



# **Paloalto-Networks**

## **Exam Questions PCNSA**

Palo Alto Networks Certified Network Security Administrator

**NEW QUESTION 1**

Which operations are allowed when working with App-ID application tags?

- A. Predefined tags may be deleted.
- B. Predefined tags may be augmented by custom tags.
- C. Predefined tags may be modified.
- D. Predefined tags may be updated by WildFire dynamic updates.

**Answer:** B

**NEW QUESTION 2**

Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?

- A. URL traffic
- B. vulnerability protection
- C. anti-spyware
- D. antivirus

**Answer:** C

**Explanation:**

**NEW QUESTION 3**

DRAG DROP

Match the Cyber-Attack Lifecycle stage to its correct description.

Reconnaissance	Drag answer here	stage where the attacker has motivation for attacking a network to deface web property
Installation	Drag answer here	stage where the attacker scans for network vulnerabilities and services that can be exploited
Command and Control	Drag answer here	stage where the attacker will explore methods such as a root kit to establish persistence
Act on the Objective	Drag answer here	stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network

A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

Reconnaissance – stage where the attacker scans for network vulnerabilities and services that can be exploited.

Installation – stage where the attacker will explore methods such as a root kit to establish persistence

Command and Control – stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.

Act on the Objective – stage where an attacker has motivation for attacking a network to deface web property

**NEW QUESTION 4**

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. egress outside

C. inside-portal

D. intercone-default

**Answer:** B

**NEW QUESTION 5**

Which type of security policy rule will match traffic that flows between the Outside zone and inside zone, but would not match traffic that flows within the zones?

A. global

B. intrazone

C. interzone

D. universal

**Answer:** C

**Explanation:**

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic-contentupdates.html#:~:text=WildFire%20signature%20updates%20are%20made,within%20a%20minute%20of%20availability>

**NEW QUESTION 6**

Which action related to App-ID updates will enable a security administrator to view the existing security policy rule that matches new application signatures?

A. Review Policies

B. Review Apps

C. Pre-analyze

D. Review App Matches

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 7**

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 8**

Which two configuration settings shown are not the default? (Choose two.)

### Palo Alto Networks User-ID Agent Setup

Enable Security Log ✓  
Server Log Monitor Frequency (sec) **15**  
Enable Session ✓  
Server Session Read Frequency (sec) **10**  
Novell eDirectory Query Interval (sec) **30**  
Syslog Service Profile  
Enable Probing  
Probe Interval (min) **20**  
Enable User Identification Timeout ✓  
User Identification Timeout (min) **45**  
Allow matching usernames without domains  
Enable NTLM  
NTLM Domain  
User-ID Collector Name

- A. Enable Security Log
- B. Server Log Monitor Frequency (sec)
- C. Enable Session
- D. Enable Probing

**Answer:** BC

#### NEW QUESTION 9

An administrator configured a Security policy rule where the matching condition includes a single application and the action is set to deny. What deny action will the firewall perform?

- A. Drop the traffic silently
- B. Perform the default deny action as defined in the App-ID database for the application
- C. Send a TCP reset packet to the client- and server-side devices
- D.

Discard the session's packets and send a TCP reset packet to let the client know the session has been terminated

**Answer:** D

**NEW QUESTION 10**

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 10**

Which statement is true regarding NAT rules?

A. Static NAT rules have precedence over other forms of NAT.

B. Translation of the IP address and port occurs before security processing.

C. NAT rules are processed in order from top to bottom.

D. Firewall supports NAT on Layer 3 interfaces only.

**Answer:** C

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-policy-rules/nat-policy-overview>

**NEW QUESTION 12**

Which data flow direction is protected in a zero trust firewall deployment that is not protected in a perimeter-only firewall deployment?

A. outbound

B. north south

- C. inbound
- D. east west

**Answer:** D

**NEW QUESTION 16**

Which two settings allow you to restrict access to the management interface? (Choose two)

- A. Mastered
- B. Not Mastered

**Answer:** A

**NEW QUESTION 21**

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 24**

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

Device SN 007251000156341	Interface ethernet1/4	NAT IP 8.8.4.4
IP Protocol udp	NAT IP 67.290.64.58	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-permission-viol	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 27

The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering “gambling” category. Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the “gambling” URL category?

- A. Add just the URL www.powerball.com to a Security policy allow rule.
- B.

Manually remove powerball.com from the gambling URL category.

