

Paloalto-Networks

Exam Questions NGFW-Engineer

Palo Alto Networks Next-Generation Firewall Engineer



NEW QUESTION 1

Which statement applies to Log Collector Groups?

- A. Log redundancy is available only if each Log Collector has the same amount of total disk storage.
- B. Enabling redundancy increases the log processing traffic in a Collector Group by 50%.
- C. In any single Collector Group, all the Log Collectors must run on the same Panorama model.
- D. The maximum number of Log Collectors in a Log Collector Group is 18 plus two hot spares.

Answer: D

Explanation:

The maximum number of Log Collectors that can be added to a Log Collector Group is 18 plus 2 hot spares, ensuring redundancy and availability in case of failure. This allows for a total of up to 20 Log Collectors in a group, providing sufficient scalability and reliability for log collection.

NEW QUESTION 2

After an engineer configures an IPSec tunnel with a Cisco ASA, the Palo Alto Networks firewall generates system messages reporting the tunnel is failing to establish.

Which of the following actions will resolve this issue?

- A. Ensure that an active static or dynamic route exists for the VPN peer with next hop as the tunnel interface.
- B. Configure the Proxy IDs to match the Cisco ASA configuration.
- C. Check that IPSec is enabled in the management profile on the external interface.
- D. Validate the tunnel interface VLAN against the peer's configuration.

Answer: B

Explanation:

The Proxy IDs (or Traffic Selectors) define the local and remote subnets that are allowed to communicate over the IPSec tunnel. If the Proxy IDs on the Palo Alto Networks firewall do not match the configuration on the Cisco ASA, the tunnel will fail to establish because the firewalls won't agree on which traffic to encrypt. Ensuring that the Proxy IDs match between the Palo Alto Networks firewall and the Cisco ASA will resolve the issue.

NEW QUESTION 3

What must be configured before a firewall administrator can define policy rules based on users and groups?

- A. User Mapping profile
- B. Authentication profile
- C. Group mapping settings
- D. LDAP Server profile

Answer: C

Explanation:

Before a firewall administrator can define policy rules based on users and groups, the Group Mapping settings must be configured. These settings enable the firewall to map users to their respective Active Directory (AD) groups. This mapping allows the firewall to use user and group information to create policy rules based on group membership.

NEW QUESTION 4

An organization has configured GlobalProtect in a hybrid authentication model using both certificate-based authentication for the pre-logout stage and SAML-based multi-factor authentication (MFA) for user logon.

How does the GlobalProtect agent process the authentication flow on Windows endpoints?

- A. The GlobalProtect agent uses the machine certificate to establish a pre-logout tunnel; upon user sign-in, it prompts for SAML-based MFA credentials, ensuring both device and user identities are validated before granting full access.
- B. The GlobalProtect agent uses the machine certificate during pre-logout for initial tunnel establishment, and then seamlessly reuses the same machine certificate for user-based authentication without requiring MFA.
- C. Once the machine certificate is validated at pre-logout, the Windows endpoint completes MFA on behalf of the user by passing existing Windows Credential Provider details to the GlobalProtect gateway without prompting the user.
- D. GlobalProtect requires the user to log in first for SAML-based MFA before establishing the pre-logout tunnel, rendering the pre-logout certificate authentication (CA) flow redundant.

Answer: A

Explanation:

In a hybrid authentication model with both certificate-based authentication for pre-logout and SAML-based multi-factor authentication (MFA) for user logon, the GlobalProtect agent processes the flow as follows:

During the pre-logout stage, the agent uses the machine certificate to authenticate and establish the initial VPN tunnel.

Once the user logs in (after the machine is connected), the agent then triggers SAML-based MFA to ensure the user is authenticated with multi-factor authentication, validating both the device and the user identity before granting full access.

This method ensures that both the device and user are properly authenticated and validated in the hybrid authentication model.

NEW QUESTION 5

Which two zone types are valid when configuring a new security zone? (Choose two.)

- A. Tunnel
- B. Intrazone
- C. Internal
- D. Virtual Wire

Answer: AD

Explanation:

When configuring a new security zone on a Palo Alto Networks firewall, the two valid zone types are:

Tunnel: A Tunnel zone is used for traffic that is associated with a VPN tunnel, such as IPSec tunnels. Traffic passing through a tunnel interface is classified into this zone.

Virtual Wire: A Virtual Wire zone is used when a firewall operates in transparent mode (also known as Layer 2 mode). In this configuration, the firewall can inspect traffic without modifying the IP address structure of the network.

NEW QUESTION 6

Without performing a context switch, which set of operations can be performed that will affect the operation of a connected firewall on the Panorama GUI?

- A. Restarting the local firewall, running a packet capture, accessing the firewall CLI
- B. Modification of local security rules, modification of a Layer 3 interface, modification of the firewall device hostname
- C. Modification of pre-security rules, modification of a virtual router, modification of an IKE Gateway Network Profile
- D. Modification of post NAT rules, creation of new views on the local firewall ACC tab, creation of local custom reports

Answer: B

Explanation:

In Panorama, without performing a context switch, the administrator can perform local configuration tasks directly on the connected firewall. The following operations can be done:

Modification of local security rules: Security rules can be modified directly on the connected firewall from the Panorama GUI.

Modification of a Layer 3 interface: Changes to the Layer 3 interfaces on the connected firewall can be done from Panorama, without needing to switch to the firewall's local interface.

Modification of the firewall device hostname: The firewall's hostname can be changed via Panorama.

NEW QUESTION 7

Which networking technology can be configured on Layer 3 interfaces but not on Layer 2 interfaces?

