

# Paloalto-Networks

## Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator



#### NEW QUESTION 1

Which security policy rule would be needed to match traffic that passes between the Outside zone and Inside zone, but does not match traffic that passes within the zones?

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

**Answer:** B

#### NEW QUESTION 2

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 3

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 4

Which attribute can a dynamic address group use as a filtering condition to determine its membership?

- A. tag
- B. wildcard mask
- C. IP address
- D. subnet mask

**Answer:** A

**Explanation:**

Dynamic Address Groups: A dynamic address group populates its members dynamically using lookups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall. <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-address-groups>

#### NEW QUESTION 5

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 6

DRAG DROP

Arrange the correct order that the URL classifications are processed within the system.

Answer Area

First	Drag answer here	PAN-DB Cloud
Second	Drag answer here	External Dynamic Lists
Third	Drag answer here	Custom URL Categories
Fourth	Drag answer here	Block List
Fifth	Drag answer here	Downloaded PAN-DB File
Sixth	Drag answer here	Allow Lists

Answer:

Answer Area

First	Block List	PAN-DB Cloud
Second	Allow Lists	External Dynamic Lists
Third	Custom URL Categories	Custom URL Categories
Fourth	External Dynamic Lists	Block List
Fifth	Downloaded PAN-DB File	Downloaded PAN-DB File
Sixth	PAN-DB Cloud	Allow Lists

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

First – Block List  
Second – Allow List  
Third – Custom URL Categories  
Fourth – External Dynamic Lists  
Fifth – Downloaded PAN-DB Files  
Sixth - PAN-DB Cloud

NEW QUESTION 7

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 8

When creating a Panorama administrator type of Device Group and Template Admin, which two things must you create first? (Choose two.)

- A. password profile
- B.

access domain

- C. admin role
- D. server profile

**Answer:** CD

**NEW QUESTION 9**

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

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

**Answer:** C

**NEW QUESTION 10**

Which two rule types allow the administrator to modify the destination zone? (Choose two )

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

**Answer:** AC

**NEW QUESTION 10**

When HTTPS for management and GlobalProtect are enabled on the same interface, which TCP port is used for management access?

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm8SCAS#:~:text=Details,using%20https%20on%20port%204443>

**NEW QUESTION 13**

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 17

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 20

What do you configure if you want to set up a group of objects based on their ports alone?

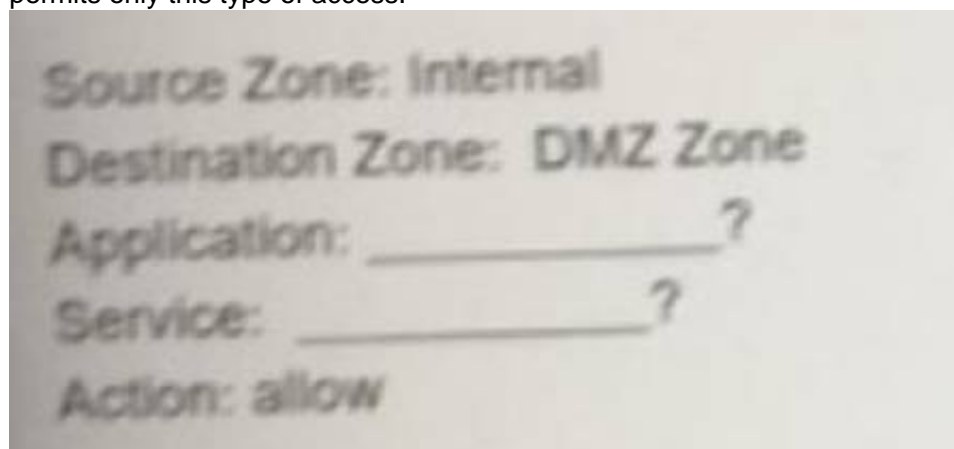
- A. Application groups
- B. Service groups
- C. Address groups
- D. Custom objects



**Answer:** B

#### NEW QUESTION 23

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 25

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 26

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 27**

Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choices to block the sameURL then which choice would be the last to block access to the URL?

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

The precedence is from the top down; First Match Wins: 1) Block list: Manually entered blocked URLs Objects - 2) Allow list: Manually entered allowed URLs Objects - 3) Custom URL Categories - 4) Cached Cached: URLs learned from External Dynamic Lists (EDLs) - 5) Pre-Defined Categories: PAN-DB or Brightcloud categories.

**NEW QUESTION 30**

How do you reset the hit count on a security policy rule?

- A. First disable and then re-enable the rule.
- B. Reboot the data-plane.
- C. Select a Security policy rule, and then select Hit Count > Reset.
- D. Type the CLI command reset hitcount <POLICY-NAME>.

**Answer:** C

**NEW QUESTION 32**

An administrator would like to use App-ID's deny action for an application and would like that action updated with dynamic updates as new content becomes available.

Which security policy action causes this?

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

**Answer:** C

**Explanation:**

Explanation/Reference: Reference:



<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-configuration-backups/revert-firewall-configuration-changes.html>

**NEW QUESTION 33**

Which rule type is appropriate for matching traffic both within and between the source and destination zones?

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

**Answer:** A

**NEW QUESTION 38**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**NEW QUESTION 42**

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 46**

What are two valid selections within an Antivirus profile? (Choose two.)

- A. deny
- B. drop
- C. default
- D. block-ip

**Answer:** BC

**NEW QUESTION 47**

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 52

Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?

- A. Palo Alto Networks Bulletproof IP Addresses
- B. Palo Alto Networks C&C IP Addresses
- C. Palo Alto Networks Known Malicious IP Addresses
- D. Palo Alto Networks High-Risk IP Addresses

Answer: A

Explanation:

To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.  
<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/content-inspection-features/edl-for-bulletproof-isps#:~:text=A%20new%20built%20in%20external,%2C%20illegal%2C%20and%20unethical%20content.>

