Vendor: Palo Alto Networks

Exam Code:ACE

Exam Name: Accredited Configuration Engineer (ACE) PAN-OS 8.0

Version: Demo

QUESTION 1

An Outbound SSL forward-proxy decryption rule cannot be created using which type of zone?

A. Virtual Wire

B. Tap

C. L3

D. L2

Correct Answer: A

QUESTION 2

In an HA configuration, which two failure detection methods rely on ICMP ping? (Choose two.)

A. hellos

B. link groups

C. path groups

D. heartbeats

Correct Answer: BC

QUESTION 3

An Antivirus Security Profile specifies Actions and WildFire Actions. Wildfire Actions enable you to configure the firewall toperform which operation?

A. Block traffic when a WildFire virus signature is detected.

B. Download new antivirus signatures from WildFire.

C. Upload traffic to WildFire when a virus is suspected.

D. Delete packet data when a virus is suspected.

Correct Answer: A

QUESTION 4

Which of the following statements is NOT True regarding a Decryption Mirror interface?

A. Requires superuser privilege

B. Supports SSL outbound

C. Can be a member of any VSYS

D. Supports SSL inbound

Correct Answer: C

QUESTION 5

When configuring a Decryption Policy Rule, which of the following are available as matching criteria in the rule? (Choose 3 answers.)

A. Source Zone

B. URL Category

C. Application

D. Service

E. Source User

Correct Answer: ABE

QUESTION 6

The "Disable Server Return Inspection" option on a security profile:

A. Can only be configured in Tap Mode

B. Should only be enabled on security policies allowing traffic to a trusted server.

C. Does not perform higher-level inspection of traffic from the side that originated the TCP SYN packet

D. Only performs inspection of traffic from the side that originated the TCP SYN-ACK packet

Correct Answer: B

QUESTION 7

In Active/Active HA environments, redundancy for the HA3 interface can be achieved by

A. Configuring a corresponding HA4 interface

B. Configuring HA3 as an Aggregate Ethernet bundle

C. Configuring multiple HA3 interfaces

D. Configuring HA3 in a redundant group

Correct Answer: B

QUESTION 8

For which firewall feature should you create forward trust and forward untrust certificates?

A. SSH decryption

B. SSL client-side certificate checking

C. SSL Inbound Inspection decryption

D. SSL forward proxy decryption

Correct Answer: D

QUESTION 9

Which three interface types can control or shape network traffic? (Choose three.)

A. Layer 2

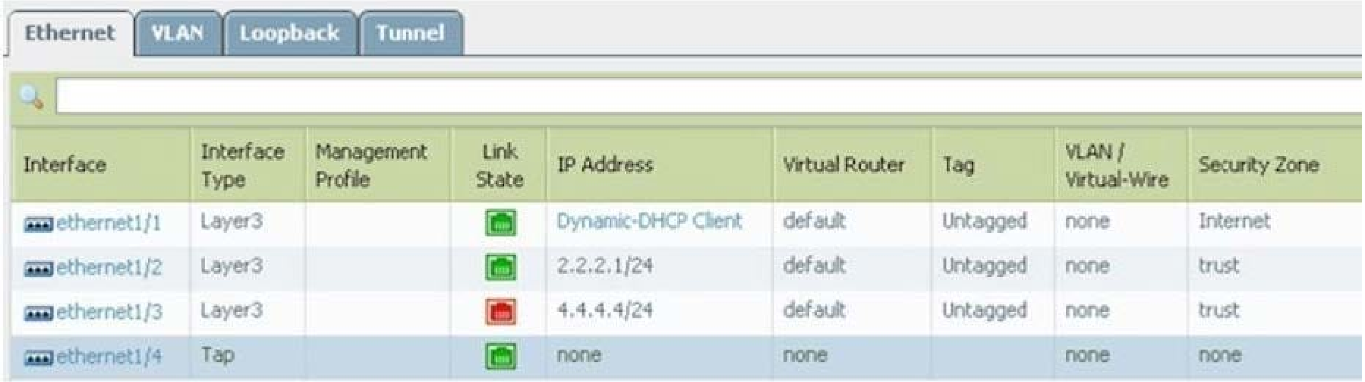
B. Tap

C. Virtual Wire

D. Layer 3

Correct Answer: ABD

QUESTION 10



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone
ethernet1/1	Layer3		🟩	Dynamic-DHCP Client	default	Untagged	none	Internet
ethernet1/2	Layer3		🟩	2.2.2.1/24	default	Untagged	none	trust
ethernet1/3	Layer3		🟥	4.4.4.4/24	default	Untagged	none	trust
ethernet1/4	Tap		🟩	none	none		none	none

Taking into account only the information in the screenshot above, answer the following question. An administrator is using SSH on port 3333 and BitTorrent on port 7777. Which statements are true?

A. The BitTorrent traffic will be allowed.

B. The SSH traffic will be allowed.

C. The SSH traffic will be denied.

D. The BitTorrent traffic will be denied.

Correct Answer: BD

QUESTION 11

Which of the following services are enabled on the MGT interface by default? (Select all correct answers.)

A. HTTPS

B. SSH

C. Telnet

D. HTTP

Correct Answer: AB

QUESTION 12

After configuring Captive Portal in Layer 3 mode, users in the Trust Zone are not receiving the Captive Portal authentication page when they launch their web browsers. How can this be corrected?

A. Ensure that all users in the Trust Zone are using NTLM-capable browsers

B. Enable "Response Pages" in the Interface Management Profile that is applied to the L3 Interface in the Trust Zone.

C. Confirm that Captive Portal Timeout value is not set below 2 seconds

D. Enable "Redirect " as the Mode type in the Captive Portal Settings

Correct Answer: AB