

## Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

<https://www.2passeasy.com/dumps/PCNSA/>



#### NEW QUESTION 1

An administrator wants to create a No-NAT rule to exempt a flow from the default NAT rule. What is the best way to do this?

- A. Create a Security policy rule to allow the traffic.
- B. Create a new NAT rule with the correct parameters and leave the translation type as None
- C. Create a static NAT rule with an application override.
- D. Create a static NAT rule translating to the destination interface.

**Answer: B**

#### NEW QUESTION 2

Actions can be set for which two items in a URL filtering security profile? (Choose two.)

- A. Block List
- B. Custom URL Categories
- C. PAN-DB URL Categories
- D. Allow List

**Answer: AD**

#### Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions>

#### NEW QUESTION 3

What is a prerequisite before enabling an administrative account which relies on a local firewall user database?

- A. Configure an authentication policy
- B. Configure an authentication sequence
- C. Configure an authentication profile
- D. Isolate the management interface on a dedicated management VLAN

**Answer: C**

#### NEW QUESTION 4

Based on the screenshot presented which column contains the link that when clicked opens a window to display all applications matched to the policy rule?

**No App Specified**  
 These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks you convert these service only security policies to application based policies.

	Name	Service	Traffic (Bytes, 30 days)	App Usage				Modified
				Apps Allowed	Apps Seen	Days with No New Apps	Compare	
3	egress-outside	application-default	25.3G	any	8	8	<a href="#">Compare</a>	2019-06-2...
1	inside-portal	any	372.6M	any	9	8	<a href="#">Compare</a>	2019-06-2...

- A. Apps Allowed
- B. Name
- C. Apps Seen
- D. Service

**Answer: C**

#### NEW QUESTION 5

Which security profile will provide the best protection against ICMP floods, based on individual combinations of a packet's source and destination IP address?

- A. DoS protection
- B. URL filtering
- C. packet buffering
- D. anti-spyware

**Answer: A**

#### NEW QUESTION 6

Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

	Name	Type	Source		Destination		Application	Service	Action
			Zone	Address	Zone	Address			
1	inside-portal	universal	inside	any	outside	203.0.113.20	any	any	Allow
2	internal-inside-dmz	universal	inside	any	dmz	any	ftp ssh ssl web-browsing	application-default	Allow
3	egress-outside	universal	inside	any	outside	any	any	application-default	Allow
4	egress-outside-content-id	universal	inside	any	outside	any	any	application-default	Allow
5	danger-simulated-traffic	universal	danger	any	danger	any	any	application-default	Allow
6	intrazone-default	intrazone	any	any	(intrazone)	any	any	any	Allow
7	intrazone-default	intrazone	any	any	any	any	any	any	Deny

- A. internal-inside-dmz
- B. engress outside
- C. inside-portal
- D. intercone-default

**Answer:** B

#### NEW QUESTION 7

Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?

- A. Windows session monitoring via a domain controller
- B. passive server monitoring using the Windows-based agent
- C. Captive Portal
- D. passive server monitoring using a PAN-OS integrated User-ID agent

**Answer:** C

#### Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-username-using-captive-portal.html>

#### NEW QUESTION 8

What is considered best practice with regards to committing configuration changes?

- A. Disable the automatic commit feature that prioritizes content database installations before committing
- B. Validate configuration changes prior to committing
- C. Wait until all running and pending jobs are finished before committing
- D. Export configuration after each single configuration change performed

**Answer:** A

#### NEW QUESTION 9

What can be achieved by selecting a policy target prior to pushing policy rules from Panorama?

- A. Doing so limits the templates that receive the policy rules
- B. Doing so provides audit information prior to making changes for selected policy rules
- C. You can specify the firewalls in a device group to which to push policy rules
- D. You specify the location as pre or post-rules to push policy rules

**Answer:** C

#### NEW QUESTION 10

What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

- A. SAML
- B. TACACS+
- C. LDAP
- D. Kerberos

**Answer:** AB

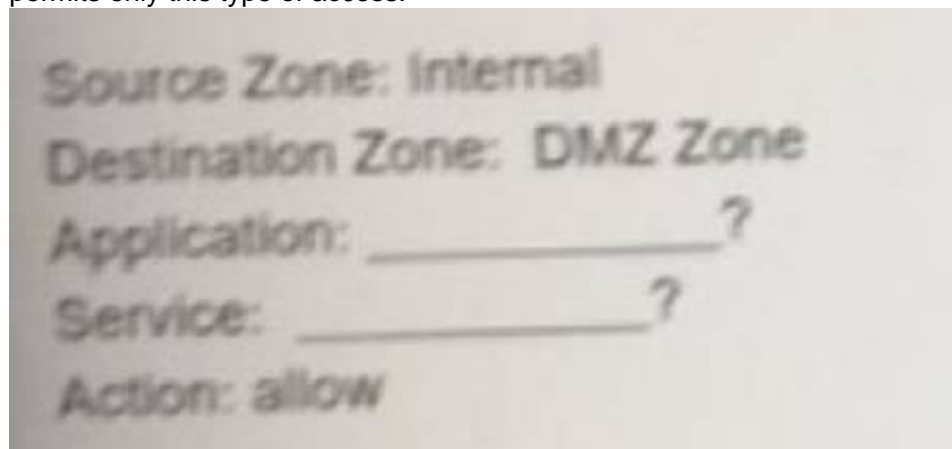
#### Explanation:

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication.html>

The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

#### NEW QUESTION 10

All users from the internal zone must be allowed only Telnet access to a server in the DMZ zone. Complete the two empty fields in the Security Policy rules that permits only this type of access.