- C. Add \*.powerball.com to the URL Filtering allow list.
- D. Create a custom URL category, add \*.powerball.com to it and allow it in the Security Profile.

Answer: CD

NEW QUESTION 31

At which point in the app-ID update process can you determine if an existing policy rule is affected by an app-ID update?

A.

after clicking Check New in the Dynamic Update window

- B. after connecting the firewall configuration
- C. after downloading the update
- D. after installing the update

**Answer:** A

**Explanation:**

Reference:<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-dynamicupdates>

**NEW QUESTION 35**

Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two.)

- A. GlobalProtect agent
- B. XML API
- C.

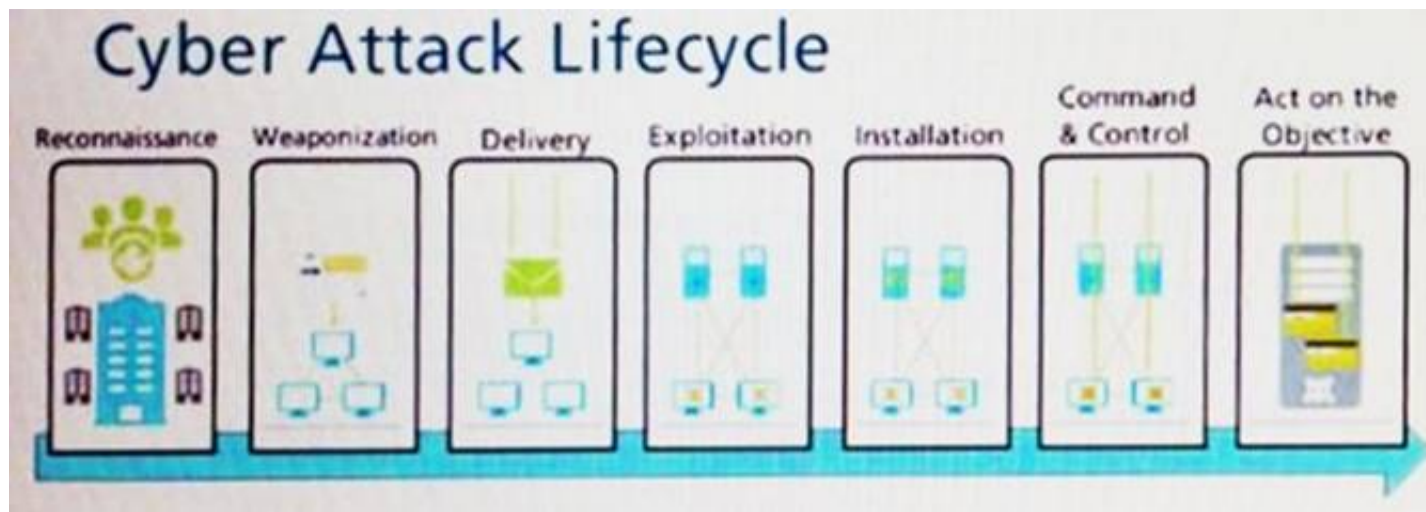
User-ID Windows-based agent

- D. log forwarding auto-tagging

**Answer:** BC

**NEW QUESTION 40**

Given the Cyber-Attack Lifecycle diagram, identify the stage in which the attacker can initiate malicious code against a targeted machine.



A.

Exploitation

- B. Installation
- C. Reconnaissance
- D. Act on Objective

**Answer:** A

#### NEW QUESTION 44

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 48

To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?

- A. Mastered
- B. Not Mastered

**Answer:** A

#### NEW QUESTION 50

Which statement is true about Panorama managed devices?

- A. Panorama automatically removes local configuration locks after a commit from Panorama
- B. Local configuration locks prohibit Security policy changes for a Panorama managed device
- C. Security policy rules configured on local firewalls always take precedence
- D. Local configuration locks can be manually unlocked from Panorama

**Answer:** D

#### Explanation:

Explanation Explanation/Reference: Reference:

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer-panorama/manage-locks-forrestricting-configuration-changes.html>

#### NEW QUESTION 51

What allows a security administrator to preview the Security policy rules that match new application signatures?

- A. Review Release Notes
- B. Dynamic Updates-Review Policies
- C. Dynamic Updates-Review App
- D. Policy Optimizer-New App Viewer

**Answer:** B

#### Explanation:

<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 52

Which option lists the attributes that are selectable when setting up an Application filters?

