CertsDeals

Free Questions for PCNSE by certsdeals

Shared by Terrell on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

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

Options:

A- To allow traffic between zones in different virtual systems without the traffic leaving the appliance

B- To allow traffic between zones in different virtual systems while the traffic is leaving the appliance

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

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

Answer:

A

Explanation:

External zones are a unique zone type on Palo Alto Networks firewalls that facilitate the movement of traffic between virtual systems on the same physical appliance. These zones are required when multiple virtual systems (vsys) are configured on a single firewall and there is a need to allow inter-vsys traffic without the need for the traffic to leave the firewall and re-enter. An external zone is associated with a specific virtual system and enables traffic to pass from one virtual system to another securely, thereby simplifying traffic management and reducing the need for additional physical interfaces or external routing to handle inter-vsys communication.

Question 2

Question Type: MultipleChoice

A firewall administrator configures the HIP profiles on the edge firewall where GlobalProtect is enabled, and adds the profiles to security rules. The administrator wants to redistribute the HIP reports to the data center firewalls to apply the same access restrictions using HIP profiles. However, the administrator can only see the HIP match logs on the edge firewall but not on the data center firewall

What are two reasons why the administrator is not seeing HIP match logs on the data center firewall? (Choose two.)

Options:

A- Log Forwarding Profile is configured but not added to security rules in the data center firewall.

B- HIP profiles are configured but not added to security rules in the data center firewall.

C- User ID is not enabled in the Zone where the users are coming from in the data center firewall.

D- HIP Match log forwarding is not configured under Log Settings in the device tab.

Answer:

B, C

Explanation:

For HIP match logs to be visible on the data center firewall, the following conditions must be met:

HIP profiles added to security rules: HIP profiles must be applied to security rules on the data center firewall to enforce access restrictions based on the received HIP reports. If the HIP profiles are not associated with the security rules, the firewall will not evaluate traffic against these profiles, and consequently, no HIP match logs will be generated.

User-ID enabled on the incoming zone: User-ID must be enabled on the zone where the users are located in the data center firewall. The User-ID feature is responsible for mapping IP addresses to user names, which is critical for applying policies based on user identity and, by extension, for HIP-based policy enforcement.

The other options (A and D) are related to logging and log forwarding but would not directly impact the generation or visibility of HIP match logs on the data center firewall itself.

