Paloalto Networks

Exam PCNSE6

Palo Alto Networks Certified Network Security Engineer 6.0

Version: 6.1

[Total Questions: 153]

Question No : 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

Question No : 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?

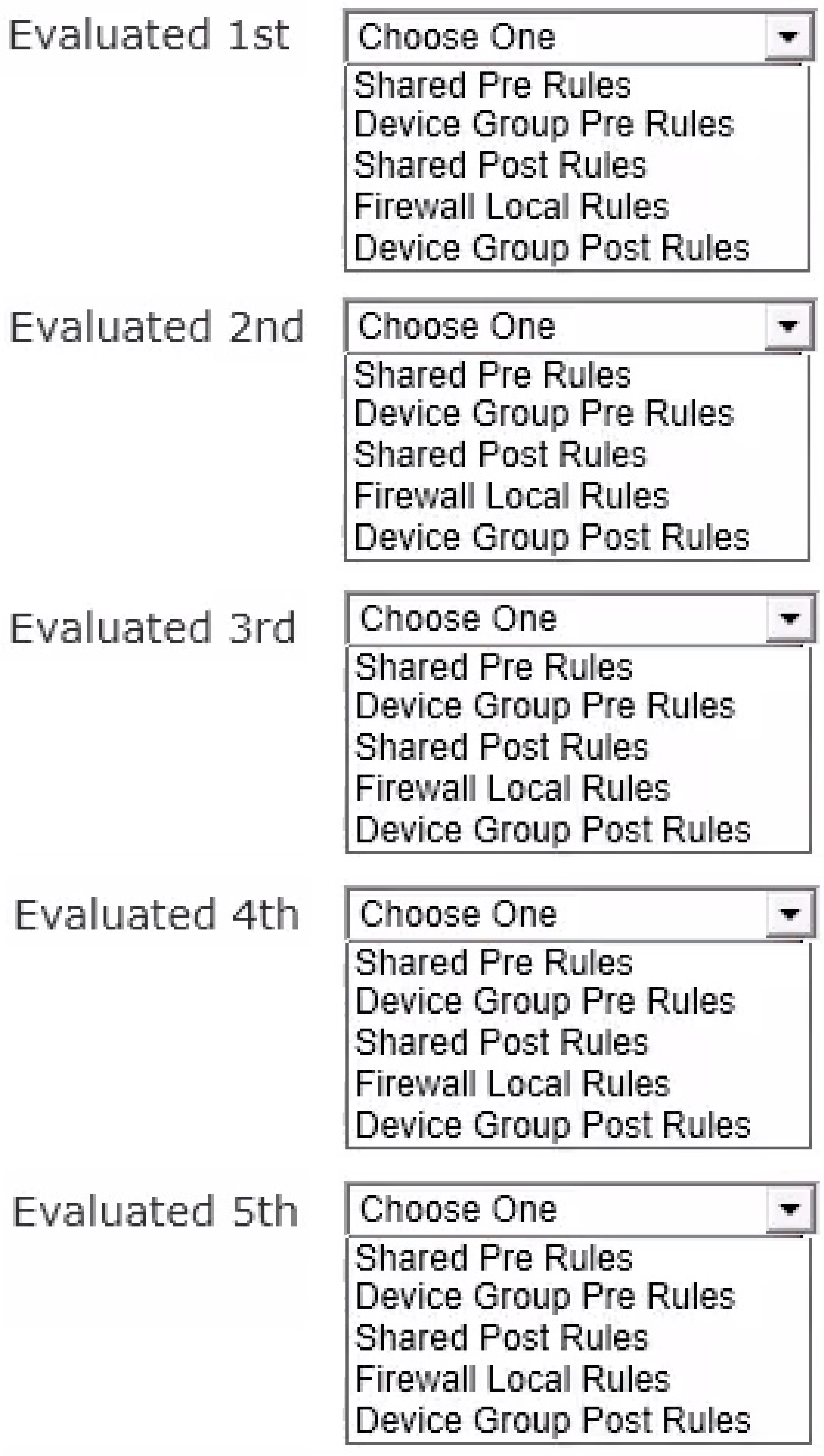
A. Revert to Running Configuration
B. Revert to last Saved Configuration
C. Load Configuration Version
D. Import Named Configuration Snapshot