NEW QUESTION 56

DRAG DROP

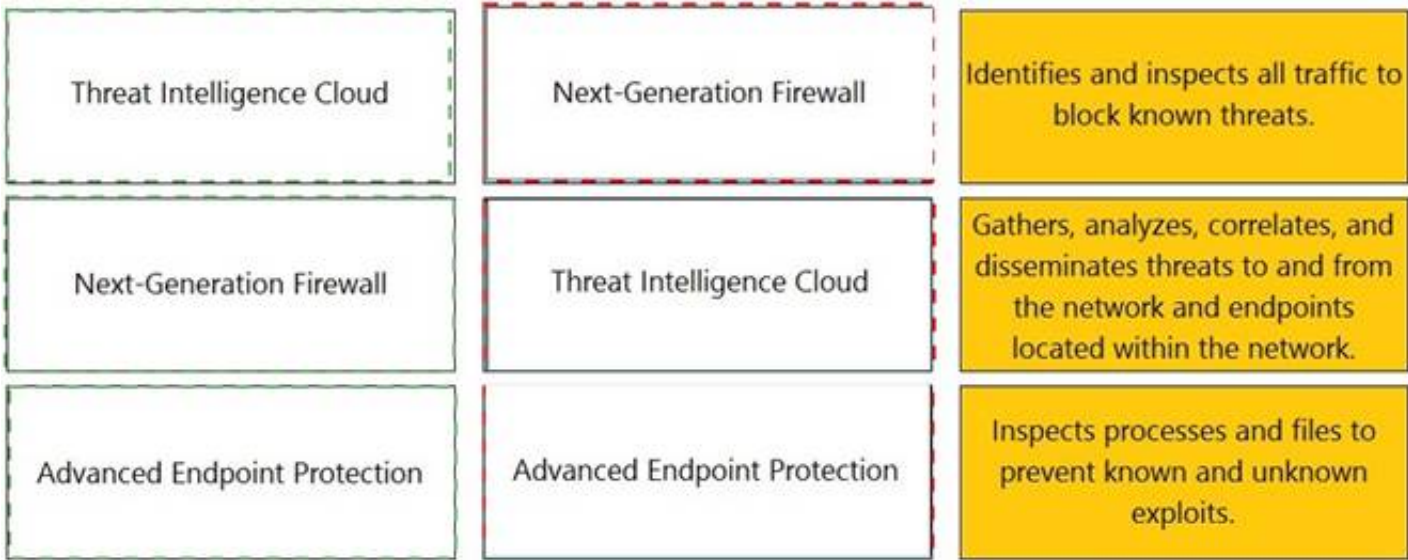
Match each feature to the DoS Protection Policy or the DoS Protection Profile.

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:



**NEW QUESTION 57**

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 58**

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 63**

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 66**

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 67

Which two statements are correct about App-ID content updates? (Choose two.)

- A. Updated application content may change how security policy rules are enforced
- B. After an application content update, new applications must be manually classified prior to use
- C. Existing security policy rules are not affected by application content updates
- D. After an application content update, new applications are automatically identified and classified

**Answer:** AD

#### NEW QUESTION 72

How is the hit count reset on a rule?

- A. select a security policy rule, right click Hit Count > Reset
- B. with a dataplane reboot
- C. Device > Setup > Logging and Reporting Settings > Reset Hit Count
- D. in the CLI, type command reset hitcount <POLICY-NAME>

**Answer:** A

#### NEW QUESTION 77

Prior to a maintenance-window activity, the administrator would like to make a backup of only the running configuration to an external location. What command in Device > Setup > Operations would provide the most operationally efficient way to achieve this outcome?

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Export Named Configuration Snapshot This option exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location. These exports often are used as backups. These XML files also can be used as templates for building other firewall configurations.

#### NEW QUESTION 78

Which two components are utilized within the Single-Pass Parallel Processing architecture on a Palo Alto Networks Firewall? (Choose two.)

- A. Layer-ID
- B. User-ID
- C. QoS-ID
- D. App-ID

**Answer:** BD

#### Explanation:

#### NEW QUESTION 79

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 83**

Which DNS Query action is recommended for traffic that is allowed by Security policy and matches Palo Alto Networks Content DNS Signatures?

- A. block
- B. sinkhole
- C. alert
- D. allow

**Answer:** B

**Explanation:**

To enable DNS sinkholing for domain queries using DNS security, you must activate your DNS Security subscription, create (or modify) an Anti-Spyware policy to reference the DNS Security service, configure the log severity and policy settings for each DNS signature category, and then attach the profile to a security policy rule. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns-security/enable-dns-security>

**NEW QUESTION 88**

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 93**

You must configure which firewall feature to enable a data-plane interface to submit DNS queries on behalf of the control plane?

- A. Admin Role profile
- B. virtual router
- C. DNS proxy
- D. service route

**Answer:** A

**NEW QUESTION 94**

Which interface does not require a MAC or IP address?

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

**Answer:** A

**NEW QUESTION 98**

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 103**

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 107**

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 109**

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 114**

If using group mapping with Active Directory Universal Groups, what must you do when configuring the User-ID?

- A. Create an LDAP Server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL
- B. Configure a frequency schedule to clear group mapping cache
- C. Configure a Primary Employee ID number for user-based Security policies
- D. Create a RADIUS Server profile to connect to the domain controllers using LDAPS on port 636 or 389

**Answer:** B

**Explanation:**

? If you have Universal Groups, create an LDAP server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information is available for all domains and subdomains.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups>

**NEW QUESTION 116**

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 120**

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

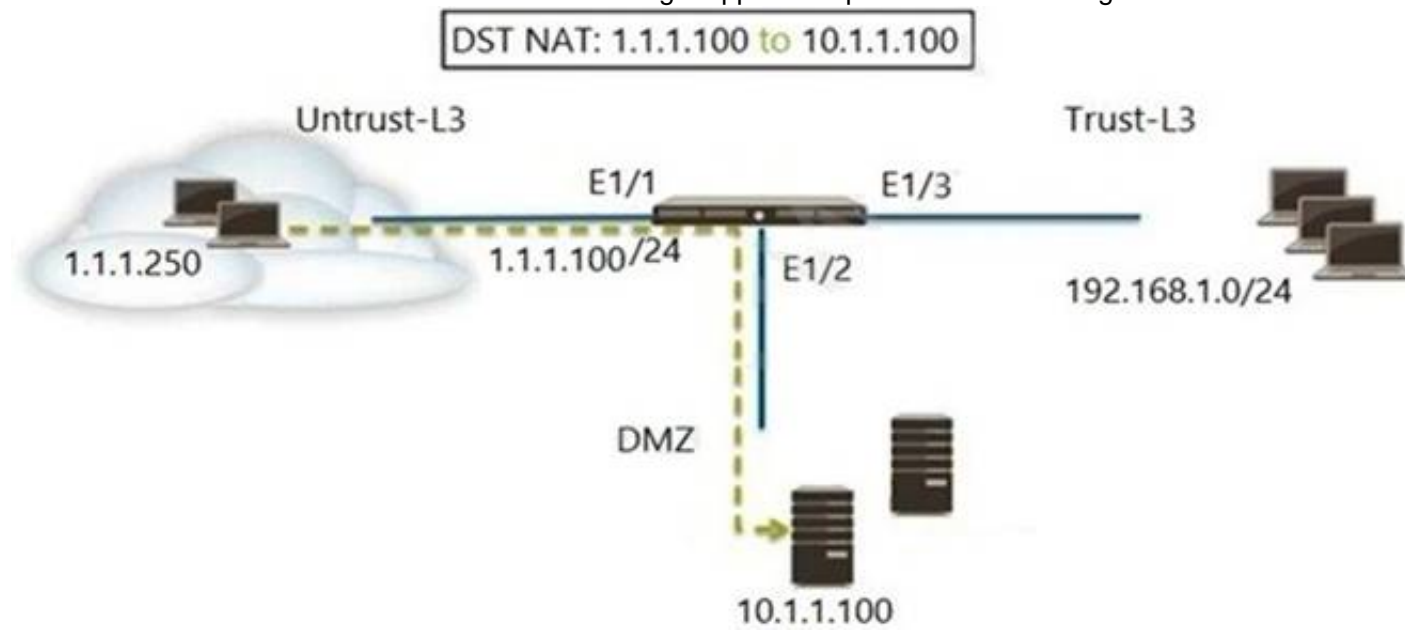
- A. any supported Palo Alto Networks firewall or Prisma Access firewall
- B. an additional subscription free of charge
- C. a firewall device running with a minimum version of PAN-OS 10.1
- D. an additional paid subscription

