

Actual exam question from Palo Alto Networks's PCNSA

Question #: 1

Topic #: 1

[\[All PCNSA Questions\]](#)

DRAG DROP -

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

Select and Place:

**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.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 2

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 3

Topic #: 1

[\[All PCNSA Questions\]](#)

---

A security administrator has configured App-ID updates to be automatically downloaded and installed. The company is currently using an application identified by App-ID as SuperApp\_base.

On a content update notice, Palo Alto Networks is adding new app signatures labeled SuperApp\_chat and SuperApp\_download, which will be deployed in 30 days.

Based on the information, how is the SuperApp traffic affected after the 30 days have passed?

- A. All traffic matching the SuperApp\_chat, and SuperApp\_download is denied because it no longer matches the SuperApp-base application
- B. No impact because the apps were automatically downloaded and installed
- C. No impact because the firewall automatically adds the rules to the App-ID interface
- D. All traffic matching the SuperApp\_base, SuperApp\_chat, and SuperApp\_download is denied until the security administrator approves the applications

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 4

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 5

Topic #: 1

[\[All PCNSA Questions\]](#)

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

Show Suggested Answer

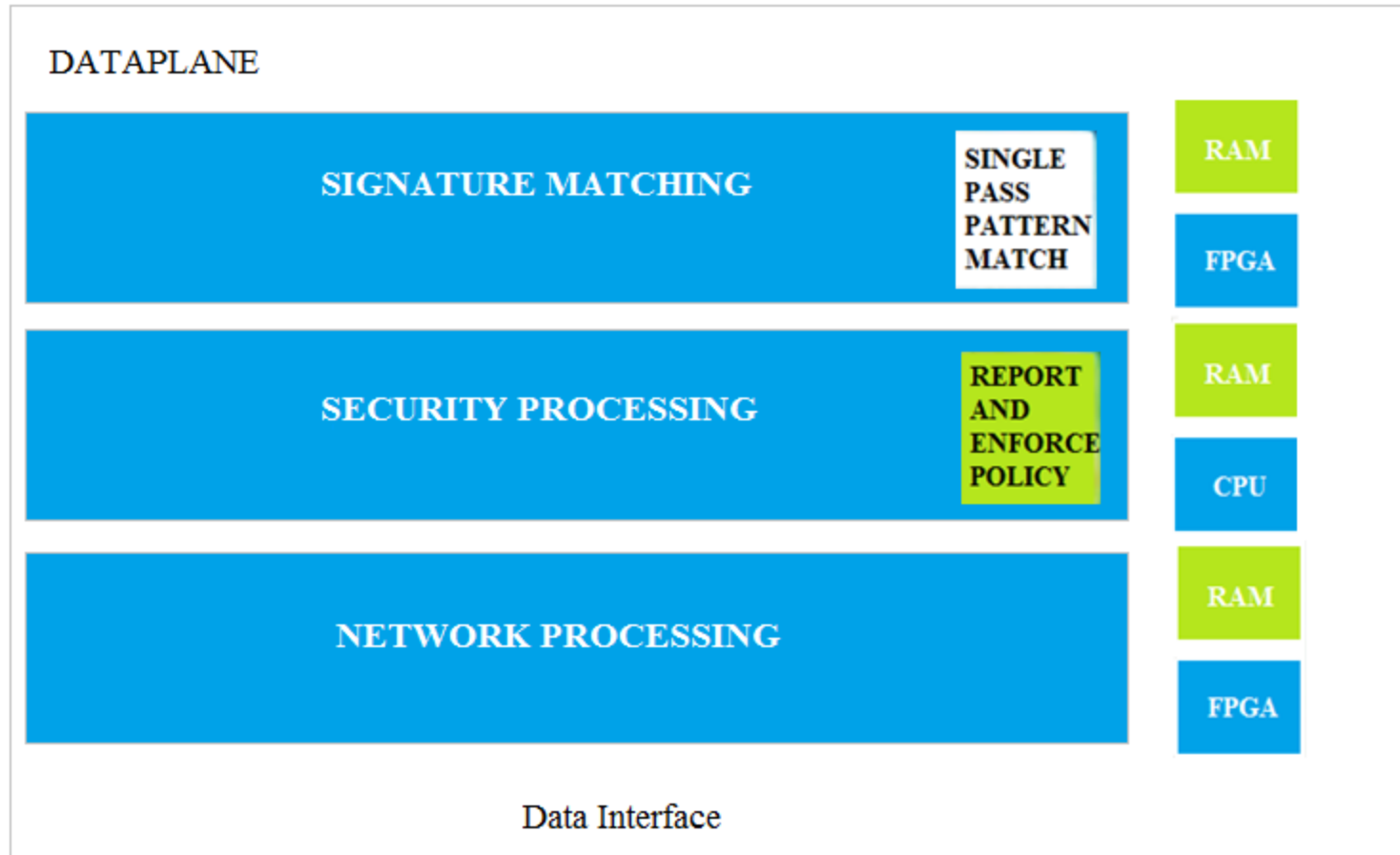
Actual exam question from Palo Alto Networks's PCNSA

Question #: 6

Topic #: 1

[\[All PCNSA Questions\]](#)

Which dataplane layer of the graphic shown provides pattern protection for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 7

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which option shows the attributes that are selectable when setting up application filters?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 8

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 9

Topic #: 1

[\[All PCNSA Questions\]](#)

DRAG DROP -

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

Select and Place:

*reconnaissance*

*installation*

*command and control*

*act on the objective*

**Answer Area**

stage that reveals the attacker's motivation for attacking a network

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

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 10

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

- A. Updated application content might 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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 11

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 12

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

- A. Create an Application Filter and name it Office Programs, then filter it on the business-systems category, office-programs subcategory
- B. Create an Application Group and add business-systems to it
- C. Create an Application Filter and name it Office Programs, then filter it on the business-systems category
- D. Create an Application Group and add Office 365, Evernote, Google Docs, and Libre Office

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 13

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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 area
- 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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 14

Topic #: 1

[\[All PCNSA Questions\]](#)

Employees are shown an application block page when they try to access YouTube. Which security policy is blocking the YouTube application?

	Name	Type	Source		Destination		Application	Service	URL Category	Action	Profile
			Zone	Address	Zone	Address					
1	Deny Google	universal	Inside	any	Outside	any	google-docs-base	application-d...	any	Deny	none
2	allowed-security serv...	universal	Inside	any	Outside	any	snmpv3 ssh ssl	application-d...	any	Allow	none
3	intrazone-default	intrazone	any	any	(intrazone)	any	any	any	any	Allow	none
4	interzone-default	interzone	any	any	any	any	any	any	any	Deny	none

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSA

Question #: 15

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 16

Topic #: 1

[\[All PCNSA Questions\]](#)

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

The screenshot shows the 'NAT Policy Rule' configuration window with the 'Translated Packet' tab selected. It is divided into two main sections: 'Source Address Translation' and 'Destination Address Translation'. The 'Source Address Translation' section contains four dropdown menus: 'Translation Type', 'Address Type', 'Interface', and 'IP Address'. The 'Destination Address Translation' section contains one dropdown menu labeled 'Translation Type' with the value 'None' selected. 'OK' and 'Cancel' buttons are located at the bottom right of the window.

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 17

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which interface does not require a MAC or IP address?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 18

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 19

Topic #: 1

[\[All PCNSA Questions\]](#)

DRAG DROP -

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

Select and Place:

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 20

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What are two differences between an implicit dependency and an explicit dependency in App-ID? (Choose two.)

- A. An implicit dependency does not require the dependent application to be added in the security policy
- B. An implicit dependency requires the dependent application to be added in the security policy
- C. An explicit dependency does not require the dependent application to be added in the security policy
- D. An explicit dependency requires the dependent application to be added in the security policy

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 21

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSA

Question #: 22

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which two App-ID applications will you need to allow in your Security policy to use facebook-chat? (Choose two.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 23

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 24

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 25

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

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

Show Suggested Answer



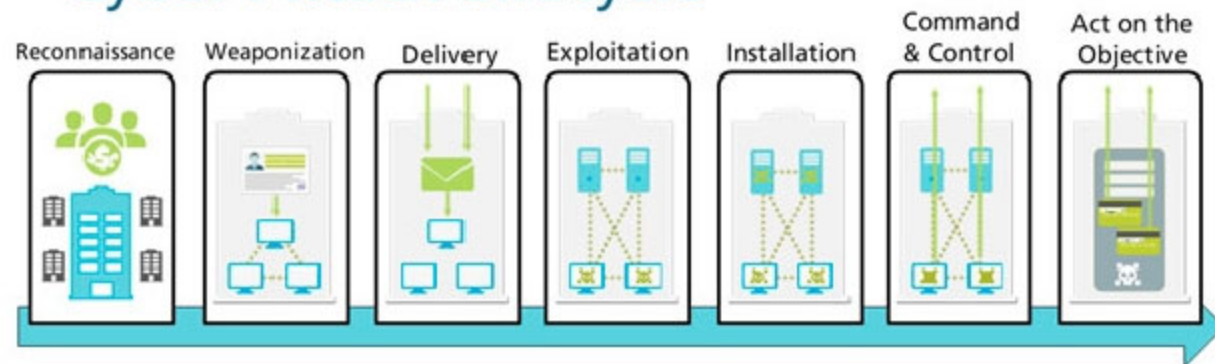
Actual exam question from Palo Alto Networks's PCNSA

Question #: 26

Topic #: 1

[\[All PCNSA Questions\]](#)

## Cyber Attack Lifecycle



At which stage of the Cyber-Attack Lifecycle would the attacker attach an infected PDF file to an email?

