



# Paloalto-Networks

## Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

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 2

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**

### NEW QUESTION 3

Which option is part of the content inspection process?

- A. IPsec tunnel encryption
- B. Packet egress process
- C. SSL Proxy re-encrypt
- D. Packet forwarding process

**Answer: C**

### NEW QUESTION 4

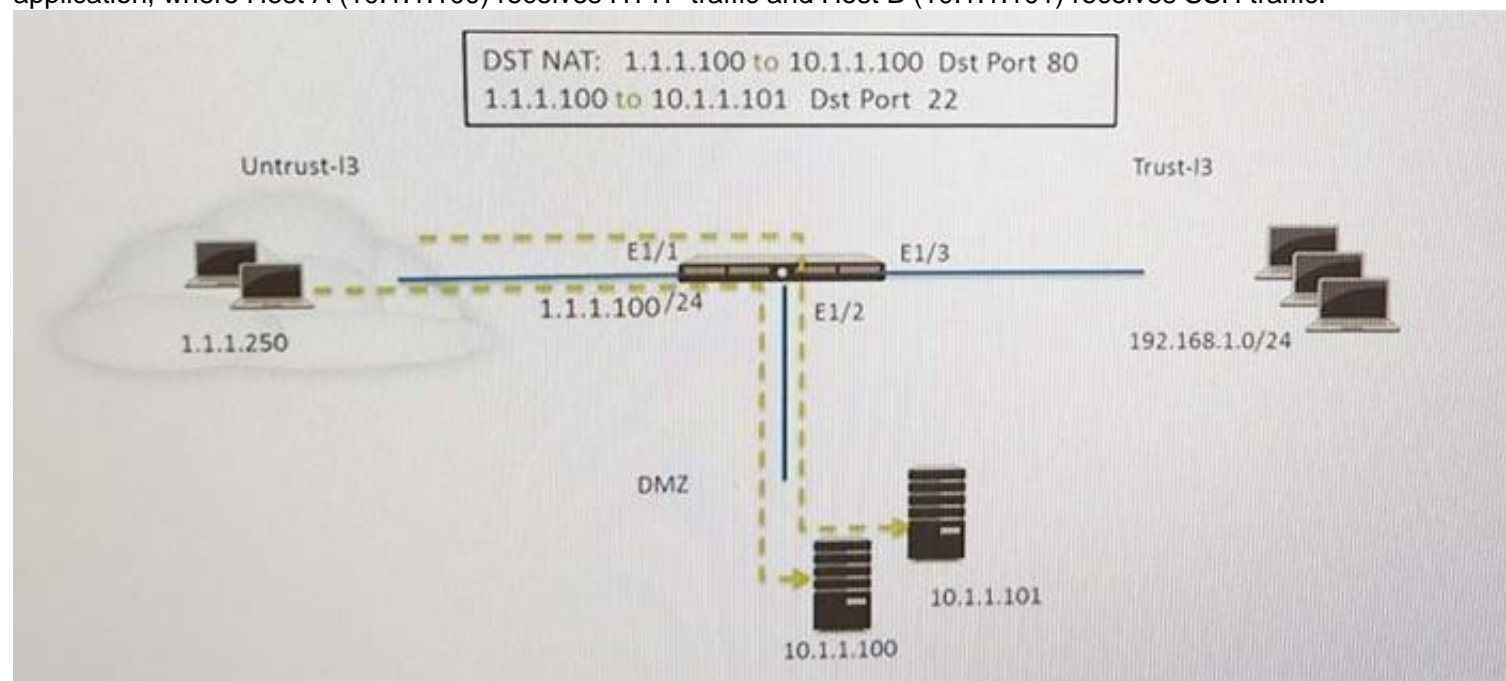
In which stage of the Cyber-Attack Lifecycle would the attacker inject a PDF file within an email?

- A. Weaponization
- B. Reconnaissance
- C. Installation
- D. Command and Control
- E. Exploitation

**Answer: A**

### NEW QUESTION 5

Refer to the exhibit. An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.



Which two Security policy rules will accomplish this configuration? (Choose two.)

- A. Untrust (Any) to DMZ (1.1.1.100), ssh - Allow
- B. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
- C. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
- D. Untrust (Any)to DMZ (10.1.1.100. 10.1.1.101), ssh, web-browsing-Allow
- E. Untrust (Any) to DMZ (1.1.1.100), web-browsing - Allow