- A. Category, Subcategory, Technology, and Characteristic
- B. Category, Subcategory, Technology, Risk, and Characteristic
- C. Name, Category, Technology, Risk, and Characteristic
- D. Category, Subcategory, Risk, Standard Ports, and Technology

**Answer:** B

#### Explanation:

Explanation/Reference: Reference:  
<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-application-filters>

#### NEW QUESTION 53

Which three statement describe the operation of Security Policy rules or Security Profiles? (Choose three)

- ☐ A. Security policy rules inspect but do not block traffic.
- ☒ B. Security Profile should be used only on allowed traffic.
- ☒ C. Security Profile are attached to security policy rules.
- ☒ D. Security Policy rules are attached to Security Profiles.
- ☐ E. Security Policy rules can block or allow traffic.

**Answer:** BCE

#### NEW QUESTION 56

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=kA10g0000000CIQSCA0>

#### NEW QUESTION 59

Which three types of authentication services can be used to authenticate user traffic flowing through the firewalls data plane? (Choose three )

- A. TACACS
- B. SAML2
- C. SAML10
- D. Kerberos
- E. TACACS+

**Answer:** ABD

#### NEW QUESTION 61

Which interface does not require a MAC or IP address?

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

**Answer:** A

#### NEW QUESTION 63

What does an application filter help you to do?

- It dynamically provides application statistics based on network, threat, and blocked activity,
- A. It dynamically filters applications based on critical, high, medium, lo
  - C. or informational severity.
  - D. It dynamically groups applications based on application attributes such as category and subcategory.
  - E. It dynamically shapes defined application traffic based on active sessions and bandwidth usage.

**Answer:** C

#### NEW QUESTION 67

Which URL Filtering Profile action does not generate a log entry when a user attempts to access a URL?

- A. override
- B. allow
- C. block
- D. continue

**Answer:** B

#### NEW QUESTION 69

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 70

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 72

An administrator wants to prevent access to media content websites that are risky  
 Which two URL categories should be combined in a custom URL category to accomplish this goal? (Choose two)

- A. Mastered
- B. Not Mastered

**Answer:** A

#### NEW QUESTION 76

Based on the graphic which statement accurately describes the output shown in the server monitoring panel?



The screenshot displays the Palo Alto Networks User-ID Agent configuration and monitoring interface. The top section shows the configuration for the 'lab.local' domain with the 'lab-kerberos' profile. The bottom section shows the 'Server Monitoring' table with one entry: 'lab-client' (Microsoft Active Directory) at 'client-a.lab.local' with status 'Connected'.

Name	Enabled	Type	Network Address	Status
lab-client	<input checked="" type="checkbox"/>	Microsoft Active Directory	client-a.lab.local	Connected

- A. The User-ID agent is connected to a domain controller labeled lab-client.

- B. The host lab-client has been found by the User-ID agent.
- C. The host lab-client has been found by a domain controller.
- D. The User-ID agent is connected to the firewall labeled lab-client.

**Answer:** A

#### NEW QUESTION 80

Selecting the option to revert firewall changes will replace what settings?

- A. Mastered
- B. Not Mastered

**Answer:** A

#### NEW QUESTION 85

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 87

Based on the security policy rules shown, ssh will be allowed on which port?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

- A. 80
- B. 53
- C. 22
- D. 23

**Answer:** C

#### Explanation:

#### NEW QUESTION 91

Which interface type can use virtual routers and routing protocols?

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

**Answer:** B

#### NEW QUESTION 94

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 98

Which URL Filtering profile action would you set to allow users the option to access a site only if they provide a URL admin password?

- A. override
- B. authorization
- C. authentication
- D. continue

**Answer:** B

**Explanation:**

Reference:

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

#### NEW QUESTION 99

When creating a custom URL category object, which is a valid type?

- A. domain match
- B. host names
- C. wildcard
- D. category match

**Answer:** D

**Explanation:**

Reference:<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-custom-objects-url-category.html>

#### NEW QUESTION 104

Assume that traffic matches a Security policy rule but the attached Security Profiles is configured to block matching traffic. Which statement accurately describes how the firewall will apply an action to matching traffic?