- A. Delivery
- B. Reconnaissance
- C. Command and Control
- D. Exploitation

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSA

Question #: 27

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

A. 2-3-4-1

B. 1-4-3-2

C. 3-1-2-4

D. 1-3-2-4

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 28

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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"

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 29

Topic #: 1

[\[All PCNSA Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 30

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



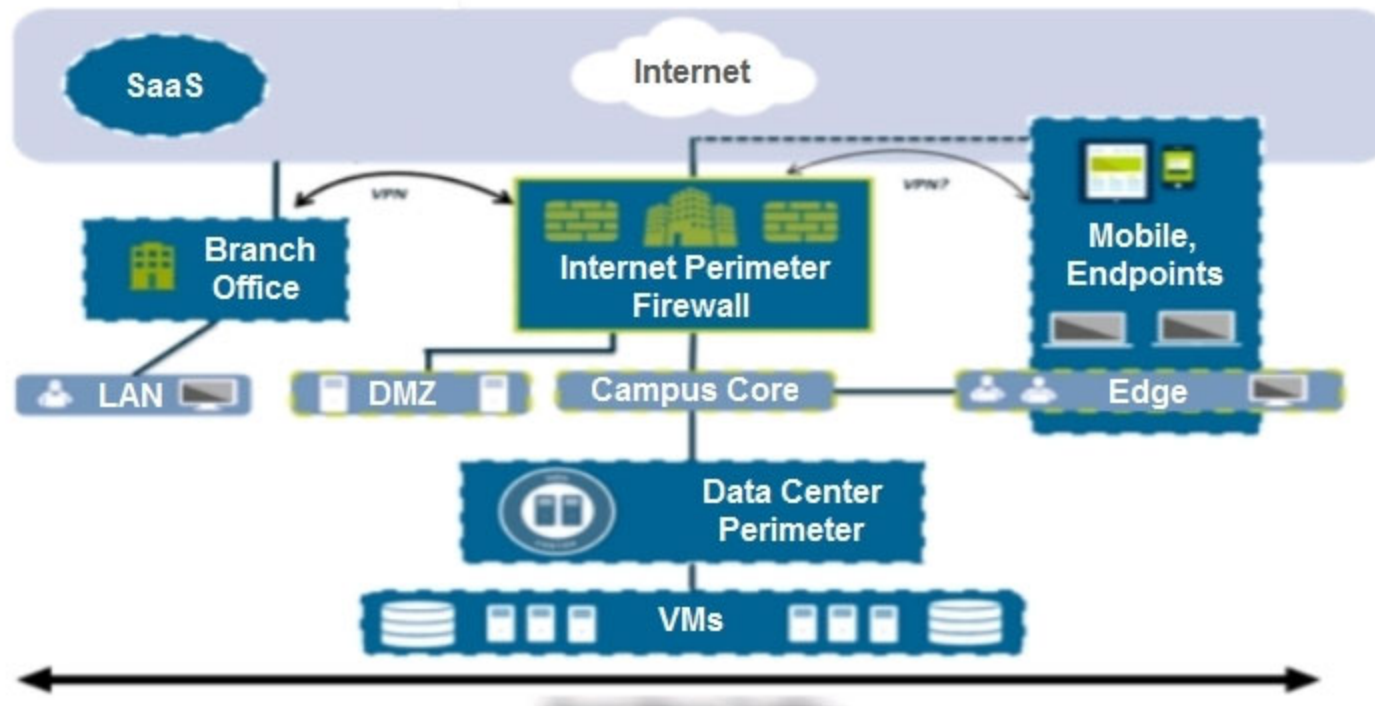
Actual exam question from Palo Alto Networks's PCNSA

Question #: 31

Topic #: 1

[\[All PCNSA Questions\]](#)

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

Show Suggested Answer

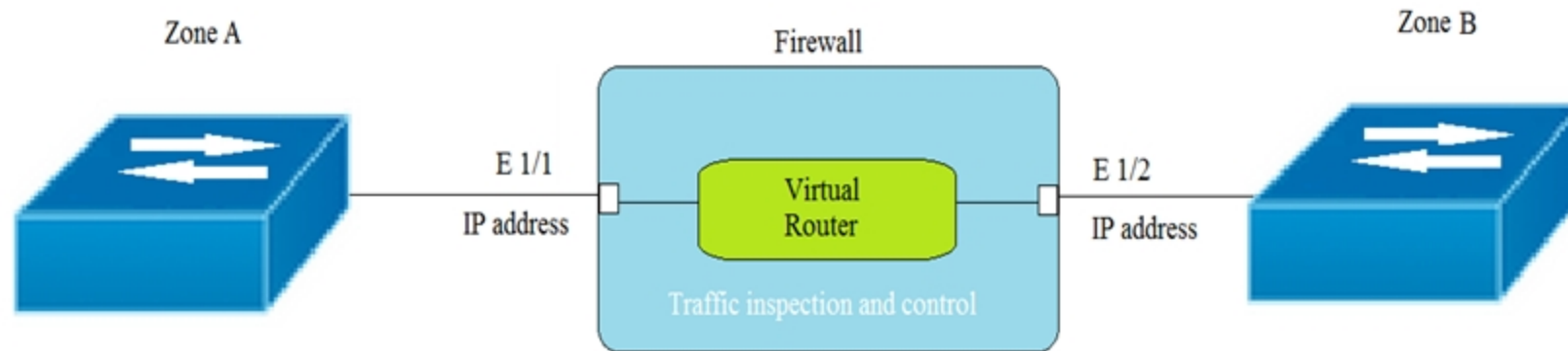
Actual exam question from Palo Alto Networks's PCNSA

Question #: 32

Topic #: 1

[\[All PCNSA Questions\]](#)

Given the topology, which zone type should zone A and zone B to be configured with?



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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 33

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

- A. domain controller
- B. TACACS+
- C. LDAP
- D. RADIUS

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 34

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 35

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 36

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 37

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 38

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 39

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 40

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which three statements describe the operation of Security policy rules and Security Profiles? (Choose three.)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 41

Topic #: 1

[\[All PCNSA Questions\]](#)

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

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
				ZONE	ADDRESS	DEVICE	ZONE	ADDRESS					
19	Allow-Office-Programs	none	universal	Internal	any	any	External	any	office-programs	application-defa...	Allow		
20	Allow-FTP	none	universal	Internal	any	any	External	FTP Server	any	FTP	Allow		
21	Allow-Social-Media	none	universal	Internal	any	any	External	any	facebook	application-defa...	Allow		
22	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	
23	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	

- A. The Allow-Office-Programs rule is using an Application Filter.
- B. In the Allow-FTP policy, FTP is allowed using App-ID.
- C. The Allow-Office-Programs rule is using an Application Group.
- D. The Allow-Social-Media rule allows all of Facebook's functions.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 42

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which type of 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. intrazone
- C. interzone
- D. universal

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 43

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

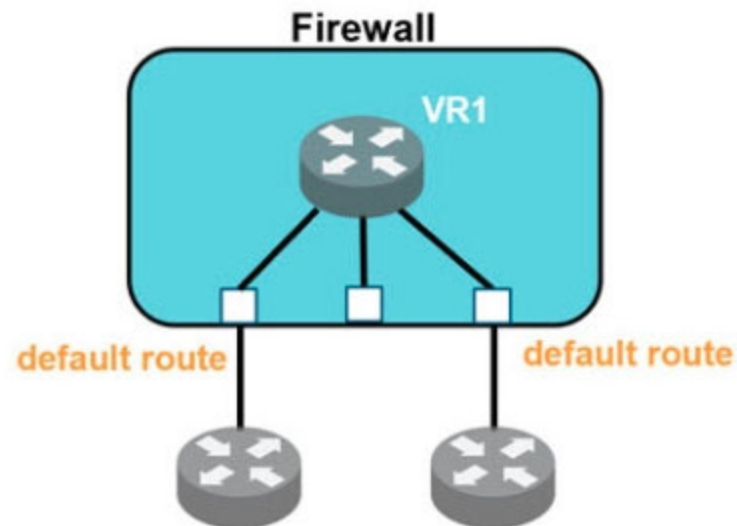
Question #: 44

Topic #: 1

[\[All PCNSA Questions\]](#)

Which two statements are correct regarding multiple static default routes when they are configured as shown in the image? (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.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

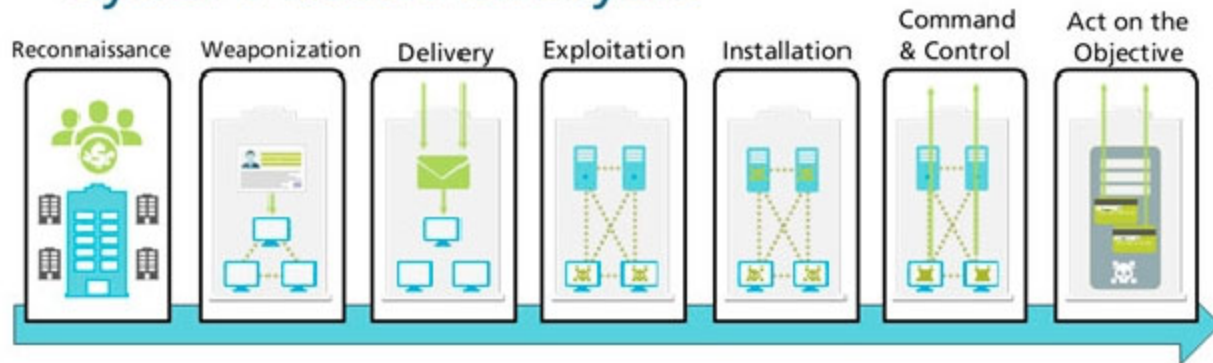
Question #: 45

Topic #: 1

[\[All PCNSA Questions\]](#)

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

## Cyber Attack Lifecycle



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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 46

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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-configuration.xml

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 47

Topic #: 1

[\[All PCNSA Questions\]](#)

In the example security policy shown, which two websites would be blocked? (Choose two.)

	Name	Tags	Source		Destination		Application	Service	URL Category	Action	Profile
			Zone	Address	Zone	Address					
1	Block-sites	outbound	inside	any	outside	any	any	social-networking	Deny	none	

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 48

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which Palo Alto Networks component provides consolidated policy creation and centralized management?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 49

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 50

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 51

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 52

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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. Panorama
- D. GlobalProtect

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 53

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An 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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 54

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 55

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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 created. 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
- D. 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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 56

Topic #: 1

[\[All PCNSA Questions\]](#)

---

How often does WildFire release dynamic updates?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 57

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 58

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Your company has 10 Active Directory domain controllers spread across multiple WAN links. All users authenticate to Active Directory. Each link has substantial network bandwidth to support all mission-critical applications. The firewall's management plane is highly utilized.

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 agent with adequate data-plane resources
- D. PAN-OS integrated agent

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 59

Topic #: 1

[\[All PCNSA Questions\]](#)

DRAG DROP -

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

Select and Place:

### 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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 60

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What must you configure to enable the firewall to access multiple Authentication Profiles to authenticate a non-local account?

