Free Questions for PCNSE by dumpshq

Shared by Castaneda on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An engineer needs to permit XML API access to a firewall for automation on a network segment that is routed through a Layer 3 sub-interface on a Palo Alto Networks firewall. However, this network segment cannot access the dedicated management interface due to the Security policy.

Without changing the existing access to the management interface, how can the engineer fulfill this request?

Options:

A- Specify the subinterface as a management interface in Setup > Device > Interfaces.

B- Add the network segment's IP range to the Permitted IP Addresses list.

C- Enable HTTPS in an Interface Management profile on the subinterface.

D- Configure a service route for HTTP to use the subinterface.

Answer:

C

Explanation:

To enable XML API access to a firewall for automation from a network segment routed through a Layer 3 sub-interface, the most straightforward approach is to use an Interface Management profile.

C) This can be achieved by:

Configuring an Interface Management profile and enabling HTTPS access on it. This profile defines management services that are permitted on the interface, including HTTPS, which is required for XML API access.

Applying this Interface Management profile to the desired Layer 3 sub-interface. This action enables HTTPS access (and thus XML API access) on the sub-interface, allowing devices on the connected network segment to communicate with the firewall for automation purposes.

This solution allows for the secure extension of management capabilities to network segments without direct access to the dedicated management interface, facilitating automation and operational efficiency without necessitating changes to existing access configurations.

Question 2

Question Type: **MultipleChoice**

A firewall engineer has determined that, in an application developed by the company's internal team, sessions often remain idle for hours before the client and server exchange any data. The application is also currently identified as unknown-tcp by the firewalls. It is determined that because of a high level of trust, the application does not require to be scanned for threats, but it needs to be properly identified in Traffic logs for reporting purposes.

Which solution will take the least time to implement and will ensure the App-ID engine is used to identify the application?

Options:

A- Create a custom application with specific timeouts and signatures based on patterns discovered in packet captures.

B- Access the Palo Alto Networks website and raise a support request through the Customer Support Portal.

C- Create a custom application with specific timeouts, then create an application override rule and reference the custom application.

D- Access the Palo Alto Networks website and complete the online form to request that a new application be added to App-ID.

Answer:

C

Explanation:

For an application that is currently identified as unknown-tcp and has sessions that often remain idle for long periods, creating a custom application and using an application override rule is the most time-efficient solution.

C) The process involves:

Creating a custom application in the Palo Alto Networks firewall and configuring it with specific timeouts to accommodate the application's idle session behavior. This step ensures that the firewall does not prematurely close the application's sessions due to inactivity.

Next, creating an application override rule that references the custom application. This rule directs the firewall to identify traffic matching the rule criteria (such as source, destination, and port information) as the custom application, bypassing the App-ID engine's regular identification process.

This approach allows for the quick implementation of a solution that ensures the application is properly identified in traffic logs without undergoing threat scanning, meeting the requirements for both identification and reporting.

Question 3

Question Type: MultipleChoice

A security engineer wants to upgrade the company's deployed firewalls from PAN-OS 10.1 to 11.0.x to take advantage of the new TLSvl.3 support for management access.

What is the recommended upgrade path procedure from PAN-OS 10.1 to 11.0.x?

Options:

A- Required: Download PAN-OS 10.2.0 or earlier release that is not EOL.
Required: Download and install the latest preferred PAN-OS 10.2 maintenance release and reboot. Required: Download PAN-OS 11.0.0. Required: Download and install the desired PAN-OS 11.0.x.

B- Required: Download and install the latest preferred PAN-OS 10.1 maintenance release and reboot.
Required: Download PAN-OS 10.2.0.
Required: Download and install the latest preferred PAN-OS 10.2 maintenance release and reboot. Required: Download PAN-OS 11.0.0. Required: Download and install the desired PAN-OS 11.0.x.

C- Optional: Download and install the latest preferred PAN-OS 10.1 release. Optional: Install the latest preferred PAN-OS 10.2 maintenance release. Required: Download PAN-OS 11.0.0. Required: Download and install the desired PAN-OS 11.0.x.

D- Required: Download and install the latest preferred PAN-OS 10.1 maintenance release and reboot. Required: Download PAN-OS 10.2.0.
Optional: Install the latest preferred PAN-OS 10.2 maintenance release. Required: Download PAN-OS 11.0.0. Required: Download and install the desired PAN-OS 11.0.x.

Answer:

B

Explanation:

Palo Alto Networks recommends following a specific upgrade path when upgrading PAN-OS to ensure compatibility and minimize the risk of issues. The recommended path involves sequential upgrades through major releases.