Choose two.

A.

Service = "any"

B. Application = "Telnet"

C. Service = "application-default"

D. Application = "any"

**Answer:** BC

#### NEW QUESTION 11

What is an advantage for using application tags?

- A. They are helpful during the creation of new zones
- B. They help with the design of IP address allocations in DHCP.
- C. They help content updates automate policy updates
- D. They help with the creation of interfaces

**Answer:** C

**NEW QUESTION 16**

How are Application Fillers or Application Groups used in firewall policy?

- A. An Application Filter is a static way of grouping applications and can be configured as a

- nested member of an Application Group
- B. An Application Filter is a dynamic way to group applications and can be configured as a nested member of an Application Group
- C. An Application Group is a dynamic way of grouping applications and can be configured as a nested member of an Application Group
- D. An Application Group is a static way of grouping applications and cannot be configured as a nested member of Application Group

**Answer:** B

**NEW QUESTION 17**

Which dynamic update type includes updated anti-spyware signatures?

- A. Applications and Threats
- B. GlobalProtect Data File
- C. Antivirus
- D. PAN-DB

**Answer:** A

**NEW QUESTION 18**

Given the detailed log information above, what was the result of the firewall traffic inspection?

Device SN 007251000516345	Interface ethernet1/4	NAT IP 8.8.4.4
IP Protocol udp	NAT IP 67.190.64.58	NAT Port 53
Log Action global-logs	NAT Port 26351	
Generated Time 2021/08/27 02:02:49	X-Forwarded-For IP 0.0.0.0	
Receive Time 2021/08/27 02:02:53		
Tunnel Type Null		
	Details	Flags
	Threat Type spyware	Captive Portal <input type="checkbox"/>
	Threat ID/Name Phishing:151.116.74.in-addr.arpa	Proxy Transaction <input type="checkbox"/>
	ID 109010001 (View in Threat Vault)	Decrypted <input type="checkbox"/>
	Category dns-phishing	Packet Capture <input type="checkbox"/>
	Content Version AppThreat-0-0	Client to Server <input checked="" type="checkbox"/>
	Severity low	Server to Client <input type="checkbox"/>
	Repeat Count 2	Tunnel Inspected <input type="checkbox"/>
	File Name	
	URL 151.116.74.in-addr.arpa	DeviceID
	Partial Hash 0	Source Device Category Virtual Machine
	Prap ID 0	Source Device Profile VMware
	Source UUID	Source Device Model
	Destination UUID	Source Device Vendor VMware, Inc.
	Dynamic User Group	Source Device OS Family
	Network Slice ID SST 0	Source Device OS Version
	Network Slice ID SD	Source Device Host ubuntu-server
	App Category networking	Source Device MAC 00:50:56:a2:19:a3
	App Subcategory infrastructure	Destination Device Category
	App Technology network-protocol	Destination Device Profile
	App Characteristic used by malware/has known vulnerability/pervasive use	Destination Device Model
	App Container	
	App Risk 3	

- A. It was blocked by the Vulnerability Protection profile action.
- B. It was blocked by the Anti-Virus Security profile action.
- C. It was blocked by the Anti-Spyware Profile action.
- D. It was blocked by the Security policy action.

Answer: C

#### NEW QUESTION 23

By default, which action is assigned to the interzone-default rule?

- A. Reset-client
- B. Reset-server
- C. Deny
- D. Allow

Answer: C

#### NEW QUESTION 24

Which solution is a viable option to capture user identification when Active Directory is not in use?

- A. Cloud Identity Engine
- B. group mapping
- C. Directory Sync Service
- D. Authentication Portal

Answer: D

#### NEW QUESTION 25

Which type security policy rule would match traffic flowing between the inside zone and outside zone within the inside zone and within the outside zone?

- A. global
- B. universal
- C. intrazone
- D. interzone

Answer: B

#### NEW QUESTION 29

Which file is used to save the running configuration with a Palo Alto Networks firewall?

- A. running-config.xml
- B. run-config.xml
- C. running-configuration.xml
- D. run-configuratin.xml



**Answer:** A

#### NEW QUESTION 32

A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago. Which utility should the company use to identify out-of-date or unused rules on the firewall?

- A. Rule Usage Filter > No App Specified
- B. Rule Usage Filter >Hit Count > Unused in 30 days
- C. Rule Usage Filter > Unused Apps
- D. Rule Usage Filter > Hit Count > Unused in 90 days

**Answer:** D

#### NEW QUESTION 37

Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

- A. Mastered
- B. Not Mastered

**Answer:** A

#### NEW QUESTION 42

What does an administrator use to validate whether a session is matching an expected NAT policy?

- A. system log
- B. test command
- C. threat log
- D. config audit

**Answer:** B

#### Explanation:

Reference:<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0CIQSCA0>

#### NEW QUESTION 44

What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?

