

# Paloalto-Networks

## Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator



#### 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

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

Which object would an administrator create to enable access to all applications in the office-programs subcategory?

- A. application filter
- B. URL category
- C. HIP profile
- D. application group

**Answer: A**

#### NEW QUESTION 4

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 5**

Which information is included in device state other than the local configuration?

- A.

uncommitted changes

- B. audit logs to provide information of administrative account changes  
C. system logs to provide information of PAN-OS changes  
D. device group and template settings pushed from Panorama

**Answer:** D

**Explanation:**

Reference:<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/device/device-setup-operations.html>

**NEW QUESTION 6**

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 7

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 8

What are three characteristics of the Palo Alto Networks DNS Security service? (Choose three.)

- A. It uses techniques such as DGA.DNS tunneling detection and machine learning.
- B. It requires a valid Threat Prevention license.
- C. It enables users to access real-time protections using advanced predictive analytics.
- D. It requires a valid URL Filtering license.
- E. It requires an active subscription to a third-party DNS Security service.

**Answer:** ABC

**Explanation:**

DNS Security subscription enables users to access real-time protections using advanced predictive analytics. When techniques such as DGA/DNS tunneling detection and machine learning are used, threats hidden within DNS traffic can be proactively identified and shared through an infinitely scalable cloud service. Because the DNS signatures and protections are stored in a cloud-based architecture, you can access the full database of ever-expanding signatures that have been generated using a multitude of data sources. This list of signatures allows you to defend against an array of threats using DNS in real-time against newly generated malicious domains. To combat future threats, updates to the analysis, detection, and prevention capabilities of the DNS Security service will be available through content releases. To access the DNS Security service, you must have a Threat Prevention license and DNS Security license.

#### NEW QUESTION 9

What are three factors that can be used in domain generation algorithms? (Choose three.)

- A. cryptographic keys
- B.

time of day

- C. other unique values
- D. URL custom categories
- E. IP address

**Answer:** ABC

**Explanation:**

Domain generation algorithms (DGAs) are used to auto-generate domains, typically in large numbers within the context of establishing a malicious command-and-control (C2) communications channel. DGA-based malware (such as Pushdo, BankPatch, and CryptoLocker) limit the number of domains from being blocked by hiding the location of their active C2 servers within a large number of possible suspects, and can be algorithmically generated based on factors such as time of day, cryptographic keys, or other unique values.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/domain-generation-algorithm-detection>

**NEW QUESTION 10**

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 10**

Which two App-ID applications will need to be allowed to use Facebook-chat? (Choose two.)

- A. facebook
- B. facebook-chat
- C. facebook-base
- D. facebook-email

**Answer:** BC

**NEW QUESTION 15**

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 18**

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 20

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

Device SN: 007251000156345	Interface: ethernet1/4	NAT IP: 8.8.8.4
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	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/persistent-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 22

An administrator is implementing an exception to an external dynamic list by adding an entry to the list manually. The administrator wants to save the changes, but the OK button is grayed out.  
What are two possible reasons the OK button is grayed out? (Choose two.)

- A. The entry contains wildcards.
- B. The entry is duplicated.
- C. The entry doesn't match a list entry.
- D. The entry matches a list entry.

Answer: BC

#### NEW QUESTION 25

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 28

If users from the Trusted zone need to allow traffic to an SFTP server in the DMZ zone, how should a Security policy with App-ID be configured?

A)

Source Zone: Trusted  
Destination Zone: DMZ  
Services: Application-Default  
Applications: SSH  
Action: Deny

B)

Source Zone: Trusted  
Destination Zone: DMZ  
Services: SSH  
Applications: Any  
Action: Allow

C)

Source Zone: Trusted  
Destination Zone: DMZ  
Services: SSH  
Applications: Any  
Action: Deny

D)

Source Zone: Trusted  
Destination Zone: DMZ  
Services: Application-Default  
Applications: SSH  
Action: Allow



