DUMPSARENA

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 11.0

Palo Alto Networks PCNSE

Version Demo

Total Demo Questions: 20

Total Premium Questions: 500

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

An engineer is tasked with configuring a Zone Protection profile on the untrust zone.

Which three settings can be configured on a Zone Protection profile? (Choose three.)

A. Ethernet SGT Protection

B. Protocol Protection
Protocol Protection: Protocol protection is used to limit or block traffic that uses certain protocols or application functions. For example, a Zone Protection profile can be configured to block traffic that uses non-standard protocols, such as IP-in-IP, or to limit the number of concurrent sessions for certain protocols, such as SIP.

C. DoS Protection
DoS Protection: DoS protection is used to protect against various types of denial-of-service (DoS) attacks, such as SYN floods, UDP floods, ICMP floods, and others. A Zone Protection profile can be configured to limit the rate of traffic for certain protocols or to drop traffic that matches specific patterns, such as malformed packets or packets with invalid headers.

D. Reconnaissance Protection
Reconnaissance Protection: Reconnaissance protection is used to prevent attackers from gathering information about the network, such as by using port scans or other techniques. A Zone Protection profile can be configured to limit the rate of traffic for certain types of reconnaissance, such as port scans or OS fingerprinting, or to drop traffic that matches specific patterns, such as packets with invalid flags or payloads.

E. Resource Protection

ANSWER: B C D

Explanation:

B. Protocol Protection: Protocol protection is used to limit or block traffic that uses certain protocols or application functions. For example, a Zone Protection profile can be configured to block traffic that uses non-standard protocols, such as IP-in-IP, or to limit the number of concurrent sessions for certain protocols, such as SIP.

C. DoS Protection: DoS protection is used to protect against various types of denial-of-service (DoS) attacks, such as SYN floods, UDP floods, ICMP floods, and others. A Zone Protection profile can be configured to limit the rate of traffic for certain protocols or to drop traffic that matches specific patterns, such as malformed packets or packets with invalid headers.

D. Reconnaissance Protection: Reconnaissance protection is used to prevent attackers from gathering information about the network, such as by using port scans or other techniques. A Zone Protection profile can be configured to limit the rate of traffic for certain types of reconnaissance, such as port scans or OS fingerprinting, or to drop traffic that matches specific patterns, such as packets with invalid flags or payloads.

QUESTION NO: 2

In a firewall, which three decryption methods are valid? (Choose three.)

A. SSL Outbound Proxyless Inspection

B. SSL Inbound Inspection

C. SSH Proxy

D. SSL Inbound Proxy

E. Decryption Mirror

ANSWER: B C E

Explanation:

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-overview.html

QUESTION NO: 3

An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router.

Which two options enable the administrator to troubleshoot this issue? (Choose two.)

A. View Runtime Stats in the virtual router.

B. View System logs.

C. Add a redistribution profile to forward as BGP updates.

D. Perform a traffic pcap at the routing stage.

ANSWER: A B

QUESTION NO: 4

An engineer is deploying multiple firewalls with common configuration in Panorama.

What are two benefits of using nested device groups? (Choose two.)

A. Inherit settings from the Shared group

B. Inherit IPSec crypto profiles
Inherit IPSec crypto profiles
This is correct because IPSec crypto profiles are one of the objects that can be inherited from a parent device group1. You can also create IPSec crypto profiles for use in shared or device group policy1.

C. Inherit all Security policy rules and objects

D. Inherit parent Security policy rules and objects
Inherit parent Security policy rules and objects
This is correct because Security policy rules and objects are also inheritable from a parent device group1. You can also create Security policy rules and objects for use in shared or device group policy1.

ANSWER: B D

Explanation:

B. Inherit IPSec crypto profiles

This is correct because IPSec crypto profiles are one of the objects that can be inherited from a parent device group1. You can also create IPSec crypto profiles for use in shared or device group policy1.

D. Inherit parent Security policy rules and objects

This is correct because Security policy rules and objects are also inheritable from a parent device group1. You can also create Security policy rules and objects for use in shared or device group policy1.