- A. authentication sequence
- B. LDAP server profile
- C. authentication server list
- D. authentication list profile

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 61

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which Security Profile mitigates attacks based on packet count?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 62

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which interface type uses virtual routers and routing protocols?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 63

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 64

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An internal host needs to connect through the firewall using source NAT to servers of the internet.

Which policy is required to enable source NAT on the firewall?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 65

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which Security Profile can provide protection against ICMP floods, based on individual combinations of a packet's source and destination IP addresses?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 66

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which path in PAN-OS 9.0 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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 67

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 68

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 69

Topic #: 1

[\[All PCNSA Questions\]](#)

DRAG DROP -

Match the network device with the correct User-ID technology.

Select and Place:

### Answer Area

Microsoft  
Exchange

Drag answer here

syslog monitoring

Linux  
authentication

Drag answer here

Terminal Services agent

Windows  
clients

Drag answer here

server monitoring

Citrix client

Drag answer here

client probing

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 70

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 71

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer

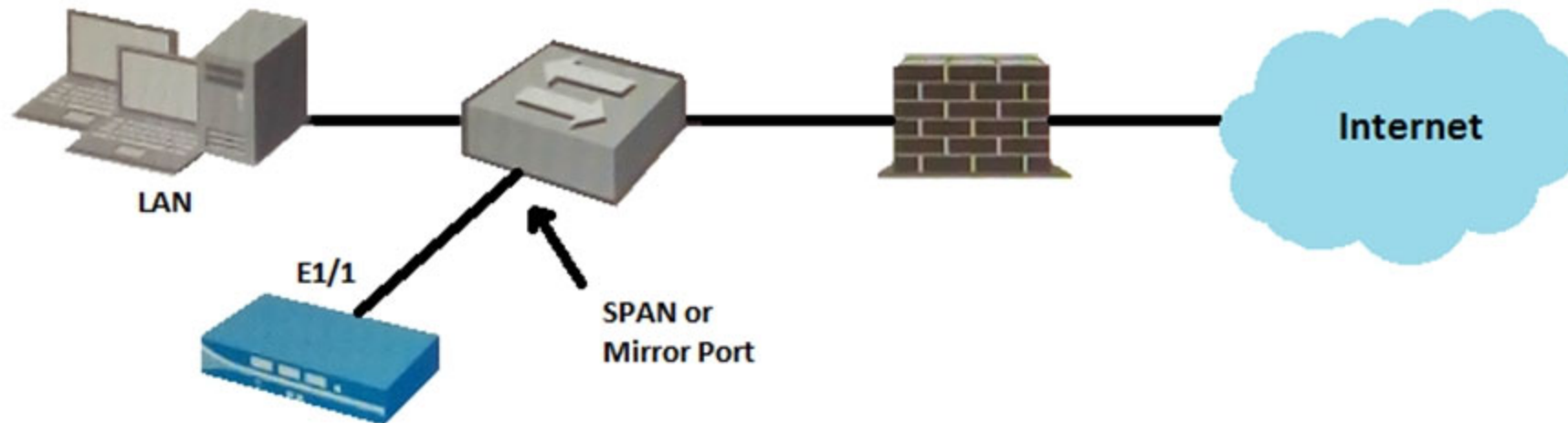


Actual exam question from Palo Alto Networks's PCNSA

Question #: 72

Topic #: 1

[\[All PCNSA Questions\]](#)



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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 73

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 74

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 75

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

- A. EDL in URL Filtering Profile
- B. Custom URL category in URL Filtering Profile
- C. Custom URL category in Security policy rule
- D. PAN-DB URL category in URL Filtering Profile

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 76

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

- A. north-south
- B. inbound
- C. outbound
- D. east-west

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 77

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 78

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which definition describes the guiding principle of the zero-trust architecture?

- A. trust, but verify
- B. always connect and verify
- C. never trust, never connect
- D. never trust, always verify

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 79

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 80

Topic #: 1

[\[All PCNSA Questions\]](#)

---

In which profile should you configure the DNS Security feature?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 81

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which two statements are true for the DNS Security service introduced in PAN-OS version 9.0? (Choose two.)

- A. It is automatically enabled and configured.
- B. It eliminates the need for dynamic DNS updates.
- C. It functions like PAN-DB and requires activation through the app portal.
- D. It removes the 100K limit for DNS entries for the downloaded DNS updates.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 82

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 83

Topic #: 1

[\[All PCNSA Questions\]](#)

---

The CFO found a malware infected USB drive in the parking lot, which when inserted infected their corporate laptop. The malware contacted a known command- and-control server, which caused the infected laptop to begin exfiltrating corporate data.

Which security profile feature could have been used to prevent the communication with the command-and-control server?

- A. Create an anti-spyware profile and enable DNS Sinkhole feature.
- B. Create an antivirus profile and enable its DNS Sinkhole feature.
- C. Create a URL filtering profile and block the DNS Sinkhole URL category
- D. Create a Data Filtering Profiles and enable its DNS Sinkhole feature.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 84

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 85

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which component provides network security for mobile endpoints by inspecting traffic routed through gateways?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 86

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 87

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 88

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Your company occupies one floor in a single building. You have two Active Directory domain controllers on a single network. The firewall's management plane is only slightly utilized.

Which User-ID agent is sufficient in your network?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 89

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 90

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which statement is true regarding a Heatmap report?

- A. When guided by authorized sales engineer, it helps determine the areas of greatest security risk
- B. It runs only on firewalls.
- C. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture.
- D. It provides a percentage of adoption for each assessment area.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 91

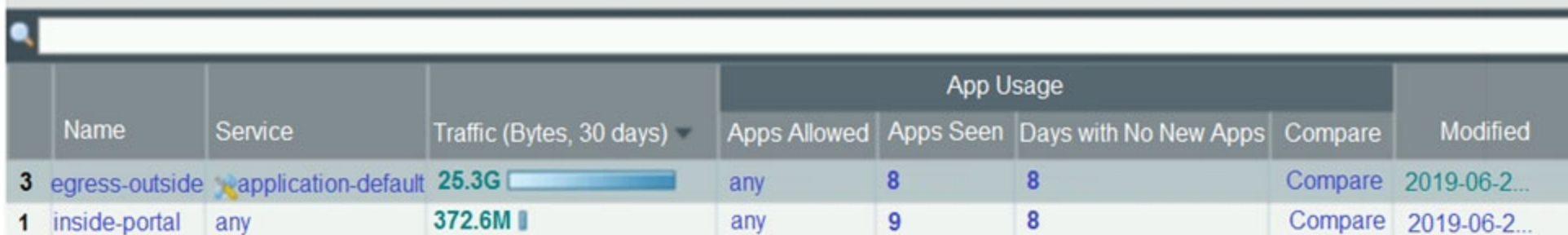
Topic #: 1

[\[All PCNSA Questions\]](#)

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

### No App Specified

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



The screenshot shows a table with columns: Name, Service, Traffic (Bytes, 30 days), App Usage (Apps Allowed, Apps Seen, Days with No New Apps, Compare), and Modified. The 'Compare' column contains links for each row.

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 92

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Access to which feature requires the PAN-OS Filtering license?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 93

Topic #: 1

[\[All PCNSA Questions\]](#)

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 groups that are imported from RADIUS authentication servers.
- B. They are the only groups visible based on the firewall's credentials.
- C. They contain only the users you allow to manage the firewall.
- D. They are used to map users to groups.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSA

Question #: 94

Topic #: 1

[\[All PCNSA Questions\]](#)

Based on the graphic, which statement accurately describes the output shown in the Server Monitoring panel?

The screenshot shows the configuration interface for a User-ID Agent. The 'User-ID Agents' tab is selected. The configuration for the 'lab-kerberos' agent is displayed, showing various settings such as 'Domain's DNS Name' (lab.local), 'Enable Security Log' (checked), 'Server Log Monitor Frequency (sec)' (2), 'Enable Session' (checked), 'Server Session Read Frequency (sec)' (10), 'Novell eDirectory Query Interval (sec)' (30), 'Syslog Service Profile', 'Enable Probing' (checked), 'Prove Interval (min)' (20), 'Enable User Identification Timeout' (checked), 'User Identification Timeout (min)' (45), 'Allow matching usernames without domains' (unchecked), 'Enable NTLM' (unchecked), 'NTLM Domain', and 'User-ID Collector Name'. Below the configuration is a 'Server Monitoring' table with the following data:

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.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 95

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

- A. Drop
- B. Deny
- C. Reset Server
- D. Reset Client

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 96

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What do Dynamic User Groups help you to do?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 97

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



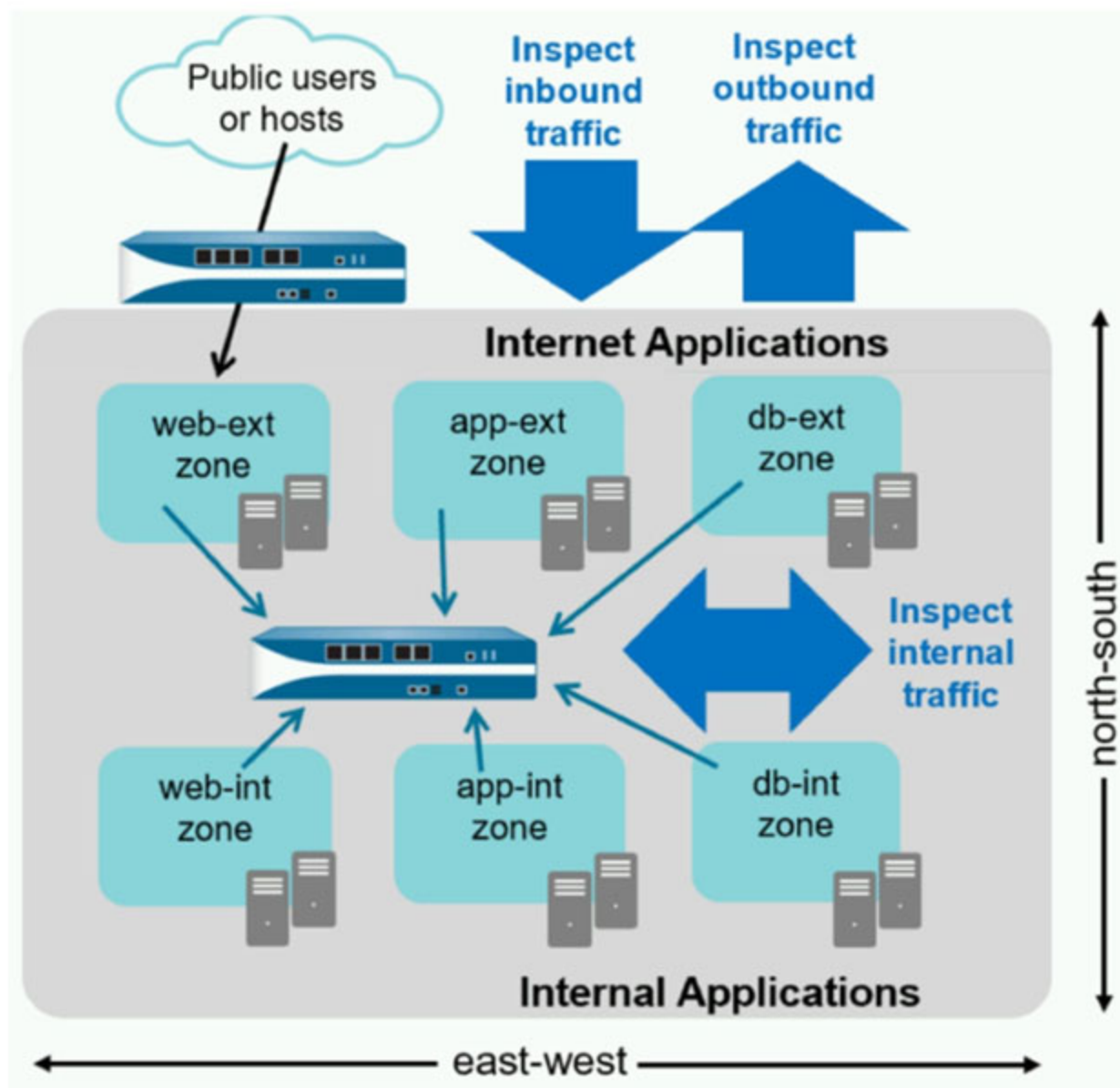
Actual exam question from Palo Alto Networks's PCNSA