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

**Answer:** D

#### NEW QUESTION 29

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 31

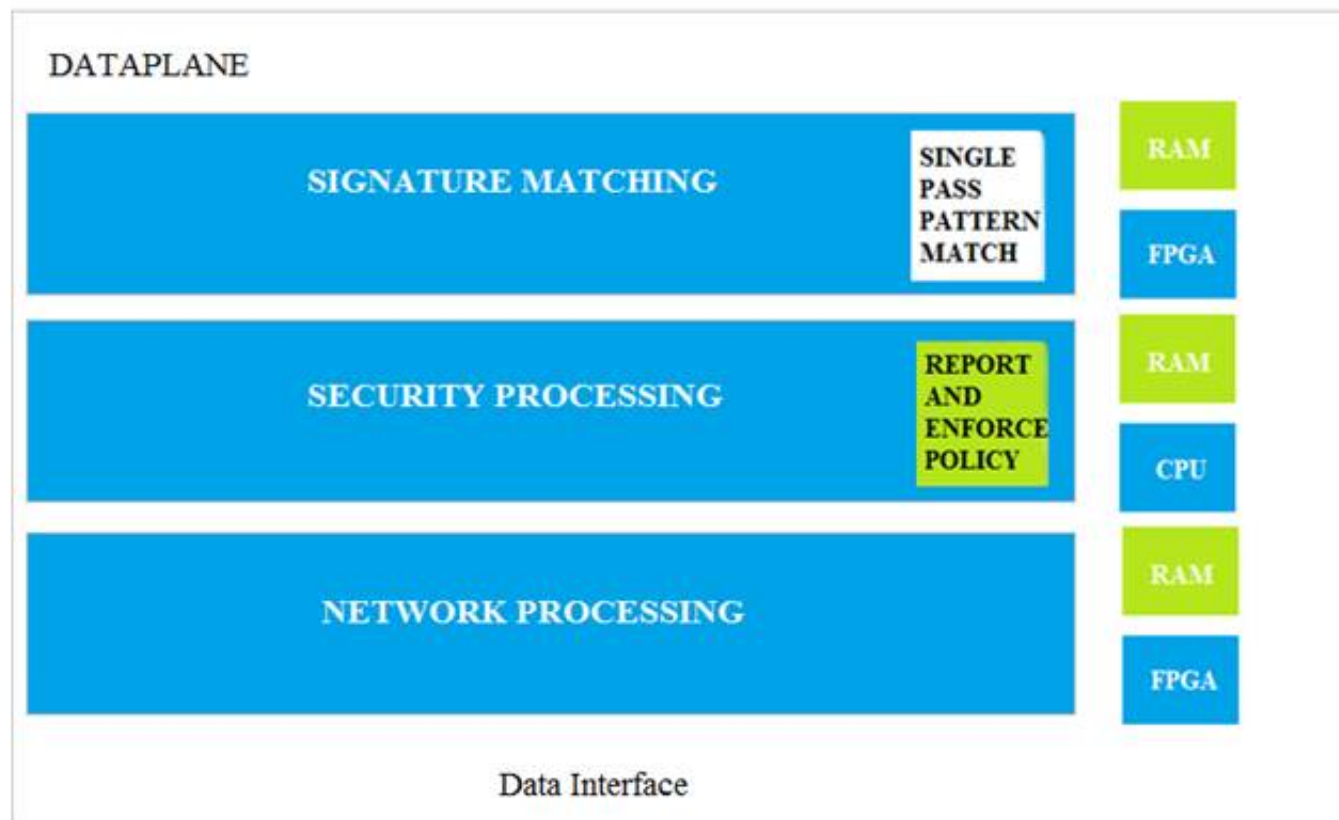
What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?

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

**Answer:** D

#### NEW QUESTION 35

Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



- A. Signature Matching
- B. Network Processing
- C. Security Processing
- D. Security Matching

**Answer:** A

#### NEW QUESTION 40

Which interface does not require a MAC or IP address?

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

**Answer:** A



#### NEW QUESTION 42

Which profile should be used to obtain a verdict regarding analyzed files?

- A. WildFire analysis
- B. Vulnerability profile
- C. Content-ID
- D. Advanced threat prevention

**Answer:** A

#### Explanation:

? A profile is a set of rules or settings that defines how the firewall performs a specific function, such as detecting and preventing threats, filtering URLs, or decrypting traffic<sup>1</sup>.

? There are different types of profiles that can be applied to different types of traffic or scenarios, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, Decryption, or WildFire Analysis<sup>1</sup>.