**Answer: AE**

### NEW QUESTION 6

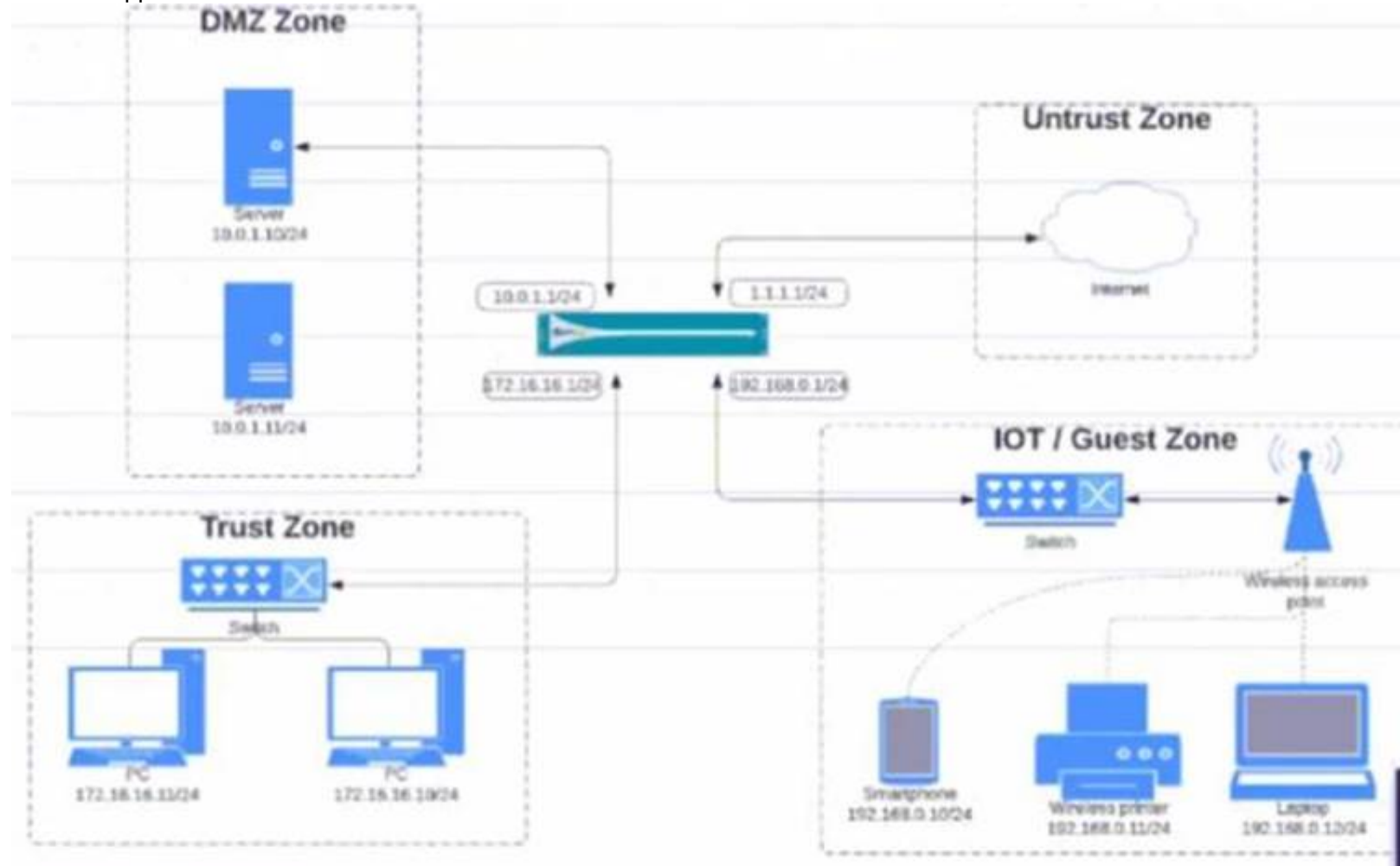
Which type security policy rule would match traffic flowing between the inside zone and outside zone within the inside zone and within the outside zone?

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

Answer: B

NEW QUESTION 7

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

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	172.16.16.0/24			Untrust	192.168.0.0/24

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

**Answer:** C

#### NEW QUESTION 8

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 9

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

#### NEW QUESTION 10

Which administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server.

Which security profile components will detect and prevent this threat after the firewall's signature database has been updated?

- A. antivirus profile applied to outbound security policies
- B. data filtering profile applied to inbound security policies
- C. data filtering profile applied to outbound security policies
- D. vulnerability profile applied to inbound security policies

**Answer:** C

#### NEW QUESTION 10

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

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

**Answer:** D

#### NEW QUESTION 11

An administrator is reviewing another administrator's Security policy log settings. Which log setting configuration is consistent with best practices for normal traffic?

- A. Log at Session Start and Log at Session End both enabled
- B. Log at Session Start disabled Log at Session End enabled
- C. Log at Session Start enabled Log at Session End disabled
- D. Log at Session Start and Log at Session End both disabled

**Answer:** B

#### NEW QUESTION 13

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 17

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.

Source Zone: Internal

Destination Zone: DMZ Zone

Application: \_\_\_\_\_?

Service: \_\_\_\_\_?

Action: allow

Choose two.

- A. Service = "any"



- B. Application = "Telnet"
- C. Service - "application-default"
- D. Application = "any"

**Answer:** BC

#### NEW QUESTION 22

Which update option is not available to administrators?

- A. New Spyware Notifications
- B. New URLs
- C. New Application Signatures
- D. New Malicious Domains
- E. New Antivirus Signatures

**Answer:** B

#### NEW QUESTION 26

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=kA10g000000ClomCAC>

#### NEW QUESTION 30

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 31

What is the minimum frequency for which you can configure the firewall to check for new WildFire antivirus signatures?

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

**Answer:** B

#### Explanation:

<b>WildFire</b>	Provides near real-time malware and antivirus signatures created as a result of the analysis done by the WildFire public cloud. WildFire signature updates are made available every five minutes. You can set the firewall to check for new updates as frequently as every minute to ensure that the firewall retrieves the latest WildFire signatures within a minute of availability. Without the WildFire subscription, you must wait at least 24 hours for the signatures to be provided in the Antivirus update.
-----------------	---

#### NEW QUESTION 35

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 36

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 41

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

- A. The running configuration with settings from the candidate configuration
- B. The candidate configuration with settings from the running configuration
- C. The device state with settings from another configuration
- D. Dynamic update scheduler settings

**Answer:** A

#### NEW QUESTION 45

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 47

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

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

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

**Answer:** C

#### NEW QUESTION 50

Which license must an administrator acquire prior to downloading Antivirus updates for use with the firewall?

- A. URL filtering
- B. Antivirus
- C. WildFire
- D. Threat Prevention

**Answer:** D

#### NEW QUESTION 54

Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?

