



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.pass4itsure.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**

Which source is the most reliable for collecting User-ID user mapping?

- A. GlobalProtect
- B. Microsoft Active Directory
- C. Microsoft Exchange
- D. Syslog Listener

Correct Answer: A

User-ID is a feature that enables you to identify and control users on your network based on their usernames instead of their IP addresses. User mapping is the process of mapping IP addresses to usernames using various sources of information. The most reliable source for collecting User-ID user mapping is GlobalProtect. GlobalProtect is a solution that provides secure access to your network and resources from anywhere. GlobalProtect agents on endpoints send user mapping information directly to the firewall or Panorama, which eliminates the need for probing other sources. GlobalProtect also supports dynamic IP address changes and roaming users.

QUESTION 2

An ISP manages a Palo Alto Networks firewall with multiple virtual systems for its tenants.

Where on this firewall can the ISP configure unique service routes for different tenants?

- A. Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Inherit Global Service Route Configuration
- B. Setup > Services > Global > Service Route Configuration > Customize
- C. Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Customize
- D. Setup > Services > Global > Service Route Configuration > Use Management Interface for all

Correct Answer: C

The best option for the ISP to configure unique service routes for different tenants is to use the Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Customize option on the firewall. This option allows the ISP to customize the service routes for each virtual system that represents a tenant. A service route is the path from the interface to the service on a server, such as DNS, email, or Panorama. By customizing the service routes for each virtual system, the ISP can ensure that each tenant uses a different interface or IP address to access these services. Option A is incorrect because it is used to inherit the global service route configuration for a virtual system, not to customize it. Option B is incorrect because it is used to customize the global service route configuration for all virtual systems, not for a specific one. Option D is incorrect because it is used to use the management interface for all service routes, not to customize them.

QUESTION 3

When you troubleshoot an SSL Decryption issue, which PAN-OS CLI command do you use to check the details of the



Forward Trust certificate, Forward Untrust certificate, and SSL Inbound Inspection certificate?

- A. show system setting ssl-decrypt certs
- B. show system setting ssl-decrypt certificate
- C. debug dataplane show ssl-decrypt ssl-stats
- D. show system setting ssl-decrypt certificate-cache

Correct Answer: B

QUESTION 4

Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

- A. User-logon (Always on)
- B. At-boot
- C. On-demand
- D. Pre-logon

Correct Answer: D

Client certificate refers to user cert, it can be used for '\\user-logon\\'/'on-demand' connect methods. Used to authenticate a user. -Machine certificate refers to device cert, it can be used for '\\pre-logon\\' connect method. This is used to authenticate a device, not a user.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIf0CAK>

QUESTION 5

A network administrator wants to deploy GlobalProtect with pre-logon for Windows 10 endpoints and follow Palo Alto Networks best practices. To install the certificate and key for an endpoint, which three components are required? (Choose three.)

- A. server certificate
- B. local computer store
- C. private key
- D. self-signed certificate
- E. machine certificate

Correct Answer: BDE

<https://docs.paloaltonetworks.com/globalprotect/9-0/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-with-pre-logon.html>



QUESTION 6

An engineer decides to use Panorama to upgrade devices to PAN-OS 10.2.

Which three platforms support PAN-OS 10.2? (Choose three.)

- A. PA-5000 Series
- B. PA-500
- C. PA-800 Series
- D. PA-220
- E. PA-3400 Series

Correct Answer: CDE

According to the Palo Alto Networks Compatibility Matrix¹, the three platforms that support PAN-OS 10.2 are: PA-800 Series² PA-220² PA-3400 Series² The PA-5000 Series and PA-500 do not support PAN-OS 10.2. To upgrade devices to PAN-OS 10.2 using Panorama, you need to determine the upgrade path³, upgrade Panorama itself⁴, and then upgrade the firewalls using Panorama⁵.

QUESTION 7

Refer to the exhibit.