Answer: A

Question No : 3 HOTSPOT

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

Choose One
- Shared Pre Rules
- Device Group Pre Rules
- Shared Post Rules
- Firewall Local Rules
- Device Group Post Rules

Evaluated 2nd

Choose One
- Shared Pre Rules
- Device Group Pre Rules
- Shared Post Rules
- Firewall Local Rules
- Device Group Post Rules

Evaluated 3rd

Choose One
- Shared Pre Rules
- Device Group Pre Rules
- Shared Post Rules
- Firewall Local Rules
- Device Group Post Rules

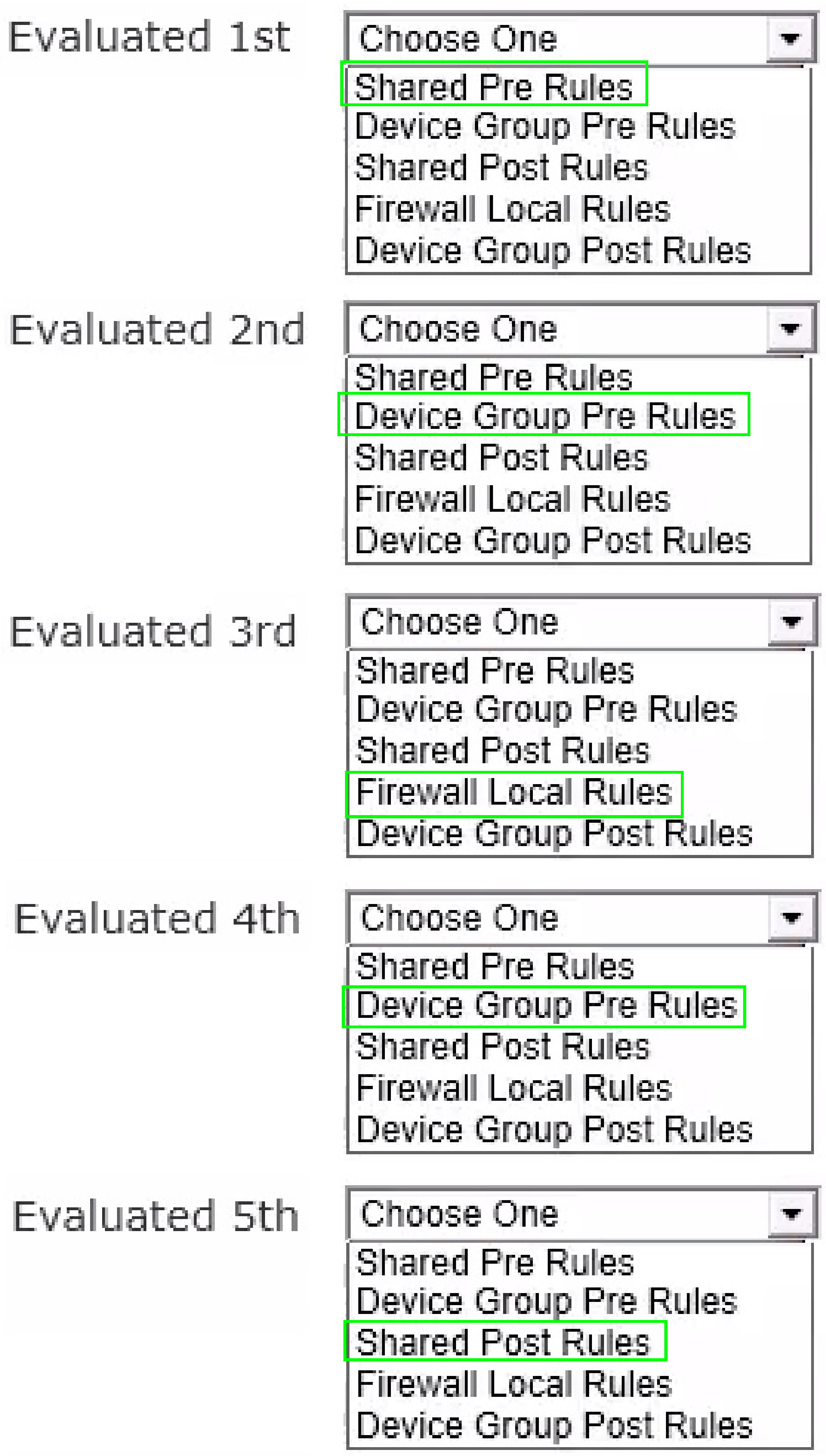
Evaluated 4th

Choose One
- Shared Pre Rules
- Device Group Pre Rules
- Shared Post Rules
- Firewall Local Rules
- Device Group Post Rules