- A. every 30 minutes
- B. every 5 minutes
- C. once every 24 hours
- D. every 1 minute

**Answer:** D

#### NEW QUESTION 49

You receive notification about new malware that infects hosts through malicious files transferred by FTP.

Which Security profile detects and protects your internal networks from this threat after you update your firewall's threat signature database?

- A. URL Filtering profile applied to inbound Security policy rules.
- B. Data Filtering profile applied to outbound Security policy rules.
- C. Antivirus profile applied to inbound Security policy rules.
- D. Vulnerability Protection profile applied to outbound Security policy rules.

**Answer:** C

#### Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles>

#### NEW QUESTION 53

Identify the correct order to configure the PAN-OS integrated USER-ID agent.

- \* 3. add the service account to monitor the server(s)
- \* 2. define the address of the servers to be monitored on the firewall
- \* 4. commit the configuration, and verify agent connection status
- \* 1. create a service account on the Domain Controller with sufficient permissions to execute the User- ID agent

- A. 2-3-4-1
- B. 1-4-3-2
- C. 3-1-2-4
- D. 1-3-2-4

**Answer:** D

NEW QUESTION 54

Which interface does not require a MAC or IP address?

- A. Virtual Wire
- B. Layer3
- C. Layer2
- D. Loopback

Answer: A

NEW QUESTION 58

A server-admin in the USERS-zone requires SSH-access to all possible servers in all current and future Public Cloud environments. All other required connections have already been enabled between the USERS- and the OUTSIDE-zone. What configuration-changes should the Firewall-admin make?

- A. Create a custom-service-object called SERVICE-SSH for destination-port-TCP-22. Create a security-rule between zone USERS and OUTSIDE to allow traffic from any source IP-address to any destination IP-address for SERVICE-SSH
- B. Create a security-rule that allows traffic from zone USERS to OUTSIDE to allow traffic from any source IP-address to any destination IP-address for application SSH
- C. In addition to option a, a custom-service-object called SERVICE-SSH-RETURN that contains source-port-TCP-22 should be create
- D. A second security-rule is required that allows traffic from zone OUTSIDE to USERS for SERVICE-SSH-RETURN for any source- IP-address to any destination- Ip-address
- E. In addition to option c, an additional rule from zone OUTSIDE to USERS for application SSH from any source-IP-address to any destination-IP-address is required to allow the return-traffic from the SSH-servers to reach the server-admin

Answer: B

NEW QUESTION 59

Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?

- A. Management
- B. High Availability
- C. Aggregate
- D. Aggregation

Answer: C

NEW QUESTION 60

An administrator has configured a Security policy where the matching condition includes a single application and the action is deny  
If the application s default deny action is reset-both what action does the firewall take\*?

- A. It sends a TCP reset to the client-side and server-side devices
- B. It silently drops the traffic and sends an ICMP unreachable code
- C. It silently drops the traffic
- D. It sends a TCP reset to the server-side device

Answer: A

NEW QUESTION 61

An internal host wants to connect to servers of the internet through using source NAT. Which policy is required to enable source NAT on the firewall?

- A. NAT policy with source zone and destination zone specified
- B. post-NAT policy with external source and any destination address
- C. NAT policy with no source of destination zone selected
- D. pre-NAT policy with external source and any destination address

Answer: A

NEW QUESTION 62

DRAG DROP

Place the steps in the correct packet-processing order of operations.

Operational Task	Answer Area
Security profile enforcement	first
decryption	second
zone protection	third
App-ID	fourth

A. Mastered



B. Not Mastered

**Answer:** A

**Explanation:**

#### NEW QUESTION 64

Which statements is true regarding a Heatmap report?

- A. When guided by authorized sales engineer, it helps determine the areas of greatest security risk.
- B. It provides a percentage of adoption for each assessment area.
- C. It runs only on firewall.

D. It provides a set of questionnaires that help uncover security risk prevention gaps across architecture.

all areas of network and security

**Answer:** B

**Explanation:**

Reference: <https://live.paloaltonetworks.com/t5/best-practice-assessment-blogs/the-best-practice-assessment-bpa-tool-for-ngfw-and-panorama/ba-p/248343>

#### NEW QUESTION 69

During the packet flow process, which two processes are performed in application identification? (Choose two.)

- A. pattern based application identification
- B. application override policy match
- C. session application identified
- D. application changed from content inspection

**Answer:** AB

**Explanation:**

Reference: <http://live.paloaltonetworks.com/t5/image/serverpage/image-id/12862i950F549C7D4E6309>

#### NEW QUESTION 71

Which Security profile can you apply to protect against malware such as worms and Trojans?

- A. data filtering
- B. antivirus
- C. vulnerability protection
- D. anti-spyware

**Answer:** B

**Explanation:**

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles#:~:text=Antivirus%20profiles%20protect%20against%20viruses,as%20well%20as%20spyware%20downloads>

#### NEW QUESTION 75

What do dynamic user groups you to do?

- A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity
- B. create a policy that provides auto-sizing for anomalous user behavior and malicious activity
- C. create a policy that provides auto-remediation for anomalous user behavior and malicious activity
- D. create a dynamic list of firewall administrators

**Answer:** C

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:text=Dynamic%20user%20groups%20help%20you,activity%20while%20maintaining%20user%20visibility.>

#### NEW QUESTION 77

The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop. Which security profile feature could have been used to prevent the communication with the CnC server?