QUESTION NO: 5

A network administrator is troubleshooting an issue with Phase 2 of an IPSec VPN tunnel. The administrator determines that the lifetime needs to be changed to match the peer.

Where should this change be made?

A. IKE Gateway profile

B. IPSec Crypto profile

C. IPSec Tunnel settings

D. IKE Crypto profile

ANSWER: C

QUESTION NO: 6

An administrator is seeing one of the firewalls in a HA active/passive pair moved to 'suspended" state due to Non-functional loop. Which three actions will help the administrator troubleshool this issue? (Choose three.)

A. Use the CLI command show high-availability flap-statistics

B. Check the HA Link Monitoring interface cables.

C. Check the High Availability > Link and Path Monitoring settings.

D. Check High Availability > Active/Passive Settings > Passive Link State

E. Check the High Availability > HA Communications > Packet Forwarding settings.

ANSWER: A B C

QUESTION NO: 7

Which action disables Zero Touch Provisioning (ZTP) functionality on a ZTP firewall during the onboarding process?

A. removing the Panorama serial number from the ZTP service

B. performing a factory reset of the firewall

C. performing a local firewall commit

D. removing the firewall as a managed device in Panorama

ANSWER: C

Explanation:

Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UiOCAU&lang=en_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com% 2FKCSArticleDetail

QUESTION NO: 8

A firewall should be advertising the static route 10.2.0.0/24 Into OSPF. The configuration on the neighbor is correct, but the route is not in the neighbor's routing table.

Which two configurations should you check on the firewall? (Choose two.)

A. In the OSFP configuration, ensure that the correct redistribution profile is selected in the OSPF Export Rules section.