- A. If it is an allowed rule, then the Security Profile action is applied last
- B. If it is a block rule then the Security policy rule action is applied last
- C. If it is an allow rule then the Security policy rule is applied last
- D. If it is a block rule then Security Profile action is applied last

**Answer:** A

#### NEW QUESTION 106

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 107

Complete the statement. A security profile can block or allow traffic

- A. on unknown-tcp or unknown-udp traffic
- B. after it is matched by a security policy that allows traffic
- C. before it is matched by a security policy
- D. after it is matched by a security policy that allows or blocks traffic

**Answer:** B

**Explanation:**

Security profiles are objects added to policy rules that are configured with an action of allow.

**NEW QUESTION 111**

Which protocol used to map username to user groups when user-ID is configured?

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

**Answer:** D

**NEW QUESTION 114**

Which action results in the firewall blocking network traffic without notifying the sender?

- ☒ A. Deny
- ☐ B: No notification
- ☐ C. Drop
- ☐ D. Reset Client

**Answer:** C

**NEW QUESTION 119**

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 121**

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

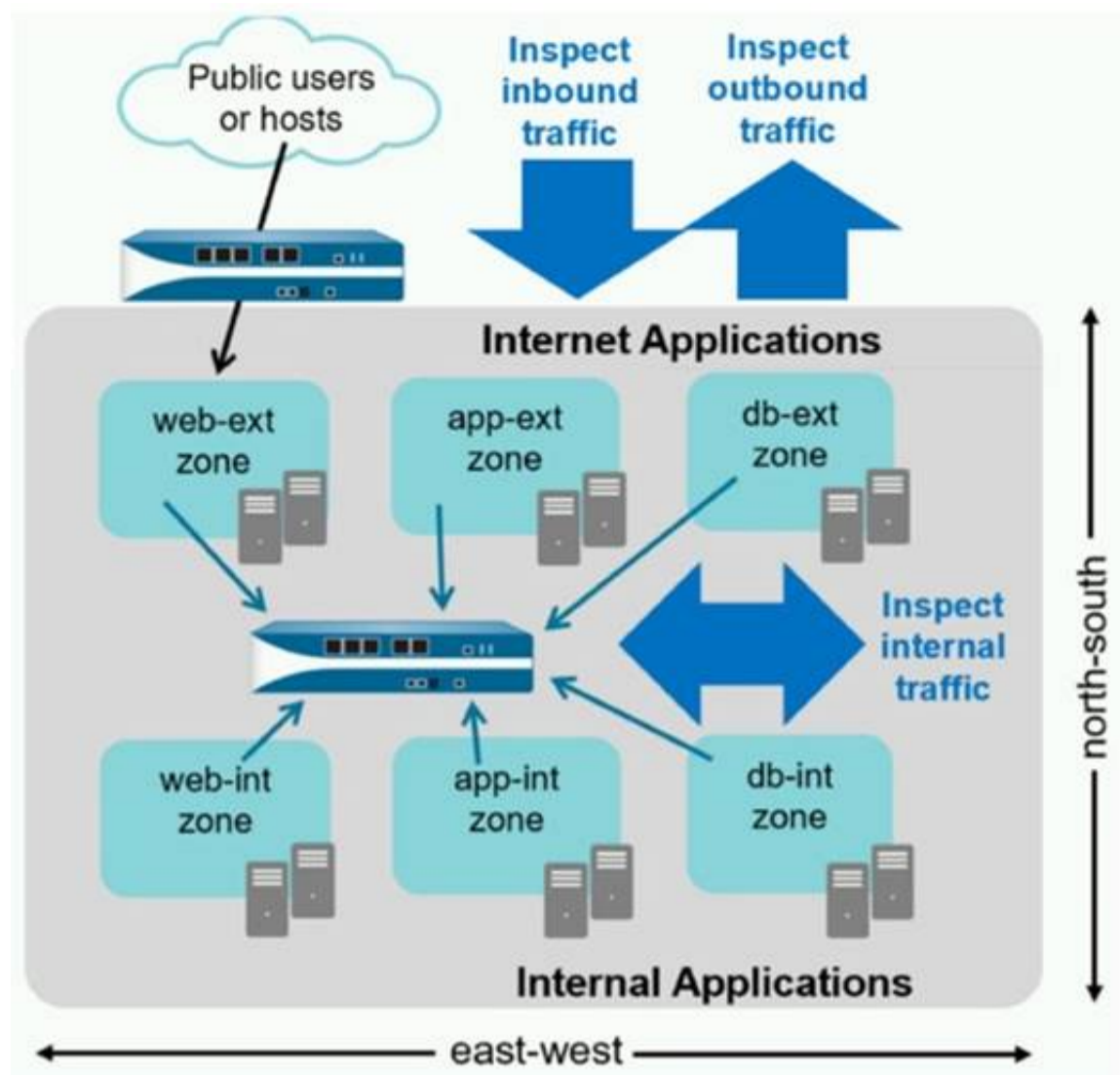
- A. Review Apps
- B. Review App Matches
- C. Pre-analyze
- D. Review Policies

**Answer:** D

**Explanation:**

**NEW QUESTION 125**

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 127

Within an Anti-Spyware security profile, which tab is used to enable machine learning based engines?