- A. Create an anti-spyware profile and enable DNS Sinkhole
- B. Create an antivirus profile and enable DNS Sinkhole
- C. Create a URL filtering profile and block the DNS Sinkhole category
- D. Create a security policy and enable DNS Sinkhole

**Answer:** A

**Explanation:**

### NEW QUESTION 82

What is the correct process for creating a custom URL category?

- A. Objects > Security Profiles > URL Category > Add
- B. Objects > Custom Objects > URL Filtering > Add
- C. Objects > Security Profiles > URL Filtering > Add
- D. Objects > Custom Objects > URL Category > Add

**Answer: D**

**Explanation:**

### NEW QUESTION 85

Given the detailed log information above, what was the result of the firewall traffic inspection?

Detailed Log View		
General	Source	Destination
Session ID 781868	Source User	Destination User
Action drop	Source 192.168.101.25	Destination 8.8.4.4
Host ID	Source DAG	Destination DAG
Application dns	Country 192.168.0.0-192.168.255.255	Country United States
Rule Outbound DNS	Port 46282	Port 53
Rule UUID ea9f3b96-e280-467c-aca5-0b1902857791	Zone Servers	Zone Internet
Device SN 007251000156341	Interface ethernet1/4	Interface ethernet1/8
IP Protocol udp	NAT IP 67.190.64.58	NAT IP 8.8.4.4
Log Action global-logs	NAT Port 26351	NAT Port 53
Generated Time 2021/08/27 02:02:49	X-Forwarded-For IP 0.0.0.0	
Receive Time 2021/08/27 02:02:53		
Tunnel Type N/A		
	Details	Flags
		Captive Portal <input type="checkbox"/>

- A. It was blocked by the Anti-Virus Security profile action.
- B. It was blocked by the Anti-Spyware Profile action.
- C. It was blocked by the Vulnerability Protection profile action.
- D. It was blocked by the Security policy action.

**Answer: B**

### NEW QUESTION 87

During the App-ID update process, what should you click on to confirm whether an existing policy rule is affected by an App-ID update?

- A. check now
- B. review policies
- C. test policy match
- D. download

**Answer: B**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/review-new-app-id-impact-on-existing-policy-rules>

### NEW QUESTION 92

What are three valid information sources that can be used when tagging users to dynamic user groups? (Choose three.)

- A. Biometric scanning results from iOS devices
- B. Firewall logs
- C. Custom API scripts
- D. Security Information and Event Management Systems (SIEMS), such as Splunk
- E. DNS Security service

**Answer: BCE**

### NEW QUESTION 95

Which three configuration settings are required on a Palo Alto networks firewall management interface?

- A. default gateway
- B. netmask
- C. IP address
- D. hostname
- E. auto-negotiation

**Answer: ABC**

**Explanation:**

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIN7CAK>

#### NEW QUESTION 99

Which two DNS policy actions in the anti-spyware security profile can prevent hacking attacks through DNS queries to malicious domains? (Choose two.)

- A. Deny
- B. Sinkhole
- C. Override
- D. Block

**Answer:** BD

#### Explanation:

? A DNS policy action is a setting in an Anti-Spyware security profile that defines

how the firewall handles DNS queries to malicious domains. A malicious domain is a domain name that is associated with a known threat, such as malware, phishing, or botnet1.

? There are four possible DNS policy actions: alert, allow, block, and sinkhole1.

? The alert action logs the DNS query and allows it to proceed to the intended destination. This action does not prevent hacking attacks, but only notifies the administrator of the potential threat1.

? The allow action allows the DNS query to proceed to the intended destination without logging it. This action does not prevent hacking attacks, but only bypasses the DNS security inspection2.

? The block action blocks the DNS query and sends a response to the client with an NXDOMAIN (non-existent domain) error code. This action prevents hacking attacks by preventing the client from resolving the malicious domain1.

? The sinkhole action redirects the DNS query to a predefined IP address (the sinkhole IP address) that is under the control of the administrator. This action prevents hacking attacks by isolating the client from the malicious domain and allowing the administrator to monitor and remediate the infected host1.

? The override action is not a valid DNS policy action, but a setting in an Anti- Spyware security profile that allows the administrator to create exceptions for specific spyware signatures that they want to override the default action or log settings3.

Therefore, the two DNS policy actions that can prevent hacking attacks through DNS queries to malicious domains are block and sinkhole.

References:

1: Enable DNS Security - Palo Alto Networks 2: How To Disable the DNS Security Feature from an Anti-Spyware Profile - Palo Alto Networks 3: Security Profile: Anti-Spyware - Palo Alto Networks

#### NEW QUESTION 103

Which Security profile must be added to Security policies to enable DNS Signatures to be checked?

- A. Anti-Spyware
- B. Antivirus
- C. Vulnerability Protection
- D. URL Filtering

**Answer:** D

#### NEW QUESTION 104

Which type of administrator account cannot be used to authenticate user traffic flowing through the firewall's data plane?

- A. Kerberos user
- B. SAML user
- C. local database user
- D. local user

**Answer:** B

#### NEW QUESTION 105

Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?