**Answer:** A



**NEW QUESTION 121**

Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.



Which Security policy rule will allow traffic to flow to the web server?

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping>

**NEW QUESTION 125**

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 126**

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

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 127**

Which statements is true regarding a Heatmap report?

- A. When guided by authorized sales engineer, it helps determine te 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 131

Based on the screenshot what is the purpose of the included groups?

	Name	Type	Source			Destination		Application	Service	Action
			Zone	Address	User	Zone	Address			
1	allow-it	universal	inside	any	it	dmz	any	it-tools	application-default	Allow

A. They are only groups visible based on the firewall's credentials.

B. They are used to map usernames to group names.

C. They contain only the users you allow to manage the firewall.

D. They are groups that are imported from RADIUS authentication servers.

**Answer: B**

**Explanation:**

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups.html>

#### NEW QUESTION 133

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

A. Mastered

B. Not Mastered

**Answer: A**

#### NEW QUESTION 138

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 140

What must be configured for the firewall to access multiple authentication profiles for external services to authenticate a non-local account?

A. authentication sequence

B. LDAP server profile

C. authentication server list

D. authentication list profile

**Answer: A**

#### NEW QUESTION 143

Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?

A. Root

B. Dynamic

C. Role-based

D. Superuser

**Answer: C**

#### NEW QUESTION 147

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 148

Which interface type can use virtual routers and routing protocols?

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

**Answer:** B

#### NEW QUESTION 151

What action will inform end users when their access to Internet content is being restricted?

- A. Create a custom 'URL Category' object with notifications enabled.
- B. Publish monitoring data for Security policy deny logs.
- C. Ensure that the 'site access' setting for all URL sites is set to 'alert'.
- D. Enable 'Response Pages' on the interface providing Internet access.

**Answer:** D

**Explanation:**

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/device/device-response-pages.html>

#### NEW QUESTION 154

Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?

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

**Answer:** D

**Explanation:**

References:<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000>

00ClomCAC

#### NEW QUESTION 156

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 161

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 163

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 168**

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 170**

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 174**

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 176**

Which two security profile types can be attached to a security policy? (Choose two.)

- A. antivirus
- B. DDoS protection
- C. threat
- D. vulnerability

**Answer:** AD

**NEW QUESTION 178**

What is the maximum volume of concurrent administrative account sessions?

- A. Unlimited
- B. 2
- C. 10
- D. 1

**Answer:** C

**NEW QUESTION 179**

An administrator would like to create a URL Filtering log entry when users browse to any gambling website. What combination of Security policy and Security profile actions is correct?

Security policy = drop, Gambling category in URL profile = allow

- A. Security policy = den
- B. Security policy = allow, Gambling category in URL profile = alert
- C. Gambling category in URL profile = block
- D. Security policy = allow, Gambling category in URL profile = alert
- E. Security policy = allow, Gambling category in URL profile = allow
- F. Gambling category in URL profile = allow

Answer: C

NEW QUESTION 180

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 182

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

- Deny
- ~~A~~: No notification
  - C. Drop
  - D. Reset Client

Answer: C

NEW QUESTION 183

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 186

Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

- A. Aperture
- B. AutoFocus
- C. Parisma SaaS
- D. GlobalProtect

Answer: C

NEW QUESTION 189

DRAG DROP

Match the cyber-attack lifecycle stage to its correct description.

reconnaissance

installation

command and control

act on the objectives

Answer Area

stage that reveals the attacker's motivation

stage where the attacker scans for network vulnerabilities to be exploited

stage where the attacker will explore methods of persistence

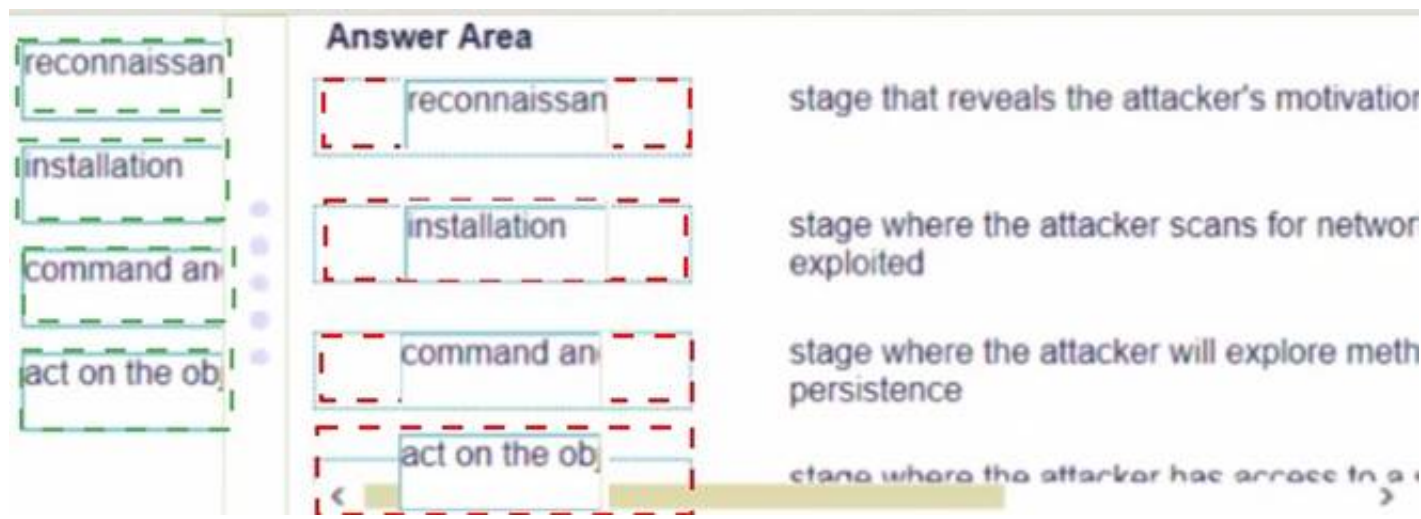
stage where the attacker has access to a system