- A. Threat Prevention License
- B. Threat Implementation License
- C. Threat Environment License
- D. Threat Protection License

**Answer:** A

#### NEW QUESTION 57

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

Detailed Log View

General

Session ID 781868  
Action drop  
Host ID  
Application dns  
Rule Outbound DNS  
Rule UUID ea9f3b96-e280-467c-aca5-0b1902857791  
Device SN 007251000156341  
IP Protocol udp  
Log Action global-logs  
Generated Time 2021/08/27 02:02:49  
Receive Time 2021/08/27 02:02:53  
Tunnel Type N/A

Source

Source User  
Source 192.168.101.25  
Source DAG  
Country 192.168.0.0-192.168.255.255  
Port 46282  
Zone Servers  
Interface ethernet1/4  
NAT IP 67.190.64.58  
NAT Port 26351  
X-Forwarded-For IP 0.0.0.0

Destination

Destination User  
Destination 8.8.4.4  
Destination DAG  
Country United States  
Port 53  
Zone Internet  
Interface ethernet1/8  
NAT IP 8.8.4.4  
NAT Port 53

Flags

Captive Portal

- 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 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. any port  
B. same port as ssl and snmpv3  
C. the default port  
D. only ephemeral ports

**Answer:** C

#### NEW QUESTION 64

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 67

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 72

Which Palo Alto network security operating platform component provides consolidated policy creation and centralized management?



- A. Prisma SaaS
- B. Panorama
- C. AutoFocus
- D. GlobalProtect

Answer: B

NEW QUESTION 76

In the example security policy shown, which two websites fcked? (Choose two.)

	Name	Tags	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Block-Sites	outbound	Inside	Any	Outside	Any	Any	any	Social-networking	Deny	None

- A. LinkedIn
- B. Facebook
- C. YouTube
- D. Amazon

Answer: AB

NEW QUESTION 80

The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering “gambling” category.

Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the “gambling” URL category?

- A. Add just the URL www.powerball.com to a Security policy allow rule.
- B. Manually remove powerball.com from the gambling URL category.
- C. Add \*.powerball.com to the URL Filtering allow list.
- D. Create a custom URL category, add \*.powerball.com to it and allow it in the Security Profile.

Answer: CD

NEW QUESTION 85

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

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

Answer: BC

NEW QUESTION 86

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

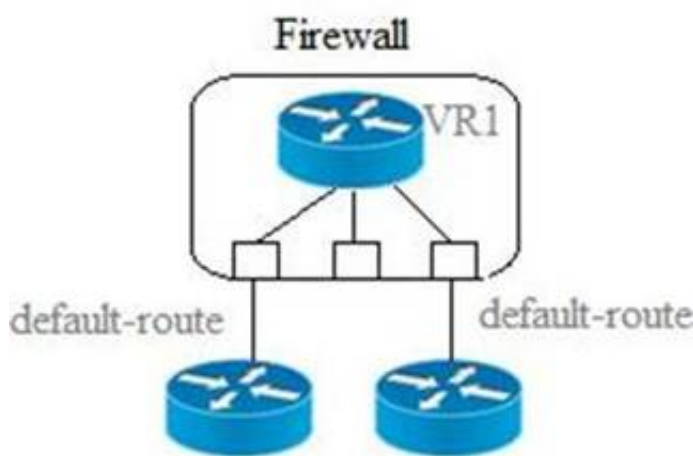
- A. Kerberos user
- B. SAML user
- C. local database user
- D. local user

Answer: B

NEW QUESTION 89

Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)

Multiple Static Default Routes



- A. Path monitoring does not determine if route is useable
- B. Route with highest metric is actively used
- C. Path monitoring determines if route is useable
- D. Route with lowest metric is actively used

**Answer:** CD

#### NEW QUESTION 93

What is a function of application tags?

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

**Answer:** C

#### NEW QUESTION 97

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

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

**Answer:** D

#### NEW QUESTION 98

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

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

**Answer:** AB

#### NEW QUESTION 99

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 looks ups 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 101

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

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

**Answer:** B

#### NEW QUESTION 105

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 110

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**

#### NEW QUESTION 112

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 115

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 120

For the firewall to use Active Directory to authenticate users, which Server Profile is required in the Authentication Profile?

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

**Answer: C**

#### NEW QUESTION 123

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

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

**Answer: AB**

#### NEW QUESTION 124

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 129

Which the app-ID application will you need to allow in your security policy to use facebook-chat?

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

**Answer:** BD

#### NEW QUESTION 131

Which built-in IP address EDL would be useful for preventing traffic from IP addresses that are verified as unsafe based on WildFire analysis Unit 42 research and data gathered from telemetry?

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

**Answer:** D

#### Explanation:

➤ Palo Alto Networks Known Malicious IP Addresses

—Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry (Share ThreatIntelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.  
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built->

#### NEW QUESTION 136

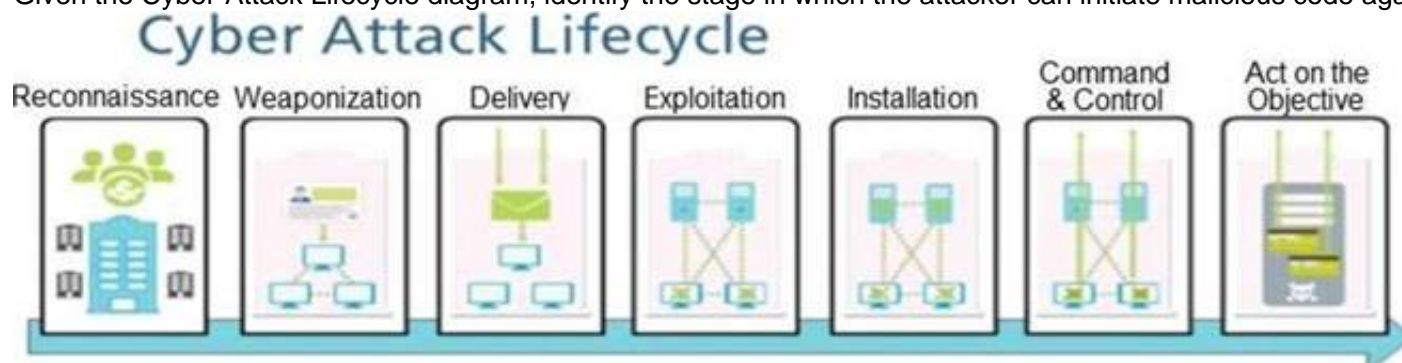
Which URL Filtering profile action would you set to allow users the option to access a site only if they provide a URL admin password?

