

PASSTCERT

QUESTION & ANSWER

Higher Quality
Better Service!

We offer free update service for one year
[HTTP://WWW.PASSTCERT.COM](http://www.passtcert.com)

Exam : PCNSE6

**Title : Palo Alto Networks Certified
Network**

Version : DEMO

1. Configuring a pair of devices into an Active/Active HA pair provides support for:

- A. Higher session count
- B. Redundant Virtual Routers
- C. Asymmetric routing environments
- D. Lower fail-over times

Answer: B

2. As a Palo Alto Networks firewall administrator, you have made unwanted changes to the Candidate configuration.






These changes may be undone by Device > Setup > Operations > Configuration Management>....and then what operation?

- A. Revert to Running Configuration
- B. Revert to last Saved Configuration
- C. Load Configuration Version
- D. Import Named Configuration Snapshot

Answer: A

3. A company has a Palo Alto Networks firewall with a single VSYS that has both locally defined rules as well as shared and device-group rules pushed from Panorama.

In what order are the policies evaluated?

Evaluated 1st	<div>Choose One </div> <div>Shared Pre Rules Device Group Pre Rules Shared Post Rules Firewall Local Rules Device Group Post Rules</div>
Evaluated 2nd	<div>Choose One </div> <div>Shared Pre Rules Device Group Pre Rules Shared Post Rules Firewall Local Rules Device Group Post Rules</div>
Evaluated 3rd	<div>Choose One </div> <div>Shared Pre Rules Device Group Pre Rules Shared Post Rules Firewall Local Rules Device Group Post Rules</div>
Evaluated 4th	<div>Choose One </div> <div>Shared Pre Rules Device Group Pre Rules Shared Post Rules Firewall Local Rules Device Group Post Rules</div>
Evaluated 5th	<div>Choose One </div> <div>Shared Pre Rules Device Group Pre Rules Shared Post Rules Firewall Local Rules Device Group Post Rules</div>

Answer:

Evaluated 1st	<div>Choose One</div> <div>Shared Pre Rules</div> <div>Device Group Pre Rules</div> <div>Shared Post Rules</div> <div>Firewall Local Rules</div> <div>Device Group Post Rules</div>
Evaluated 2nd	<div>Choose One</div> <div>Shared Pre Rules</div> <div>Device Group Pre Rules</div> <div>Shared Post Rules</div> <div>Firewall Local Rules</div> <div>Device Group Post Rules</div>
Evaluated 3rd	<div>Choose One</div> <div>Shared Pre Rules</div> <div>Device Group Pre Rules</div> <div>Shared Post Rules</div> <div>Firewall Local Rules</div> <div>Device Group Post Rules</div>
Evaluated 4th	<div>Choose One</div> <div>Shared Pre Rules</div> <div>Device Group Pre Rules</div> <div>Shared Post Rules</div> <div>Firewall Local Rules</div> <div>Device Group Post Rules</div>
Evaluated 5th	<div>Choose One</div> <div>Shared Pre Rules</div> <div>Device Group Pre Rules</div> <div>Shared Post Rules</div> <div>Firewall Local Rules</div> <div>Device Group Post Rules</div>

4.A company hosts a publicly-accessible web server behind their Palo Alto Networks firewall, with this configuration information:

Users outside the company are in the "Untrust-L3" zone. The web server physically resides in the "Trust-L3" zone. Web server public IP address: 1.1.1.1


Web server private IP address: 192.168.1.10

Which NAT Policy rule will allow users outside the company to access the web server?

A. ☐

Original Packet								Translated Packet	
Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Servi...	Source Translation	Destination Translation	
1 Web_server_Inbound	 Trust-L3	 Untrust-L3	any	 192.168.1.10	any	any	static-ip 1.1.1.1 bi-directional: yes	none	

B. ☐

Original Packet								Translated Packet	
Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Servi...	Source Translation	Destination Translation	
1 Web_server_Inbound	 Untrust-L3	 Trust-L3	any	any	 1.1.1.1	any	none	address: 192.168.1.10	

C. ☐

Original Packet								Translated Packet	
Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Servi...	Source Translation	Destination Translation	
1 Web_server_Inbound	 Untrust-L3	 Trust-L3	any	any	 192.168.1.10	any	none	address: 1.1.1.1	

D. ☐

		Original Packet						Translated Packet	
	Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Servi...	Source Translation	Destination Translation
1	Web_server_Inbound	 Untrust-L3	 Untrust-L3	any	any	 192.168.1.10	any	none	address: 1.1.1.1

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

Answer: B

5.Wildfire may be used for identifying which of the following types of traffic?

- A. URL content
B. DHCP
C. DNS
D. Viruses

Answer: D