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.certbus.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

Why are external zones required to be configured on a Palo Alto Networks NGFW in an environment with multiple virtual systems?

A. To allow traffic between zones in different virtual systems while the traffic is leaving the appliance

B. External zones are required because the same external zone can be used on different virtual systems

C. To allow traffic between zones in different virtual systems without the traffic leaving the appliance

D. Multiple external zones are required in each virtual system to allow the communications between virtual systems

Correct Answer: C

External zones are required to allow traffic between zones in different virtual systems, without the traffic leaving the firewall. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/virtual-systems/communication-between-virtual-systems/ inter-vsys-traffic-that-remains-within-the-firewall/external-zone

---

QUESTION 2

Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS?version, and serial number?

A. debug system details

B. show session info

C. show system info

D. show system details

Correct Answer: C

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClZuCAK

Reference:

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical- documentation/pan-os-60/PAN-OS-6.0- CLI-ref.pdf

---

QUESTION 3

Where is information about packet buffer protection logged?

A. Alert entries are in the Alarms log Entries for dropped traffic, discarded sessions, and blocked IP address are in the Threat log

B. All entries are in the System log

C. Alert entries are in the System log Entries for dropped traffic, discarded sessions and blocked IP addresses are in the

Threat log

D. All entries are in the Alarms log

Correct Answer: C

The firewall records alert events in the System log, and records events for dropped traffic, discarded sessions, and blocked IP address in the Threat log.

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNGFCA4

QUESTION 4

When is it necessary to activate a license when provisioning a new Palo Alto Networks firewall?

A. When configuring Certificate Profiles

B. When configuring GlobalProtect portal

C. When configuring User Activity Reports

D. When configuring Antivirus Dynamic Updates

Correct Answer: D

QUESTION 5

While troubleshooting an SSL Forward Proxy decryption issue which PAN-OS CLI command would you use to check the details of the end-entity certificate that is signed by the Forward Trust Certificate or Forward Untrust Certificate?

A. show system setting ssl-decrypt certs

B. show systea setting ssl-decrypt certificate-cache

C. show systen setting ssl-decrypt certificate

D. debug dataplane show ssl-decrypt ssl-stats

Correct Answer: A

QUESTION 6

An administrator is required to create an application-based Security policy rule to allow Evernote.

The Evernote application implicitly uses SSL and web browsing.

What is the minimum the administrator needs to configure in the Security rule to allow only Evernote?

A. Add the Evernote application to the Security policy rule, then add a second Security policy rule containing both HTTP and SSL.

B. Add the HTTP, SSL, and Evernote applications to the same Security policy

C. Add only the Evernote application to the Security policy rule.

D. Create an Application Override using TCP ports 443 and 80.

Correct Answer: C

https://live.paloaltonetworks.com/t5/blogs/what-is-application-dependency/ba-p/344330 To create an application-based Security policy rule to allow Evernote, the administrator only needs to add the Evernote application to the Security policy rule. The Evernote application is a predefined App-ID that identifies the traffic generated by the Evernote client or web interface. The Evernote application implicitly uses SSL and web browsing as dependencies, which means that the firewall automatically allows these applications when the Evernote application is allowed. Therefore, there is no need to add HTTP, SSL, or web browsing applications to the same Security policy rule. Adding these applications would broaden the scope of the rule and potentially allow unwanted traffic12. References: App-ID Overview, Create a Security Policy Rule

QUESTION 7

Refer to Exhibit:

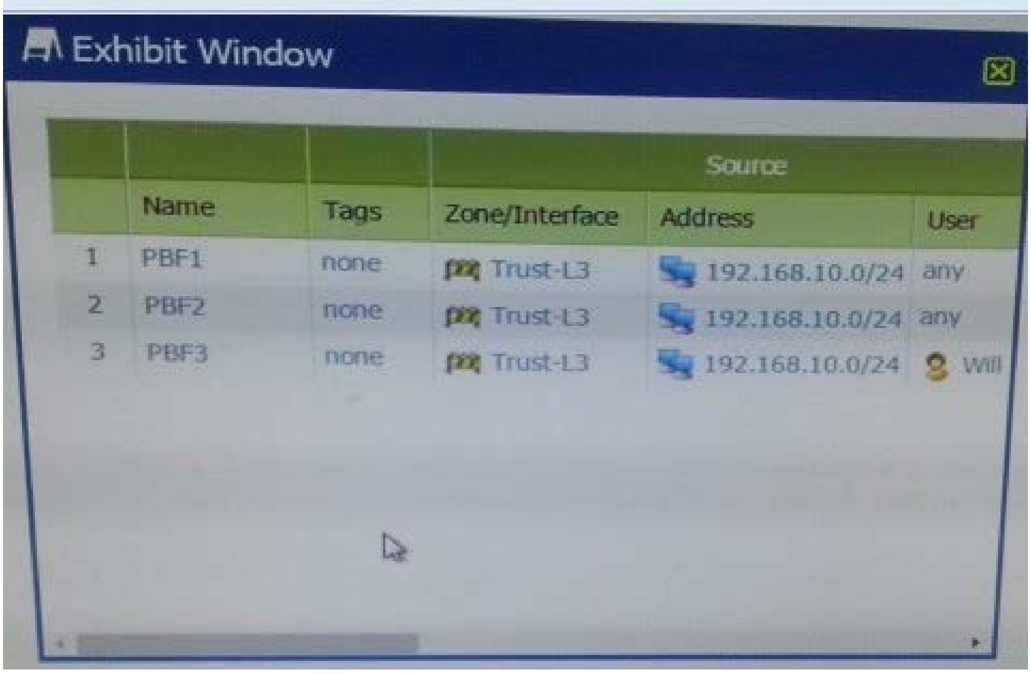

Exhibit Window

			Source		
	Name	Tags	Zone/Interface	Address	User
1	PBF1	none	Trust-L3	192.168.10.0/24	any
2	PBF2	none	Trust-L3	192.168.10.0/24	any
3	PBF3	none	Trust-L3	192.168.10.0/24	Will

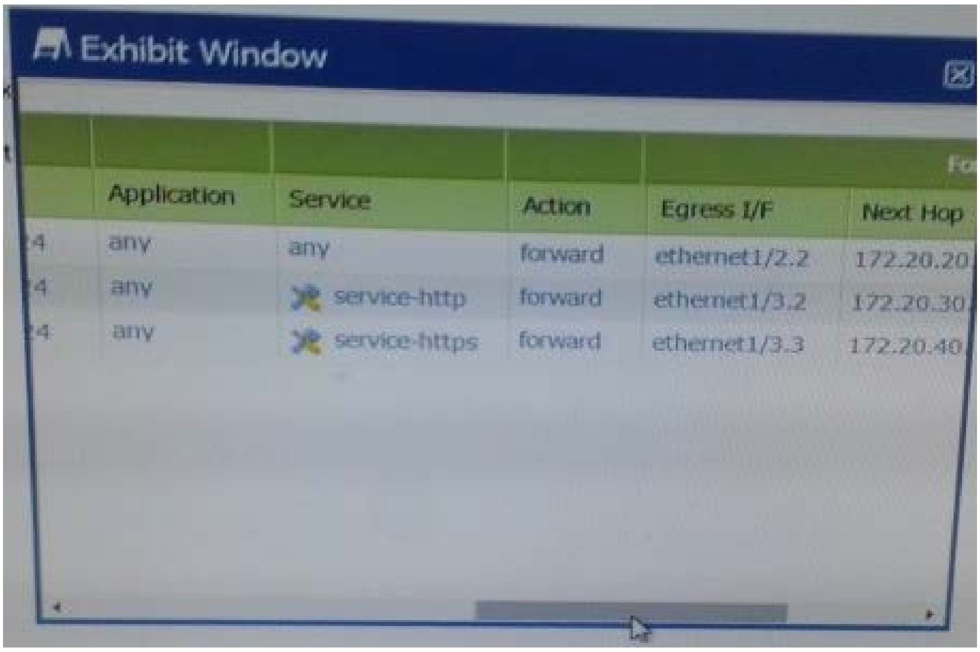

Exhibit Window

					Fo
	Application	Service	Action	Egress I/F	Next Hop
4	any	any	forward	ethernet1/2.2	172.20.20
4	any	service-http	forward	ethernet1/3.2	172.20.30
4	any	service-https	forward	ethernet1/3.3	172.20.40

A firewall has three PDF rules and a default route with a next hop of 172.29.19.1 that is configured in the default VR. A user named XX-bes a PC with a 192.168.101.10 IP address.

He makes an HTTPS connection to 172.16.10.29.

What is the next hop IP address for the HTTPS traffic from Wills PC.

A. 172.20.30.1

B. 172.20.20.1

C. 172.20.10.1

D. 172.20.40.1

Correct Answer: B

QUESTION 8

An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the internet. Which configuration will enable the firewall to download and install application updates automatically?

A. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from themanagement interfaced destined for the update servers goes out of the interface acting as your internet connection.

B. Configure a security policy rule to allow all traffic to and from the update servers.

C. Download and install application updates cannot be done automatically if the MGT port cannot reach the internet.

D. Configure a service route for Palo Alto networks services that uses a dataplane interface that can route traffic to the internet, and create a security policy rule to allow the traffic from that interface to the update servers if necessary.

Correct Answer: D

"By default, the firewall uses management interface to communicate to various servers including DNS, Email, Palo Alto Updates, User-ID agent, Syslog, Panorama etc. Service routes are used so that the communication between the firewall and servers go through the dataplane."https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGJCA0 "The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list."https://docs.paloaltonetworks.com/pan-os/7-1/pan-osweb-interface- help/device/device-dynamic-updates#

QUESTION 9

Which PAN-OS policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

A. Security policy

B. Decryption policy

C. Authentication policy

D. Application Override policy

Correct Answer: C

Authentication policy enables you to authenticate end users before they can access services and applications. Whenever a user requests a service or application (such as by visiting a web page), the firewall evaluates Authentication policy. Based on the matching Authentication policy rule, the firewall then prompts the user to authenticate using one or more methods (factors), such as login and password, Voice, SMS, Push, or One- time Password (OTP) authentication https:// docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication- policy

QUESTION 10

Which two statements correctly identify the number of Decryption Broker security chains that are supported on a pair of decryption-forwarding interfaces\\'? (Choose two)

A. A single transparent bridge security chain is supported per pair of interfaces

B. L3 security chains support up to 32 security chains

C. L3 security chains support up to 64 security chains

D. A single transparent bridge security chain is supported per firewall

Correct Answer: AD

QUESTION 11

An engineer configures SSL decryption in order to have more visibility to the internal users\\' traffic when it is regressing the firewall. Which three types of interfaces support SSL Forward Proxy? (Choose three.)

A. High availability (HA)

B. Layer 2

C. Virtual Wire

D. Tap

E. Layer 3

Correct Answer: BCE

PAN-OS can decrypt and inspect SSL inbound and outbound connections going through the firewall. SSL decryption can occur on interfaces in virtual wire, Layer 2 or Layer 3 mode
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClmyCAC

QUESTION 12

A firewall engineer needs to patch the company\\'s Palo Alto Networks firewalls to the latest version of PAN-OS. The company manages its firewalls by using Panorama. Logs are forwarded to Dedicated Log Collectors, and file samples are forwarded to WildFire appliances for analysis.

What must the engineer consider when planning deployment?

A. Only Panorama and Dedicated Log Collectors must be patched to the target PAN-OS version before updating the firewalls.

B. Panorama, Dedicated Log Collectors, and WildFire appliances must have the target PAN-OS version downloaded, after which the order of patching does not matter.

C. Panorama, Dedicated Log Collectors, and WildFire appliances must be patched to the target PAN-OS version before updating the firewalls.

D. Only Panorama must be patched to the target PAN-OS version before updating the firewalls.

Correct Answer: C

https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os "When upgrading firewalls that you manage with Panorama or firewalls that are configured to forward content to a WildFire appliance, you must first upgrade Panorama and its Log Collectors and then upgrade the WildFire appliance before you upgrade the firewalls."

QUESTION 13

Which value in the Application column indicates UDP traffic that did not match an App-ID signature?

A. not-applicable

B. incomplete

C. unknown-ip

D. unknown-udp

Correct Answer: D

To safely enable applications you must classify all traffic, across all ports, all the time. With App-ID, the only applications that are typically classified as unknown traffic--tcp, udp or non-syn-tcp--in the ACC and the Traffic logs are commercially available applications that have not yet been added to App-ID, internal or custom applications on your network, or potential threats. https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects- in-policy/create-a-custom-application

QUESTION 14

An administrator needs to upgrade an NGFW to the most current version of PAN-OS?software. The following is occurring:

Firewall has Internet connectivity through e1/1.

Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.

Service route is configured, sourcing update traffic from e1/1.

A communication error appears in the System logs when updates are performed.

Download does not complete.

What must be configured to enable the firewall to download the current version of PAN-OS software?

A. DNS settings for the firewall to use for resolution

B. scheduler for timed downloads of PAN-OS software

C. static route pointing application PaloAlto-updates to the update servers

D. Security policy rule allowing PaloAlto-updates as the application

Correct Answer: D

QUESTION 15

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.