B) The detailed upgrade path from PAN-OS 10.1 to 11.0.x involves:

First, upgrading to the latest preferred maintenance release of the current PAN-OS version (10.1) to ensure that all the latest fixes and improvements are applied.

Next, upgrading to the base version of the next major release (PAN-OS 10.2.0), followed by upgrading to the latest preferred maintenance release of PAN-OS 10.2. This step ensures that the firewall is on a stable and supported version before proceeding to the next major release.

Finally, upgrading to the base version of PAN-OS 11.0 (11.0.0), followed by the desired PAN-OS 11.0.x version. This step completes the upgrade to the new major version, providing access to new features and improvements, such as TLSv1.3 support for management access.

This sequential upgrade path is designed to ensure a smooth transition between major versions, maintaining system stability and security.

Question 4

Question Type: **MultipleChoice**

What would allow a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain?

Options:

A- an Authentication policy with 'unknown' selected in the Source User field

B- an Authentication policy with 'known-user' selected in the Source User field

C- a Security policy with 'known-user' selected in the Source User field

D- a Security policy with 'unknown' selected in the Source User field

Answer:

A

Explanation:

For a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain, the most effective method is to use an Authentication policy targeting users not yet identified by the system.

A) an Authentication policy with 'unknown' selected in the Source User field:

An Authentication policy allows the firewall to challenge unidentified users for credentials. By selecting 'unknown' in the Source User field, the policy targets users who have not yet been identified by the firewall, which would include users on new BYOD devices not joined to the domain.

Once the user provides valid credentials, the firewall can authenticate the user and map their identity to subsequent sessions, enabling the application of user-based policy rules and monitoring.

This approach ensures that new and unknown devices can be properly authenticated and identified without compromising security or requiring the device to be part of the corporate domain.

Question 5

Question Type: MultipleChoice

An administrator has a Palo Alto Networks NGFW. All security subscriptions and decryption are enabled and the system is running close to its resource limits.

Knowing that using decryption can be resource-intensive, how can the administrator reduce the load on the firewall?

Options:

A- Use RSA instead of ECDSA for traffic that isn't sensitive or high-priority.

B- Use the highest TLS protocol version to maximize security.

C- Use ECDSA instead of RSA for traffic that isn't sensitive or high-priority.

D- Use SSL Forward Proxy instead of SSL Inbound Inspection for decryption.

Answer:

C

Explanation:

Decryption can be resource-intensive, and in scenarios where the firewall is nearing its resource limits, optimizing decryption practices is crucial. One way to do this is by choosing more efficient encryption algorithms that require less computational power.

C) Use ECDSA instead of RSA for traffic that isn't sensitive or high-priority:

Elliptic Curve Digital Signature Algorithm (ECDSA) is known for requiring smaller key sizes compared to RSA for a comparable level of security. This translates to less computational overhead during the encryption and decryption processes.

By using ECDSA for traffic that isn't sensitive or high-priority, the administrator can reduce the processing load associated with decryption on the firewall. This is particularly beneficial in scenarios where resource optimization is necessary.

It's important to note that this approach does not compromise the security of encrypted traffic. Instead, it offers a more resource-efficient way to manage decryption, thus helping to maintain firewall performance even when system resources are under significant demand.

By judiciously applying this strategy, administrators can manage the decryption workload on the firewall, ensuring continued protection and inspection of encrypted traffic without overburdening the firewall's resources.

Question 6

Question Type: MultipleChoice

Which function does the HA4 interface provide when implementing a firewall cluster which contains firewalls configured as active-passive pairs?

Options:

A- Perform packet forwarding to the active-passive peer during session setup and asymmetric traffic flow.

B- Perform synchronization of routes, IPSec security associations, and User-ID information.

C- Perform session cache synchronization for all HA cluster members with the same cluster ID.

D- Perform synchronization of sessions, forwarding tables, and IPSec security associations between firewalls in an HA pair.

Answer:

D

Explanation:

In a High Availability (HA) configuration, particularly in an active-passive setup, it's crucial that the passive unit is kept up to date with the current state of the active unit. This ensures a seamless transition in the event of a failover. The HA4 interface is dedicated to this synchronization task.

D) Perform synchronization of sessions, forwarding tables, and IPSec security associations between firewalls in an HA pair:

The HA4 interface is responsible for the synchronization of critical stateful information between the active and passive units in an HA pair. This includes session information, ensuring that the passive unit can continue existing sessions without interruption if it needs to become active.

In addition to session information, HA4 also synchronizes forwarding tables, which contain information on how to route packets, and IPSec security associations, which are necessary for maintaining secure VPN tunnels.

This synchronization ensures that both units in an HA pair have identical information regarding the current state of the network, sessions, and security associations, enabling a smooth and immediate transition to the passive unit in case the active unit fails.