- A. Inline Cloud Analysis
- B. Signature Exceptions
- C. Machine Learning Policies
- D. Signature Policies

**Answer:** A

#### Explanation:

? An Anti-Spyware security profile is a set of rules that defines how the firewall detects and prevents spyware from compromising hosts on the network. Spyware is a type of malware that collects information from the infected system, such as keystrokes, browsing history, or personal data, and sends it to an external command-and-control (C2) server<sup>1</sup>.

? An Anti-Spyware security profile consists of four tabs: Signature Policies, Signature Exceptions, Machine Learning Policies, and Inline Cloud Analysis<sup>1</sup>.

? The Signature Policies tab allows you to configure the actions and log settings for each spyware signature category, such as adware, botnet, keylogger, phishing, or worm. You can also enable DNS Security to block malicious DNS queries and responses<sup>1</sup>.

? The Signature Exceptions tab allows you to create exceptions for specific spyware signatures that you want to override the default action or log settings. For example, you can allow a signature that is normally blocked by the profile, or block a signature that is normally alerted by the profile<sup>1</sup>.

? The Machine Learning Policies tab allows you to configure the actions and log settings for machine learning based signatures that detect unknown spyware variants. You can also enable WildFire Analysis to submit unknown files to the cloud for further analysis<sup>1</sup>.

? The Inline Cloud Analysis tab allows you to enable machine learning based engines that detect unknown spyware variants in real time. These engines use cloud-based models to analyze the behavior and characteristics of network traffic and identify malicious patterns. You can enable inline cloud analysis for HTTP/HTTPS traffic, SMTP/SMTPS traffic, or IMAP/IMAPS traffic<sup>1</sup>.

Therefore, the tab that is used to enable machine learning based engines is the Inline

Cloud Analysis tab. References:

1: Security Profile: Anti-Spyware - Palo Alto Networks

#### NEW QUESTION 130

An administrator would like to silently drop traffic from the internet to a ftp server. Which Security policy action should the administrator select?

- A. Reset-server
- B. Block
- C. Deny
- D. Drop

**Answer:** D

#### NEW QUESTION 132

Which firewall plane provides configuration, logging, and reporting functions on a separate processor?

- A. control
- B. network processing
- C. data
- D. security processing

**Answer:** A

#### NEW QUESTION 134

An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the Subcategory office-programs. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes you defined for the filter. <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-an-application-filter.html>

#### NEW QUESTION 137

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.

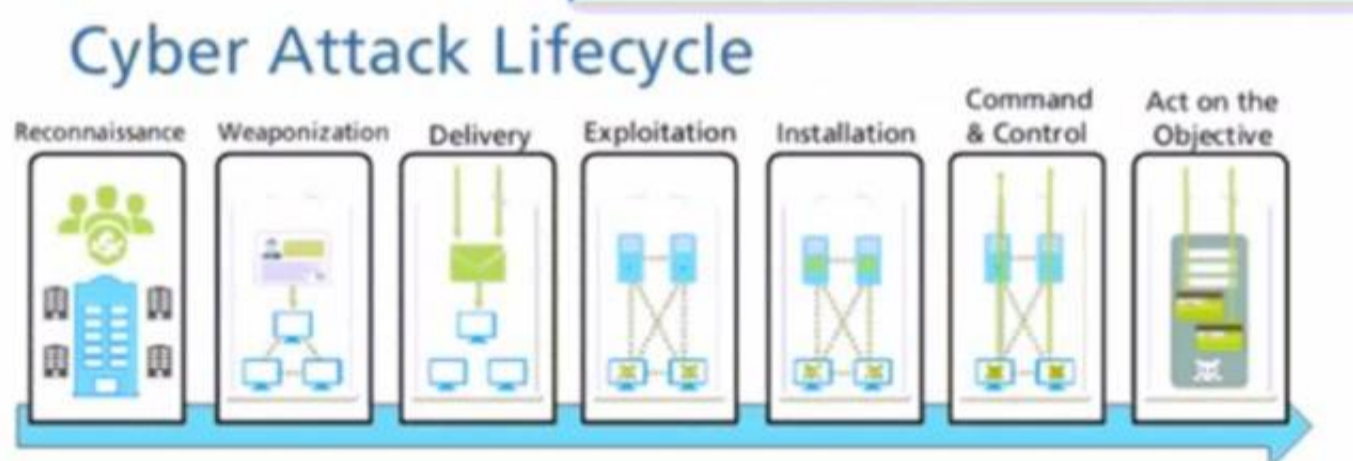
Which command in Device > Setup > Operations would provide the most operationally efficient way to accomplish this?