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

**Answer:** B

#### NEW QUESTION 137

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



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

**Answer:** A

#### NEW QUESTION 141

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

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

**Answer:** A

#### NEW QUESTION 142

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

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

**Answer:** ABD

#### NEW QUESTION 143

Which Security policy action will message a user's browser that their web session has been terminated?

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

**Answer:** B

#### NEW QUESTION 146

Which tab would an administrator click to create an address object?

- A. Device
- B. Policies
- C. Monitor
- D. Objects

**Answer:** D

#### NEW QUESTION 148

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 153

Which statement best describes the use of Policy Optimizer?

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

**Answer:** B

#### NEW QUESTION 157

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. save named configuration snapshot
- B. export device state
- C. export named configuration snapshot
- D. save candidate config

**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 159

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

- A. 80
- B. 8443
- C. 4443
- D. 443

**Answer:** C



**NEW QUESTION 162**

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-overvie>

**NEW QUESTION 166**

Which prevention technique will prevent attacks based on packet count?

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

**Answer:** A

**NEW QUESTION 167**

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 172**

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

**NEW QUESTION 174**

Match each rule type with its example

	Answer Area	
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:**

	Answer Area	
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 177

Order the steps needed to create a new security zone with a Palo Alto Networks firewall.

Step 1	Drag answer here	Select Zones from the list of available items
Step 2	Drag answer here	Assign interfaces as needed
Step 3	Drag answer here	Select Network tab
Step 4	Drag answer here	Specify Zone Name
Step 5	Drag answer here	Select Add
Step 6	Drag answer here	Specify Zone Type

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

- Step 1 – Select network tab  
Step 2 – Select zones from the list of available items  
Step 3 – Select Add  
Step 4 – Specify Zone Name

Step 5 – Specify Zone Type  
Step 6 – Assign interfaces as needed

#### NEW QUESTION 181

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

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

**Answer:** A

#### NEW QUESTION 185

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

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

**Answer:** A

#### NEW QUESTION 186

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#:~:tex>

#### NEW QUESTION 187

Which two matching criteria are used when creating a Security policy involving NAT? (Choose two.)

- A. Post-NAT address
- B. Post-NAT zone
- C. Pre-NAT zone
- D. Pre-NAT address

**Answer:** BD

#### NEW QUESTION 191

Place the following steps in the packet processing order of operations from first to last.

content inspection		first
QOS shaping applied		second
Security policy lookup		third
DoS protection		fourth

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:



## Answer Area

	DoS protection	first
	Security policy lookup	second
	content inspection	third
	QOS shaping applied	fourth

### NEW QUESTION 192

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**

### NEW QUESTION 194

An administrator would like to see the traffic that matches the interzone-default rule in the traffic logs. What is the correct process to enable this logging?

- A. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session Start and click OK
- B. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session End and click OK
- C. This rule has traffic logging enabled by default no further action is required
- D. Select the interzone-default rule and click Override on the Actions tab select Log at Session End and click OK

**Answer: D**

### NEW QUESTION 195

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

	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. 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 197

An administrator would like to block access to a web server, while also preserving resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)

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

**Answer: AC**

### NEW QUESTION 198

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 202

Which path is used to save and load a configuration with a Palo Alto Networks firewall?

- A. Device>Setup>Services
- B. Device>Setup>Management

- C. Device>Setup>Operations
- D. Device>Setup>Interfaces

Answer: C

NEW QUESTION 207

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 212

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

App Usage

	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE	MODIFIED	CREATED
55	Outbound Traffic	application default	1.7T	any	192	258	Compliant	2022-01-06 18:30:02	2020-11-16
25	Outbound Traffic	application default	6.3G	any	29	447	Compliant	2022-01-06 18:30:02	2020-11-16
29	Outbound Traffic	application default	952.3M	any	2	448	Compliant	2022-01-06 18:30:02	2020-11-16
20	Outbound Traffic	application default	508.0M	any	75	448	Compliant	2022-01-06 18:30:02	2020-11-16
31	Outbound Traffic	application default	235.1M	any	7	448	Compliant	2022-01-06 18:30:02	2020-11-16
32	Outbound Traffic	application default	140.8M	any	1	448	Compliant	2022-01-06 18:30:02	2020-11-16
47	Outbound Traffic	application default	23.1M	any	5	448	Compliant	2022-01-06 18:30:02	2020-11-16
27	Outbound Traffic	application default	22.8M	any	2	448	Compliant	2022-01-06 18:30:02	2020-11-16
30	Outbound Traffic	application default	1.2M	any	1	445	Compliant	2022-01-06 18:30:02	2020-11-16
28	Outbound Traffic	application default	590.2k	any	1	445	Compliant	2022-01-06 18:30:02	2020-11-16
17	Outbound Traffic	application default	0	any	2	452	Compliant	2022-01-06 18:30:02	2020-11-16
24	Outbound Traffic	application default	0	any	1	459	Compliant	2022-01-06 18:30:02	2020-11-16

