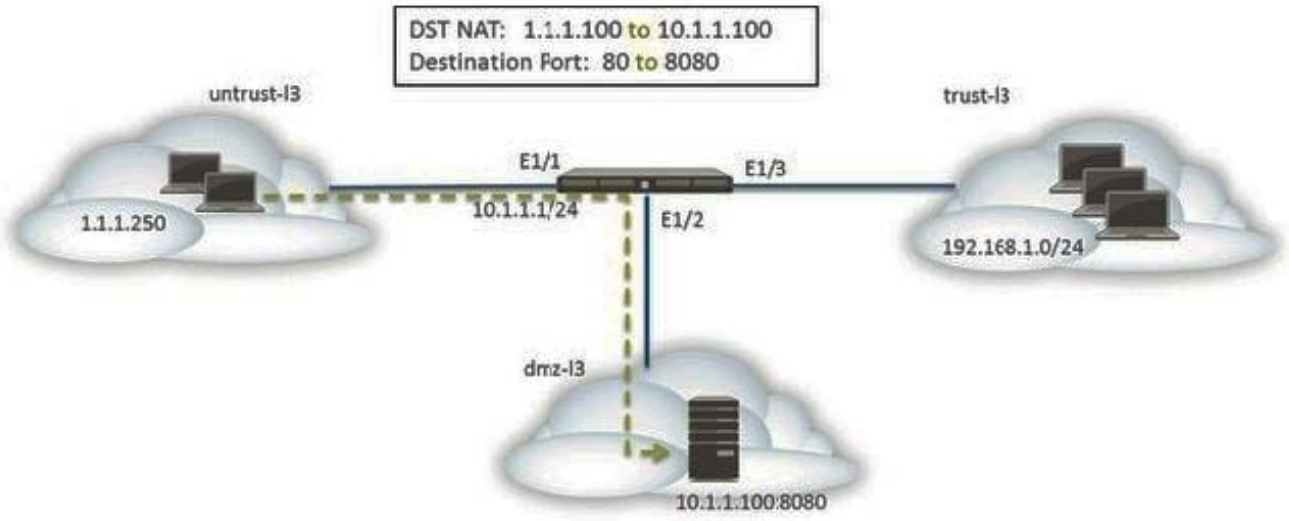
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

QUESTION 1

The web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 on TCP Port 80. The destination NAT rule is configured to translate both IP address and report to

10.1.1.100 on TCP Port 8080.



Which NAT and security rules must be configured on the firewall? (Choose two)

A. A security policy with a source of any from untrust-I3 Zone to a destination of 10.1.1.100 in dmz-I3 zone using web-browsing application

B. A NAT rule with a source of any from untrust-I3 zone to a destination of 10.1.1.100 in dmz-zone using service-http service.

C. A NAT rule with a source of any from untrust-I3 zone to a destination of 1.1.1.100 in untrust-I3 zone using service-http service.

D. A security policy with a source of any from untrust-I3 zone to a destination of 1.1.100 in dmz-I3 zone using web-browsing application.

Correct Answer: CD

QUESTION 2

You have upgraded your Panorama and Log Collectors lo 10.2 x. Before upgrading your firewalls using Panorama, what do you need do?

A. Refresh your licenses with Palo Alto Network Support - Panorama/Licenses/Retrieve License Keys from License Server.

B. Re-associate the firewalls in Panorama/Managed Devices/Summary.

C. Commit and Push the configurations to the firewalls.

D. Refresh the Mastor Key in Panorama/Master Key and Diagnostic

Correct Answer: C

QUESTION 3

An administrator creates an SSL decryption rule decrypting traffic on all ports. The administrator also creates a Security policy rule allowing only the applications DNS, SSL, and web-browsing.

The administrator generates three encrypted BitTorrent connections and checks the Traffic logs. There are three entries. The first entry shows traffic dropped as application Unknown. The next two entries show traffic allowed as application

SSL.