? The WildFire Analysis profile is a profile that enables the firewall to submit unknown files or email links to the cloud-based WildFire service for analysis and verdict determination<sup>2</sup>. WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware<sup>3</sup>. WildFire uses a variety of malware detection techniques, such as static analysis, dynamic analysis, machine learning, and intelligent run-time memory analysis, to identify and protect against unknown threats<sup>4</sup>.

? The Vulnerability Protection profile is a profile that protects the network from exploits that target known software vulnerabilities. It allows the administrator to configure the actions and log settings for each vulnerability severity level, such as critical, high, medium, low, or informational<sup>5</sup>.

? Content-ID is not a profile, but a feature of the firewall that performs multiple functions to identify and control applications, users, content, and threats on the network. Content-ID consists of four components: App-ID, User-ID, Content Inspection, and Threat Prevention.

? Advanced Threat Prevention is not a profile, but a term that refers to the comprehensive approach of Palo Alto Networks to prevent sophisticated and unknown threats. Advanced Threat Prevention includes WildFire, but also other products and services, such as DNS Security, Cortex XDR, Cortex XSOAR, and AutoFocus. Therefore, the profile that should be used to obtain a verdict regarding analyzed files is the WildFire Analysis profile.

References:

1: Security Profiles - Palo Alto Networks 2: WildFire Analysis Profile - Palo Alto

Networks 3: WildFire - Palo Alto Networks 4: Advanced Wildfire as an ICAP Alternative | Palo Alto Networks 5: Vulnerability Protection Profile - Palo Alto Networks  
: [Content-ID - Palo Alto Networks] : [Advanced Threat Prevention - Palo Alto Networks]

#### NEW QUESTION 43

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 46

Which plane on a Palo Alto Networks firewall provides configuration logging and reporting functions on a separate processor?

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

**Answer:** C

#### NEW QUESTION 48

What are the requirements for using Palo Alto Networks EDL Hosting Service?

- A. any supported Palo Alto Networks firewall or Prisma Access firewall
- B. an additional subscription free of charge
- C. a firewall device running with a minimum version of PAN-OS 10.1
- D. an additional paid subscription

**Answer:** A

#### NEW QUESTION 52

DRAG DROP

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 55

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

User MappingConnection SecurityUser-ID AgentsTerminal Services AgentsGroup Mapping SettingsCaptive Portal Settings

Domain's DNS Namelab.localKerberos Server Profilelab-kerberos

Enable Security Log☒

Server Log Monitor Frequency (sec)2

Enable Session☒

Server Session Read Frequency (sec)10

Novell eDirectory Query Interval (sec)30

Syslog Service Profile

Enable Probing☒

Prove 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

Server Monitoring

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 59

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 62

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 67

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

Detailed Log View		
General	Source	Destination
<p>Session ID 781868</p> <p>Action drop</p> <p>Host ID</p> <p>Application dns</p> <p>Rule Outbound DNS</p> <p>Rule UUID ea9f3b96-e280-467c-aca5-0b1902857791</p> <p>Device SN 007251000156341</p> <p>IP Protocol udp</p> <p>Log Action global-logs</p> <p>Generated Time 2021/08/27 02:02:49</p> <p>Receive Time 2021/08/27 02:02:53</p> <p>Tunnel Type N/A</p>	<p>Source User</p> <p>Source 192.168.101.25</p> <p>Source DAG</p> <p>Country 192.168.0.0-192.168.255.255</p> <p>Port 46282</p> <p>Zone Servers</p> <p>Interface ethernet1/4</p> <p>NAT IP 67.190.64.58</p> <p>NAT Port 26351</p> <p>X-Forwarded-For IP 0.0.0.0</p>	<p>Destination User</p> <p>Destination 8.8.4.4</p> <p>Destination DAG</p> <p>Country United States</p> <p>Port 53</p> <p>Zone Internet</p> <p>Interface ethernet1/8</p> <p>NAT IP 8.8.4.4</p> <p>NAT Port 53</p>
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 69

Which path in PAN-OS 10.0 displays the list of port-based security policy rules?