- 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 138

At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?



- A. delivery
- B. command and control
- C. exploitation
- D. reconnaissance
- E. installation

**Answer:** A

#### NEW QUESTION 140

What are three Palo Alto Networks best practices when implementing the DNS Security Service? (Choose three.)

- A. Implement a threat intel program.
- B. Configure a URL Filtering profile.
- C. Train your staff to be security aware.
- D. Rely on a DNS resolver.
- E. Plan for mobile-employee risk

**Answer:** ABD

#### NEW QUESTION 143

Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?

- A. Active Directory monitoring
- B. Windows session monitoring
- C. Windows client probing
- D. domain controller monitoring

**Answer:** A

#### NEW QUESTION 146

An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact a command-and-control (C2) server. Which two security profile components will detect and prevent this threat after the firewall's signature database has been updated? (Choose two.)

- A. vulnerability protection profile applied to outbound security policies
- B. anti-spyware profile applied to outbound security policies
- C. antivirus profile applied to outbound security policies
- D. URL filtering profile applied to outbound security policies

**Answer:** BD

#### NEW QUESTION 150

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, HTT
- 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 155

An administrator would like to apply a more restrictive Security profile to traffic for file sharing applications. The administrator does not want to update the Security policy or object when new applications are released.

Which object should the administrator use as a match condition in the Security policy?

- ☐ the Content Delivery Networks URL category
- ☒ the Online Storage and Backup URL category
- C. an application group containing all of the file-sharing App-IDs reported in the traffic logs
- D. an application filter for applications whose subcategory is file-sharing

**Answer:** D

#### NEW QUESTION 160

What is a function of application tags?

- A. creation of new zones
- B. application prioritization
- C. automated referenced applications in a policy
- D. IP address allocations in DHCP

**Answer:** C

#### NEW QUESTION 165

According to the best practices for mission critical devices, what is the recommended interval for antivirus updates?

- A. by minute
- B. hourly
- C. daily
- D. weekly

**Answer:** C

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-threat-content-updates/best-practices-mission-critical.html>

**NEW QUESTION 166**

Which action can be set in a URL Filtering Security profile to provide users temporary access to all websites in a given category using a provided password?

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

The user will see a response page indicating that a password is required to allow access to websites in the given category. With this option, the security administrator or help-desk person would provide a password granting temporary access to all websites in the given category. A log entry is generated in the URL Filtering log. The Override webpage doesn't display properly on client systems configured to use a proxy server.

**NEW QUESTION 169**

The firewall sends employees an application block page when they try to access Youtube. Which Security policy rule is blocking the youtube application?

	Name	Type	Source		Destination		Application	Service	URL Category	Action	Profile
			Zone	Address	Zone	Address					
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

- A. intrazone-default
- B. Deny Google
- C. allowed-security services
- D. interzone-default

**Answer: D**

**NEW QUESTION 174**

Which statement best describes a common use of Policy Optimizer?

- A. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications.
- B. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected.
- C. Policy Optimizer can display which Security policies have not been used in the last 90 days.
- D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exist
- E. Admins can then manually enable policies they want to keep and delete ones they want to remove.

**Answer: C**

**NEW QUESTION 175**

What is a recommended consideration when deploying content updates to the firewall from Panorama?

- A. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
- B. Content updates for firewall A/A HA pairs need a defined master device.
- C. Before deploying content updates, always check content release version compatibility.
- D. After deploying content updates, perform a commit and push to Panorama.