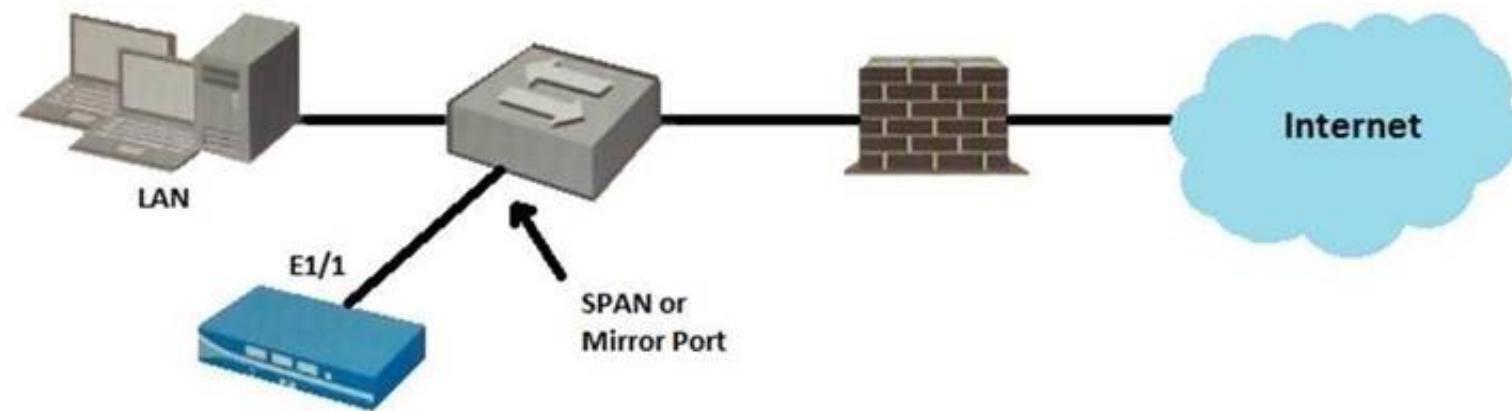
- A. Rules without App Controls
- B. New App Viewer
- C. Rule Usage
- D. Unused Unused Apps

Answer: C

NEW QUESTION 213

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 215

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

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

**Answer:** C

#### NEW QUESTION 219

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 221

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

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

**Answer:** C

#### NEW QUESTION 225

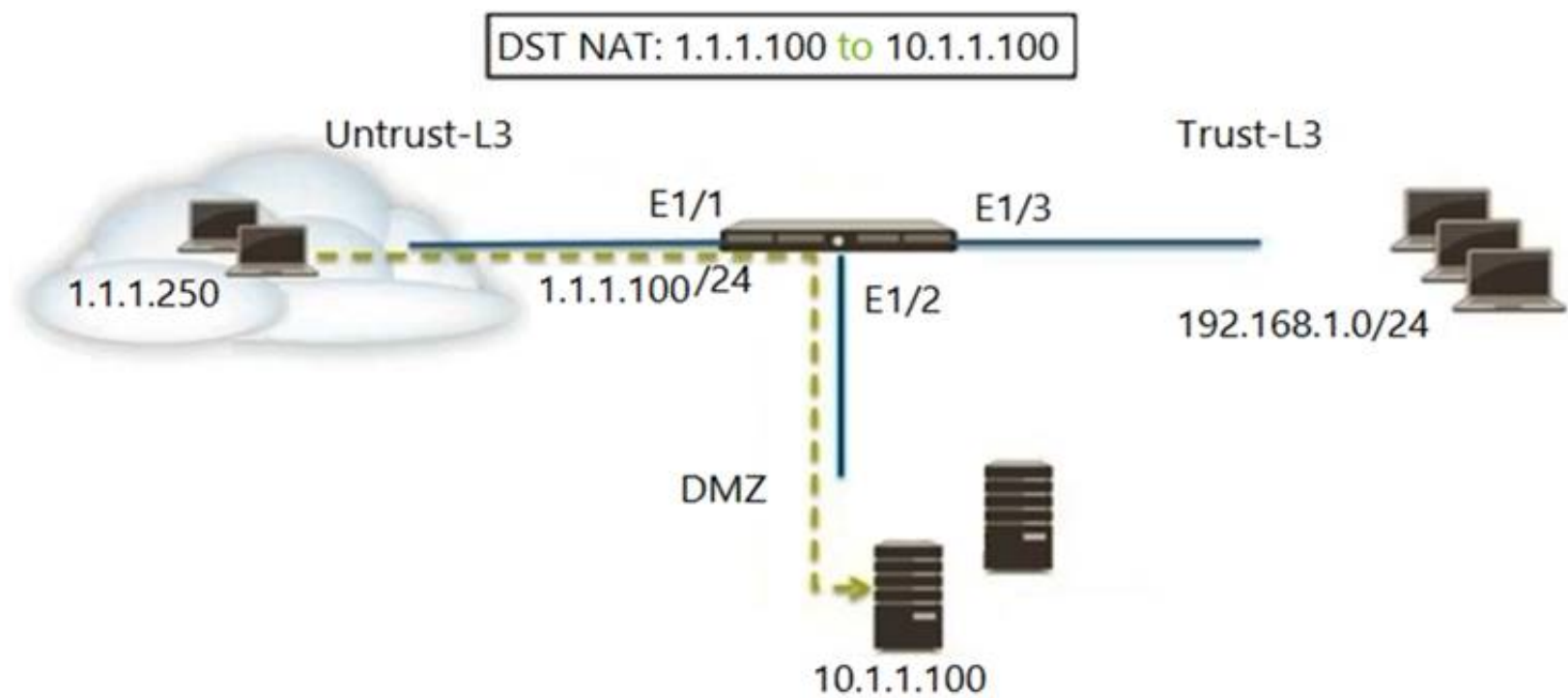
How are Application Fillers or Application Groups used in firewall policy?

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

**Answer:** B

#### NEW QUESTION 230

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. Untrust (any) to DMZ (10.1.1.100), web browsing -Allow
- B. Untrust (any) to Untrust (1.1.1.100), web browsing - Allow
- C. Untrust (any) to Untrust (10.1.1.100), web browsing -Allow
- D. Untrust (any) to DMZ (1.1.1.100), web browsing - Allow

Answer: D

NEW QUESTION 232

You receive notification about a new malware that infects hosts. An infection results in the infected host attempting to contact a command-and-control server. Which Security Profile when applied to outbound Security policy rules detects and prevents this threat from establishing a command-and-control connection?

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

Answer: D

Explanation:

Anti-Spyware Security Profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients.

