PCNSE$^{Q\&As}$

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

Pass Palo Alto Networks PCNSE Exam with 100% Guarantee

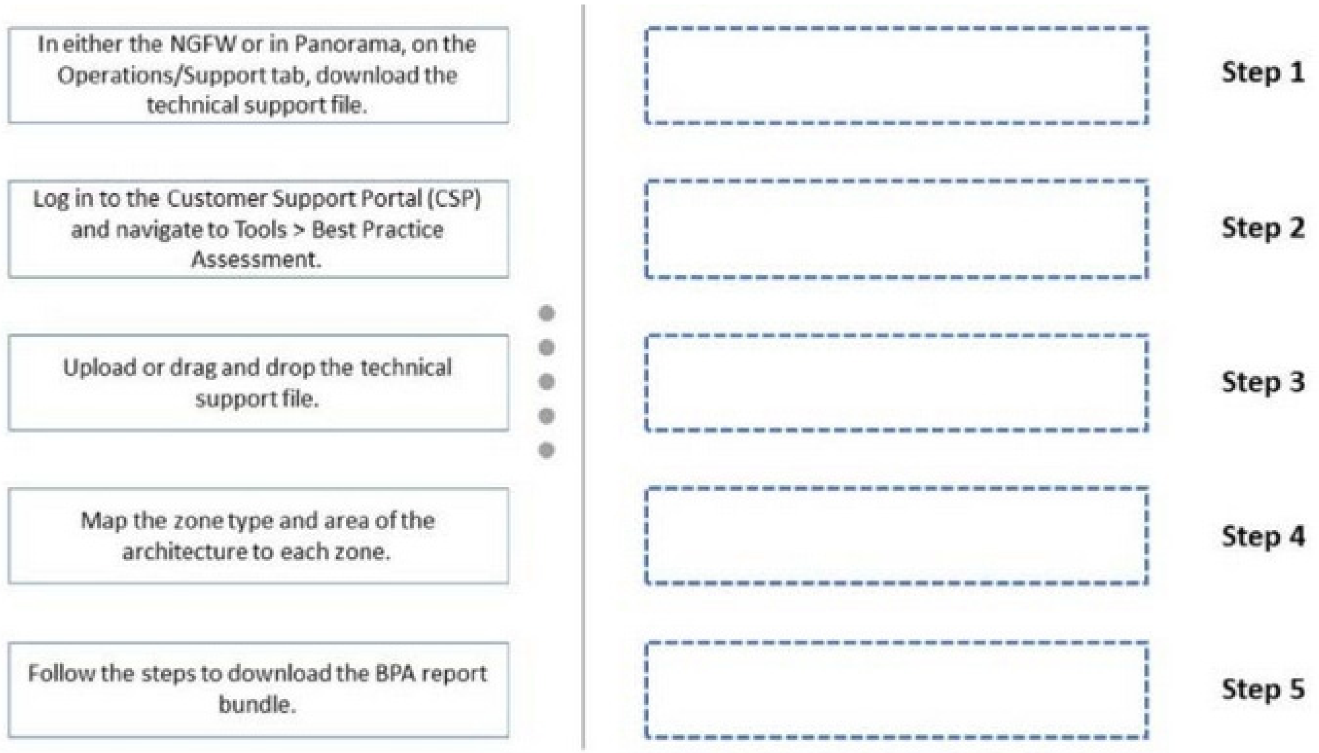
Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

QUESTION 1

DRAG DROP

Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.

Select and Place:



In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.

Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.

Upload or drag and drop the technical support file.

Map the zone type and area of the architecture to each zone.

Follow the steps to download the BPA report bundle.