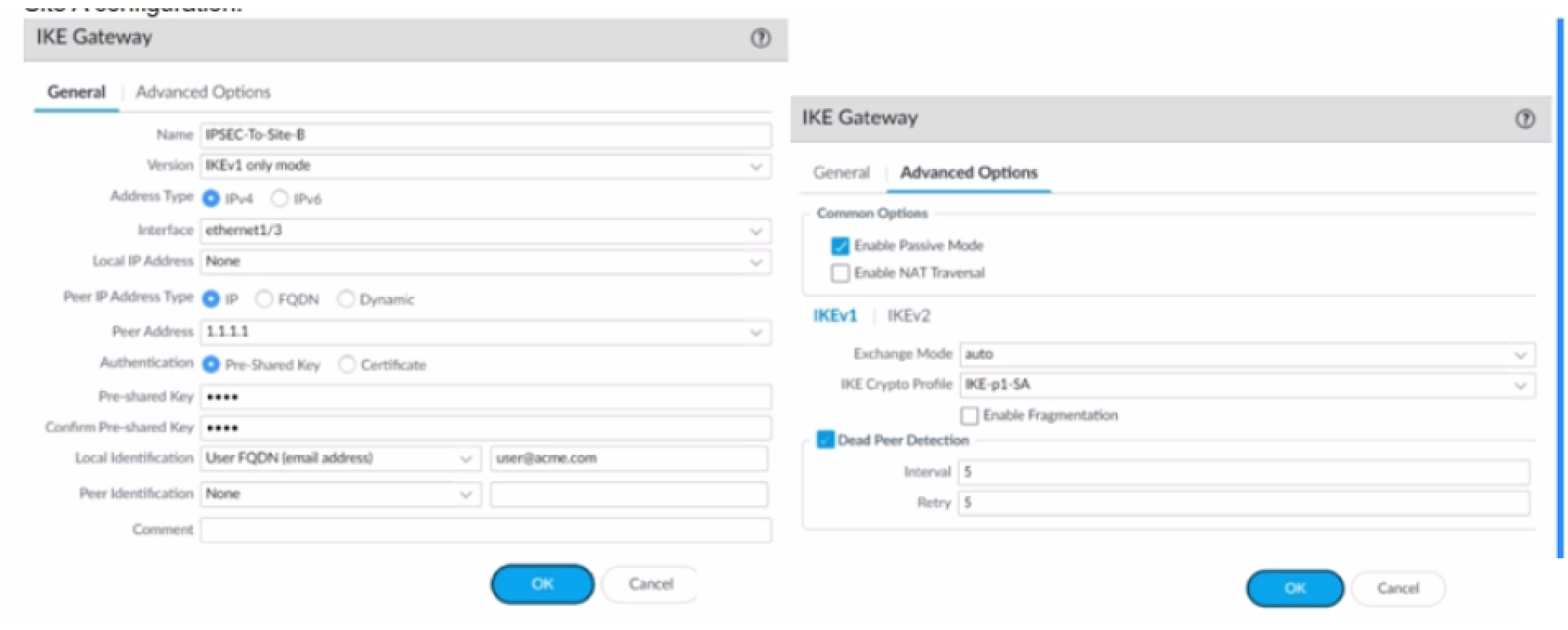
Question 3

Question Type: **MultipleChoice**

A firewall administrator is configuring an IPSec tunnel between Site A and Site B. The Site A firewall uses a DHCP assigned address on the outside interface of the firewall, and the Site B firewall uses a static IP address assigned to the outside interface of the firewall. However, the use of dynamic peering is not working.

Refer to the two sets of configuration settings provided. Which two changes will allow the configurations to work? (Choose two.)

Site A configuration:



IKE Gateway

General | Advanced Options

Name	IPSEC-To-Site-B
Version	IKEv1 only mode
Address Type	● IPv4 ○ IPv6
Interface	ethernet1/3
Local IP Address	None
Peer IP Address Type	● IP ○ FQDN ○ Dynamic
Peer Address	1.1.1.1
Authentication	● Pre-Shared Key ○ Certificate
Pre-shared Key	••••
Confirm Pre-shared Key	••••
Local Identification	User FQDN (email address) — user@acme.com
Peer Identification	None
Comment	

IKE Gateway

General | Advanced Options

Common Options

☑ Enable Passive Mode

☐ Enable NAT Traversal

IKEv1 | IKEv2

Exchange Mode	auto
IKE Crypto Profile	IKE-p1-SA
	☐ Enable Fragmentation

☑ Dead Peer Detection

Interval	5
Retry	5

Options:

A- Enable NAT Traversal on Site B firewall

B- Configure Local Identification on Site firewall

C- Disable passive mode on Site A firewall

D- Match IKE version on both firewalls.

Answer:

C, D

Explanation:

The image shows an IKE Gateway configuration where Site B is set to IKEv1 only mode, and passive mode is not enabled. For dynamic peering to work when Site A is using a DHCP assigned address:

Passive mode on Site A needs to be disabled. In passive mode, the firewall will not initiate the IKE negotiation and will only respond to negotiation requests from the peer. Since Site A has a dynamic IP, it must be able to initiate the connection to Site B, which has a static IP.

Matching the IKE version between Site A and Site B is also necessary for successful IPSec tunnel establishment. Since Site B is set to IKEv1 only mode, Site A also needs to be configured to use IKEv1 to ensure that both sites are using the same version for the IKE negotiation process.