- A. GlobalProtect
- B. AutoFocus
- C. Aperture
- D. Panorama

**Answer:** A

#### Explanation:

GlobalProtect: GlobalProtect safeguards your mobile workforce by inspecting all traffic using your next-generation firewalls deployed as internet gateways, whether at the perimeter, in the Demilitarized Zone (DMZ), or in the cloud.

#### NEW QUESTION 110

Which link in the web interface enables a security administrator to view the security policy rules that match new application signatures?

- A. Review Apps
- B. Review App Matches
- C. Pre-analyze
- D. Review Policies

**Answer:** D

**Explanation:**

#### NEW QUESTION 111

By default, what is the maximum number of templates that can be added to a template stack?

- A. 6
- B. 8
- C. 10
- D. 12

**Answer: B**

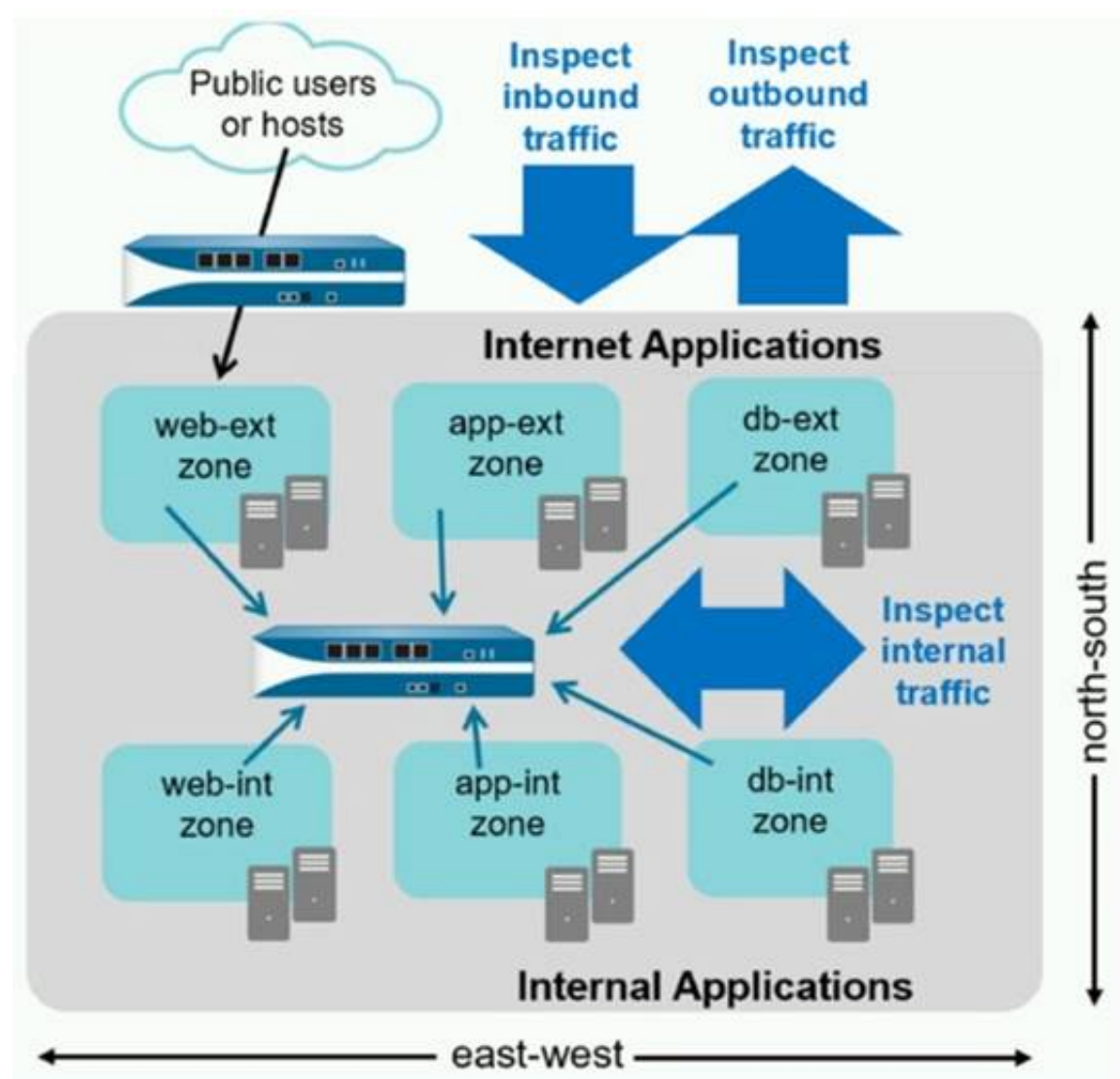
**Explanation:**

By default, the maximum number of templates that can be added to a template stack is 8. This is the recommended limit for performance reasons, as adding more templates may result in sluggish responses on the user interface. However, starting from PAN-OS 8.1.10 and 9.0.4, you can use a debug command to increase the maximum number of templates per stack to 16. This command requires a commit operation to take effect.

A template stack is a collection of templates that you can use to push common settings to multiple firewalls or Panorama managed collectors. A template contains the network and device settings that you want to share across devices, such as interfaces, zones, virtual routers, DNS, NTP, and login banners. You can create multiple templates for different device groups or locations and add them to a template stack in a hierarchical order. The settings in the lower templates override the settings in the higher templates if there are any conflicts. You can then assign a template stack to one or more devices and push the configuration changes.