NEW QUESTION 233

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 236

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

	Answer Area	
reconnaissance	<input type="text"/>	stage that reveals the attacker's motivation
installation	<input type="text"/>	stage where the attacker scans for network
command and control	<input type="text"/>	exploited
act on the objectives	<input type="text"/>	stage where the attacker will explore methods of persistence
	<input type="text"/>	stage where the attacker has access to a system

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

reconnaissance

installation

command and control

act on the objectives

Answer Area

reconnaissance

installation

command and control

act on the objectives

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

NEW QUESTION 240

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

No App Specified

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

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

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

Answer: C

NEW QUESTION 245

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 249

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 253

Starting with PAN-OS version 9.1, application dependency information is now reported in which two locations? (Choose two.)

- A. on the App Dependency tab in the Commit Status window
- B. on the Policy Optimizer's Rule Usage page
- C. on the Application tab in the Security Policy Rule creation window
- D. on the Objects > Applications browser pages

Answer: AC

NEW QUESTION 256

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

- A. change the logging action on the rule
- B. review the System Log

- C. refresh the Traffic Log
- D. tune your Traffic Log filter to include the dates

**Answer:** A

#### NEW QUESTION 257

What is the main function of Policy Optimizer?

- A. reduce load on the management plane by highlighting combinable security rules
- B. migrate other firewall vendors' security rules to Palo Alto Networks configuration
- C. eliminate "Log at Session Start" security rules
- D. convert port-based security rules to application-based security rules

**Answer:** D

#### NEW QUESTION 258

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 262

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 267

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 269

An administrator would like to override the default deny action for a given application and instead would like to block the traffic and send the ICMP code "communication with the destination is administratively prohibited"  
Which security policy action causes this?

- A. Drop
- B. Drop, send ICMP Unreachable
- C. Reset both
- D. Reset server

**Answer:** B

#### NEW QUESTION 271

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

#### NEW QUESTION 274

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

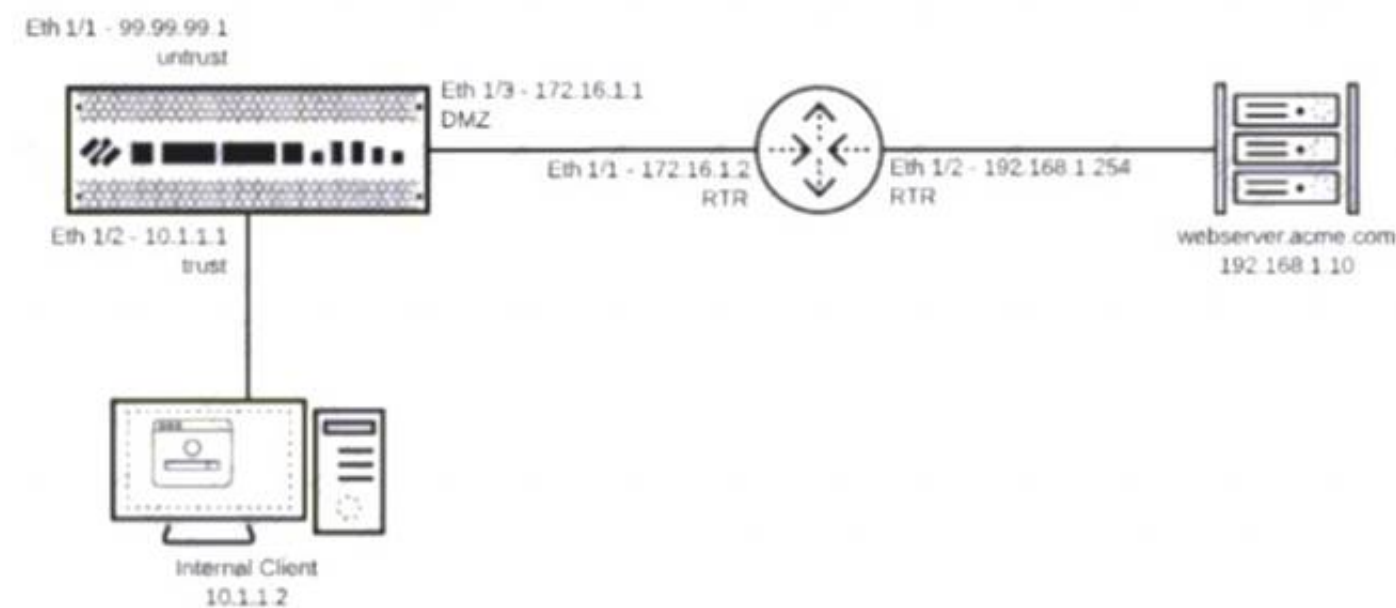


Answer: D

#### NEW QUESTION 275

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 280

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 285

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

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

Answer: ABD

#### NEW QUESTION 286

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

#### NEW QUESTION 288

In a security policy what is the quickest way to reset all policy rule hit counters to zero?

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

Answer: C

#### NEW QUESTION 290

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

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



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

**Answer:** CD

#### NEW QUESTION 294

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

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

**Answer:** AD

#### Explanation:

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

#### NEW QUESTION 296

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

- A. enabling the Content-ID filter
- B. administrative management services
- C. restricting HTTP and telnet using App-ID
- D. permitted IP addresses