Step 1

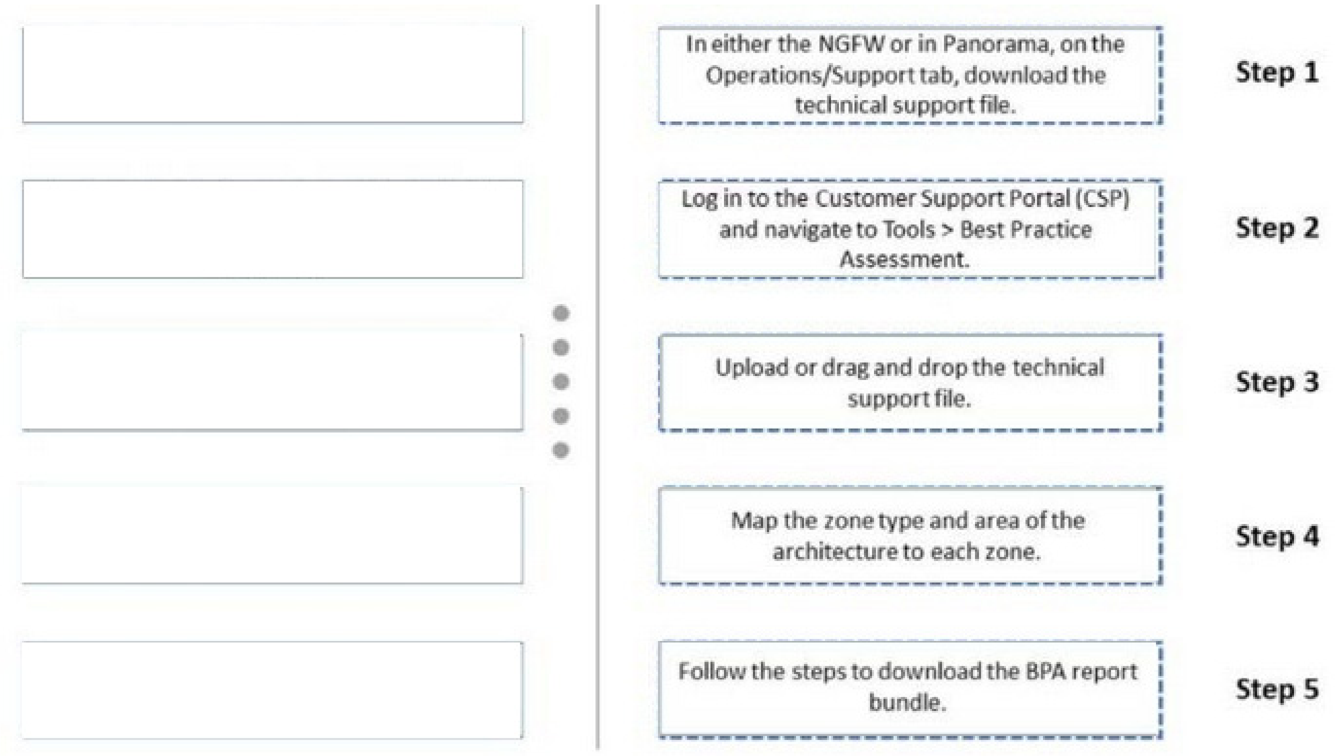
Step 2

Step 3

Step 4

Step 5

Correct Answer:



In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file. Step 1

Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment. Step 2

Upload or drag and drop the technical support file. Step 3

Map the zone type and area of the architecture to each zone. Step 4

Follow the steps to download the BPA report bundle. Step 5

Step 1. In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.

Step 2. Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.

Step 3. Upload or drag and drop the technical support file.

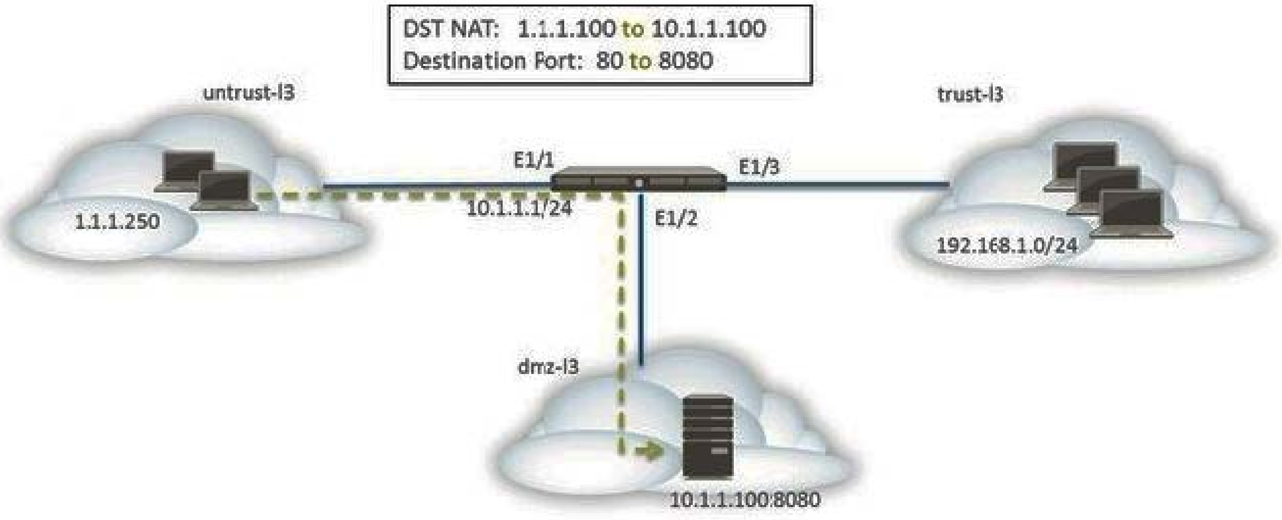
Step 4. Map the zone type and area of the architecture to each zone.