Question #: 98

Topic #: 1

[\[All PCNSA Questions\]](#)

You notice that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would you 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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSA

Question #: 99

Topic #: 1

[\[All PCNSA Questions\]](#)

DRAG DROP -

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

Select and Place:

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 100

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 101

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 102

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 103

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 104

Topic #: 1

[\[All PCNSA Questions\]](#)

Based on the shown security policy, which Security policy rule would match all FTP traffic from the inside zone to the outside zone?

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

- A. interzone-default
- B. internal-inside-dmz
- C. inside-portal
- D. egress-outside

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 105

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which type of firewall configuration contains in-progress configuration changes?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 106

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which three configuration settings are required on a Palo Alto Network firewall management interface? (Choose three.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 107

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What is an advantage for using application tags?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 108

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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 Now in the Dynamic Update window
- B. after committing the firewall configuration
- C. after installing the update
- D. after downloading the update

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 109

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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 detects and prevents this threat from establishing a command-and-control connection?

- A. Vulnerability Protection Profile applied to outbound Security policy rules.
- B. Anti-Spyware Profile applied to outbound security policies.
- C. Antivirus Profile applied to outbound Security policy rules
- D. Data Filtering Profile applied to outbound Security policy rules.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 110

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which statement is true regarding a Best Practice Assessment?

- A. It runs only on firewalls.
- B. It shows how current configuration compares to Palo Alto Networks recommendations.
- C. When guided by an authorized sales engineer, it 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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 111

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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](http://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](http://www.powerball.com) to a Security policy allow rule.
- B. Manually remove [powerball.com](http://powerball.com) from the gambling URL category.
- C. Add [\\*.powerball.com](http://*.powerball.com) to the URL Filtering allow list.
- D. Create a custom URL category, add [\\*.powerball.com](http://*.powerball.com) to it and allow it in the Security Profile.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 112

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which Palo Alto Networks service protects cloud-based applications such as Dropbox and Salesforce by monitoring permissions and shares and scanning files for sensitive information?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 113

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 114

Topic #: 1

[\[All PCNSA Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 115

Topic #: 1

[\[All PCNSA Questions\]](#)

---

You receive notification about new malware that is being used to attack hosts. The malware exploits a software bug in common application. Which Security Profile detects and blocks access to this threat after you update the firewall's threat signature database?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 116

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Palo Alto Networks firewall architecture accelerates content inspection performance while minimizing latency using which two components? (Choose two.)

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 118

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



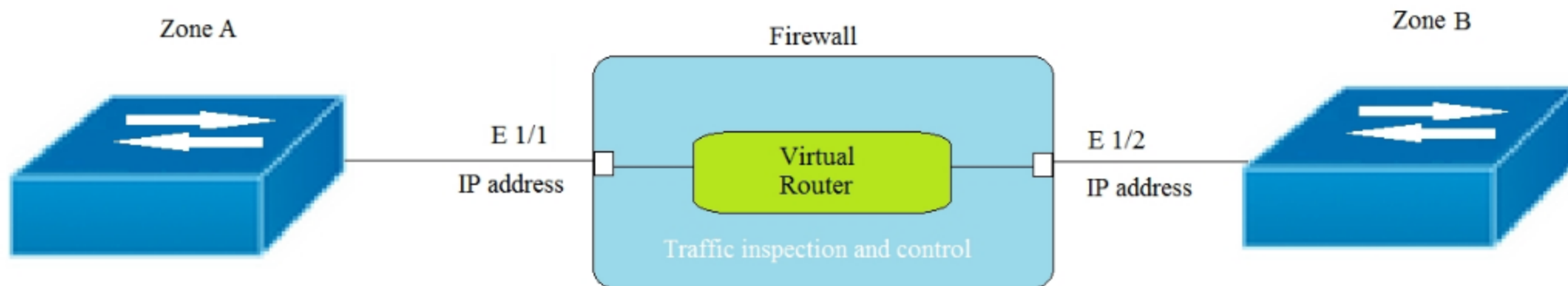
Actual exam question from Palo Alto Networks's PCNSA

Question #: 119

Topic #: 1

[\[All PCNSA Questions\]](#)

Given the topology, which zone type should zone A and zone B to be configured with?



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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSA

Question #: 120

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Assume a custom URL Category Object of `NO-FILES` has been created to identify a specific website.

How can file uploading/downloading be restricted for the website while permitting general browsing access to that website?

- A. Create a Security policy with a URL Filtering profile that references the site access setting of block to NO-FILES.
- B. Create a Security policy that references NO-FILES as a URL Category qualifier with an appropriate File Blocking profile.
- C. Create a Security policy with a URL Filtering profile that references the site access setting of continue to NO-FILES.
- D. Create a Security policy that references NO-FILES as a URL Category qualifier with an appropriate Data Filtering profile.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 121

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 122

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 123

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 124

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator wishes to follow best practices for logging traffic that traverses the firewall.

Which log setting is correct?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 125

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 126

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 127

Topic #: 1

[\[All PCNSA Questions\]](#)

---

The Palo Alto Networks NGFW was configured with a single virtual router named VR-1.  
What changes are required on VR-1 to route traffic between two interfaces on the NGFW?

- A. Add static routes to route between the two interfaces
- B. Add interfaces to the virtual router
- C. Add zones attached to interfaces to the virtual router
- D. Enable the redistribution profile to redistribute connected routes

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 128

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 129

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 130

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 131

Topic #: 1

[\[All PCNSA Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 132

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 133

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 134

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer

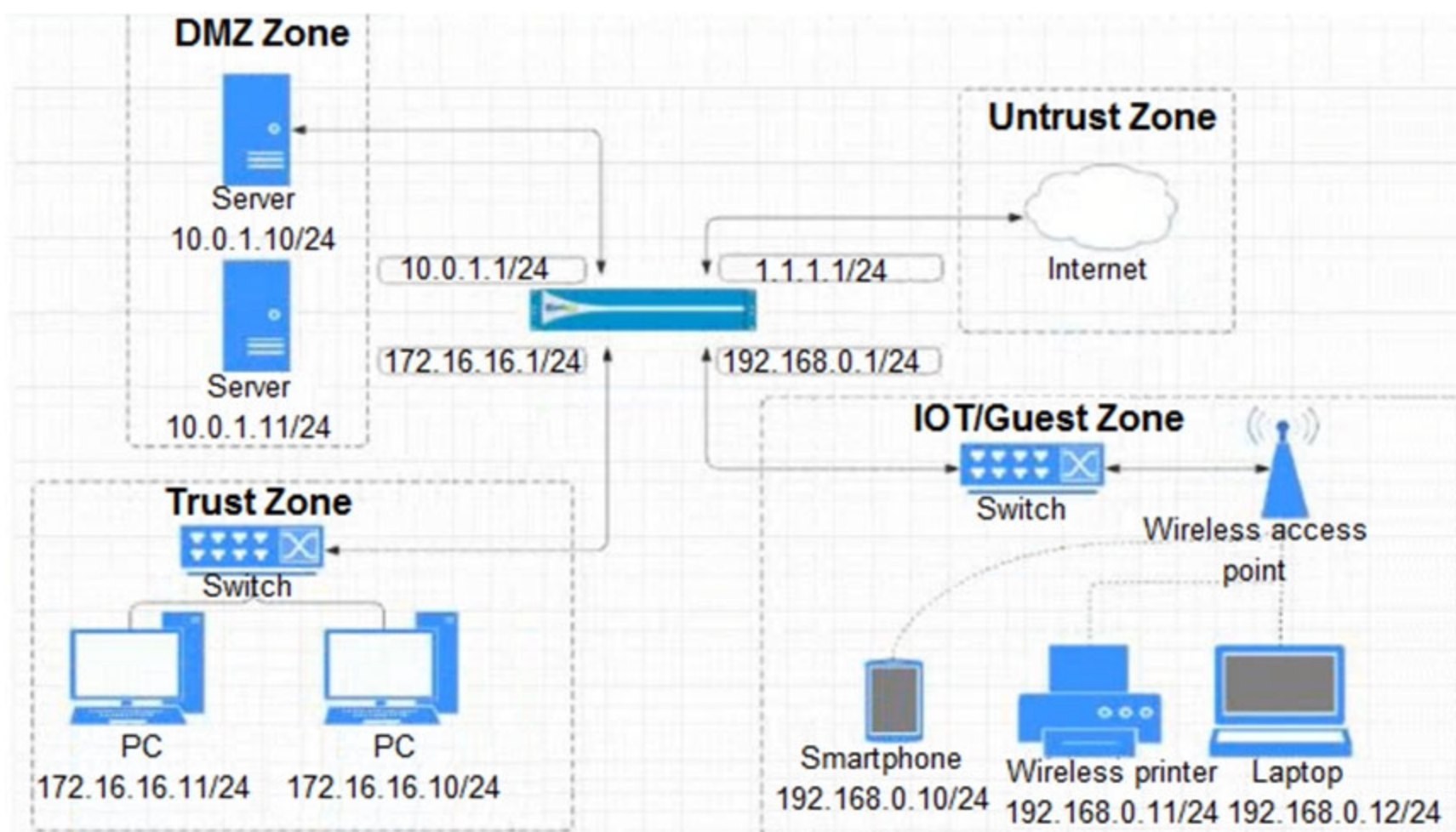


Actual exam question from Palo Alto Networks's PCNSA

Question #: 135

Topic #: 1

[\[All PCNSA Questions\]](#)



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			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
03-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	app

B.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
04-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	app

C.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
01-A	none	universal	IOT-Guest Trust	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	app

D.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
02-A	none	universal	IOT-Guest Trust	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	app

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 136

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which license is required to use the Palo Alto Networks built-in IP address EDLs?