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:





**NEW QUESTION 193**

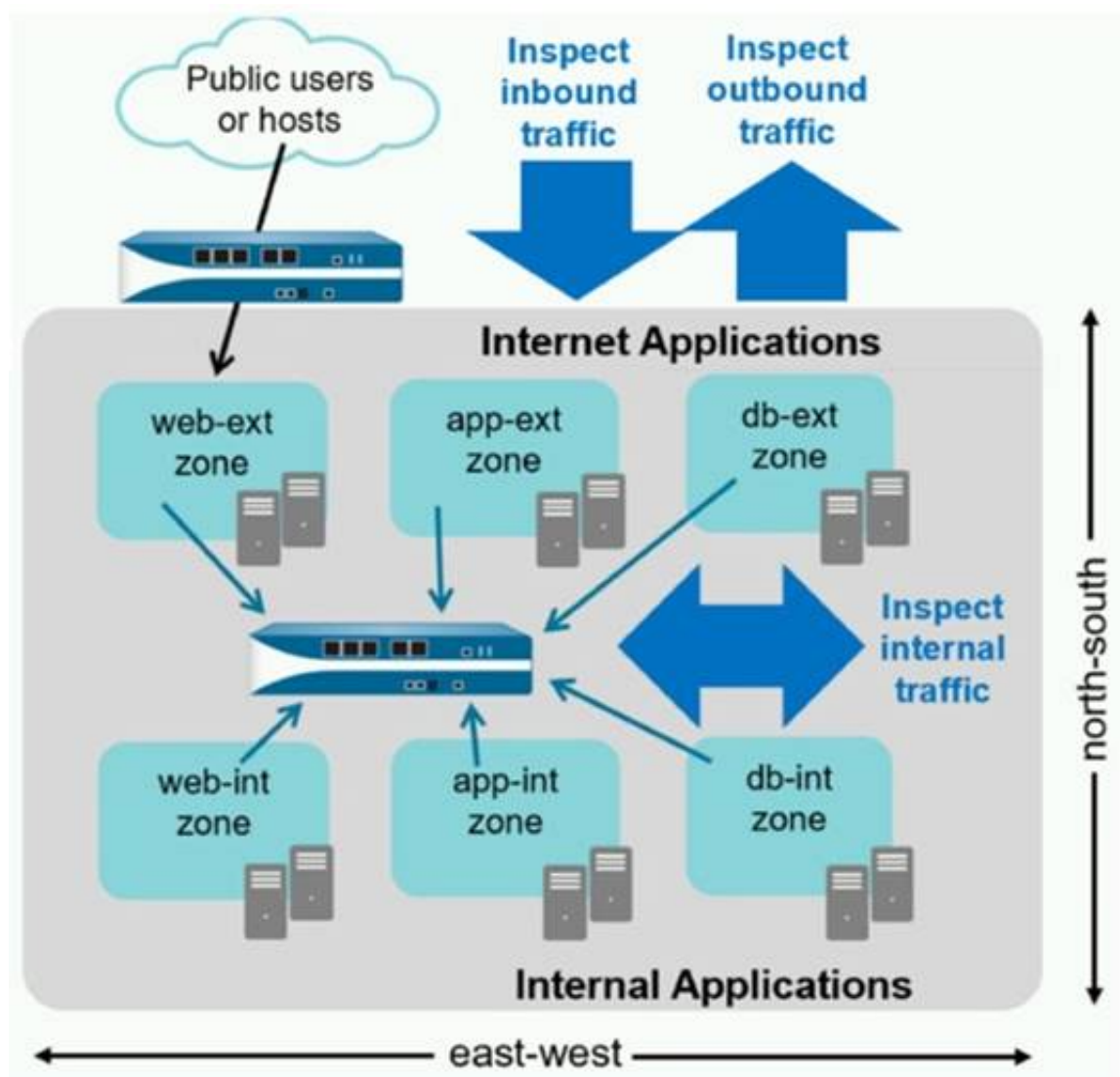
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration. Why doesn't the administrator see the traffic?

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

**Answer: D**

**NEW QUESTION 194**

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?