- A. DDNS
- B. Link Duplex
- C. NetFlow
- D. LLDP

Answer: C

Explanation:

NetFlow is a Layer 3 (network layer) protocol that collects and monitors IP traffic flows. It is typically configured on Layer 3 interfaces because it relies on IP information for traffic flow analysis, which is not available on Layer 2 interfaces. Layer 2 interfaces handle frames within the local network, and they don't have IP-related details that NetFlow uses to generate traffic statistics.

NEW QUESTION 8

During an upgrade to the routing infrastructure in a customer environment, the network administrator wants to implement Advanced Routing Engine (ARE) on a Palo Alto Networks firewall.

Which firewall models support this configuration?

- A. PA-5280, PA-7080, PA-3250, VM-Series
- B. PA-455, VM-Series, PA-1410, PA-5450
- C. PA-3260, PA-5410, PA-850, PA-460
- D. PA-7050, PA-1420, VM-Series, CN-Series

Answer: C

Explanation:

The Advanced Routing Engine (ARE) is supported on Palo Alto Networks firewalls that utilize the PAN-OS 11.0+ software and have the required hardware architecture. The supported models include PA-3200 Series, PA-5400 Series, PA-800 Series, and PA-400 Series. These models provide enhanced routing capabilities, including BGP, OSPF, and more complex routing policies.

PA-3260 and PA-5410 are part of the PA-3200 and PA-5400 Series, which are known to support ARE.

PA-850 and PA-460 are within the PA-800 and PA-400 Series, which also support ARE

NEW QUESTION 9

Which two statements apply to configuring required security rules when setting up an IPSec tunnel between a Palo Alto Networks firewall and a third-party gateway? (Choose two.)

- A. For incoming and outgoing traffic through the tunnel, creating separate rules for each direction is optional.
- B. The IKE negotiation and IPSec/ESP packets are allowed by default via the intrazone default allow policy.
- C. For incoming and outgoing traffic through the tunnel, separate rules must be created for each direction.
- D. The IKE negotiation and IPSec/ESP packets are denied by default via the interzone default deny policy.

Answer: CD

Explanation:

Separate rules must be created for each direction: Palo Alto Networks firewalls enforce security policies based on traffic direction. To allow bidirectional communication through the IPSec tunnel, two separate rules are required - one for incoming and one for outgoing traffic.

IKE negotiation and IPSec/ESP packets are denied by default: Palo Alto Networks firewalls use an interzone default deny policy, meaning that unless an explicit policy allows IKE (UDP 500/4500) and ESP (protocol 50) traffic, the firewall will block these packets, preventing tunnel establishment. Therefore, administrators must create explicit rules permitting IKE and IPSec/ESP traffic to the firewall's external interface.

NEW QUESTION 10

In a Palo Alto Networks environment, GlobalProtect has been enabled using certificate-based authentication for both users and devices. To ensure proper validation of certificates, one or more certificate profiles are configured. What function do certificate profiles serve in this context?

- A. They store private keys for users and devices, effectively allowing the firewall to issue or reissue certificates if the primary Certificate Authority (CA) becomes unavailable, providing a built-in fallback CA to maintain continuous certificate issuance and authentication.
- B. They define trust anchors (root / intermediate Certificate Authorities (CAs)), specify revocation checks (CRL/OCSP), and map certificate attributes (e.g., CN) for user or device authentication.
- C. They allow the firewall to bypass certificate validation entirely, focusing only on username / password-based authentication.
- D. They provide a one-click mechanism to distribute certificates to all endpoints without relying on external enrollment methods.

Answer: B

Explanation:

In the context of GlobalProtect with certificate-based authentication, certificate profiles are used to ensure proper validation of the certificates. They perform the following functions: Define trust anchors, which are the root and intermediate Certificate Authorities (CAs) that the firewall trusts to authenticate certificates. Specify revocation checks, such as CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol), to ensure that the certificates being used have not been revoked. Map certificate attributes, such as the Common Name (CN), which helps in authenticating users and devices based on their certificates.

NEW QUESTION 10

An NGFW engineer is establishing bidirectional connectivity between the accounting virtual system (VSYS) and the marketing VSYS. The traffic needs to transition between zones without leaving the firewall (no external physical connections). The interfaces for each VSYS are assigned to separate virtual routers (VRs), and inter-VR static routes have been configured. An external zone has been created correctly for each VSYS. Security policies have been added to permit the desired traffic between each zone and its respective external zone. However, the desired traffic is still unable to successfully pass from one VSYS to the other in either direction.

Which additional configuration task is required to resolve this issue?

- A. Create a transit VSYS and route all inter-VSYS traffic through it.
- B. Add each VSYS to the list of visible virtual systems of the other VSYS.
- C. Enable the ??allow inter-VSYS traffic?? option in both external zone configurations.
- D. Create Security policies to allow the traffic between the two external zones.

Answer: B

Explanation:

In Palo Alto Networks firewalls, each virtual system (VSYS) is typically isolated from other VSYSs, meaning that traffic between different VSYSs cannot pass through the firewall by default. In this case, since the interfaces for each VSYS are assigned to separate virtual routers (VRs), and the desired traffic is still not passing between the two VSYSs, the firewall needs to be explicitly configured to allow traffic between them. The required configuration is to add each VSYS to the list of visible virtual systems of the other VSYS. This allows inter-VSYS communication to be enabled, effectively permitting the traffic to pass between the zones of different VSYSs.

NEW QUESTION 14

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NGFW-Engineer Practice Exam Features:

- * NGFW-Engineer Questions and Answers Updated Frequently
- * NGFW-Engineer Practice Questions Verified by Expert Senior Certified Staff
- * NGFW-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NGFW-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NGFW-Engineer Practice Test Here](#)