- A. Policies> Security> Rule Usage> No App Specified
- B. Policies> Security> Rule Usage> Port only specified
- C. Policies> Security> Rule Usage> Port-based Rules
- D. Policies> Security> Rule Usage> Unused Apps

**Answer: A**

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/security-policy-rule-optimization/migrate-port-based-to-app-id-based-security-policy-rules.html>

#### NEW QUESTION 73

How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

- A. Disable automatic updates during weekdays
- B. Automatically “download and install” but with the “disable new applications” option used
- C. Automatically “download only” and then install Applications and Threats later, after the administrator approves the update
- D. Configure the option for “Threshold”

**Answer: D**

#### NEW QUESTION 78

An administrator needs to create a Security policy rule that matches DNS traffic within the LAN zone, and also needs to match DNS traffic within the DMZ zone. The administrator does not want to allow traffic between the DMZ and LAN zones.

Which Security policy rule type should they use?

- ☐ default
- ☒ universal
- ☐ intrazone
- ☐ interzone

**Answer:** C

#### NEW QUESTION 83

Which Security profile would you apply to identify infected hosts on the protected network uwall user database?

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

**Answer:** A

#### NEW QUESTION 87

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 89

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

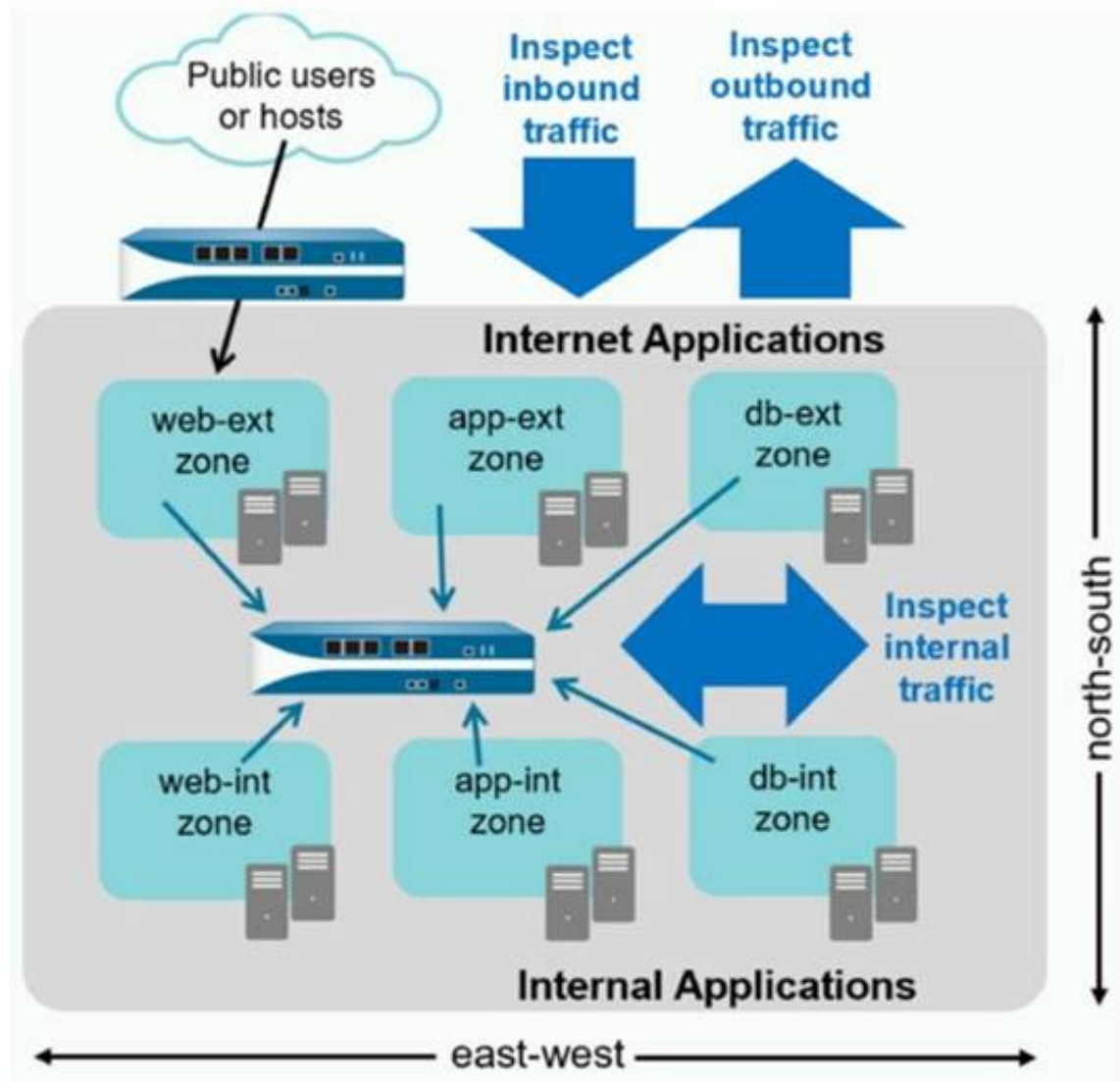
**Answer:** D

**Explanation:**

#### NEW QUESTION 93

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 96

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 AutoFocus<sup>1</sup>.  
 ? 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 destination<sup>1</sup>.  