**Answer:** AC

#### NEW QUESTION 297

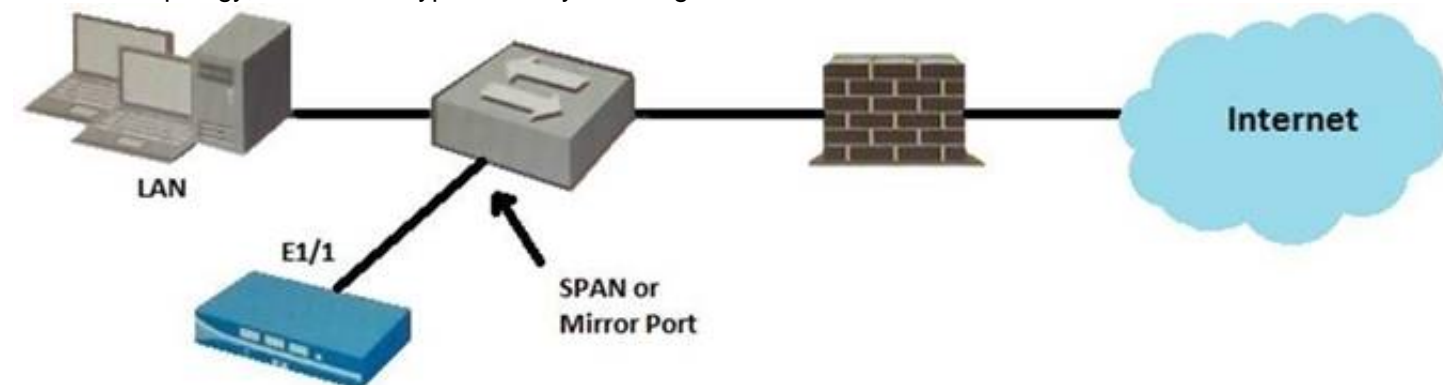
Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two.)

- A. GlobalProtect agent
- B. XML API
- C. User-ID Windows-based agent
- D. log forwarding auto-tagging

**Answer:** BC

#### NEW QUESTION 299

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 303

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

Palo Alto Networks User-ID Agent Setup

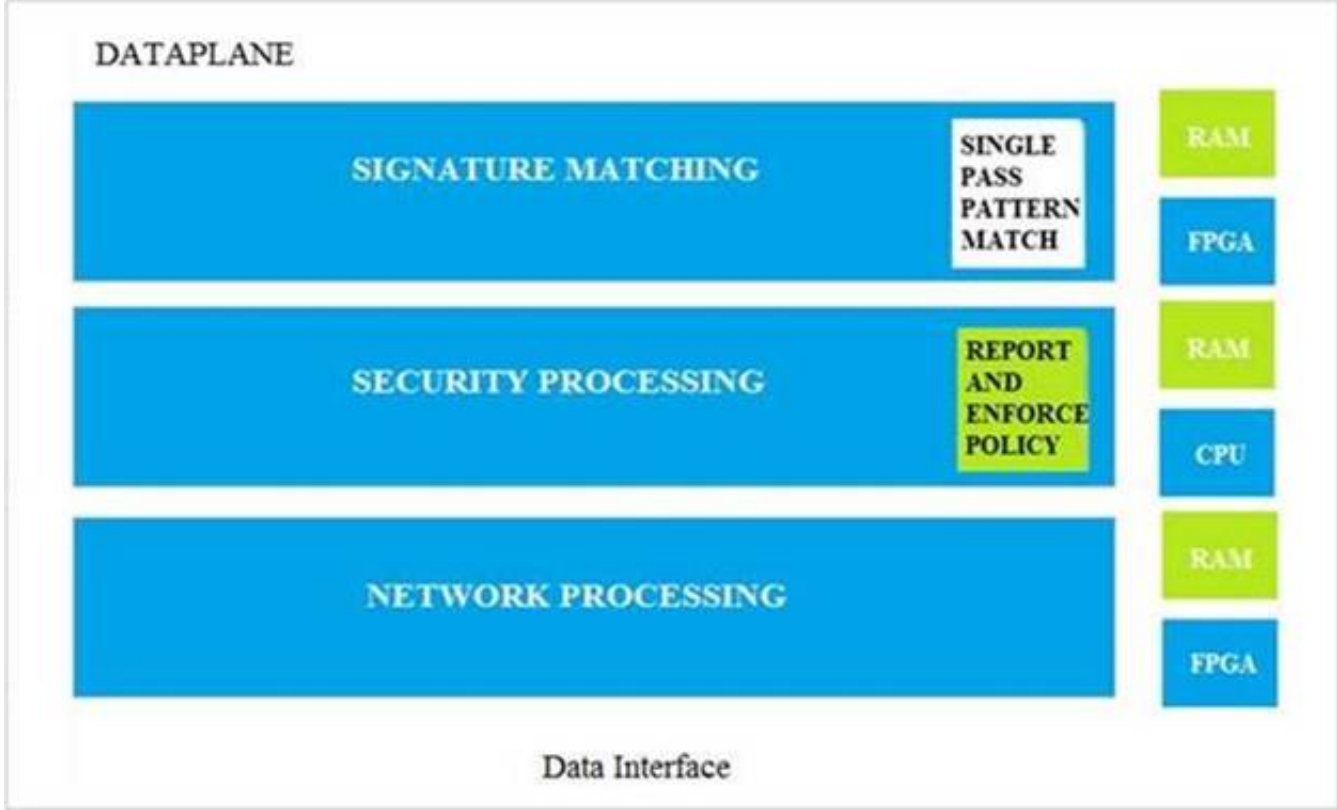
Enable Security Log ✓  
Server Log Monitor Frequency (sec) **15**  
Enable Session ✓  
Server Session Read Frequency (sec) **10**  
Novell eDirectory Query Interval (sec) **30**  
Syslog Service Profile  
Enable Probing  
Probe Interval (min) **20**  
Enable User Identification Timeout ✓  
User Identification 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 304

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 309

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

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

**Answer:** D

#### NEW QUESTION 312

Which statement is true regarding a Prevention Posture Assessment?

- A. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
- B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
- C. It provides a percentage of adoption for each assessment area
- D. It performs over 200 security checks on Panorama/firewall for the assessment

**Answer:** B

#### NEW QUESTION 315

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?

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

**Answer:** C

#### NEW QUESTION 316

Which interface does not require a MAC or IP address?

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

**Answer:** A

#### NEW QUESTION 318

How frequently can wildfire updates be made available to firewalls?