Device Group

DATACENTER_DG

Q

	NAME	LOCATION	ADDRESS
<input type="checkbox"/>	Server-1	DATACENTER_DG	2.2.2.2
<input type="checkbox"/>	Server-1	Shared	1.1.1.1

Device Group

DC_FW_DG

Q

	NAME	LOCATION	ADDRESS
<input type="checkbox"/>	Server-1	DC_FW_DG	3.3.3.3
<input type="checkbox"/>	Server-1	Shared	1.1.1.1

Device Group

FW-1_DG

Q

	NAME	LOCATION	ADDRESS
<input type="checkbox"/>	Server-1	FW-1_DG	4.4.4.4
<input type="checkbox"/>	Server-1	Shared	1.1.1.1

☐

NAME ^

☐

Shared

☐

DATACENTER_DG

☐

DC_FW_DG

☐

FW-1_DG

☐

REGIONAL_DG

☐

OFFICE_FW_DG

Review the screenshots and consider the following information:

- FW-1 is assigned to the FW-1_DG device group, and FW-2 is assigned to OFFICE_FW_DG.
- There are no objects configured in REGIONAL_DG and OFFICE_FW_DG device groups. Which IP address will be pushed to the firewalls inside Address Object Server-1?
 - Server-1 on FW-1 will have IP 1.1.1.1. Server-1 will not be pushed to FW-2.
 - Server-1 on FW-1 will have IP 3.3.3.3. Server-1 will not be pushed to FW-2.
 - Server-1 on FW-1 will have IP 2.2.2.2. Server-1 will not be pushed to FW-2.
 - Server-1 on FW-1 will have IP 4.4.4.4. Server-1 on FW-2 will have IP 1.1.1.1.

Correct Answer: D

FW-1 will get the value from FW-DG1 while FW-2 will get the value from the Shared DG since no values are present in its parent DGs. <https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-devicegroups/manage-precedence-of-inherited-objects>

**QUESTION 8**

A security engineer has configured a GlobalProtect portal agent with four gateways.

Which GlobalProtect Gateway will users connect to based on the chart provided?

GATEWAY NAME	PRIORITY	RESPONSE TIME
East	Highest	35 ms
South	High	25 ms
West	Medium	50 ms
Central	Low	20 ms

- A. East
- B. South
- C. West
- D. Central

Correct Answer: B

QUESTION 9

A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and port. Which option when enabled with the correction threshold would mitigate this attack without dropping legitimate traffic to other hosts inside the network?

- A. Zone Protection Policy with UDP Flood Protection
- B. QoS Policy to throttle traffic below maximum limit
- C. Security Policy rule to deny traffic to the IP address and port that is under attack
- D. Classified DoS Protection Policy using destination IP only with a Protect action

Correct Answer: D

QUESTION 10

Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address?



- A. Set the type to Aggregate, clear the session\\'s box and set the Maximum concurrent Sessions to 4000.
- B. Set the type to Classified, clear the session\\'s box and set the Maximum concurrent Sessions to 4000.
- C. Set the type Classified, check the Sessions box and set the Maximum concurrent Sessions to 4000.
- D. Set the type to aggregate, check the Sessions box and set the Maximum concurrent Sessions to 4000.