 ? 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 services<sup>23</sup>.  
 ? 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 service<sup>1</sup>.  
 ? 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 97

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

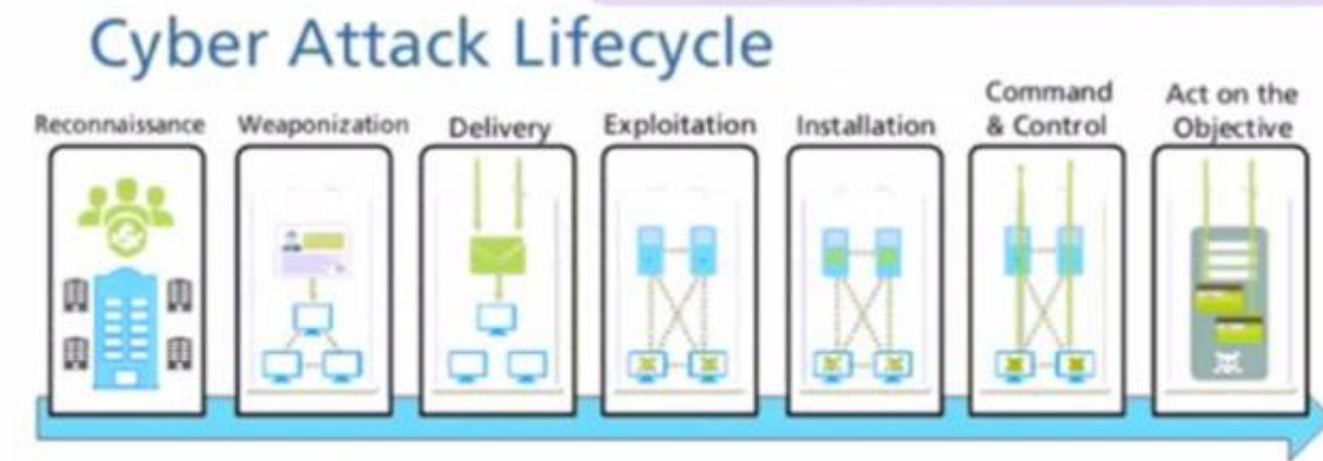
**Answer: A**

#### 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 98

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



delivery

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

**Answer: A**

#### NEW QUESTION 101

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 102

Which objects would be useful for combining several services that are often defined together?

- A. shared service objects
- B. service groups
- C. application groups
- D. application filters

**Answer: B**

#### Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-services.html>

#### NEW QUESTION 105

An administrator is reviewing the Security policy rules shown in the screenshot below. Which statement is correct about the information displayed?



- A. Eleven rules use the "Infrastructure\*" tag.
- B. The view Rulebase as Groups is checked.
- C. There are seven Security policy rules on this firewall.
- D. Highlight Unused Rules is checked.

**Answer:** B

**Explanation:**

**NEW QUESTION 106**

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 110**

To what must an interface be assigned before it can process traffic?

- A. Security Zone
- B. Security policy
- C. Security Protection
- D. Security profile

**Answer:** A

**NEW QUESTION 113**

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?

- A. the Content Delivery Networks URL category
- B. 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 116**