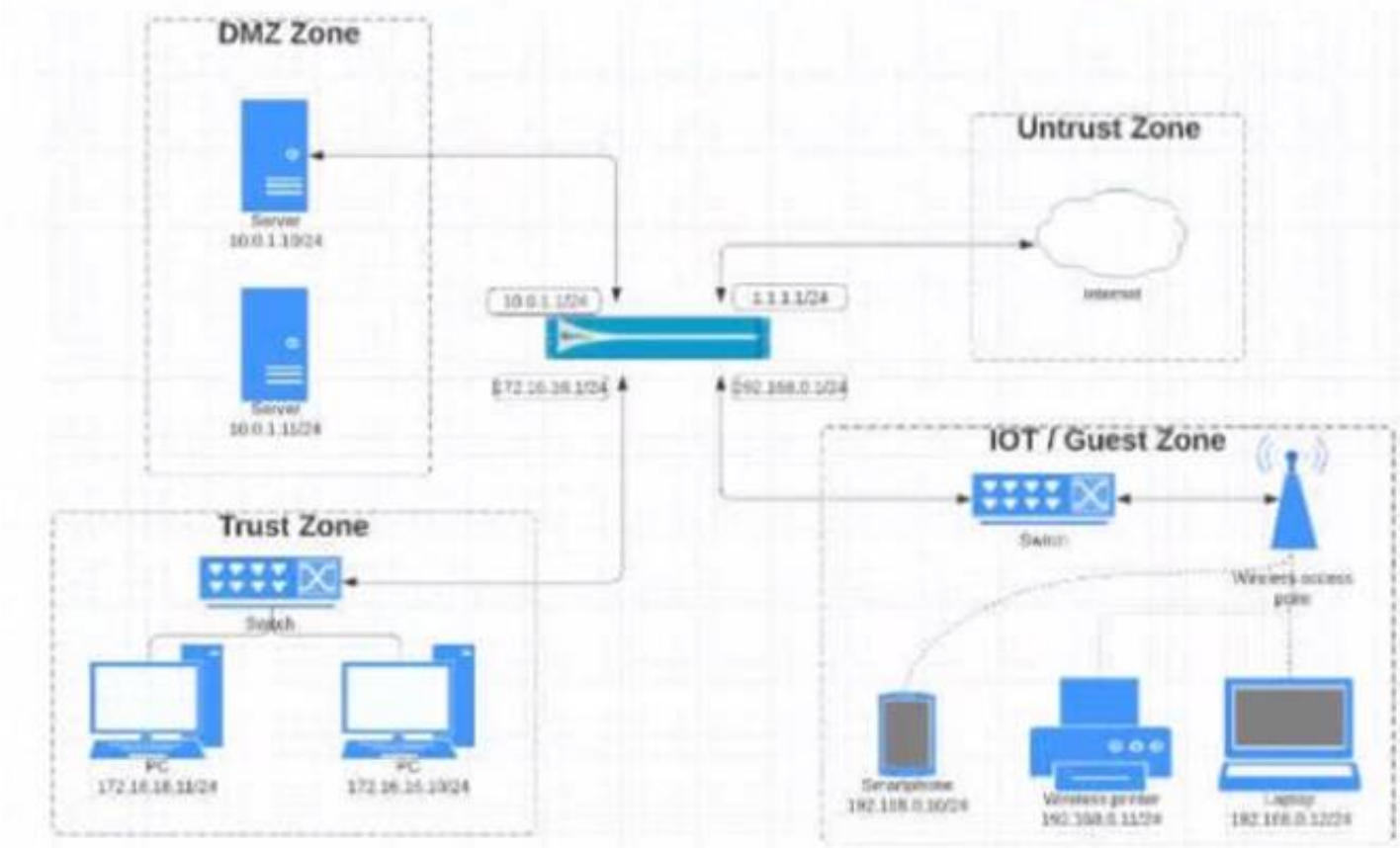
- A. branch office traffic
- B. north-south traffic
- C. perimeter traffic
- D. east-west traffic

**Answer: D**

**NEW QUESTION 197**

View the diagram.





What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

A)

Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	ZONE				
172.16.16.0/24	any	any	DMZ	1.1.1.0/24	any	any	ssh	application-default	any	Allow
192.168.0.0/24			Untrust	10.0.1.0/24			ssh			
							web-browsing			

B)

Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	ZONE				
10.0.1.0/24	any	any	DMZ	1.1.1.0/24	any	any	ssh	application-default	any	Allow
172.16.16.0/24			Untrust	192.168.0.0/24			ssh			
							web-browsing			

C)

Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	ZONE				
172.16.16.0/24	any	any	DMZ	any	any	any	ssh	application-default	any	Allow
192.168.0.0/24			Untrust				ssh			
							web-browsing			

D)

Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	ZONE				
172.16.16.0/24	any	any	DMZ	any	any	any	ssh	application-default	any	Allow
192.168.0.0/24			Untrust				ssh			
							web-browsing			

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

Answer: C

NEW QUESTION 201

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) server1.  
? An Anti-Spyware security profile consists of four tabs: Signature Policies, Signature Exceptions, Machine Learning Policies, and Inline Cloud Analysis1.  
? 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 responses1.

? 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 profile1.

? 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 analysis1.

? 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 traffic1.

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 202**  
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 204**  
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.		Universal
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.		Intrazone
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 and from zone B to zone A, but not traffic within zones A or B.		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 would apply to traffic from zone A to zone B and from zone B to zone A, but not traffic within zones A or B.	Universal
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. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.	Intrazone
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 and from zone B to zone A, but not traffic within zones A or 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.	Interzone

**NEW QUESTION 205**  
What are three differences between security policies and security profiles? (Choose three.)

- A. Security policies are attached to security profiles
- B. Security profiles are attached to security policies
- C. Security profiles should only be used on allowed traffic
- D. Security profiles are used to block traffic by themselves

E. Security policies can block or allow traffic

**Answer:** BCE

**NEW QUESTION 208**

Which two Palo Alto Networks security management tools provide a consolidated creation of policies, centralized management and centralized threat intelligence. (Choose two.)

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

**Answer:** BD

**NEW QUESTION 211**

What can be achieved by disabling the Share Unused Address and Service Objects with Devices setting on Panorama?

- A. Increase the backup capacity for configuration backups per firewall
- B. Increase the per-firewall capacity for address and service objects
- C. Reduce the configuration and session synchronization time between HA pairs
- D. Reduce the number of objects pushed to a firewall

**Answer:** D

**NEW QUESTION 215**

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 217**

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 219**

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 221**

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 226

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 230

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:**

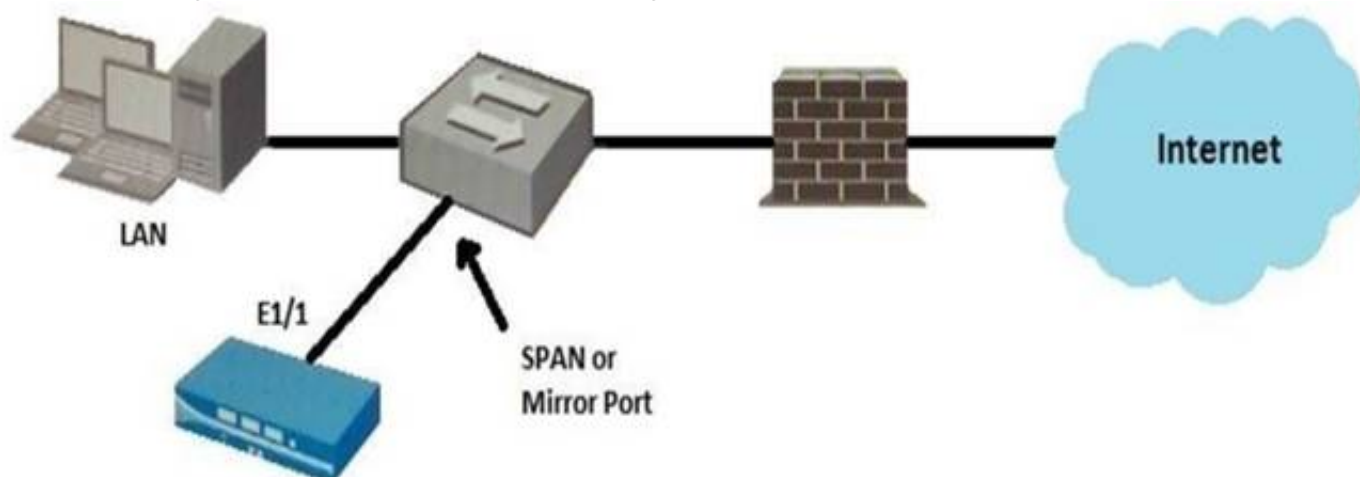
<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfaces>

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 232

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 237

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 238

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 242

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 245

An administrator is investigating a log entry for a session that is allowed and has the end reason of aged-out. Which two fields could help in determining if this is normal? (Choose two.)