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

**Answer:** D

#### NEW QUESTION 321

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 324

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 329

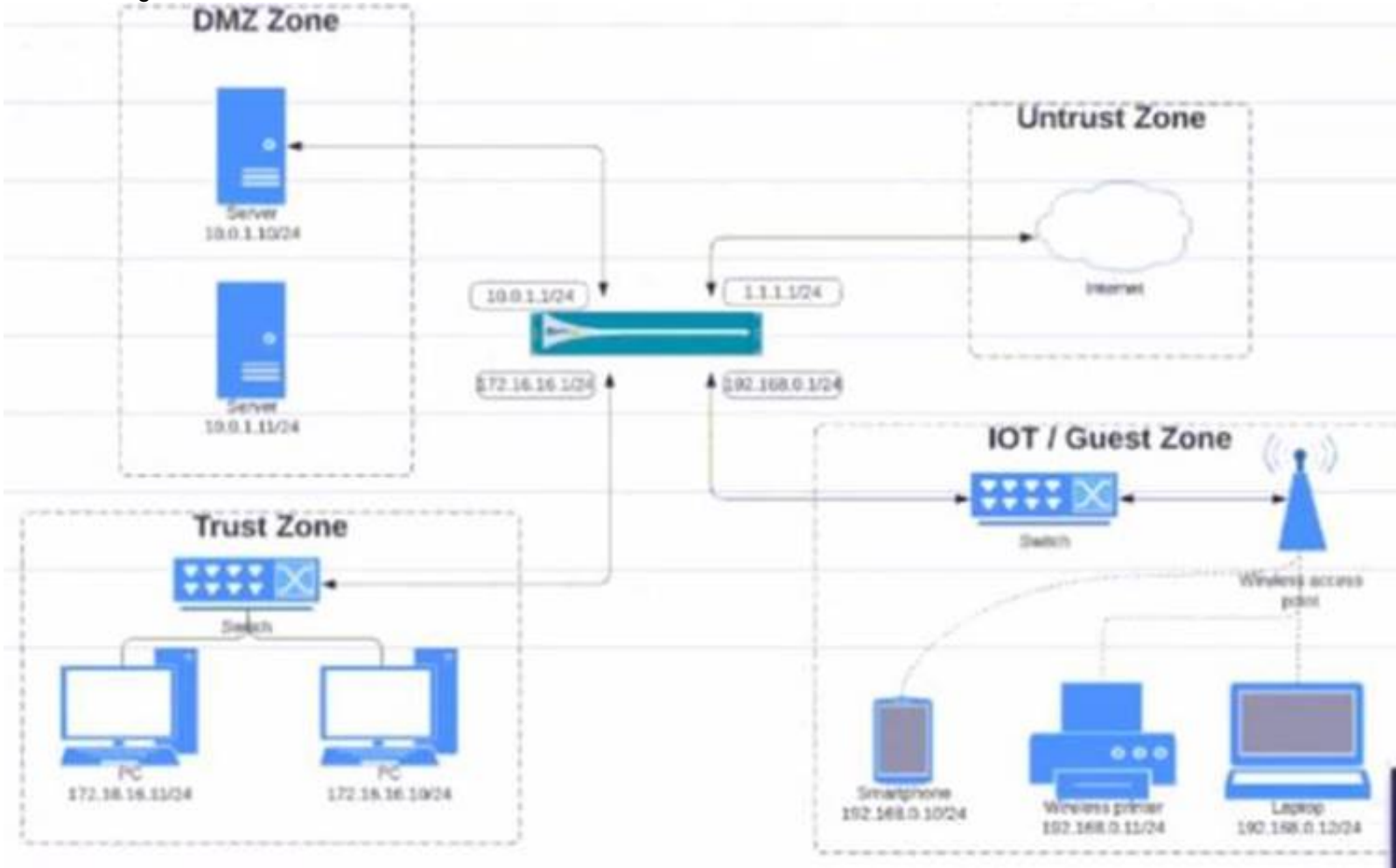
A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT, Finance, and HR. Which two types of traffic will the rule apply to? (Choose two)

- A. traffic between zone IT and zone Finance
- B. traffic between zone Finance and zone HR
- C. traffic within zone IT
- D. traffic within zone HR

**Answer:** CD

NEW QUESTION 334

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

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	172.16.16.0/24			Untrust	192.168.0.0/24

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

Answer: C

NEW QUESTION 337

An administrator needs to allow users to use only certain email applications.



How should the administrator configure the firewall to restrict users to specific email applications?

- A. Create an application filter and filter it on the collaboration category, email subcategory.
- B. Create an application group and add the email applications to it.
- C. Create an application filter and filter it on the collaboration category.
- D. Create an application group and add the email category to it.

**Answer:** B

#### NEW QUESTION 338

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



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

**Answer:** A

#### NEW QUESTION 340

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

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

**Answer:** C

#### NEW QUESTION 342

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

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

**Answer:** B

#### NEW QUESTION 346

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

- A. GlobalProtect



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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 347**

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 349**

Which type firewall configuration contains in-progress configuration changes?

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

**Answer:** C

**NEW QUESTION 351**

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 356**

Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

	FROM										SESSION END						
TYPE	ZONE	TO ZONE	INGRESS IF	SOURCE	NAT	APPLIED	EGRESS IF	DESTINATION	PORT	APPLICATION	ACTION	REASON	BYTES	ACTION	LOG	BYTES	BYTES
																SENT	RECEIVED
end	LAN	Internet	ethernet1/2	192.168.200.100	yes		ethernet1/5	198.54.12.97	443	web-browsing	allow	threat	5.8K	from-policy	default	2.7K	541
																	traffic

- A. The web session was unsuccessfully decrypted.
- B. The traffic was denied by security profile.
- C. The traffic was denied by URL filtering.
- D. The web session was decrypted.

**Answer:** D

**NEW QUESTION 361**

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

**NEW QUESTION 363**

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

#### NEW QUESTION 367

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

#### NEW QUESTION 370

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 375

.....

## Relate Links

**100% Pass Your PCNSA Exam with ExamBible Prep Materials**

<https://www.exambible.com/PCNSA-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>