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

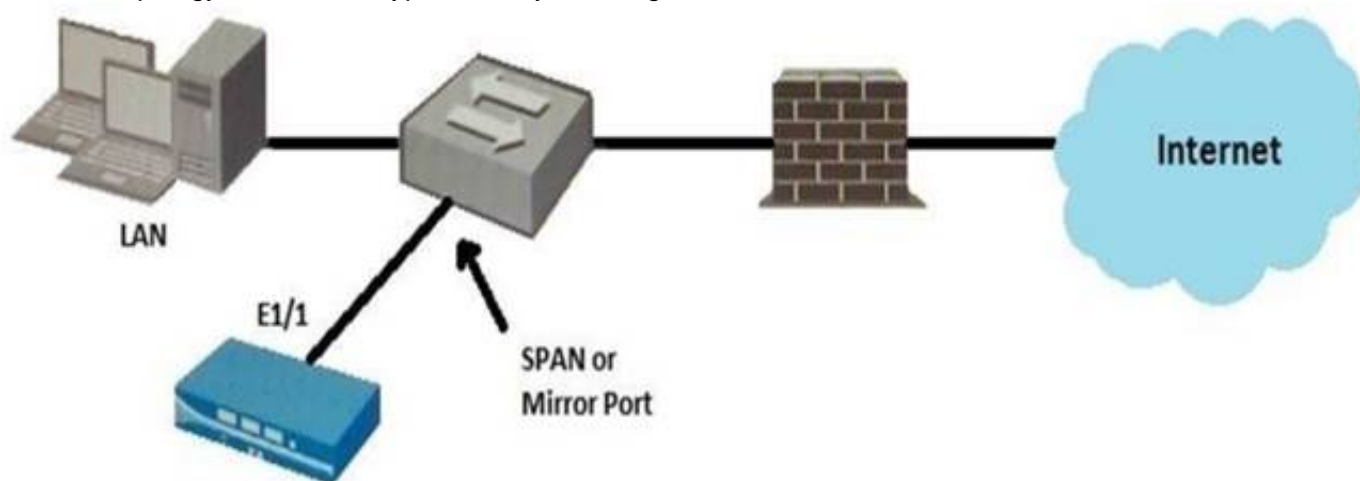
**Answer:** C

**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 117**

Given the topology, which zone type should you configure for firewall interface E1/1?



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

**Answer:** A

**NEW QUESTION 121**



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 124

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 125

Which statement is true regarding a Best Practice Assessment?

- A. The BPA tool can be run only on firewalls
- B. It provides a percentage of adoption for each assessment data
- C. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities
- D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

**Answer:** C

#### NEW QUESTION 130

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 132

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 136

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 141

Your company is highly concerned with their Intellectual property being accessed by unauthorized resources. There is a mature process to store and include metadata tags for all confidential documents.

Which Security profile can further ensure that these documents do not exit the corporate network?

- A. File Blocking
- B. Data Filtering
- C. Anti-Spyware
- D. URL Filtering

**Answer:** B

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-data-filtering>

**NEW QUESTION 143**

An administrator needs to add capability to perform real-time signature lookups to block or sinkhole all known malware domains. Which type of single unified engine will get this result?

- A. User-ID
- B. App-ID
- C. Security Processing Engine
- D. Content-ID

**Answer:** A

**NEW QUESTION 148**

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 149**

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 152**

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 156**

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 159**

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 161

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 166

Given the screenshot what two types of route is the administrator configuring? (Choose two)

Virtual Router - Static Route - IPv4

Name0.0.0.0

Destination0.0.0.0/0

Interfaceethernet1/1

Next HopIP Address

10.46.172.1

Admin Distance10 - 240

Metric10

Route TableUnicast

BFD ProfileDisable BFD

☐ Path Monitoring

Failure Condition

Any

All

Preemptive Hold Time (min)2

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
--------------------------	------	--------	-----------	----------------	--------------------	------------

- A. default route
- B. OSPF
- C. BGP
- D. static route

Answer: A

NEW QUESTION 170

An administrator would like to determine the default deny action for the application dns- over-https  
Which action would yield the information?

- A. View the application details in beacon paloaltonetworks.com

- B. Check the action for the Security policy matching that traffic
- C. Check the action for the decoder in the antivirus profile
- D. View the application details in Objects > Applications

**Answer:** D

**Explanation:**

**NEW QUESTION 173**

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 175**

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 180**

Based on the screenshot what is the purpose of the group in User labelled "it"?

	Name	Type	Source		Destination		Application
			Zone	Address	Zone	Address	
1	allow-it	universal	inside	any	it	dmz	it-tools

- A. Allows users to access IT applications on all ports
- B. Allows users in group "DMZ" to access IT applications
- C. Allows "any" users to access servers in the DMZ zone
- D. Allows users in group "it" to access IT applications

**Answer:** D

**NEW QUESTION 181**

.....

## 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](#)**