Correct Answer: C

QUESTION 11

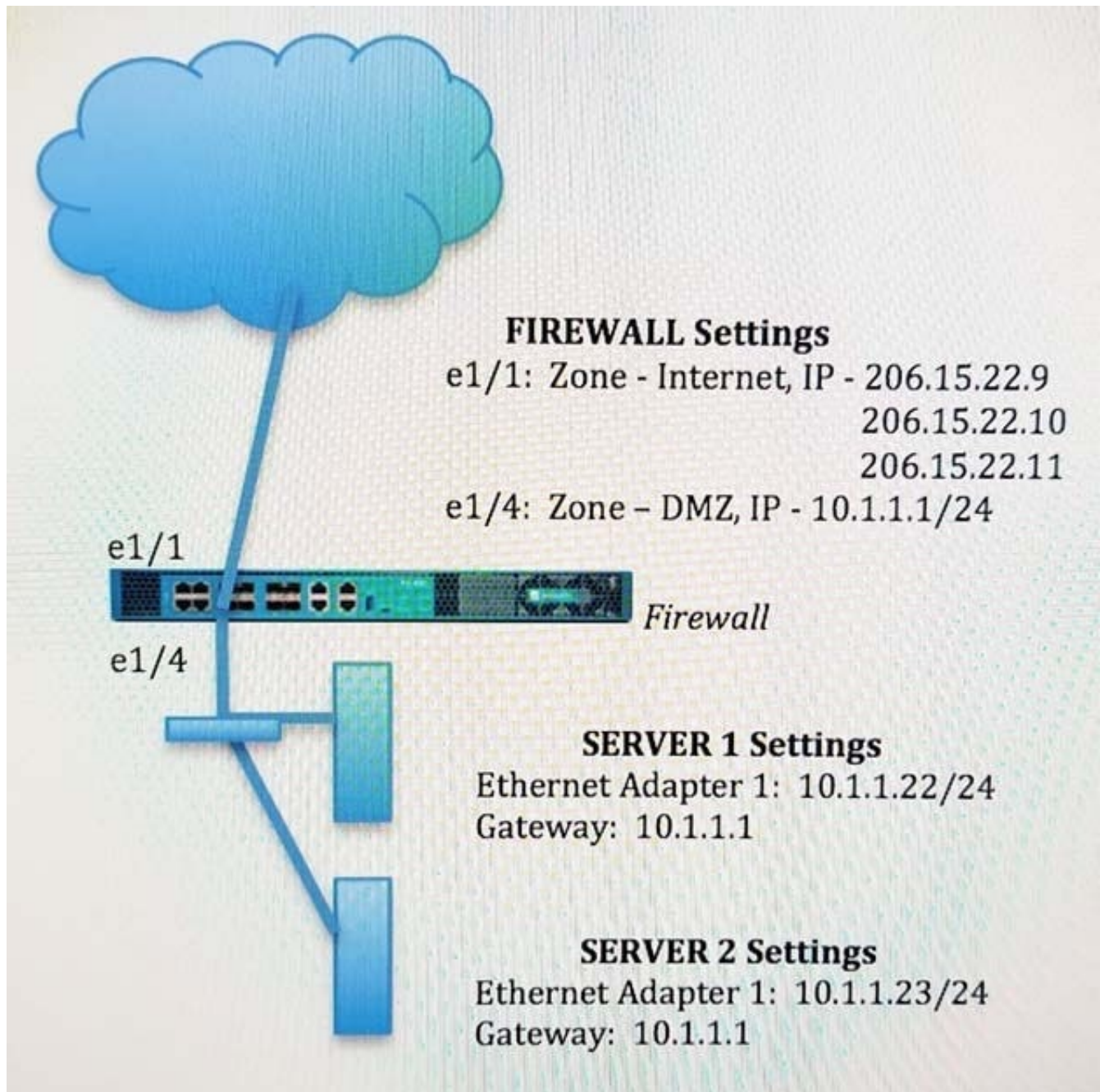
Which field is optional when creating a new Security Policy rule?

- A. Name
- B. Description
- C. Source Zone
- D. Destination Zone
- E. Action

Correct Answer: B

QUESTION 12

An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22



Based on the information shown in the image, which NAT rule will forward web-browsing traffic correctly?



A.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

B.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP

C.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: None

D.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 80/TCP



- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: C

NAT zones are just whatever interface traffic is going to. The source (the big cloud internet) is obviously internet, and the destination zone is the internet facing interface of the firewall, so the destination is also internet. It then is translated into an IP that the internal network can read.

QUESTION 13

Which configuration task is best for reducing load on the management plane?

- A. Disable logging on the default deny rule
- B. Enable session logging at start
- C. Disable pre-defined reports
- D. Set the URL filtering action to send alerts

Correct Answer: C

QUESTION 14

How are IPV6 DNS queries configured to user interface ethernet1/3?

- A. Network > Virtual Router > DNS Interface
- B. Objects > CustomerObjects > DNS
- C. Network > Interface Mgrnt
- D. Device > Setup > Services > Service Route Configuration

Correct Answer: D

QUESTION 15

An engineer is in the planning stages of deploying User-ID in a diverse directory services environment. Which server OS platforms can be used for server monitoring with User-ID?

- A. Microsoft Terminal Server, Red Hat Linux, and Microsoft Active Directory
- B. Microsoft Active Directory, Red Hat Linux, and Microsoft Exchange



C. Microsoft Exchange, Microsoft Active Directory, and Novell eDirectory

D. Novell eDirectory, Microsoft Terminal Server, and Microsoft Active Directory

Correct Answer: C

[PCNSE VCE Dumps](#)

[PCNSE Study Guide](#)

[PCNSE Braindumps](#)