B. Within the redistribution profile ensure that Redist is selected.

C. Ensure that the OSPF neighbor state Is "2-Way."

D. In the redistribution profile check that the source type is set to "ospf."

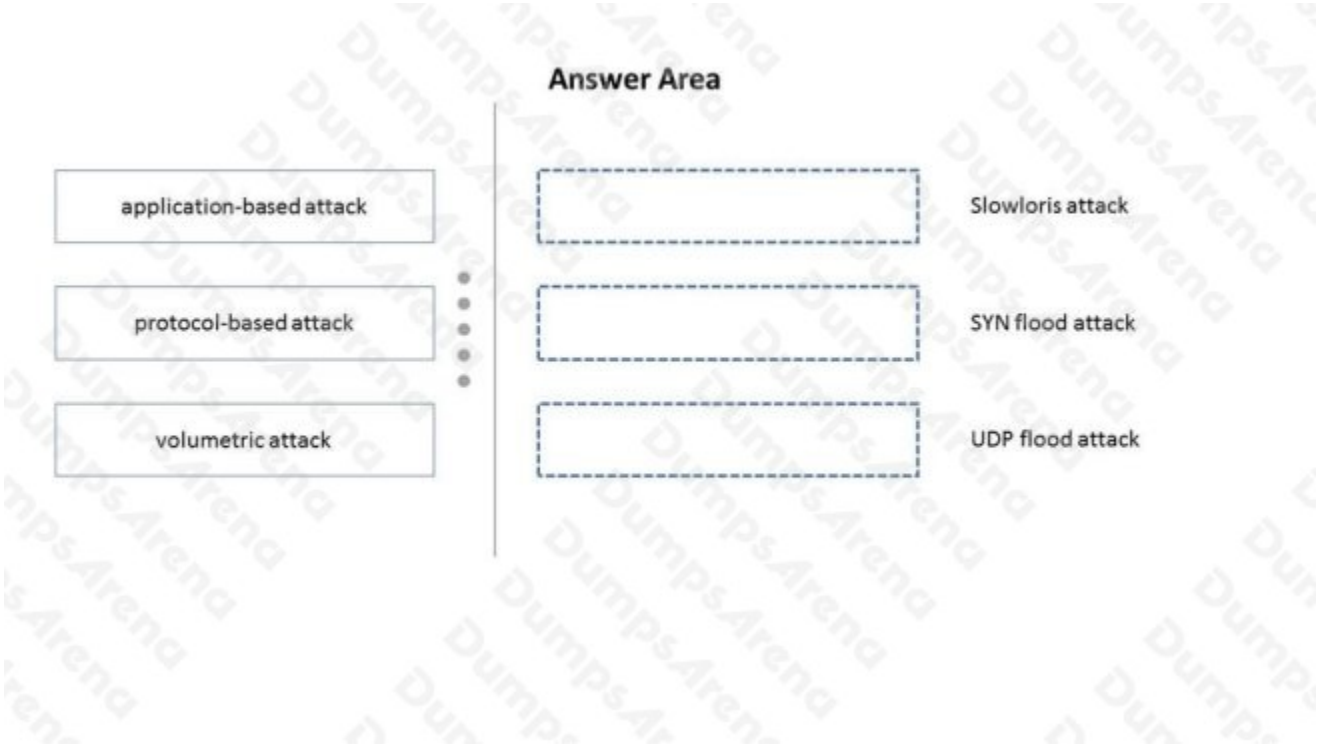
ANSWER: A B

QUESTION NO: 9 - (DRAG DROP)

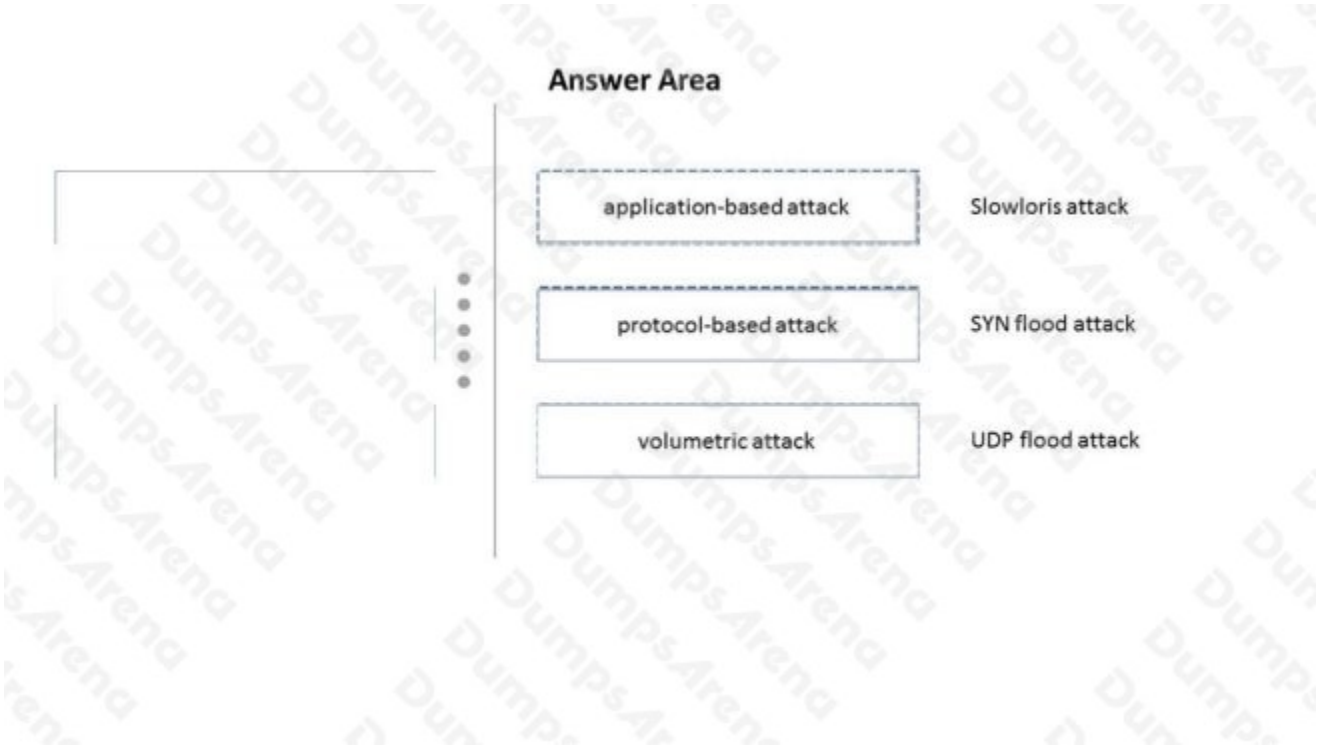
DRAG DROP

Match each type of DoS attack to an example of that type of attack.

