Free Questions for PCNSA by go4braindumps

Shared by Kline on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What are the two main reasons a custom application is created? (Choose two.)

Options:

A- To correctly identify an internal application in the traffic log

B- To change the default categorization of an application

C- To visually group similar applications

D- To reduce unidentified traffic on a network

Answer:

A, D

Explanation:

https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/use-application-objects-in-policy/create-a-custom-application

Question 2

Question Type: **MultipleChoice**

An administrator manages a network with 300 addresses that require translation. The administrator configured NAT with an address pool of 240 addresses and found that connections from addresses that needed new translations were being dropped.

Which type of NAT was configured?

Options:

A- Static IP

B- Dynamic IP

C- Destination NAT

D- Dynamic IP and Port

Answer:

B

Explanation:

The size of the NAT pool should be equal to the number of internal hosts that require address translations. By default, if the source address pool is larger than the NAT address pool and eventually all of the NAT addresses are allocated, new connections that need address translation are dropped. To override this default behavior, use Advanced (Dynamic IP/Port Fallback) to enable the use of DIPP addresses when necessary

Question 3

Question Type: MultipleChoice

When HTTPS for management and GlobalProtect are enabled on the same data plane interface, which TCP port is used for management access?

Options:

A- 80

B- 443

C- 4443

D- 8443

Answer:

C

Explanation:

The GlobalProtect Portal can be accessed by going to the IP address of the designated interface using https on port 443. The WebUI on the same interface can be accessed by going to the interface's IP address using https on port 4443. The port for WebUI management is changed because the tcp/443 socket used by GlobalProtect takes precedence

Question 4

Question Type: MultipleChoice

An administrator creates a new Security policy rule to allow DNS traffic from the LAN to the DMZ zones. The administrator does not change the rule type from its default value.

What type of Security policy rule is created?

Options:

A- Tagged

B- Intrazone

C- Universal

D- Interzone

Answer:

C

Question 5

Question Type: **MultipleChoice**

Which feature must be configured to enable a data plane interface to submit DNS queries originated from the firewall on behalf of the control plane?

Options:

A- Service route

B- Admin role profile

C- DNS proxy

D- Virtual router

Answer:

A

Explanation:

By default, the firewall uses the management (MGT) interface to access external services, such as DNS servers, external authentication servers, Palo Alto Netw orks services such as soft ware, URL updates, licenses, and AutoFocus. An alternative to using the MGT interface is configuring a data port (a standard interface) to access these services. The path from the interface to th e service on a server is aservice route. [Palo Alto Networks]

PAN-OS 10 -> Device -> Setup -> Services -> Service Features -> Service Route Configuration

Question 6

Question Type: **MultipleChoice**

How would a Security policy need to be written to allow outbound traffic using Secure Shell (SSH) to destination ports tcp/22 and tcp/4422?

Options:

A- The admin creates a custom service object named 'tcp-4422' with port tcp/4422.
The admin then creates a Security policy allowing application 'ssh' and service 'tcp-4422'.

B- The admin creates a custom service object named 'tcp-4422' with port tcp/4422.
The admin then creates a Security policy allowing application 'ssh', service 'tcp-4422'. and service 'application-default'.

C- The admin creates a Security policy allowing application 'ssh' and service 'application-default'.

D- The admin creates a custom service object named 'tcp-4422' with port tcp/4422.
The admin also creates a custom service object named 'tcp-22' with port tcp/22.
The admin then creates a Security policy allowing application 'ssh', service 'tcp-4422'. and service 'tcp-22'.