- A. DNS Security
- B. Threat Prevention
- C. WildFire
- D. SD-Wan

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 137

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which statement is true about Panorama managed devices?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 138

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 139

Topic #: 1

[\[All PCNSA Questions\]](#)

DRAG DROP -

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

Select and Place:

### Answer Area

content inspection

first

QOS shaping applied

second

Security policy lookup

third

DoS protection

fourth

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 140

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which type of address object is `10.5.1.1/0.127.248.2`?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 141

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

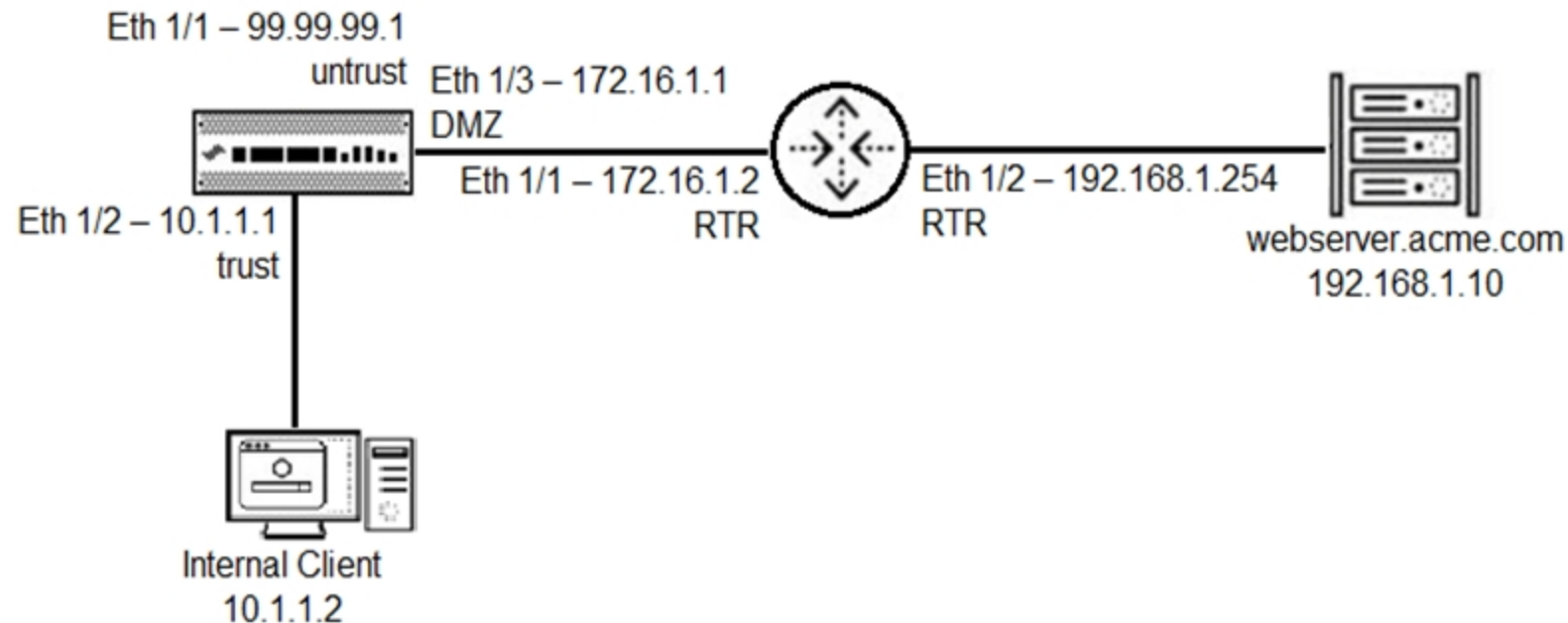
Question #: 142

Topic #: 1

[\[All PCNSA Questions\]](#)

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 1/2 with a next-hop of 172.16.1.2.
- B. 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
- 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.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 143

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 144

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 145

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 146

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

- A. SAML 2.0
- B. Kerberos
- C. TACACS
- D. TACACS+
- E. SAML 1.0

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 147

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 148

Topic #: 1

[\[All PCNSA Questions\]](#)

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

Virtual Router - Static Route - IPv4

Name	0.0.0.0
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address
	10.46.172.1
Admin Distance	10 – 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Path Monitoring

Failure Condition  Any  All Preemptive Hold Time (min) 2

Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count
------	--------	-----------	----------------	--------------------	------------

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 149

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 150

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 151

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 152

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator wants to prevent access to media content websites that are risky.

Which two URL categories should be combined in a custom URL category to accomplish this goal? (Choose two.)

- A. recreation-and-hobbies
- B. streaming-media
- C. known-risk
- D. high-risk

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSA

Question #: 153

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which dynamic update type includes updated anti-spyware signatures?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 154

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator would like to silently drop traffic from the internet to a ftp server.

Which Security policy action should the administrator select?

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSA

Question #: 155

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which object would an administrator create to block access to all high-risk applications?

- A. HIP profile
- B. Vulnerability Protection profile
- C. application group
- D. application filter

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 156

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which option is part of the content inspection process?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 157

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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`

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 158

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 159

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer



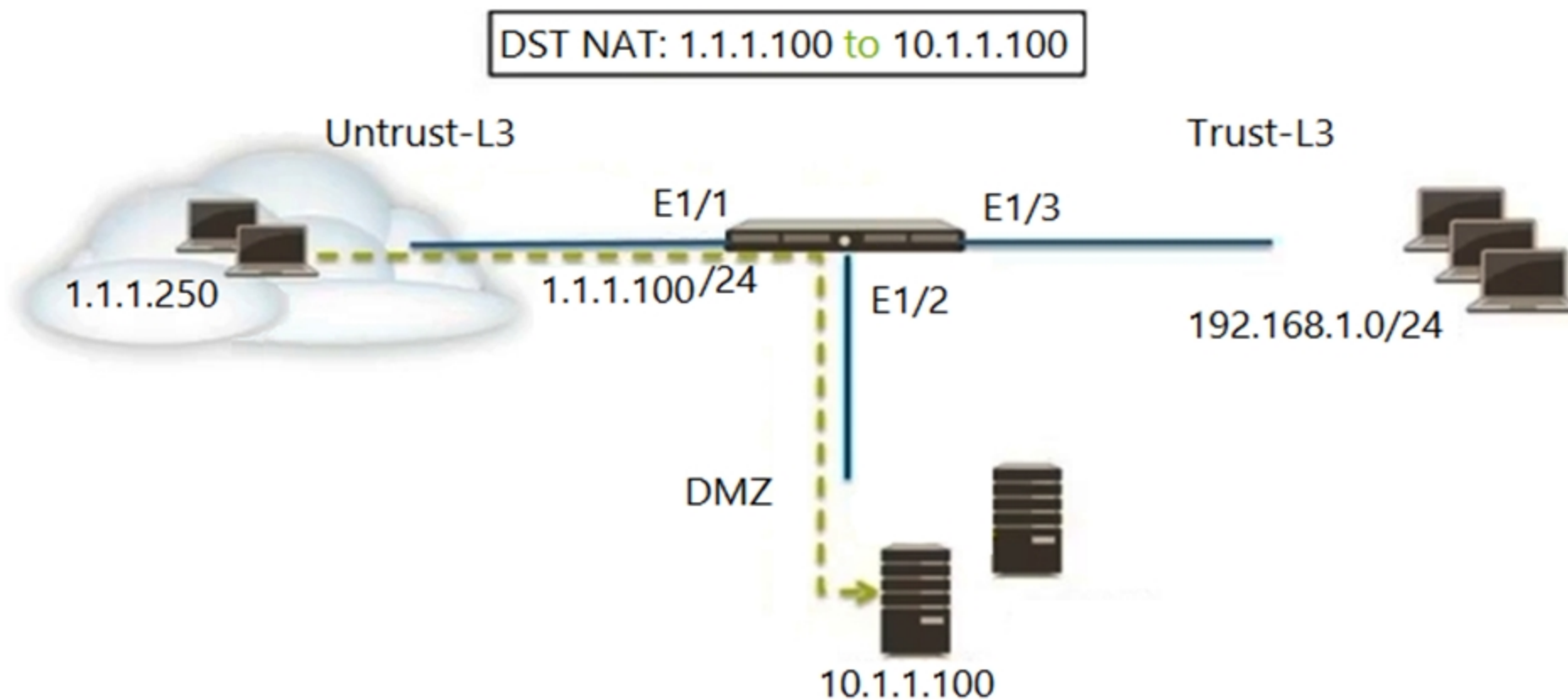
Actual exam question from Palo Alto Networks's PCNSA

Question #: 160

Topic #: 1

[\[All PCNSA Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 161

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 162

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 163

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 164

Topic #: 1

[\[All PCNSA Questions\]](#)

DRAG DROP -

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

Select and Place:

### Operational Task

Security profile enforcement

decryption

zone protection

App-ID

### Answer Area

first

second

third

fourth

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 165

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which Security policy match condition would an administrator use to block traffic from IP addresses on the Palo Alto Networks EDL of Known Malicious IP Addresses list?

