

PCNSE^{Q&As}

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 11.x

Pass Palo Alto Networks PCNSE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/pcnse.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours.

Which two steps are likely to mitigate the issue? (Choose TWO)

- A. Exclude video traffic
- B. Enable decryption
- C. Block traffic that is not work-related
- D. Create a Tunnel Inspection policy

Correct Answer: AC

This is because excluding video traffic from being sent over the VPN will reduce the amount of bandwidth being used during peak hours, allowing more bandwidth to be available for other types of traffic. Blocking non-work related traffic will also reduce the amount of bandwidth being used, further freeing up bandwidth for work-related traffic. Enabling decryption and creating a Tunnel Inspection policy are not likely to mitigate the issue of decreased performance during peak-use hours, as they do not directly address the issue of limited bandwidth availability during these times.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PP3ICAW>

QUESTION 2

YouTube videos are consuming too much bandwidth on the network, causing delays in mission-critical traffic. The administrator wants to throttle YouTube traffic. The following interfaces and zones are in use on the firewall:

*

ethernet1/1, Zone: Untrust (Internet-facing)

*

ethernet1/2, Zone: Trust (client-facing)

A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet1/1 has a QoS profile called Outbound, and interface Ethernet1/2 has a QoS

profile called Inbound.

Which setting for class 6 will throttle YouTube traffic?

- A. Outbound profile with Guaranteed Ingress
- B. Outbound profile with Maximum Ingress
- C. Inbound profile with Guaranteed Egress
- D. Inbound profile with Maximum Egress

Correct Answer: D

QUESTION 3

An engineer is configuring a firewall with three interfaces:

1.

MGT connects to a switch with internet access.

2.

Ethernet1/1 connects to an edge router.

3.

Ethernet1/2 connects to a visualization network.

The engineer needs to configure dynamic updates to use a dataplane interface for internet traffic. What should be configured in Setup > Services > Service Route Configuration to allow this traffic?

A. Set DNS and Palo Alto Networks Services to use the ethernet1/1 source interface.

B. Set DNS and Palo Alto Networks Services to use the ethernet1/2 source interface.

C. Set DNS and Palo Alto Networks Services to use the MGT source interface.

D. Set DDNS and Palo Alto Networks Services to use the MGT source interface.

Correct Answer: A

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIGJCA0>

QUESTION 4

A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers. Which option will protect the individual servers?

A. Enable packet buffer protection on the Zone Protection Profile.

B. Apply an Anti-Spyware Profile with DNS sinkholing.

C. Use the DNS App-ID with application-default.

D. Apply a classified DoS Protection Profile.

Correct Answer: D

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles>

To protect critical web or DNS servers on your network, protect the individual servers. To do this, set appropriate flooding and resource protection thresholds in a DoS protection profile, and create a DoS protection policy rule that applies the profile to each server's IP address by adding the IP addresses as the rule's destination criteria.

QUESTION 5

What are the differences between using a service versus using an application for Security Policy match?

- A. Use of a "service" enables the firewall to take action after enough packets allow for App- ID identification
- B. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers Use of an "application" allows the firewall to take action after enough packets allow for App-ID identification regardless of the ports being used.
- C. There are no differences between "service" or "application" Use of an "application" simplifies configuration by allowing use of a friendly application name instead of port numbers.
- D. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers. Use of an "application" allows the firewall to take immediate action if the port being used is a member of the application standard port list

Correct Answer: B

<https://live.paloaltonetworks.com/t5/blogs/what-are-applications-and-services/ba-p/342508#> A service on the Palo Alto Networks firewall is a TCP or UDP port which port is open or closed and does not look beyond Layer 4. An application

it goes into Layer 7 inspection to ascertain which application is active in a data flow and will enforce "normal" behavior onto it, DNS Query

<https://live.paloaltonetworks.com/t5/blogs/what-are-applications-and-services/ba-p/342508#>

Concept 1

A service on the Palo Alto Networks firewall is a TCP or UDP port, as it would be defined on a traditional firewall or access list. It simply defines which port is open or closed and does not look beyond Layer 4.

Concept 2

An application is what makes the Palo Alto Networks next-generation firewall so powerful; it goes into Layer 7 inspection to ascertain which application is active in a data flow and will enforce "normal" behavior onto it (e.g., a session identified as DNS that suddenly sends an SQL query is abnormal and will be blocked).