DUMPSARENA

Palo Alto Networks Network Security Generalist

Palo Alto Networks NetSec-Generalist

Version Demo

Total Demo Questions: 6

Total Premium Questions: 67

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

What is the main security benefit of adding a CN-Series firewall to an existing VM-Series firewall deployment when the customer is using containers?

A. It provides perimeter threat detection and inspection outside the container itself.

B. It prevents lateral threat movement within the container itself.

C. It monitors and logs traffic outside the container itself.

D. It enables core zone segmentation within the container itself.

ANSWER: B

Explanation:

It prevents lateral threat movement within the container itself. More precisely, the CN-Series extends security enforcement into the Kubernetes container environment, where workloads, pods, and services communicate dynamically. A VM-Series firewall can secure traffic at virtual-machine, virtual-network, and north-south boundaries, while CN-Series is designed to provide visibility and policy enforcement for containerized workloads within Kubernetes. This added enforcement helps apply least-privilege connectivity between application components and inspect allowed application traffic using Palo Alto Networks security policies and threat-prevention capabilities. As a result, if a workload is compromised, controls can limit its ability to reach other workloads or services unnecessarily, reducing the opportunity for an attacker or malware to move laterally through the cluster. This is the key complementary benefit in a deployment that already uses VM-Series: security coverage is extended to the container-native layer and to the dynamic east-west communications that occur there. Palo Alto Networks describes CN-Series as a Kubernetes-native next-generation firewall solution for securing containerized applications and Kubernetes clusters. See the CN-Series documentation and the CN-Series product overview for its Kubernetes-focused security capabilities.

QUESTION NO: 2

A network administrator places several internal application servers and their users in the same security zone during an initial migration. The organization wants to enforce least-privilege access between those systems before introducing additional zones.

Which policy action should the administrator take?

A. Create an interzone Security policy rule for the application servers.

B. Create an intrazone Security policy rule that permits only the required applications.

C. Configure a destination NAT rule for communications within the zone.

D. Enable a Zone Protection profile to replace the intrazone-default rule.

ANSWER: B

Explanation:

Create an intrazone Security policy rule that explicitly allows only the required application traffic and denies the remaining traffic. By default, the firewall allows traffic between interfaces in the same zone through the intrazone-default rule. An explicit intrazone rule placed above that default rule enables the administrator to define the permitted applications, users, sources, destinations, and Security profiles for communications within the zone.

Creating an interzone rule would not control traffic that remains within the same zone. Changing the default rule to broadly deny traffic could disrupt required communications without defining the intended least-privilege access.

QUESTION NO: 3

An administrator manages branch firewalls through Panorama. The administrator wants to centrally configure shared network connectivity settings while allowing each device group to maintain its own Security policy and address objects.

Which two settings should be configured in a Panorama template? (Choose two.)

A. Ethernet interfaces

B. Virtual routers

C. Security policy rules

D. Address objects

ANSWER: A B

Explanation:

Panorama templates manage device and network configuration, including interfaces and virtual routers. These settings define how each firewall connects to networks and forwards traffic. Template variables can be used when a shared template requires device-specific values.

Security policy rules and address objects are managed through device groups because they are policy and object configuration rather than network configuration. This separation allows a common network baseline to be used across firewalls while policy is applied according to the appropriate device-group hierarchy.

QUESTION NO: 4

An organization hosts multiple private web servers in a DMZ and uses a single public IP address for outbound internet access. The administrator must ensure that simultaneous outbound connections from different internal servers can be translated without assigning a dedicated public IP address to each server.

Which source NAT translation type should the administrator configure?

A. Dynamic IP and Port

B. Static IP

C. Destination NAT

D. Bi-directional static NAT

ANSWER: A

Explanation:

Dynamic IP and Port (DIPP) is appropriate because it translates multiple private source addresses to one or more public IP addresses and differentiates concurrent sessions by assigning unique source ports. This enables many internal servers to share a limited public address pool while maintaining distinct session mappings.

Static IP NAT creates a fixed one-to-one translation and requires a dedicated public address for each mapped private address. Destination NAT publishes an internal resource to external clients and does not provide the required outbound source translation.

QUESTION NO: 5

A security operations team wants to automatically quarantine endpoints that generate a high-confidence threat event. The quarantine policy must begin applying without an administrator manually editing address objects.

Which two configurations support this workflow? (Choose two.)

A. Create a Dynamic Address Group that matches the quarantine tag.

B. Create a static address group containing all endpoint addresses.

C. Configure a Log Forwarding profile with a tagging action.

D. Create a HIP profile that matches the threat signature.

ANSWER: A C

Explanation:

A **Log Forwarding profile with a tagging action** can register a quarantine tag for an IP address when a matching threat log is generated. A **Dynamic Address Group** that matches the same tag can then be used as the source or destination in a restrictive Security policy rule. Static address groups require manual maintenance, and a HIP profile evaluates endpoint posture reported by GlobalProtect rather than tags registered from firewall logs.

QUESTION NO: 6

Which two security profiles must be updated to prevent data exfiltration in outbound traffic on NGFWs? (Choose two.)

A. Data Filtering

B. DoS Protection

C. File Blocking

D. Antivirus

ANSWER: A C

Explanation:

Data Filtering is a core outbound data-loss-prevention control on Palo Alto Networks NGFWs. A Data Filtering profile inspects traffic that matches a Security policy for configured data patterns, including predefined patterns for sensitive information and custom patterns tailored to an organization's confidential data. The profile can generate alerts or block transmissions when a configured threshold is reached. Keeping its patterns, thresholds, and attachment to the appropriate outbound Security rules current ensures that the firewall identifies protected information as data classifications and business requirements evolve.

File Blocking complements content-pattern inspection by controlling which file types users may upload, download, or transfer through applications allowed by Security policy. For outbound traffic, it can block or alert on file types that are not authorized to leave the organization, including archive and document formats that could contain sensitive information. Maintaining the file-type controls for sanctioned outbound applications reduces opportunities to package and transfer data through web, email, or file-sharing channels. These profiles must be attached to the relevant Security policy rules for enforcement. Palo Alto Networks documents Data Filtering at Data Filtering Profiles and file-transfer controls at File Blocking Profiles.