#### NEW QUESTION 114

An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



- A. branch office traffic
- B. north-south traffic
- C. perimeter traffic
- D. east-west traffic

**Answer: D**

#### NEW QUESTION 119

How are service routes used in PAN-OS?

- A. By the OSPF protocol, as part of Dijkstra's algorithm, to give access to the various services offered in the network
- B. To statically route subnets so they are joinable from, and have access to, the Palo Alto Networks external services
- C. For routing, because they are the shortest path selected by the BGP routing protocol
- D. To route management plane services through data interfaces rather than the management interface

**Answer: D**

**Explanation:**

? Service routes are a feature of PAN-OS that allows the administrator to customize the interface that the firewall uses to send requests to external services, such



as DNS, email, Palo Alto Networks updates, User-ID agent, syslog, Panorama, dynamic updates, URL updates, licenses, and AutoFocus1.

? By default, the firewall uses the management interface for all service routes, unless the packet destination IP address matches the configured destination service route, in which case the source IP address is set to the source address configured for the destination1.

? However, in some scenarios, the administrator may want to use a different interface for service routes, such as when the management interface does not have public internet access, or when the administrator wants to isolate or monitor the traffic for certain services23.

? To configure service routes, the administrator can select Device > Setup > Services > Service Route Configuration and customize each service with a source interface and a source address. The administrator can also configure destination service routes to specify a destination IP address and a gateway for each service1.

? Service routes are not related to routing protocols such as OSPF or BGP, which are used to exchange routing information between routers and determine the best path to reach a network destination. Service routes are only used to change the interface that the firewall uses to communicate with external services. Therefore, service routes are used to route management plane services through data interfaces rather than the management interface.

References:

1: Configure Service Routes - Palo Alto Networks 2: Setting a Service Route for Services to Use a Dataplane's Interface - Palo Alto Networks 3: How to Perform Updates when Management Interface does not have Public Internet Access - Palo Alto Networks

NEW QUESTION 122

DRAG DROP

Match each rule type with its example

Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

Create a policy with source zones A and B and destination zone A and B. The rule should apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A.

Create a policy with source zones A and B and destination zone A and B. The rule would apply to traffic from zone A to zone B, from zone B to zone A, but not traffic within zones A or B.

Answer Area

Universal

Intrazone

Interzone

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

Create a policy with source zones A and B and destination zone A and B. The rule should apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A.

Create a policy with source zones A and B and destination zone A and B. The rule would apply to traffic from zone A to zone B, from zone B to zone A, but not traffic within zones A or B.

Answer Area

Create a policy with source zones A and B and destination zone A and B. The rule would apply to traffic from zone A to zone B, from zone B to zone A, but not traffic within zones A or B.

Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

Create a policy with source zones A and B and destination zone A and B. The rule should apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A.

Universal

Intrazone

Interzone

NEW QUESTION 124

Which User-ID agent would be appropriate in a network with multiple WAN links, limited network bandwidth, and limited firewall management plane resources?

- A. Windows-based agent deployed on the internal network
- B. PAN-OS integrated agent deployed on the internal network
- C. Citrix terminal server deployed on the internal network
- D. Windows-based agent deployed on each of the WAN Links

Answer: A

Explanation:

Another reason to choose the Windows agent over the integrated PAN-OS agent is to save processing cycles on the firewall's management plane.

NEW QUESTION 129

Given the image, which two options are true about the Security policy rules. (Choose two.)

	Name	Tags	Type	Source			Destination			Match Usage			Application	Service	Action	Profile
				Zone	Address	User	Zone	Address	HIP Profile	Hit Count	Last Hit	First Hit				
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser...	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin...	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

- A. The Allow Office Programs rule is using an Application Filter
- B. In the Allow FTP to web server rule, FTP is allowed using App-ID
- C. The Allow Office Programs rule is using an Application Group

D. In the Allow Social Networking rule, allows all of Facebook's functions

**Answer:** AD

**Explanation:**

In the Allow FTP to web server rule, FTP is allowed using port based rule and not APP-ID.

**NEW QUESTION 130**

After making multiple changes to the candidate configuration of a firewall, the administrator would like to start over with a candidate configuration that matches the running configuration.

Which command in Device > Setup > Operations would provide the most operationally efficient way to accomplish this?

- A. Import named config snapshot
- B. Load named configuration snapshot
- C. Revert to running configuration
- D. Revert to last saved configuration

**Answer:** C

**NEW QUESTION 132**

What is the purpose of the automated commit recovery feature?

- A. It reverts the Panorama configuration.
- B. It causes HA synchronization to occur automatically between the HA peers after a push from Panorama.
- C. It reverts the firewall configuration if the firewall recognizes a loss of connectivity to Panorama after the change.
- D. It generates a config log after the Panorama configuration successfully reverts to the last running configuration.

**Answer:** C

**Explanation:**

Reference:<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer-panorama/enable-automated-commit-recovery.html>

**NEW QUESTION 135**

Which administrative management services can be configured to access a management interface?

