Palo Alto Networks ACE Exam

Volume: 91 Questions

Question No : 1
Which of the following describes the sequence of the Global Protect agent connecting to a Gateway?

A. The Agent connects to the Portal obtains a list of Gateways, and connects to the Gateway with the fastest SSL response time

B. The agent connects to the closest Gateway and sends the HIP report to the portal

C. The agent connects to the portal, obtains a list of gateways, and connects to the gateway with the fastest PING response time

D. The agent connects to the portal and randomly establishes a connection to the first available gateway

Answer: A

Question No : 2
If the Forward Proxy Ready shows “no” when running the command show system setting ssl-decrypt setting, what is most likely the cause?

A. SSL forward proxy certificate is not generated

B. Web interface certificate is not generated

C. Forward proxy license is not enabled on the box n

D. SSL decryption rule is not created

Answer: D

Question No : 3
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

Answer: B

Question No : 4
As the Palo Alto Networks administrator, you have enabled Application Block pages. Afterward, some users do not receive web-based feedback for all denied applications. Why would this be?

A. Some users are accessing the Palo Alto Networks firewall through a virtual system that does not have Application Block pages enabled.

B. Application Block Pages will only be displayed when Captive Portal is configured

C. Some Application ID's are set with a Session Timeout value that is too low.

D. Application Block Pages will only be displayed when users attempt to access a denied web-based application.

Answer: D

Question No : 5
As the Palo Alto Networks administrator responsible for User Identification, you are looking for the simplest method of mapping network users that do not sign into LDAP. Which information source would allow reliable User ID mapping for these users, requiring the least amount of configuration?

A. WMI Query

B. Exchange CAS Security Logs

C. Captive Portal

D. Active Directory Security Logs

Answer: C

Question No : 6
Which of the following options may be enabled to reduce system overhead when using Content ID?

A. STP

B. VRRP

C. RSTP

D. DSRI

Answer: D

Question No : 7
Configuring a pair of devices into an Active/Active HA pair provides support for:

A. Higher session count

B. Redundant Virtual Routers

C. Asymmetric routing environments

D. Lower fail-over times

Answer: B

Question No : 8
Which of the following types of protection are available in DoS policy?

A. Session Limit, SYN Flood, UDP Flood

B. Session Limit, Port Scanning, Host Swapping, UDP Flood

C. Session Limit, SYN Flood, Host Swapping, UDP Flood

D. Session Limit, SYN Flood, Port Scanning, Host Swapping

Answer: A

Question No : 9
Which of the following interfaces types will have a MAC address?

A. Layer 3

B. Tap

C. Vwire

D. Layer 2

Answer: D

Question No : 10
To allow the PAN device to resolve internal and external DNS host names for reporting and for security policies, an administrator can do the following:

A. Create a DNS Proxy Object with a default DNS Server for external resolution and a DNS server for internal domain. Then, in the device settings, point to this proxy object for DNS resolution.

B. In the device settings define internal hosts via a static list.

C. In the device settings set the Primary DNS server to an external server and the secondary to an internal server.

D. Create a DNS Proxy Object with a default DNS Server for external resolution and a DNS server for internal domain. Then, in the device settings, select the proxy object as the Primary DNS and create a custom security rule which references that object for

Answer: A

Question No : 11
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

Answer: B

Question No : 12
A user complains that they are no longer able to access a needed work application after you have implemented vulnerability and anti-spyware profiles. The user's application uses a unique port. What is

the most efficient way to allow the user access to this application?

A. Utilize an Application Override Rule, referencing the custom port utilzed by this application. Application Override rules bypass all Layer 7 inspection, thereby allowing access to this application.

B. In the Threat log, locate the event which is blocking access to the user's application and create a IP-based exemption for this user.

C. In the vulnerability and anti-spyware profiles, create an application exemption for the user's application.

D. Create a custom Security rule for this user to access the required application. Do not apply vulnerability and anti-spyware profiles to this rule.

Answer: B

Question No : 13
For non-Microsoft clients, what Captive Portal method is supported?

A. NTLM Auth

B. User Agent

C. Local Database

D. Web Form Captive Portal

Answer: D

Question No : 14
When creating a Security Policy to allow Facebook in PAN-OS 5.0, how can you be sure that no other web-browsing traffic is permitted?

A. Ensure that the Service column is defined as "application-default" for this security rule. This will automatically include the implicit web-browsing application dependency.

B. Create a subsequent rule which blocks all other traffic

C. When creating the rule, ensure that web-browsing is added to the same rule. Both applications will be processed by the Security policy, allowing only Facebook to be accessed. Any other applications can be permitted in subsequent rules.