- A. destination address
- B. source address
- C. destination zone
- D. source zone

[Show Suggested Answer](#)







Actual exam question from Palo Alto Networks's PCNSA

Question #: 166

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 167

Topic #: 1

[\[All PCNSA Questions\]](#)

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

TYPE	FROM ZONE	TO ZONE	INGRESS I/F	SOURCE	NAT APPLIED	EGRESS I/F	DESTINATION	TO PORT	APPLICATION	ACTION	SESSION END REASON	BYTES	ACTION SOURCE	LOG ACTION	BYTES SENT	BYTES RECEIVED	LOG TYPE
end	LAN	Internet	ethernet1/2	192.168.200.100	yes	ethernet1/5	198.54.12.97	443	web-browsing	allow	threat	3.3k	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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSA

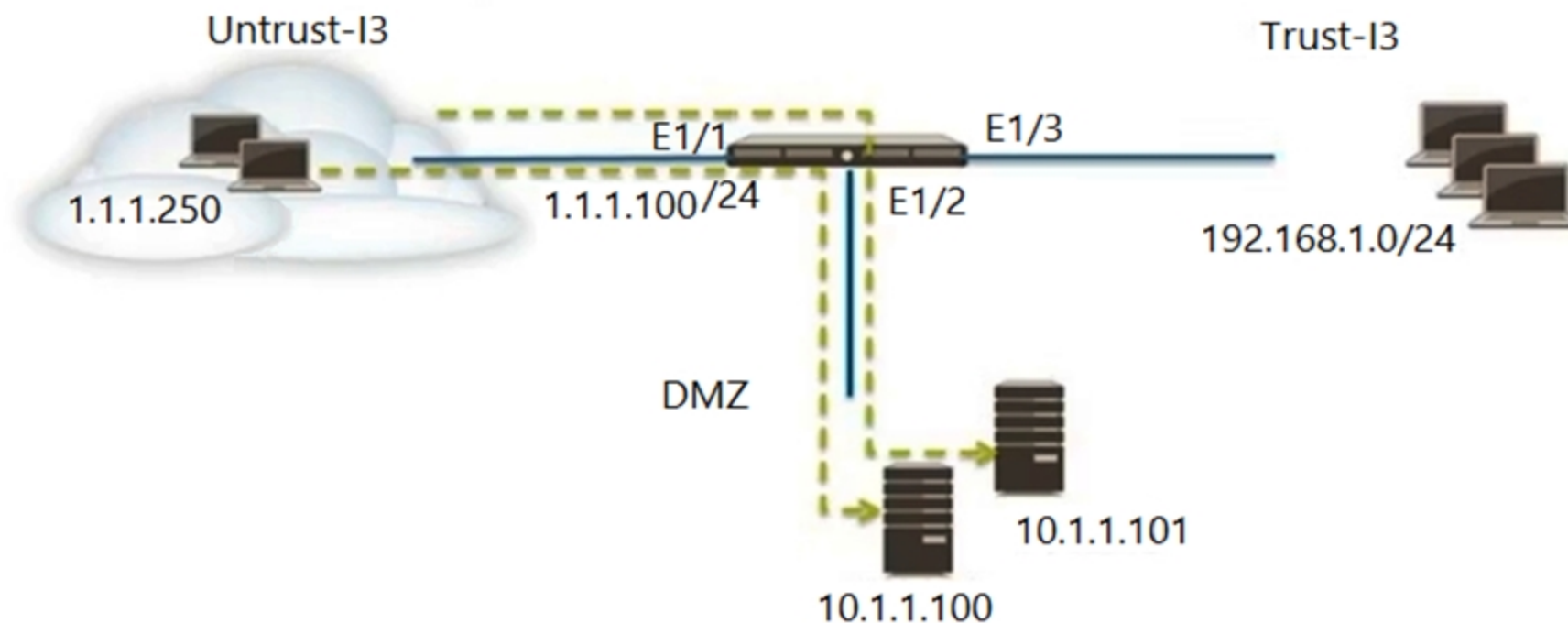
Question #: 168

Topic #: 1

[\[All PCNSA Questions\]](#)

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.

DST NAT: 1.1.1.100 to 10.1.1.100 Dst Port 80  
1.1.1.100 to 10.1.1.101 Dst Port 22



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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 169

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 170

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 171

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 172

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 173

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 174

Topic #: 1

[\[All PCNSA Questions\]](#)

Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?

The screenshot shows a configuration window titled "General Settings" with a help icon in the top right corner. The window contains the following fields and options:

- Hostname:
- Domain:
- Accept DHCP server provided Hostname
- Accept DHCP server provided Domain
- Login Banner:
- Force Admins to Acknowledge Login Banner
- SSL/TLS Service Profile:
- Time Zone:
- Locale:
- Latitude:
- Longitude:
- Automatically Acquire Commit Lock
- Certificate Expiration Check
- Use Hypervisor Assigned MAC Addresses
- Advanced Routing
- Tunnel Acceleration

At the bottom of the window are two buttons: "OK" and "Cancel".

- A. It defines the SSL/TLS encryption strength used to protect the management interface.
- B. It defines the CA certificate used to verify the client's browser.
- C. It defines the certificate to send to the client's browser from the management interface.
- D. It defines the firewall's global SSL/TLS timeout values.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 175

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 176

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 177

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 178

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 179

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 180

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 181

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 182

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSA

Question #: 183

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which security policy match condition would an administrator use to block traffic to IP addresses on the Palo Alto Networks Bulletproof IP Addresses list?

- A. source address
- B. destination address
- C. source zone
- D. destination zone

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 184

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 185

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which stage of the cyber attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?

- A. reconnaissance
- B. delivery
- C. installation
- D. exploitation

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 186

Topic #: 1

[\[All PCNSA Questions\]](#)

---

A coworker found a USB labeled "confidential in the parking lot. They inserted the drive and it infected their corporate laptop with unknown malware. The malware caused the laptop to begin infiltrating corporate data.

Which Security Profile feature could have been used to detect the malware on the laptop?

- A. DNS Sinkhole
- B. WildFire Analysis
- C. Antivirus
- D. DoS Protection

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 187

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What must be configured before setting up Credential Phishing Prevention?

- A. Threat Prevention
- B. Anti Phishing Block Page
- C. User-ID
- D. Anti Phishing profiles

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 188

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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. allow
- D. alert

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 189

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which statement best describes a common use of Policy Optimizer?

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 191

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An address object of type IP Wildcard Mask can be referenced in which part of the configuration?

- A. Security policy rule
- B. ACC global fitter
- C. NAT address pool
- D. external dynamic list

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 192

Topic #: 1

[\[All PCNSA Questions\]](#)

---

You receive notification about a new malware that infects hosts. An infection results in the infected host attempting to contact 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. Anti-Spyware Profile
- B. Data Filtering Profile
- C. Antivirus Profile
- D. Vulnerability Protection Profile

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 193

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which Palo Alto Networks component provides consolidated policy creation?

- A. Policy Optimizer
- B. Prisma SaaS
- C. GlobalProtect
- D. Panorama

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 194

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 195

Topic #: 1

[\[All PCNSA Questions\]](#)

---

According to best practices, how frequently should WildFire updates be made to perimeter firewalls?

- A. every 10 minutes
- B. every minute
- C. every 5 minutes
- D. in real time

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 197

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 198

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 199

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 200

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 201

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which action would an administrator take to ensure that a service object will be available only to the selected device group?

- A. ensure that disable override is selected
- B. uncheck the shared option
- C. ensure that disable override is cleared
- D. create the service object in the specific template

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 202

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 203

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSA

Question #: 204

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Access to which feature requires a URL Filtering license?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 205

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What is the main function of the Test Policy Match function?

- A. ensure that policy rules are not shadowing other policy rules
- B. confirm that rules meet or exceed the Best Practice Assessment recommendations
- C. confirm that policy rules in the configuration are allowing donning the correct traffic
- D. verify that policy rules from Expedition are valid

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 206

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer

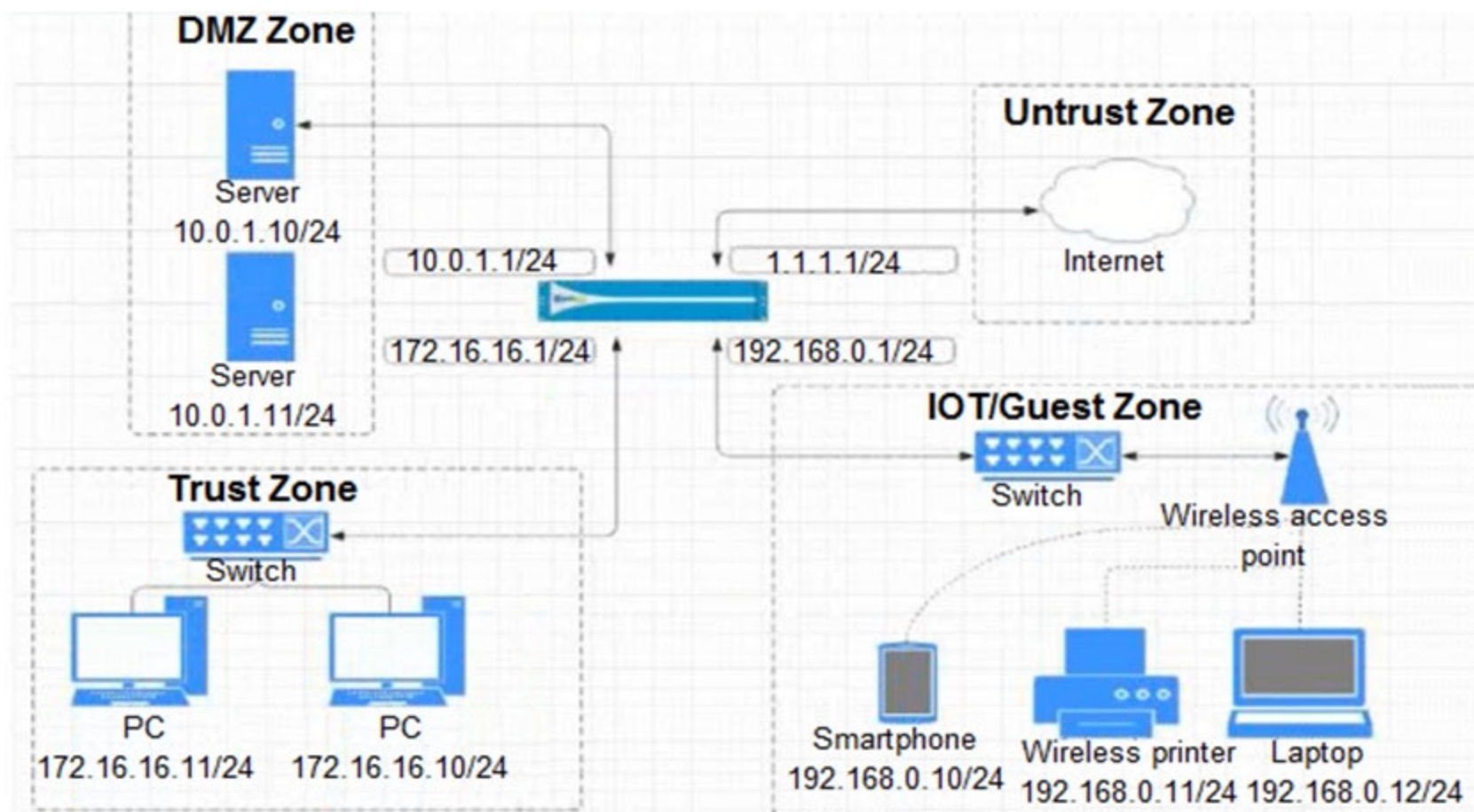


Actual exam question from Palo Alto Networks's PCNSA

Question #: 207

Topic #: 1

[\[All PCNSA Questions\]](#)



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		
03-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	application-default

B.