Step 5.Follow the steps to download the BPA report bundle.

QUESTION 2

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 3

During the process of developing a decryption strategy and evaluating which websites are required for corporate users to access, several sites have been identified that cannot be decrypted due to technical reasons. In this case, the technical reason is unsupported ciphers. Traffic to these sites will therefore be blocked if decrypted.

How should the engineer proceed?

A. Allow the firewall to block the sites to improve the security posture

B. Add the sites to the SSL Decryption Exclusion list to exempt them from decryption

C. Install the unsupported cipher into the firewall to allow the sites to be decrypted

D. Create a Security policy to allow access to those sites

Correct Answer: B

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-exclusions Traffic that breaks decryption for technical reasons, such as using a pinned certificate, an incomplete certificate chain, unsupported ciphers, or mutual authentication (attempting to decrypt the traffic results in blocking the traffic). Palo Alto Networks provides a predefined SSL Decryption Exclusion list (DeviceCertificate ManagementSSL Decryption Exclusion) that excludes hosts with applications and services that are known to break decryption technically from SSL Decryption by default. If you encounter sites that break decryption technically and are not on the SSL Decryption Exclusion list, you can add them to list manually by server hostname. The firewall blocks sites whose applications and services break decryption technically unless you add them to the SSL Decryption Exclusion list.

QUESTION 4

What must be used in Security Policy Rule that contain addresses where NAT policy applies?

A. Pre-NAT addresse and Pre-NAT zones

B. Post-NAT addresse and Post-Nat zones

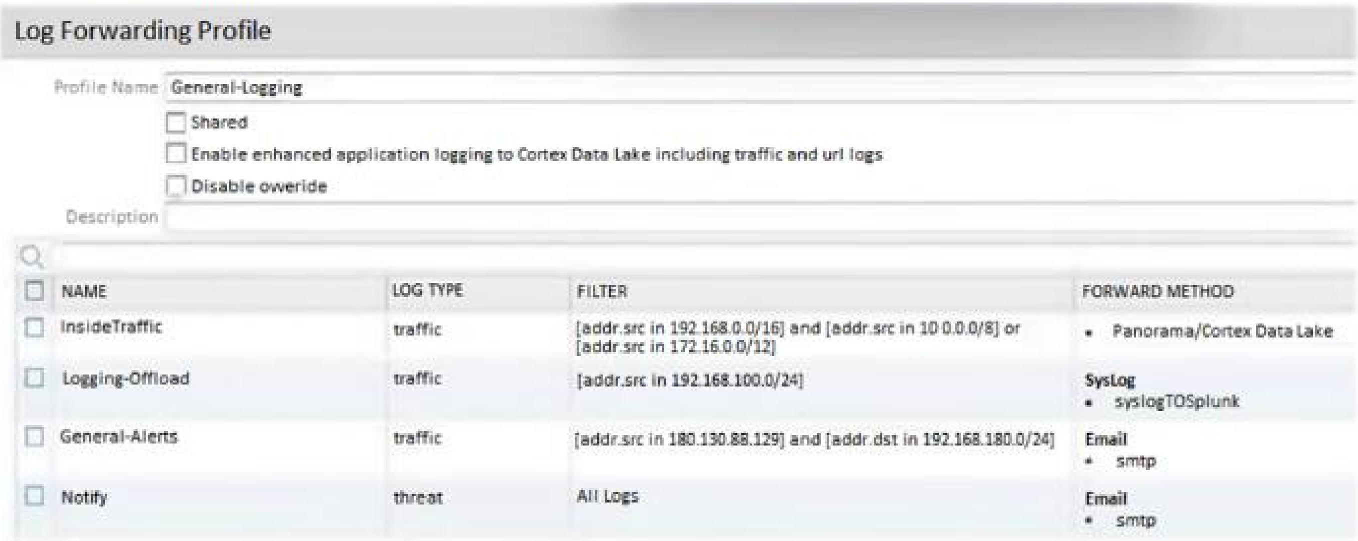
C. Pre-NAT addresse and Post-Nat zones

D. Post-Nat addresses and Pre-NAT zones

Correct Answer: C

QUESTION 5

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)