**Answer: C**

**NEW QUESTION 180**

Users from the internal zone need to be allowed to Telnet into a server in the DMZ zone. Complete the security policy to ensure only Telnet is allowed. Security Policy: Source Zone: Internal to DMZ Zone services "Application defaults", and action = Allow

- A. Destination IP: 192.168.1.123/24
- B. Application = 'Telnet'
- C. Log Forwarding
- D. USER-ID = 'Allow users in Trusted'

**Answer: B**

**NEW QUESTION 184**

When creating a Source NAT policy, which entry in the Translated Packet tab will display the options Dynamic IP and Port, Dynamic, Static IP, and None?

**NAT Policy Rule**

**General**   **Original Packet**   **Translated Packet**

Source Address Translation		Destination Address Translation	
Translation Type	<input type="text" value="v"/>	Translation Type	<input type="text" value="None"/>
Address Type	<input type="text" value="v"/>		
Interface	<input type="text" value="v"/>		
IP Address	<input type="text" value="v"/>		

**OK**   **Cancel**

- A. Translation Type
- B. Interface
- C. Address Type
- D. IP Address

**Answer:** A

#### NEW QUESTION 188

A network has 10 domain controllers, multiple WAN links, and a network infrastructure with bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?

- A. Windows-based agent on a domain controller
- B. Captive Portal
- C. Citrix terminal server with adequate data-plane resources
- D. PAN-OS integrated agent

**Answer:** A

#### NEW QUESTION 193

A network administrator is required to use a dynamic routing protocol for network connectivity.

Which three dynamic routing protocols are supported by the NGFW Virtual Router for this purpose? (Choose three.)

- A. RIP
- B. OSPF
- C. IS-IS
- D. EIGRP
- E. BGP

**Answer:** ABE

#### NEW QUESTION 194

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 197

Why does a company need an Antivirus profile?

- A. Mastered
- B. Not Mastered

**Answer:** A

#### NEW QUESTION 200

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 203**

A website is unexpectedly allowed due to miscategorization.

What are two ways to resolve this issue for a proper response? (Choose two.)

- A. Identify the URL category being assigned to the website. Edit the active URL Filtering profile and update that category's site access settings to block.
- B. Create a URL category and assign the affected URL. Update the active URL Filtering profile site access setting for the custom URL category to block.
- C. Review the categorization of the website on <https://urlfiltering.paloaltonetworks.co>
- D. Submit for "request change", identifying the appropriate categorization, and wait for confirmation before testing again.
- E. Create a URL category and assign the affected URL. Add a Security policy with a URL category qualifier of the custom URL category below the original policy.
- F. Set the policy action to Deny.

**Answer:** CD

**NEW QUESTION 207**

An administrator wants to create a NAT policy to allow multiple source IP addresses to be translated to the same public IP address. What is the most appropriate NAT policy to achieve this?

- A. Dynamic IP and Port
- B. Dynamic IP
- C. Static IP
- D. Destination

**Answer:** A

**NEW QUESTION 212**

Which type of profile must be applied to the Security policy rule to protect against buffer overflows illegal code execution and other attempts to exploit system flaws?

- A. anti-spyware
- B. URL filtering
- C. vulnerability protection
- D. file blocking

**Answer:** C

**Explanation:**

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection.html>

Vulnerability Protection Security Profiles protect against threats entering the network. For example, Vulnerability Protection Security Profiles protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection Security Profile protects clients and servers from all known critical-, high-, and medium-severity threats. You also can create exceptions that enable you to change the response to a specific signature.

**NEW QUESTION 217**

The PowerBall Lottery has reached a high payout amount and a company has decided to help employee morale by allowing employees to check the number, but doesn't want to unblock the gambling URL category.

Which two methods will allow the employees to get to the PowerBall Lottery site without the company unlocking the gambling URL category? (Choose two.)

- A. Add all the URLs from the gambling category except powerball.com to the block list and then set the action for the gambling category to allow.
- B. Manually remove powerball.com from the gambling URL category.
- C. Add \*.powerball.com to the allow list
- D. Create a custom URL category called PowerBall and add \*.powerball.com to the category and set the action to allow.