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

C.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
01-A	none	universal	IOT-Guest Trust	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	application-default

D.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
02-A	none	universal	IOT-Guest Trust	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default	any	Allow

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 208

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What are the three DNS Security categories available to control DNS traffic? (Choose three.)

- A. Parked Domains
- B. Spyware Domains
- C. Vulnerability Domains
- D. Phishing Domains
- E. Malware Domains

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 209

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 210

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

1. trust for internal networks
2. untrust to the internet

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 211

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 212

Topic #: 1

[\[All PCNSA Questions\]](#)

### Detailed Log View

General	Source	Destination
Session ID: 781868	Source User:	Destination User:
Action: drop	Source: 192.168.101.25	Destination: 8.8.4.4
Host ID:	Source DAG:	Destination DAG:
Application: dns	Country: 192.168.0.0-192.168.255.255	Country: United States
Rule: Outbound DNS	Port: 46282	Port: 53
Rule UUID: ea913b96-e280-467c-aca5-0b1902857791	Zone: Servers	Zone: Internet
Device SN: 007251000156341	Interface: ethernet1/4	Interface: ethernet1/8
IP Protocol: udp	NAT IP: 67.190.64.58	NAT IP: 8.8.4.4
Log Action: global-logs	NAT Port: 26351	NAT Port: 53
Generated Time: 2021/08/27 02:02:49	X-Forwarded-For IP: 0.0.0.0	
Receive Time: 2021/08/27 02:02:53		
Tunnel Type: N/A		

Details	Flags
Threat Type: spyware	Captive Portal: <input type="checkbox"/>
Threat ID/Name: Phishing:151.116.74.in-addr.arpa	Proxy Transaction: <input type="checkbox"/>
ID: 109010001 (View in Threat Vault)	Decrypted: <input type="checkbox"/>
Category: dns-phishing	Packet Capture: <input type="checkbox"/>
Content Version: AppThreat-0-0	Client to Server: <input checked="" type="checkbox"/>
Severity: low	Server to Client: <input type="checkbox"/>
Repeat Count: 2	Tunnel Inspected: <input type="checkbox"/>
File Name:	
URL: 151.116.74.in-addr.arpa	
Partial Hash: 0	
Pcap ID: 0	
Source UUID:	
Destination UUID:	
Dynamic User Group:	
Network Slice ID SST: 0	
Network Slice ID SD:	
App Category: networking	
App Subcategory: infrastructure	
App Technology: network-protocol	
App Characteristic: used-by-malware.has-known-vulnerability.pervasive-use	
App Container:	
App Risk: 3	

DeviceID
Source Device Category: Virtual Machine
Source Device Profile: VMware
Source Device Model:
Source Device Vendor: VMware, Inc.
Source Device OS Family:
Source Device OS Version:
Source Device Host: ubuntu-server
Source Device MAC: 00:50:56:a2:19:d3
Destination Device Category:
Destination Device Profile:
Destination Device Model:

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 213

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator wants to create a No-NAT rule to exempt a flow from the default NAT rule.

What is the best way to do this?

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

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSA

Question #: 214

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 215

Topic #: 1

[\[All PCNSA Questions\]](#)

---

When an ethernet interface is configured with an IPv4 address, which type of zone is it a member of?

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 216

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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?

- A. Security policy = deny, Gambling category in URL profile = block
- B. Security policy = drop, Gambling category in URL profile = allow
- C. Security policy = allow, Gambling category in URL profile = alert
- D. Security policy = allow, Gambling category in URL profile = allow

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 217

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSA

Question #: 218

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 219

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 220

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What are three valid ways to map an IP address to a username? (Choose three.)

- A. a user connecting into a GlobalProtect gateway using a GlobalProtect Agent
- B. WildFire verdict reports
- C. DHCP Relay logs
- D. using the XML API
- E. usernames inserted inside HTTP Headers

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 221

Topic #: 1

[\[All PCNSA Questions\]](#)

---

How is an address object of type IP range correctly defined?

- A. 192.168.40.1-192.168.40.255
- B. 192.168.40.1-255
- C. 192.168.40.1, 192.168.40.255
- D. 192.168.40.1/24

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 222

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 223

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

- A. address groups
- B. custom objects
- C. application groups
- D. service groups

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 224

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What are two valid selections within a Vulnerability Protection profile? (Choose two.)

- A. deny
- B. drop
- C. default
- D. sinkhole

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 225

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which three interface deployment methods can be used to block traffic flowing through the Palo Alto Networks firewall? (Choose three.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 226

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator would like to override the default deny action for a given application, and instead would like to block the traffic.

Which security policy action causes this?

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSA

Question #: 227

Topic #: 1

[\[All PCNSA Questions\]](#)

---

When creating an Admin Role profile, if no changes are made, which two administrative methods will you have full access to? (Choose two.)

- A. web UI
- B. XML API
- C. command line
- D. RESTAPI

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 228

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 229

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which list of actions properly defines the order of steps needed to add a local database user account and create a new group to which this user will be assigned?

- A. 1. Navigate to Device > Local User Database > Users and click Add. 2. Enter a Name for the user. 3. Enter and Confirm a Password or Hash. 4. Enable the account and click OK. 5. Navigate to Device > Local User Database > User Groups and click Add. 6. Enter a Name for the group. 7. Add the user to the group and click OK.
- B. 1. Navigate to Device > Authentication Profile > Users and click Add. 2. Enter a Name for the user. 3. Enter and Confirm a Password or Hash. 4. Enable the account and click OK. 5. Navigate to Device > Local User Database > User Groups and click Add. 6. Enter a Name for the group. 7. Add the user to the group and click OK.
- C. 1. Navigate to Device > Users and click Add. 2. Enter a Name for the user. 3. Enter and Confirm a Password or Hash. 4. Enable the account and click OK. 5. Navigate to Device > User Groups and click Add. 6. Enter a Name for the group. 7. Add the user to the group and click OK.
- D. 1. Navigate to Device > Admins and click Add. 2. Enter a Name for the user. 3. Enter and Confirm a Password or Hash. 4. Enable the account and click OK. 5. Navigate to Device > User Groups and click Add. 6. Enter a Name for the group. 7. Add the user to the group and click OK.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 230

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

- A. server profile
- B. admin role
- C. password profile
- D. access domain

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 231

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator is configuring a NAT rule.

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

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

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 232

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator wants to prevent hacking attacks through DNS queries to malicious domains.

Which two DNS policy actions can the administrator choose in the Anti-Spyware Security Profile? (Choose two.)

- A. deny
- B. block
- C. sinkhole
- D. override

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSA

Question #: 233

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator is creating a NAT policy.

Which combination of address and zone are used as match conditions? (Choose two.)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 234

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

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

[Show Suggested Answer](#)