Select and Place:



ANSWER:



Explanation:

Reference: https://www.hackingarticles.in/dos-penetration-testing-part-1/#:~:text=Protocol%2DBased%20Attack%3A%20This%20kind,unresponsive%20to%20other%20legitimate%20requests

QUESTION NO: 10

A company is deploying User-ID in their network. The firewall learn needs to have the ability to see and choose from a list of usernames and user groups directly inside the Panorama policies when creating new security rules

How can this be achieved?

A. By configuring Data Redistribution Client in Panorama > Data Redistribution

B. By configuring User-ID source device in Panorama > Managed Devices

C. By configuring User-ID group mapping in Panorama > User Identification

D. By configuring Master Device in Panorama > Device Groups

ANSWER: C

Explanation:

User-ID group mapping is a feature that allows Panorama to retrieve user and group information from directory services such as LDAP or Active Directory1. This information can be used to enforce security policies based on user identity and group membership.

To configure User-ID group mapping on Panorama, you need to perform the following steps1:

By configuring User-ID group mapping on Panorama, you can see and choose from a list of usernames and user groups directly inside the Panorama policies when creating new security rules2.

QUESTION NO: 11

Where can an administrator see both the management-plane and data-plane CPU utilization in the WebUI?

A. System Resources widget

B. System Logs widget

C. Session Browser

D. General Information widget

ANSWER: A

Explanation:

The System Resources widget of the Exadata WebUI, displays a real-time overview of the various resources like CPU, Memory, and I/O usage across the entire Exadata Database Machine. It shows the usage of both management-plane and data-plane CPU utilization.

System Resources Widget Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or Panorama). https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/dashboard/dashboard-widgets.html

QUESTION NO: 12

What can an engineer use with GlobalProtect to distribute user-specific client certificates to each GlobalProtect user?

A. Certificate profile

B. SSL/TLS Service profile

C. OCSP Responder

D. SCEP

ANSWER: D

QUESTION NO: 13

The manager of the network security team has asked you to help configure the company's Security Profiles according to Palo Alto Networks best practice As part of that effort, the manager has assigned you the Vulnerability Protection profile for the internet gateway firewall.

Which action and packet-capture setting for items of high severity and critical severity best matches Palo Alto Networks best practice?

A. action 'reset-both' and packet capture 'extended-capture'

B. action 'default' and packet capture 'single-packet'

C. action 'reset-both' and packet capture 'single-packet'

D. action 'reset-server' and packet capture 'disable'

ANSWER: C

Explanation:

https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles

"Enable extended-capture for critical, high, and medium severity events and single-packet capture for low severity events. " https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection

QUESTION NO: 14

A firewall administrator has been asked to configure a Palo Alto Networks NGFW to prevent against compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.

Which Security Profile type will prevent these behaviors?

A. Anti-Spyware

B. WildFire

C. Vulnerability Protection

D. Antivirus

ANSWER: A

Explanation:

Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/anti-spyware-profiles

QUESTION NO: 15

In an existing deployment, an administrator with numerous firewalls and Panorama does not see any WildFire logs in Panorama. Each firewall has an active WildFire subscription On each firewall. WildFire togs are available.

This issue is occurring because forwarding of which type of logs from the firewalls to Panorama is missing?

A. Threat logs

B. Traffic togs

C. System logs

D. WildFire logs

ANSWER: D

Explanation:

When an administrator has numerous firewalls and Panorama, WildFire logs need to be forwarded from the firewalls to Panorama in order for them to be visible in Panorama. WildFire logs contain information about malicious files that have been detected by WildFire and provide detailed information such as the file's hash value, severity, and other attributes. This information can then be used to help identify threats and take appropriate security measures. Proper configuration of forwarding WildFire logs is essential for monitoring malicious activity and ensuring the security of the network.

QUESTION NO: 16

An engineer needs to see how many existing SSL decryption sessions are traversing a firewall

What command should be used?