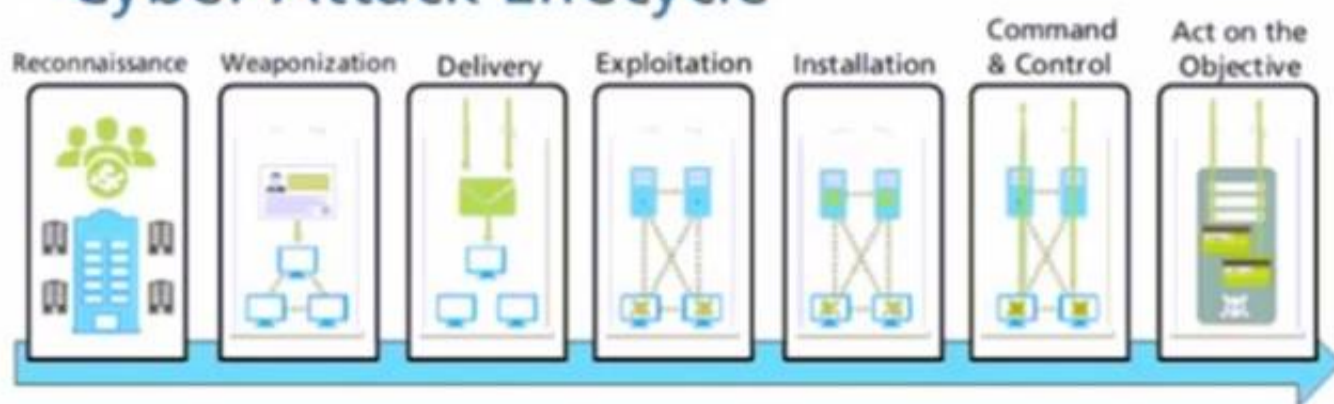
**Answer:** CD

**Explanation:**

**NEW QUESTION 222**

Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.

## Cyber Attack Lifecycle



Exploitation

- A. Installation  
B. Reconnaissance  
C. Act on the Objective

**Answer:** A

### NEW QUESTION 223

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

- A. authentication  
B. decryption  
C. application override  
D. 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 225

Which rule type is appropriate for matching traffic occurring within a specified zone?

- A. Interzone  
B. Universal  
C. Intrazone  
D. Shadowed

**Answer:** C

### NEW QUESTION 226

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 230

How frequently can wildfire updates be made available to firewalls?

- A. every 15 minutes  
B. every 30 minutes  
C. every 60 minutes  
D. every 5 minutes

**Answer:** D

### NEW QUESTION 235

What must be considered with regards to content updates deployed from Panorama?

- A. Content update schedulers need to be configured separately per device group.  
B. Panorama can only install up to five content versions of the same type for potential rollback scenarios.  
C. A PAN-OS upgrade resets all scheduler configurations for content updates.  
D. Panorama can only download one content update at a time for content updates of the same type.

**Answer:** D

**Explanation:**

Reference:<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-licenses-and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/schedule-a-content-update-using-panorama.html>

#### NEW QUESTION 240

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 244

Your company occupies one floor in a single building you have two active directory domain controllers on a single networks the firewall s management plane is only slightly utilized.

Which user-ID agent sufficient in your network?

- A. PAN-OS integrated agent deployed on the firewall
- B. Windows-based agent deployed on the internal network a domain member
- C. Citrix terminal server agent deployed on the network
- D. Windows-based agent deployed on each domain controller

**Answer:** D

**Explanation:**

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configureuser-mapping-using-the-windows-user-id-agent/configure-the-windows-based-user-id-agent-for-usermapping.html>

#### NEW QUESTION 248

Which interface type requires no routing or switching but applies Security or NAT policy rules before passing allowed traffic?

- A. Layer 3
- B. Virtual Wire
- C. Tap
- D. Layer 2

**Answer:** A

#### NEW QUESTION 253

Which prevention technique will prevent attacks based on packet count?

- A. zone protection profile
- B. URL filtering profile
- C. antivirus profile
- D. vulnerability profile

**Answer:** A

#### NEW QUESTION 257

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 258

An administrator is troubleshooting an issue with traffic that matches the intrazone-default rule, which is set to default configuration. What should the administrator do?

- A. Mastered
- B. Not Mastered

**Answer:** A

#### NEW QUESTION 262

In which profile should you configure the DNS Security feature?

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

**Answer:** B

**Explanation:**

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/dns-security/enable-dnssecurity.html>

#### NEW QUESTION 265

Which five Zero Trust concepts does a Palo Alto Networks firewall apply to achieve an integrated approach to prevent threats? (Choose five.)

- A. User identification
- B. Filtration protection
- C. Vulnerability protection
- D. Antivirus
- E. Application identification
- F. Anti-spyware

**Answer:** ACDEF

#### NEW QUESTION 269

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 273

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The PCNSA Practice Test Here](#)**