- A. Packets sent/received
- B. IP Protocol
- C. Action
- D. Decrypted

**Answer:** BD

#### NEW QUESTION 248

Which type of address object is "10 5 1 1/0 127 248 2"?

- A. IP subnet
- B. IP wildcard mask
- C. IP netmask
- D. IP range

**Answer:** B

#### NEW QUESTION 252

Palo Alto Networks firewall architecture accelerates content map minimizing latency using which two components'? (Choose two )

- A. Network Processing Engine
- B. Policy Engine
- C. Single Stream-based Engine
- D. Parallel Processing Hardware

**Answer:** B

#### NEW QUESTION 255

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 259

An administrator wishes to follow best practices for logging traffic that traverses the firewall Which log setting is correct?

- A. Disable all logging
- B. Enable Log at Session End
- C. Enable Log at Session Start
- D. Enable Log at both Session Start and End

Answer: B

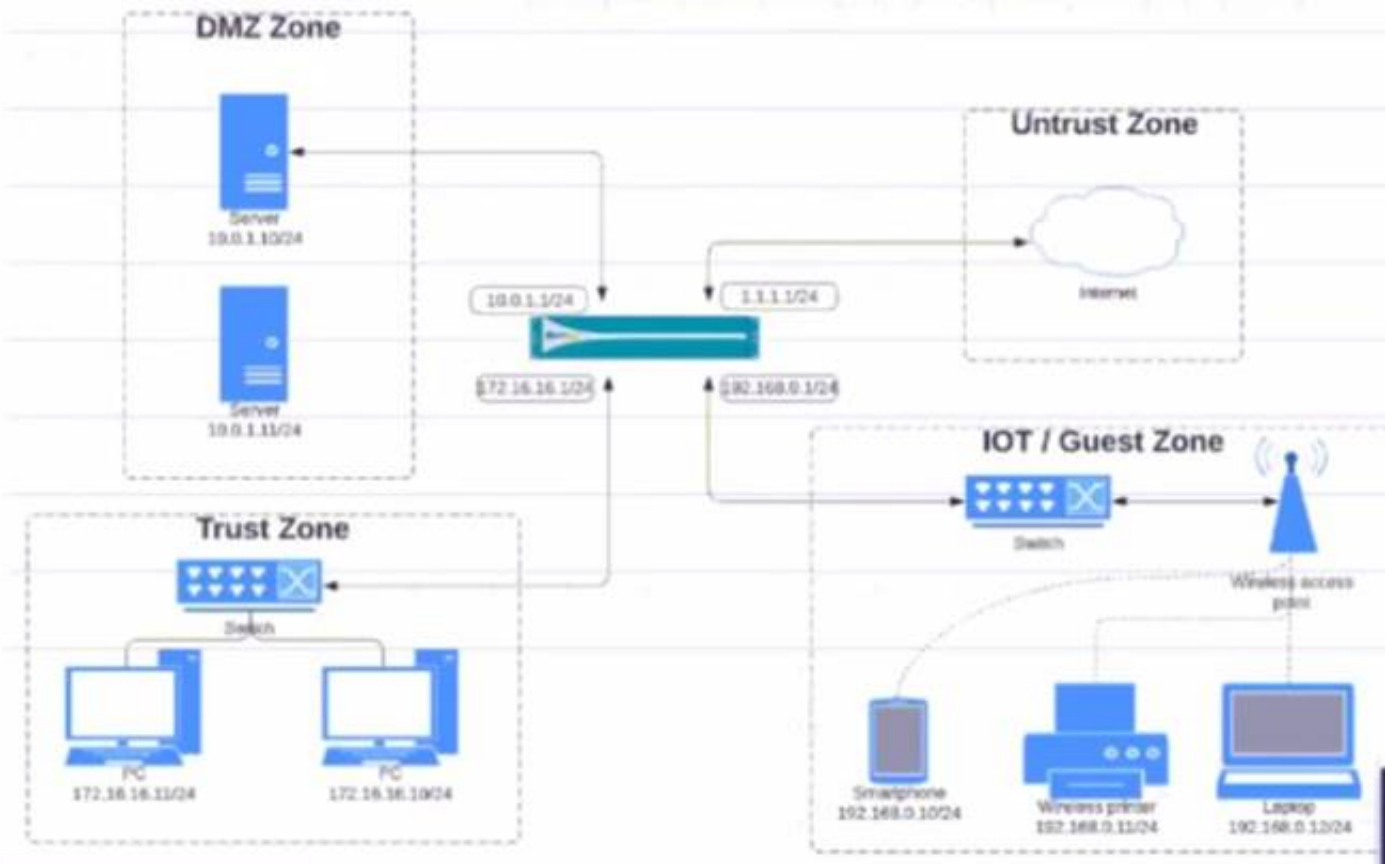
Explanation:

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clt5CAC>

NEW QUESTION 260

Given the network diagram, traffic should be permitted for both Trusted and Guest users to access general Internet and DMZ servers using SSH. web-browsing and SSL applications



Which policy achieves the desired results?

A)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
04-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	

B)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
03-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	1.1.1.0/
			Trust	192.168.0.0/24			Untrust	10.0.1.0

C)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
02-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	



D)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
01-A	none	universal	IoT-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/24
			Trust	172.16.16.0/12			Untrust	192.168.0.0/16

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

Answer: C

NEW QUESTION 265

How often does WildFire release dynamic updates?

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

Answer: A

NEW QUESTION 267

Why does a company need an Antivirus profile?