A. show dataplane pool statistics I match proxy

B. debug dataplane pool statistics I match proxy

C. debug sessions I match proxy

D. show sessions all

ANSWER: B

QUESTION NO: 17

An engineer configures SSL decryption in order to have more visibility to the internal users' traffic when it is regressing the firewall.

Which three types of interfaces support SSL Forward Proxy? (Choose three.)

A. High availability (HA)

B. Layer

C. Virtual Wire

D. Tap

E. Layer 3

ANSWER: B C E

Explanation:

SSL Forward Proxy is a feature that allows the firewall to decrypt and inspect outbound SSL traffic from internal users to external servers1. The firewall acts as a proxy (MITM) generating a new certificate for the accessed URL and presenting it to the client during SSL handshake2.

SSL Forward Proxy can be configured on any interface type that supports security policies, which are Layer 2, Virtual Wire, and Layer 3 interfaces1. These interface types allow the firewall to apply security profiles and URL filtering on the decrypted SSL traffic.

QUESTION NO: 18

Given the following configuration, which route is used for destination 10.10.0.4?

set network virtual-router 2 routing-table ip static-route "Route 1" nexthop ip-address 192.168.1.2 set network virtual-router 2 routing-table ip static-route "Route 1" metric 30

set network virtual-router 2 routing-table ip static-route "Route 1" destination 10.10.0.0/24

set network virtual-router 2 routing-table ip static-route "Route 1" re route-table unicast

set network virtual-router 2 routing-table ip static-route "Route 2" nexthop ip-address 192.168.1.2

set network virtual-router 2 routing-table ip static-route "Route 2" metric 20

set network virtual-router 2 routing-table ip static-route "Route 2" destination 10.10.0.0/24 set network virtual-router 2 routing-table ip static-route "Route 2" route-table unicast set network virtual-router 2 routing-table ip static-route "Route 3" nexthop ip-address 10.10.20.1

set network virtual-router 2 routing-table ip static-route "Route 3" metric 5

set network virtual-router 2 routing-table ip static-route "Route 3" destination 0.0.0.0/0 set network virtual-router 2 routing-table ip static-route "Route 3" route-table unicast set network virtual-router 2 routing-table ip static-route "Route 4" nexthop ip-address 192.168.1.2

set network virtual-router 2 routing-table ip static-route "Route 4" metric 10

set network virtual-router 2 routing-table ip static-route "Route 4" destination 10.10.1.0/25 set network virtual-router 2 routing-table ip static-route "Route 4" route-table unicast

A. Route 1

B. Route 3

C. Route 2

D. Route 4

ANSWER: C

Explanation:

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/network/network-virtual-routers/more-runtime-stats-for-a-virtual-router/routing-tab.html

QUESTION NO: 19

An administrator is configuring a Panorama device group

Which two objects are configurable? (Choose two)

A. DNS Proxy

B. Address groups

C. SSL/TLS roles

D. URL Filtering profiles

ANSWER: B D

Explanation:

URL filtering is a feature in Palo Alto Networks firewalls that allows administrators to block access to specific URLs [1]. This feature can be configured via four different objects: Custom URL categories in URL Filtering profiles, PAN-DB URL categories in URL Filtering profiles, External Dynamic Lists (EDL) in URL Filtering profiles, and Custom URL categories in Security policy rules. The evaluation order for URL filtering is: Custom URL categories in URL Filtering profile, PAN-DB URL categories in URL Filtering profile, EDL in URL Filtering profile, and Custom URL category in Security policy rule. This

information can be found in the Palo Alto Networks PCNSE Study Guide, which can be accessed here: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/resource-library/palo-alto-networks-pcnse-study-guide.html.

QUESTION NO: 20

A network security administrator wants to configure SSL inbound inspection.

Which three components are necessary for inspecting the HTTPS traffic as it enters the firewall? (Choose three.)

A. An SSL/TLS Service profile

B. The web server's security certificate with the private key

C. A Decryption profile

D. A Decryption policy

E. The client's security certificate with the private key

ANSWER: B C D

Explanation:

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-inbound-inspection