Evaluated 5th

Choose One
- Shared Pre Rules
- Device Group Pre Rules
- Shared Post Rules
- Firewall Local Rules
- Device Group Post Rules

Answer:



Evaluated 1st

Choose One
[✓ Shared Pre Rules]
Device Group Pre Rules
Shared Post Rules
Firewall Local Rules
Device Group Post Rules

Evaluated 2nd

Choose One
Shared Pre Rules
[✓ Device Group Pre Rules]
Shared Post Rules
Firewall Local Rules
Device Group Post Rules

Evaluated 3rd

Choose One
Shared Pre Rules
Device Group Pre Rules
Shared Post Rules
[✓ Firewall Local Rules]
Device Group Post Rules

Evaluated 4th

Choose One
Shared Pre Rules
[✓ Device Group Pre Rules]
Shared Post Rules
Firewall Local Rules
Device Group Post Rules

Evaluated 5th

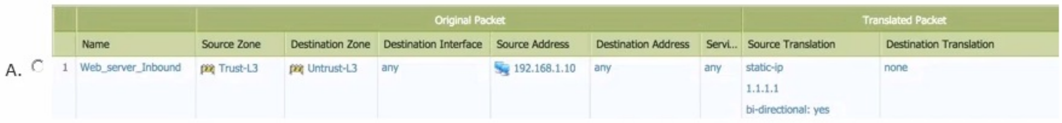
Choose One
Shared Pre Rules
Device Group Pre Rules
[✓ Shared Post Rules]
Firewall Local Rules
Device Group Post Rules

Question No : 4

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

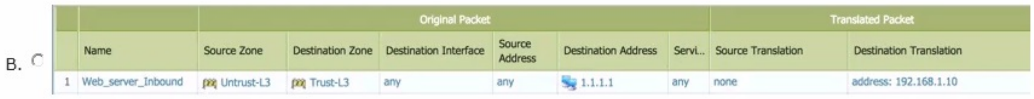
- Users outside the company are in the "Untrust-L3" zone.
- The web server physically resides in the "Trust-L3" zone.
- Web server public IP address: 1.1.1.1
- Web server private IP address: 192.168.1.10

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



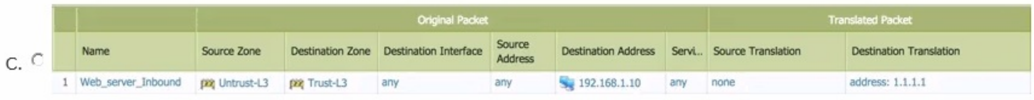
A. ○

		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



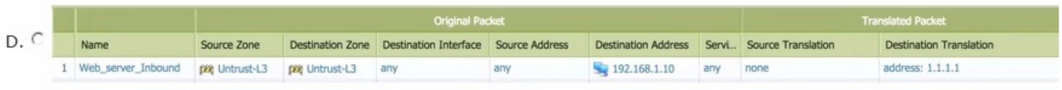
B. ○

		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

Question No : 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

Question No : 6

In PAN-OS 5.0, how is Wildfire enabled?

A. Via the "Forward" and "Continue and Forward" File-Blocking actions
B. A custom file blocking action must be enabled for all PDF and PE type files
C. Wildfire is automatically enabled with a valid URL-Filtering license
D. Via the URL-Filtering "Continue" Action.

Answer: A

Question No : 7

The IT department has received complaints about VoIP call jitter when the sales staff is making or receiving calls. QoS is enabled on all firewall interfaces, but there is no QoS policy written in the rulebase. The IT manager wants to find out what traffic is causing the jitter in real time when a user reports the jitter.

Which feature can be used to identify, in real-time, the applications taking up the most bandwidth?

A. Application Command Center (ACC)
B. QoS Statistics
C. QoS Log
D. Applications Report

Answer: A
Reference: http://www.newnet66.org/Support/Resources/Using-The-ACC.pdf

Question No : 8

Which two steps are required to make Microsoft Active Directory users appear in the firewall's traffic log? Choose 2 answers

A. Enable User-ID on the zone object for the source zone.
B. Enable User-ID on the zone object for the destination zone.
C. Configure a RADIUS server profile to point to a domain controller.
D. Run the User-ID Agent using an Active Directory account that has "domain administrator" permissions.
E. Run the User-ID Agent using an Active Directory account that has "event log viewer" permissions.