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 268

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 271

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 275

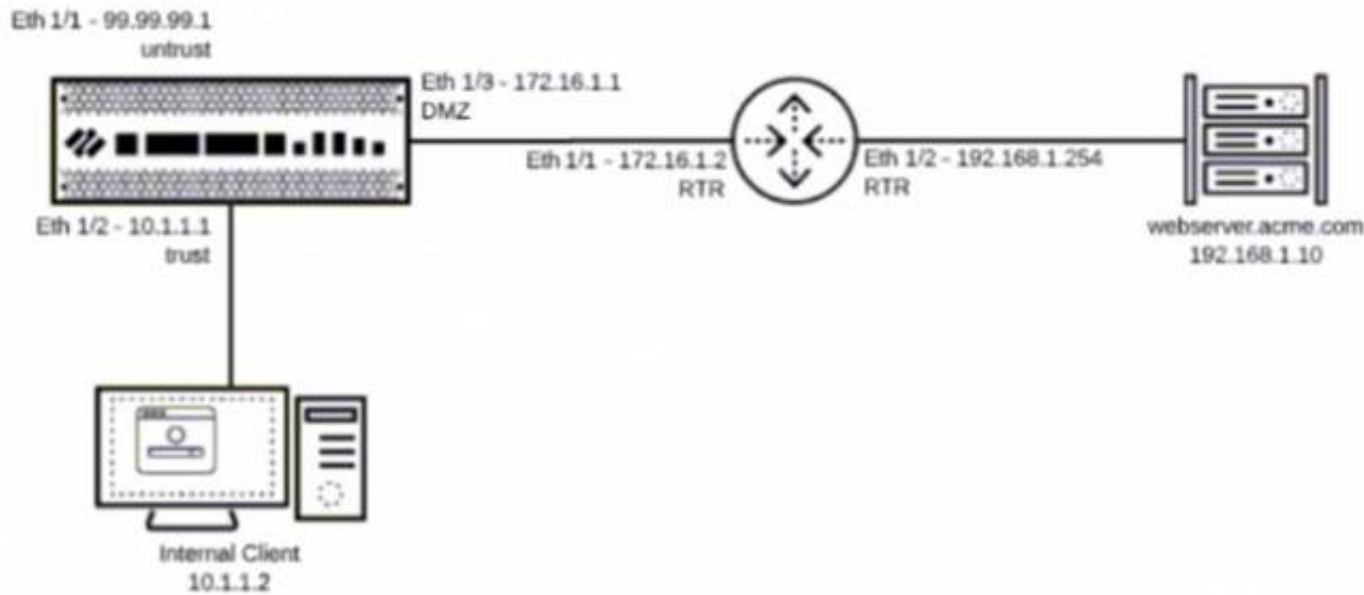
An administrator wants to create a NAT policy to allow multiple source IP addresses to be translated to the same public IP address. What is the most appropriate NAT policy to achieve this?

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

Answer: A

NEW QUESTION 277

You have been tasked to configure access to a new web server located in the DMZ  
Based on the diagram what configuration changes are required in the NGFW virtual router to route traffic from the 10.1.1.0/24 network to 192.168.1.0/24?



- A. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next- hop of 192.168 1.10
- B. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/2 with a next- hop of 172.16.1.2
- C. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next- hop of 172.16.1.2
- D. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next- hop of 192.168.1.254

**Answer: C**

#### NEW QUESTION 279

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 283

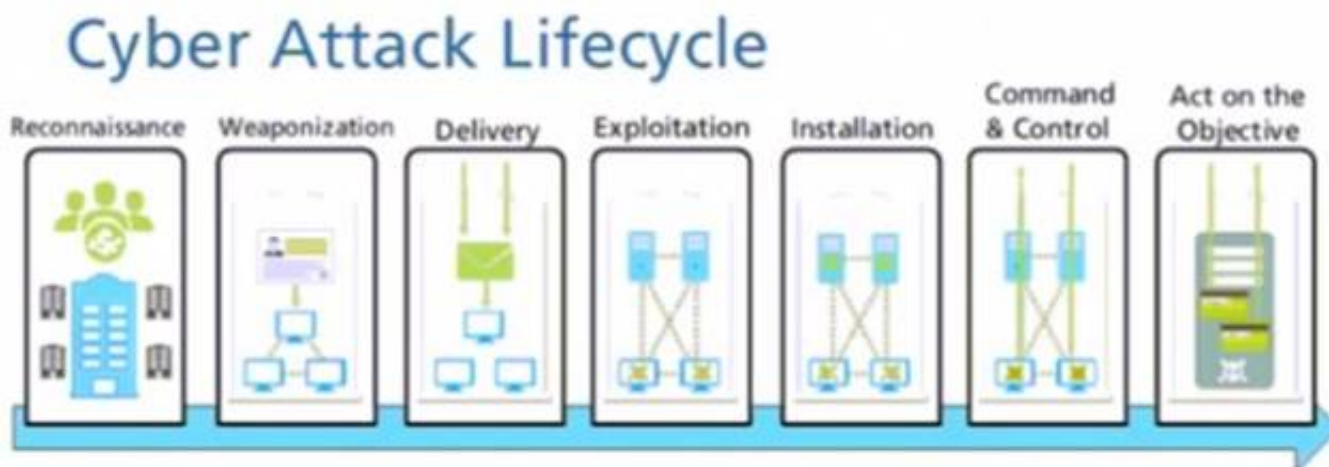
Where within the firewall GUI can all existing tags be viewed?

- A. Network > Tags
- B. Monitor > Tags
- C. Objects > Tags
- D. Policies > Tags

**Answer: C**

#### NEW QUESTION 285

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



Exploitation

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

**Answer: A**

#### NEW QUESTION 288

Which type firewall configuration contains in-progress configuration changes?

- A. backup
- B. running
- C. candidate
- D. committed

**Answer:** C

**NEW QUESTION 290**

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

- A. authentication
- B. decryption
- C 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 293**

How many zones can an interface be assigned with a Palo Alto Networks firewall?

- A. two
- B. three
- C. four
- D. one

**Answer:** D

**NEW QUESTION 294**

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 295**

An administrator is configuring a NAT rule

At a minimum, which three forms of information are required? (Choose three.)

- A. name
- B. source zone
- C. destination interface
- D. destination address
- E. destination zone

**Answer:** BDE

**NEW QUESTION 298**

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 301**

An administrator wants to prevent users from submitting corporate credentials in a phishing attack. Which Security profile should be applied?

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

Answer: B

NEW QUESTION 302

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 307

Which three filter columns are available when setting up an Application Filter? (Choose three.)

- A. Parent App

B. Category

C. Risk

D. Standard Ports

E. Subcategory

Answer: BCE

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects- application-filters>

NEW QUESTION 309

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 314

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 318

Access to which feature requires PAN-OS Filtering licens?