- A. HTTP, CLI, SNMP, HTTPS
- B. HTTPS, SSH telnet SNMP
- C. SSH: telnet HTTP, HTTPS
- D. HTTPS, HTTP
- E. CLI, API

**Answer:** D

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfaces>

You can use the following user interfaces to manage the Palo Alto Networks firewall:

? Use the Web Interface to perform configuration and monitoring tasks with relative ease. This graphical interface allows you to access the firewall using HTTPS (recommended) or HTTP and it is the best way to perform administrative tasks.

? Use the Command Line Interface (CLI) to perform a series of tasks by entering commands in rapid succession over SSH (recommended), Telnet, or the console port. The CLI is a no-frills interface that supports two command modes, operational and configure, each with a distinct hierarchy of commands and statements. When you become familiar with the nesting structure and syntax of the commands, the CLI provides quick response times and administrative efficiency.

? Use the XML API to streamline your operations and integrate with existing, internally developed applications and repositories. The XML API is a web service implemented using HTTP/HTTPS requests and responses.

? Use Panorama to perform web-based management, reporting, and log collection for multiple firewalls. The Panorama web interface resembles the firewall web interface but with additional functions for centralized management.

**NEW QUESTION 138**

An administrator has an IP address range in the external dynamic list and wants to create an exception for one specific IP address in this address range. Which steps should the administrator take?

- A. Add the address range to the Manual Exceptions list and exclude the IP address by selecting the entry.
- B. Add each IP address in the range as a list entry and then exclude the IP address by adding it to the Manual Exceptions list.
- C. Select the address range in the List Entries list.
- D. A column will open with the IP addresses
- E. Select the entry to exclude.
- F. Add the specific IP address from the address range to the Manual Exceptions list by using regular expressions to define the entry.

**Answer:** D

**NEW QUESTION 141**

An administrator would like to protect against inbound threats such as buffer overflows and illegal code execution. Which Security profile should be used?

- A. Antivirus
- B. URL filtering
- C. Anti-spyware
- D. Vulnerability protection



**Answer:** C

#### NEW QUESTION 142

Choose the option that correctly completes this statement. A Security Profile can block or allow traffic .

- A. on either the data plane or the management plane.
- B. after it is matched by a security policy rule that allows traffic.
- C. before it is matched to a Security policy rule.
- D. after it is matched by a security policy rule that allows or blocks traffic.

**Answer:** B

#### Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html>

After a packet has been allowed by the Security policy, Security Profiles are used to scan packets for threats, vulnerabilities, viruses, spyware, malicious URLs, data exfiltration, and exploitation software.

#### NEW QUESTION 145

Why should a company have a File Blocking profile that is attached to a Security policy?

- A. To block uploading and downloading of specific types of files
- B. To detonate files in a sandbox environment
- C. To analyze file types
- D. To block uploading and downloading of any type of files

**Answer:** A

#### NEW QUESTION 149

Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP –to-user mappings as soon as possible with minimal downtime and minimal configuration changes to the wireless devices themselves. The wireless devices are from various manufactures.

Given the scenario, choose the option for sending IP-to-user mappings to the NGFW.

- A. syslog
- B. RADIUS
- C. UID redistribution
- D. XFF headers

**Answer:** A

#### NEW QUESTION 154

Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?

- A. SAML
- B. Multi-Factor Authentication
- C. Role-based
- D. Dynamic

**Answer:** C

#### Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types.html>

#### NEW QUESTION 155

A Security Profile can block or allow traffic at which point?

- A. after it is matched to a Security policy rule that allows traffic
- B. on either the data plane or the management plane
- C. after it is matched to a Security policy rule that allows or blocks traffic
- D. before it is matched to a Security policy rule

**Answer:** A

#### NEW QUESTION 160

When is the content inspection performed in the packet flow process?

- A. after the application has been identified
- B. after the SSL Proxy re-encrypts the packet
- C. before the packet forwarding process
- D. before session lookup

**Answer:** A

**Explanation:**

Reference:<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0CIVHCA0>

**NEW QUESTION 161**

A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT. Finance, and HR. Which two types of traffic will the rule apply to? (Choose two)

- A. Mastered
- B. Not Mastered

**Answer: A**

**NEW QUESTION 165**

URL categories can be used as match criteria on which two policy types? (Choose two.)

- A. authentication
- B. decryptionC application override
- C. NAT

**Answer: AB**

**Explanation:**

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-category-as-policy-match-criteria.html>

**NEW QUESTION 169**

Which component is a building block in a Security policy rule?

- A. decryption profile
- B. destination interface
- C. timeout (min)
- D. application

**Answer: D**

**Explanation:**

Reference:  
<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security/buildingblocks-in-a-security-policy-rule.html>

**NEW QUESTION 171**

Which two firewall components enable you to configure SYN flood protection thresholds? (Choose two.)

- A. QoS profile
- B. DoS Protection profile
- C. Zone Protection profile
- D. DoS Protection policy

**Answer: BC**

**Explanation:**

Reference:  
<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles>

**NEW QUESTION 175**

Which firewall feature do you need to configure to query Palo Alto Networks service updates over a data-plane interface instead of the management interface?