Which action will stop the second and subsequent encrypted BitTorrent connections from being allowed as SSL?

A. Create a decryption rule matching the encrypted BitTorrent traffic with action "No- Decrypt," and place the rule at the top of the Decryption policy.

B. Create a Security policy rule that matches application "encrypted BitTorrent" and place the rule at the top of the Security policy.

C. Disable the exclude cache option for the firewall.

D. Create a Decryption Profile to block traffic using unsupported cyphers, and attach the profile to the decryption rule.

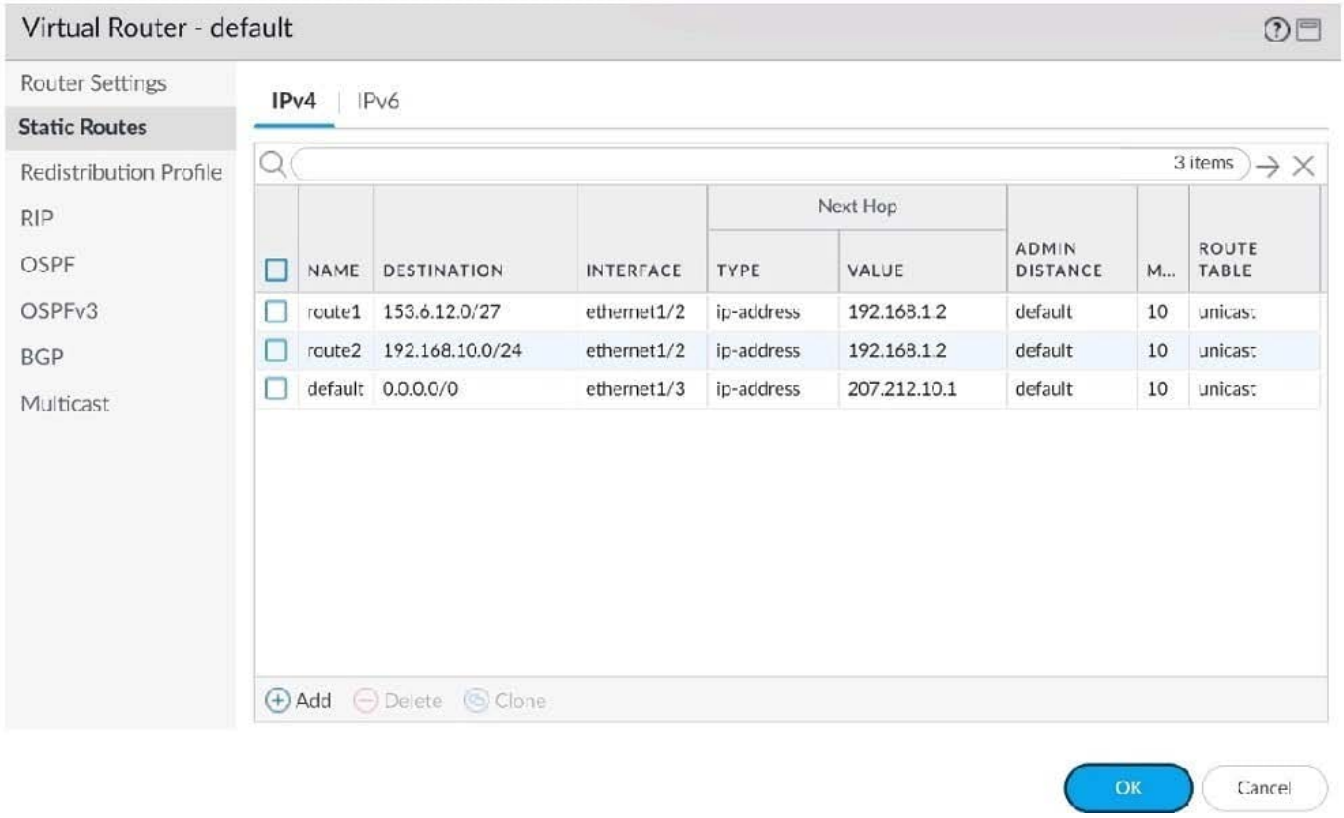
Correct Answer: D

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRtCAK Block sessions that use cipher suites you don\\'t support. You configure which cipher suites (encryption algorithms) to allow on the SSL Protocol Settings tab. Don\\'t allow users to connect to sites with weak cipher suites.