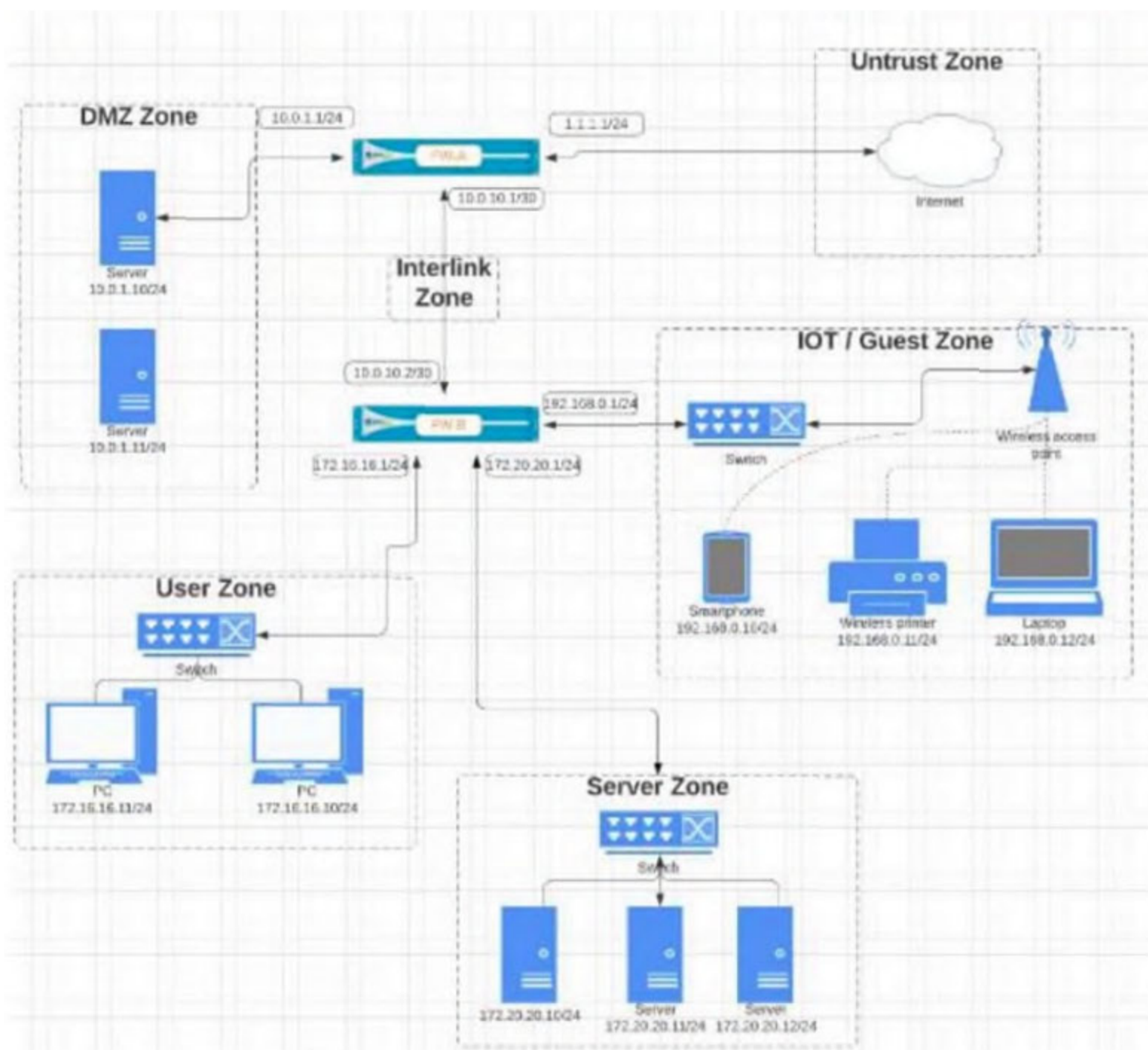


Actual exam question from Palo Alto Networks's PCNSA

Question #: 235

Topic #: 1

[\[All PCNSA Questions\]](#)



Given the network diagram, traffic must be permitted for SSH and MYSQL from the DMZ to the SERVER zones, crossing two firewalls. In addition, traffic should be permitted from the SERVER zone to the DMZ on SSH only.

Which rule group enables the required traffic?

A.

NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
FW-A_RuleGroup-01-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	InterLink	10.0.10.0/30	any	mysql	application-default	any	Allow	
FW-B_RuleGroup-01-X	FW-B	universal	InterLink	10.0.10.0/30	any	any	Server	172.20.20.0/24	any	mysql	application-default	any	Allow	
FW-A_RuleGroup-01-Y	FW-A	universal	InterLink	10.0.10.0/30	any	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow	
FW-B_RuleGroup-01-Z	FW-B	universal	Server	172.20.20.0/24	any	any	InterLink	10.0.10.0/30	any	ssh	application-default	any	Allow	

B.

NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
FW-A_RuleGroup-03-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	Server	172.20.20.0/24	any	mysql	application-default	any	Allow	
FW-B_RuleGroup-03-X	FW-B	universal	DMZ	10.0.1.0/24	any	any	Server	172.20.20.0/24	any	mysql	application-default	any	Allow	
FW-A_RuleGroup-03-Y	FW-A	universal	Server	172.20.20.0/24	any	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow	
FW-B_RuleGroup-03-Z	FW-B	universal	Server	172.20.20.0/24	any	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow	

C.

NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
FW-A_RuleGroup-02-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	InterLink	172.20.20.0/24	any	mysql	application-default	any	Allow	
FW-B_RuleGroup-02-X	FW-B	universal	InterLink	10.0.1.0/24	any	any	Server	172.20.20.0/24	any	mysql	application-default	any	Allow	
FW-A_RuleGroup-02-Y	FW-A	universal	InterLink	172.20.20.0/24	any	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow	
FW-B_RuleGroup-02-Z	FW-B	universal	Server	172.20.20.0/24	any	any	InterLink	10.0.1.0/24	any	ssh	application-default	any	Allow	

D.

NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
FW-A_RuleGroup-04-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	Server	172.20.20.0/24	any	mysql	application-default	any	Allow	
FW-B_RuleGroup-04-X	FW-B	universal	InterLink	10.0.1.0/24	any	any	Server	172.20.20.0/24	any	mysql	application-default	any	Allow	
FW-A_RuleGroup-04-Y	FW-A	universal	Server	172.20.20.0/24	any	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow	
FW-B_RuleGroup-04-Z	FW-B	universal	Server	172.20.20.0/24	any	any	InterLink	10.0.1.0/24	any	ssh	application-default	any	Allow	

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 236

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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. service route
- B. dynamic updates
- C. SNMP setup
- D. data redistribution

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 237

Topic #: 1

[\[All PCNSA Questions\]](#)

---

In order to fulfill the corporate requirement to backup the configuration of Panorama and the Panorama-managed firewalls securely, which protocol should you select when adding a new scheduled config export?

- A. HTTPS
- B. SMB v3
- C. SCP
- D. FTP

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 238

Topic #: 1

[\[All PCNSA Questions\]](#)

---

All users from the internal zone must be allowed only HTTP access to a server in the DMZ zone.

Complete the empty field in the Security policy using an application object to permit only this type of access.

Source Zone: Internal -

Destination Zone: DMZ Zone -

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

Service: application-default -

Action: allow

- A. Application = "any"
- B. Application = "web-browsing"
- C. Application = "ssl"
- D. Application = "http"

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 239

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator wants to prevent users from unintentionally accessing malicious domains where data can be exfiltrated through established connections to remote systems.

From the Pre-defined Categories tab within the URL Filtering profile, what is the right configuration to prevent such connections?

- A. Set the hacking category to continue.
- B. Set the phishing category to override.
- C. Set the malware category to block.
- D. Set the Command and Control category to block.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 240

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator would like to follow the best-practice approach to log the traffic that traverses the firewall.

What action should they take?

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSA

Question #: 241

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which two protocols are available on a Palo Alto Networks Firewall Interface Management Profile? (Choose two.)

- A. HTTPS
- B. RDP
- C. SCP
- D. SSH

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 242

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 243

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 244

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator would like to override the default deny action for a given application, and instead would like to block the traffic.

Which security policy action causes this?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 245

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What does an application filter help you to do?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 246

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

- A. continue
- B. override
- C. hold
- D. exclude

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 247

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which type of address object is www.paloaltonetworks.com?

- A. named address
- B. IP range
- C. FQDN
- D. IP netmask

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSA

Question #: 248

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 249

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 250

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 251

Topic #: 1

[\[All PCNSA Questions\]](#)

An administrator is reviewing the Security policy rules shown in the screenshot below.

Which statement is correct about the information displayed?

NAME	TAGS	TYPE	ZONE	Source	Destination	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT	LAST HIT	FIRST HIT
32 CPE Endpoint	IT Applications	inbound	int	10.0.0.1	10.0.0.2	any	application...	Allow	none	0	2022-03-08 13:30:26	2022-02-03	
33 Tunnel/Traffic	IT Applications	inbound	int	1.1.1.1	1.1.1.2	any	application...	Allow	none	0	-	-	
34 IT Desktop Floored	IT Applications	inbound	int	any	any	any	any	Allow	none	22589	2022-03-08 13:39:44	2022-02-03	
35 IT Desktop UserMP	IT Applications	inbound	int	any	any	any	any	Allow	none	11344	2022-03-08 13:38:50	2022-02-03	
36 IT Sanctioned SaaS A...	IT Applications	inbound	int	any	any	any	any	Allow	none	52442409	2022-03-08 13:40:24	2022-02-03	
37 IT Sanctioned SaaS A...	IT Applications	inbound	int	any	any	any	any	Allow	none	7408987	2022-03-08 13:40:24	2022-02-03	
38 IT Desktop Appl...	IT Applications	inbound	int	any	any	any	any	Allow	none	0	-	-	

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 252

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 253

Topic #: 1

[\[All PCNSA Questions\]](#)

DRAG DROP

-

Match each rule type with its example.

### Answer Area

Create a policy with source zones A and B. The rule will apply to 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 zones 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 zones 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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 254

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 255

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which statement is true regarding NAT rules?

- A. Translation of the IP address and port occurs before security processing.
- B. Firewall supports NAT on Layer 3 interfaces only.
- C. Static NAT rules have precedence over other forms of NAT.
- D. NAT rules are processed in order from top to bottom.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 256

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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. Deny
- C. Drop
- D. Reset both

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 257

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 258

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 259

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator would like to see the traffic that matches the intrazone-default rule in the traffic logs.

What is the correct process to enable this logging?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 260

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What is a function of application tags?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 262

Topic #: 1

[\[All PCNSA Questions\]](#)

---

What are two valid selections within an Anti-Spyware profile? (Choose two.)

- A. Random early drop
- B. Drop
- C. Deny
- D. Default

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 263

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 264

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which Security policy set should be used to ensure that a policy is applied first?

- A. Local firewall policy
- B. Shared pre-rulebase
- C. Parent device-group pre-rulebase
- D. Child device-group pre-rulebase

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 265

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator is trying to implement an exception to an external dynamic list manually. Some entries are shown underlined in red.

What would cause this error?

- A. Entries contain symbols.
- B. Entries are wildcards.
- C. Entries contain regular expressions.
- D. Entries are duplicated.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 266

Topic #: 1

[\[All PCNSA Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 267

Topic #: 1

[\[All PCNSA Questions\]](#)

---

Which Security profile can be used to detect and block compromised hosts from trying to communicate with external command-and-control (C2) servers?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 268

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator is trying to enforce policy on some (but not all) of the entries in an external dynamic list.

What is the maximum number of entries that they can be excluded?

- A. 50
- B. 100
- C. 200
- D. 1,000

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSA

Question #: 269

Topic #: 1

[\[All PCNSA Questions\]](#)

---

A website is unexpectedly allowed due to miscategorization.

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

A. 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.

B. Review the categorization of the website on <https://urlfiltering.paloaltonetworks.com>.

Submit for "request change", identifying the appropriate categorization, and wait for confirmation before testing again.

C. 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.

D. 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.

Set the policy action to Deny.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 270

Topic #: 1

[\[All PCNSA Questions\]](#)

---

If the firewall interface E1/1 is connected to a SPAN or mirror port, which interface type should E1/1 be configured as?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSA

Question #: 271

Topic #: 1

[\[All PCNSA Questions\]](#)

---

An administrator manages a network with 300 addresses that require translation. The administrator configured NAT with an address pool of 240 addresses and found that connections from addresses that needed new translations were being dropped.

Which type of NAT was configured?

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

Show Suggested Answer