- A. Data redistribution
- B. Dynamic updates
- C. SNMP setup
- D. Service route

**Answer: D**

**NEW QUESTION 178**

The compliance officer requests that all evasive applications need to be blocked on all perimeter firewalls out to the internet The firewall is configured with two zones;

- \* 1. trust for internal networks
- \* 2. untrust to the internet

Based on the capabilities of the Palo Alto Networks NGFW, what are two ways to configure a security policy using App-ID to comply with this request? (Choose two )

- A. Create a deny rule at the top of the policy from trust to untrust with service application- default and add an application filter with the evasive characteristic
- B. Create a deny rule at the top of the policy from trust to untrust over any service and select evasive as the application

- C. Create a deny rule at the top of the policy from trust to untrust with service application- default and select evasive as the application  
D. Create a deny rule at the top of the policy from trust to untrust over any service and add an application filter with the evasive characteristic

**Answer:** AD

#### NEW QUESTION 180

What are the two default behaviors for the intrazone-default policy? (Choose two.)

- A. Allow  
B. Logging disabled  
C. Log at Session End  
D. Deny

**Answer:** AB

#### NEW QUESTION 184

DRAG DROP

Match the Palo Alto Networks Security Operating Platform architecture to its description.

Threat Intelligence Cloud	Drag answer here	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Drag answer here	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Drag answer here	Inspects processes and files to prevent known and unknown exploits.

- A. Mastered  
B. Not Mastered

**Answer:** A

#### Explanation:

Threat Intelligence Cloud – Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.

Next-Generation Firewall – Identifies and inspects all traffic to block known threats  
Advanced Endpoint Protection - Inspects processes and files to prevent known and unknown exploits

#### NEW QUESTION 185

Access to which feature requires PAN-OS Filtering licenss?

- A. PAN-DB database  
B. URL external dynamic lists  
C. Custom URL categories  
D. DNS Security

**Answer:** A

#### Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/activate-licenses-and-subscriptions.html>

#### NEW QUESTION 186

Starting with PAN\_OS version 9.1 which new type of object is supported for use within the user field of a security policy rule?

- A. local username  
B. dynamic user group  
C. remote username  
D. static user group

**Answer:** B

#### NEW QUESTION 188

An administrator is updating Security policy to align with best practices. Which Policy Optimizer feature is shown in the screenshot below?

	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	App Usage				MODIFIED	CREATED
				APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE		
55	Unexpected Traffic	application-default	1.7T	any	142	258	Compare	2022-01-06 18:30:02	2020-11-16
25	Outbound Trust2	application-default	6.5G	any	26	447	Compare	2022-01-06 18:30:02	2020-11-16
29	CorObj6003	application-default	912.3M	any	1	448	Compare	2022-01-06 18:30:02	2020-11-16
20	2019-08-13c380t E...	application-default	508.0M	any	18	448	Compare	2022-01-06 18:30:02	2020-11-16
31	CorObj-wf2	application-default	235.1M	any	1	448	Compare	2022-01-06 18:30:02	2020-11-16
32	GRE-EndPoint	application-default	140.8M	any	1	448	Compare	2022-01-06 18:30:02	2020-11-16
47	Workstation-appdet...	any	23.1M	any	5	448	Compare	2022-01-06 18:30:02	2020-11-16
27	CorObj6006	application-default	22.8M	any	2	448	Compare	2022-01-06 18:30:02	2020-11-16
30	CorObj-WC	application-default	1.2M	any	1	446	Compare	2022-01-06 18:30:02	2020-11-16
28	CorObj6004	application-default	590.2k	any	1	445	Compare	2022-01-06 18:30:02	2020-11-16
17	LogSinkholeTraffic	application-default	0	any	2	432	Compare	2022-01-06 18:30:02	2020-11-16
24	Outbound Trust	application-default	0	any	1	419	Compare	2022-01-06 18:30:02	2020-11-16

- A. Rules without App Controls
- B. New App Viewer
- C. Rule Usage
- D. Unused Unused Apps

Answer: C

#### NEW QUESTION 190

Which URL profiling action does not generate a log entry when a user attempts to access that URL?

- A. Override
- B. Allow
- C. Block
- D. Continue

Answer: B

#### NEW QUESTION 194

Which administrator type utilizes predefined roles for a local administrator account?

- A. Superuser
- B. Role-based
- C. Dynamic
- D. Device administrator

Answer: C

#### NEW QUESTION 197

An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration. Why doesn't the administrator see the traffic?

- A. Logging on the interzone-default policy is disabled.
- B. Traffic is being denied on the interzone-default policy.
- C. The Log Forwarding profile is not configured on the policy.
- D. The interzone-default policy is disabled by default.

Answer: A

#### NEW QUESTION 200

Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping. What is the quickest way to reset the hit counter to zero in all the security policy rules?

- A. At the CLI enter the command reset rules and press Enter
- B. Highlight a rule and use the Reset Rule Hit Counter > Selected Rules for each rule
- C. Reboot the firewall
- D. Use the Reset Rule Hit Counter > All Rules option

Answer: D

#### NEW QUESTION 202

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCNSA Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PCNSA Product From:

<https://www.2passeasy.com/dumps/PCNSA/>

## Money Back Guarantee

### PCNSA Practice Exam Features:

- \* PCNSA Questions and Answers Updated Frequently
- \* PCNSA Practice Questions Verified by Expert Senior Certified Staff
- \* PCNSA Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* PCNSA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year