Answer: A,E

Question No : 9

Administrative Alarms can be enabled for which of the following except?

A. Certificate Expirations
B. Security Violation Thresholds
C. Security Policy Tags
D. Traffic Log capacity

Answer: A

Question No : 10

Where in the firewall GUI can an administrator see how many sessions of web-browsing traffic have occurred in the last day?

A. Monitor->Session Browser
B. Monitor->App Scope->Summary
C. Objects->Applications->web-browsing
D. ACC->Application

Answer: D
Reference: http://www.newnet66.org/Support/Resources/Using-The-ACC.pdf

Question No : 11

Which of the following are accurate statements describing the HA3 link in an Active-Active HA deployment?

A. HA3 is used for session synchronization
B. The HA3 link is used to transfer Layer 7 information
C. HA3 is used to handle asymmetric routing
D. HA3 is the control link

Answer: A

Question No : 12

Which of the following would be a reason to use an XML API to communicate with a Palo Alto Networks firewall?

A. So that information can be pulled from other network resources for User-ID
B. To allow the firewall to push UserID information to a Network Access Control (NAC) device.
C. To permit sys logging of User Identification events

Answer: B

Question No : 13

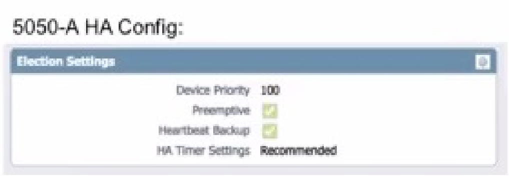
When Network Address Translation has been performed on traffic, Destination Zones in Security rules should be based on:

A. Post-NAT addresses
B. The same zones used in the NAT rules
C. Pre-NAT addresses
D. None of the above

Answer: A

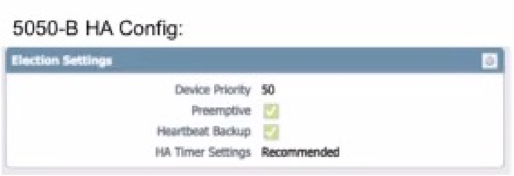
Question No : 14

Two firewalls are configured in an Active/Passive High Availability (HA) pair with the following election settings:


5050-A HA Config:

Election Settings

Device Priority 100
Preemptive ☑
Heartbeat Backup ☑
HA Timer Settings Recommended


5050-B HA Config:

Election Settings

Device Priority 50
Preemptive ☑
Heartbeat Backup ☑
HA Timer Settings Recommended

Firewall 5050-B is presently in the "Active" state and 5050-A is presently in the "Passive" state. Firewall 5050-B reboots causing 5050-A to become Active.

Which firewall will be in the "Active" state after firewall 5050-B has completed its reboot and is back online?

A. Both firewalls are active (split brain)
B. Firewall 5050-B
C. Firewall 5050-A
D. It could be either firewall

Answer: B
Reference: https://live.paloaltonetworks.com/docs/DOC-2926

Question No : 15

Which three engines are built into the Single-Pass Parallel Processing Architecture?
Choose 3 answers

A. Application Identification (App-ID)
B. Group Identification (Group-ID)
C. User Identification (User-ID)
D. Threat Identification (Threat-ID)
E. Content Identification (Content-ID)

Answer: A,C,E
Reference: https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/white-papers/single-pass-parallel-processing-architecture.pdf page 5

Question No : 16

In an Anti-Virus profile, changing the action to “Block” for IMAP or POP decoders will result in the following:

A. The connection from the server will be reset
B. The Anti-virus profile will behave as if “Alert” had been specified for the action
C. The traffic will be dropped by the firewall
D. Error 541 being sent back to the server

Answer: B

Question No : 17

Subsequent to the installation of new licenses, the firewall must be rebooted

A. True
B. False

Answer: B

Question No : 18

When setting up GlobalProtect, what is the job of the GlobalProtect Portal? Select the best answer

A. To maintain the list of remote GlobalProtect Portals and list of categories for checking the client machine
B. To maintain the list of GlobalProtect Gateways and list of categories for checking the client machine
C. To load balance GlobalProtect client connections to GlobalProtect Gateways
D. None of the above

Answer: B