QUESTION 4

A firewall engineer creates a destination static NAT rule to allow traffic from the internet to a webserver hosted behind the edge firewall. The pre-NAT IP address of the server is 153.6 12.10, and the post-NAT IP address is 192.168.10.10. Refer to the routing and interfaces information below.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1				none	none	Untagged	none	none
ethernet1/2	Layer3	Inside		192.168.1.1/24	default	Untagged	none	Inside
ethernet1/3	Layer3			Dynamic-DHCP Client	default	Untagged	none	Outside



What should the NAT rule destination zone be set to?

A. None

B. Outside

C. DMZ

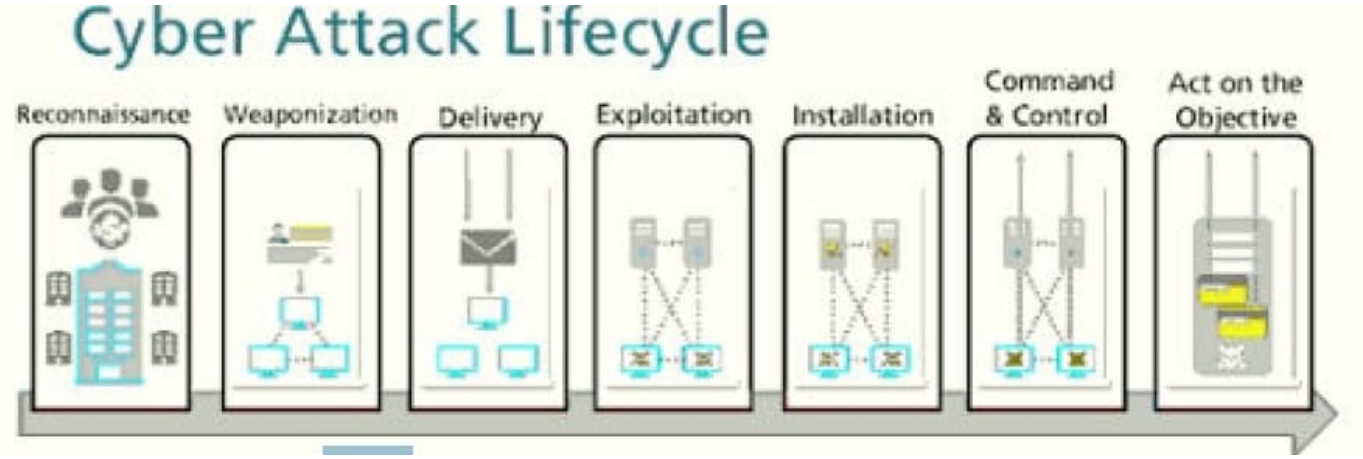
D. Inside

Correct Answer: B

The destination zone in the NAT rule is determined after the route lookup of the destination IP address in the original packet (that is, the pre-NAT destination IP address). https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networkingadmin/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping The NAT rule destination zone should be set to the zone where the traffic is destined before NAT. In this case, the traffic from the internet is destined to the pre-NAT IP address of the server, which is 153.6.12.10. This IP address belongs to the Outside zone, as shown in the routing and interfaces information. Therefore, the NAT rule destination zone should be set to Outside. The other options are not correct. None is not a valid option for the NAT rule destination zone. Inside and DMZ are the zones where the traffic is destined after NAT, which is 192.168.10.10.

References: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/networking/nat/source-and-destination-nat/configure-destination-nat

QUESTION 5



At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?

A. exploitation

B. IP command and control

C. delivery

D. reconnaissance

Correct Answer: D