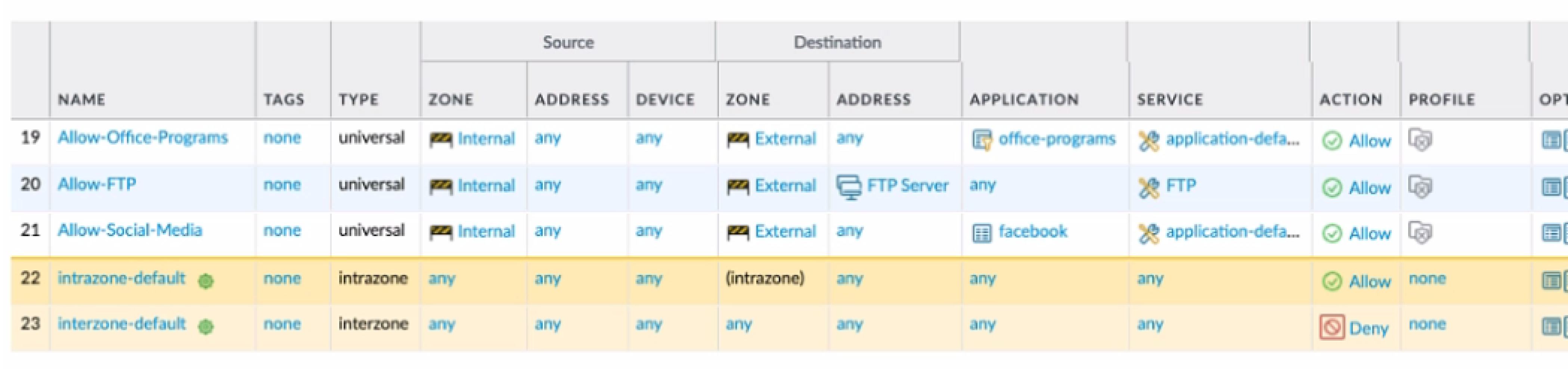
Answer:

D

Question 7

Question Type: MultipleChoice

Based on the image provided, which two statements apply to the Security policy rules? (Choose two.)



				Source			Destination						
	NAME	TAGS	TYPE	ZONE	ADDRESS	DEVICE	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPT
19	Allow-Office-Programs	none	universal	Internal	any	any	External	any	office-programs	application-defa...	Allow		
20	Allow-FTP	none	universal	Internal	any	any	External	FTP Server	any	FTP	Allow		
21	Allow-Social-Media	none	universal	Internal	any	any	External	any	facebook	application-defa...	Allow		
22	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	
23	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	

Options:

A- The Allow-Office-Programs rule is using an application filter.

B- The Allow-Office-Programs rule is using an application group.

C- The Allow-Social-Media rule allows all Facebook functions.

D- In the Allow-FTP policy, FTP is allowed using App-ID.

Answer:

A, C

Question 8

Question Type: **MultipleChoice**

Where in Panorama Would Zone Protection profiles be configured?

Options:

A- Shared

B- Templates

C- Device Groups

D- Panorama tab

Answer:

B

Explanation:

https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewalls-using-panorama/set-up-your-centralized-configuration-and-policies/use-templates-to-administer-a-base-configuration

Question 9

Question Type: **MultipleChoice**

What is the best-practice approach to logging traffic that traverses the firewall?

Options:

A- Enable both log at session start and log at session end.

B- Enable log at session start only.

C- Enable log at session end only.

D- Disable all logging options.

Answer:

C

Explanation:

The best-practice approach to logging traffic that traverses the firewall is to enable log at session end only. This option allows the firewall to generate a log entry only when a session ends, which reduces the load on the firewall and the log storage. The log entry contains information such as the source and destination IP addresses, ports, zones, application, user, bytes, packets, and duration of the session.The log at session end option also provides more accurate information about the session, such as the final application and user, the total bytes and packets, and the session end reason1. To enable log at session end only, you need to:

Create or modify a Security policy rule that matches the traffic that you want to log.

Select the Actions tab in the policy rule and check the Log at Session End option.

Commit the changes to the firewall or Panorama and the managed firewalls.

Question 10

Question Type: **MultipleChoice**

Which setting is available to edit when a tag is created on the local firewall?

Options:

A- Location

B- Color

C- Order

D- Priority

Answer:

B

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-tags/create-tags