NAT Traversal is used when there are NAT devices between the two endpoints, but there's no indication that this is the case here. Additionally, local identification on Site A is not necessarily related to the issue with dynamic peering not working.

Question 4

Question Type: MultipleChoice

A root cause analysis investigation into a recent security incident reveals that several decryption rules have been disabled. The security team wants to generate email alerts when decryption rules are changed.

How should email log forwarding be configured to achieve this goal?

Options:

A- With the relevant configuration log filter inside Device > Log Settings

B- With the relevant system log filter inside Objects > Log Forwarding

C- With the relevant system log filter inside Device > Log Settings

D- With the relevant configuration log filter inside Objects > Log Forwarding

Answer:

C

Explanation:

To generate email alerts when decryption rules are changed in a Palo Alto Networks firewall, you would configure email log forwarding based on specific system logs that capture changes to decryption policies. This is done by setting up log forwarding profiles with filters that match events related to decryption rule modifications. These profiles are then applied to the relevant log types within the firewall's log settings.

To specifically monitor for changes to decryption rules, you would navigate to the Device > Log Settings section of the firewall's web interface. Here, you can configure log forwarding for system logs, which capture configuration changes among other system-level events. By creating a filter that looks for logs associated with decryption rule changes, and associating this filter with an email server profile, the firewall can automatically send out email alerts whenever a decryption rule is modified.

This setup ensures that the security team is promptly notified of any changes to the decryption policies, allowing for quick review and action if the changes were unauthorized or unintended. It is an essential part of maintaining the security posture of the network and ensuring compliance with organizational policies on encrypted traffic inspection.

Question 5

Question Type: **MultipleChoice**

What happens when an A/P firewall pair synchronizes IPsec tunnel security associations (SAs)?

Options:

A- Phase 1 and Phase 2 SAs are synchronized over HA3 links.

B- Phase 2 SAs are synchronized over HA2 links.

C- Phase 1 and Phase 2 SAs are synchronized over HA2 links.

D- Phase 1 SAs are synchronized over HA1 links.

Answer:

B

Explanation:

In a High Availability (HA) setup with Palo Alto Networks firewalls, the synchronization of IPsec tunnel Security Associations (SAs) is an important aspect to ensure seamless failover and continued secure communication. Specifically, for Phase 2 SAs, they are synchronized over the HA2 links. The HA2 link is dedicated to synchronizing sessions, forwarding tables, IPSec SA, ARP tables, and other critical information between the active and passive firewalls in an HA pair. This ensures that the passive unit can immediately take over in case the active unit fails, without the need for re-establishing IPsec tunnels, thereby maintaining secure communications without interruption. It's important to note that Phase 1 SAs, which are responsible for establishing the secure tunnel itself, are not synchronized between the HA pair, as these need to be re-established upon failover to ensure secure key exchange.

Question 6

Question Type: **MultipleChoice**

An engineer is configuring Packet Buffer Protection on ingress zones to protect from single-session DoS attacks.

Which sessions does Packet Buffer Protection apply to?

Options:

A- It applies to existing sessions and is global.

B- It applies to new sessions and is not global.

C- It applies to existing sessions and is not global.

D- It applies to new sessions and is global.

Answer:

A

Explanation:

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection

Question 7

Question Type: **MultipleChoice**

Which CLI command displays the physical media that are connected to ethernet1/8?

Options:

A- > show system state filter-pretty sys.si. p8. stats

B- > show system state filter-pretty sys.sl.p8.phy

C- > show system state filter-pretty sys.sl.p8.med

D- > show interface ethernet1/8

Answer:

B

Explanation:

The CLI command 'show system state filter-pretty sys.sl.p8.phy' is used to display detailed physical layer information, which would include the physical media connected to a specific interface such as ethernet1/8. This command is designed to filter the output to show relevant physical layer information for the specified interface. For more information on Palo Alto Networks CLI commands and their outputs, refer to the 'PAN-OS CLI Reference Guide'.