- 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 322

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 327

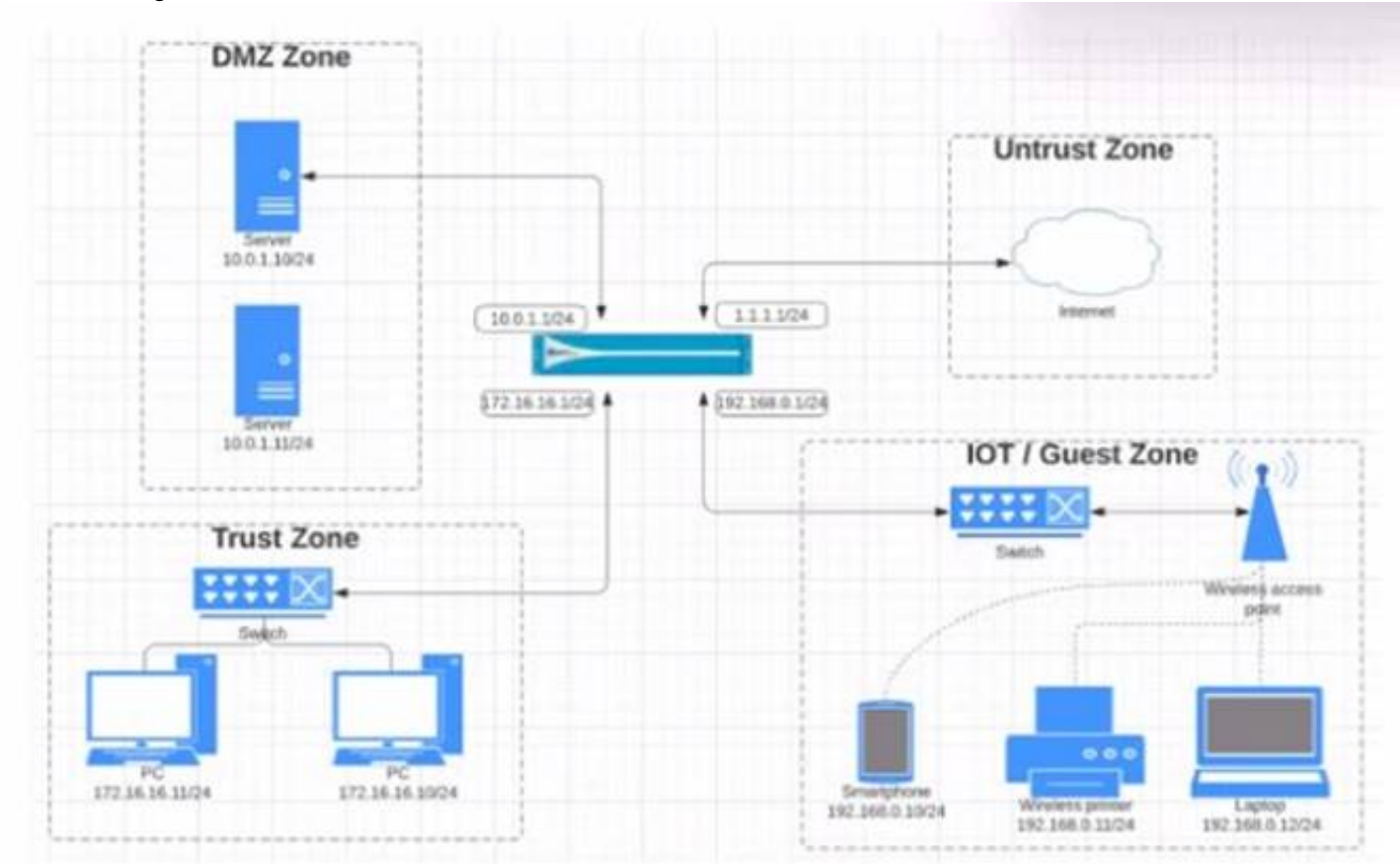
Starting with PAN\_OS version 9.1 which new type of object is supported for use within the user field of a security policy rule?

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

Answer: B

NEW QUESTION 329

View the diagram.



What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

A)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
00-A	None	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any	any	ssh	application-default
			Trust	192.168.0.0/24			Untrust			ssh	web-browsing

B)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
00-A	None	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	1.1.1.0/24	any	ssh	application-default
			Trust	192.168.0.0/24			Untrust	10.0.1.0/24		ssh	web-browsing

C)



NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
G1-A	none	server	K12-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/24	any	vpn	application-default
			Trust	172.16.16.0/12			Untrust	192.168.0/24		all	web-browsing

D)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		

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

**Answer:** C

**NEW QUESTION 334**

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 338**

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 339**

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 340**

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

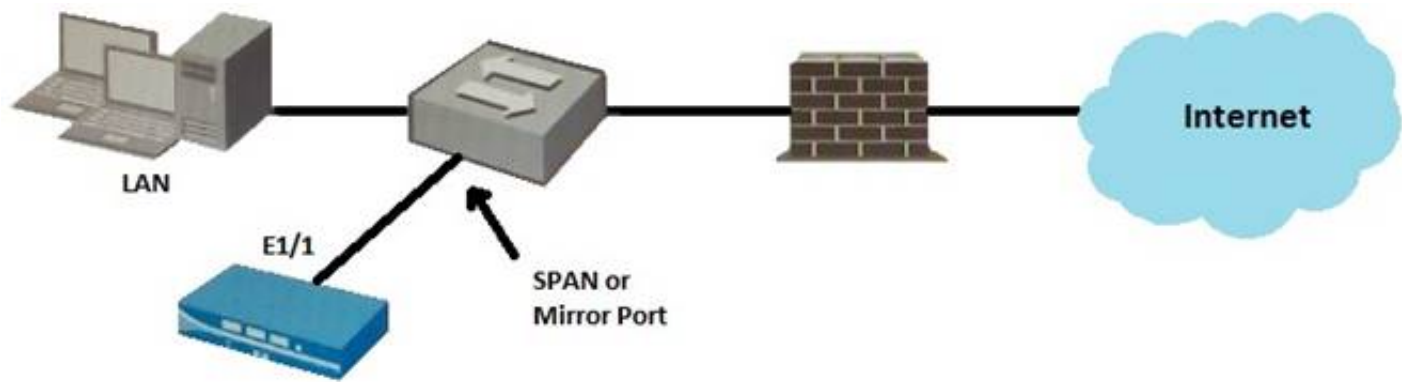
- A. Override
- B. Allow
- C. Block
- D. Continue

**Answer:** B

**NEW QUESTION 345**

Given the topology, which zone type should interface E1/1 be configured with?





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

Answer: A

NEW QUESTION 346

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

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

- Allows users to access IT applications on all ports
- A: 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 351

.....

## 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](#)**