PaloAltoNetworks.PCNSA.v2023-11-07.q222

Exam Code:	PCNSA
Exam Name:	Palo Alto Networks Certified Network Security Administrator
Certification Provider:	Palo Alto Networks
Free Question Number:	222
Version:	v2023-11-07
# of views:	4923
# of Questions views:	2220
https://www.exam-tests.com/PCNSA-exam/PaloAltoNetworks.PCNSA.v2023-11-07.q222.html	

NEW QUESTION: 1
Which component is a building block in a Security policy rule?
A. decryption profile
B. destination interface
C. timeout (min)
D. application
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security/buildingblocks-in-a-security-policy-rule.html

NEW QUESTION: 2
Files are sent to the WildFire cloud service via the WildFire Analysis Profile. How are these files used?
A. Malware analysis
B. WildFire signature updates
C. Spyware analysis
D. Domain Generation Algorithm (DGA) learning
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
Based on the graphic which statement accurately describes the output shown in the server monitoring panel?

A. The User-ID agent is connected to the firewall labeled lab-client.

B. The host lab-client has been found by a domain controller.

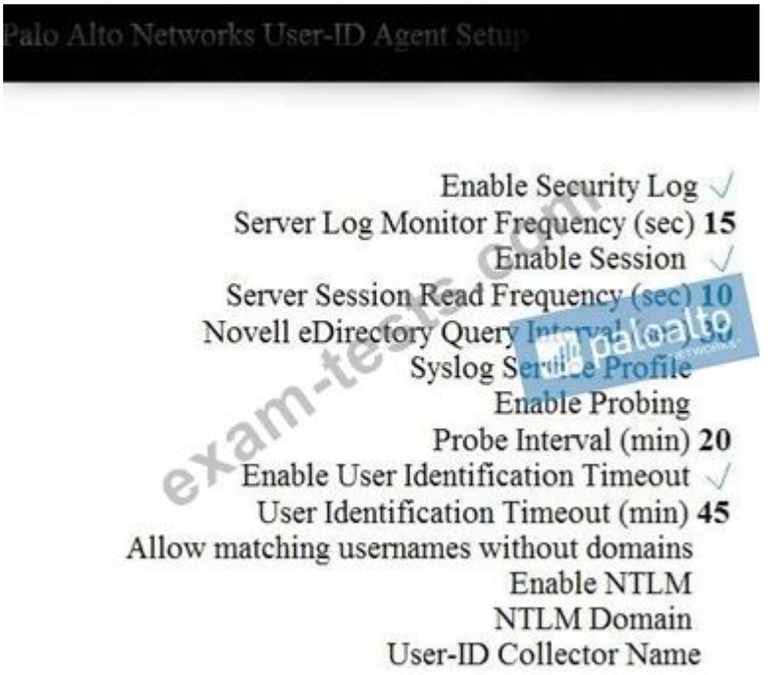
C. The host lab-client has been found by the User-ID agent.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 4

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



A. Enable Security Log

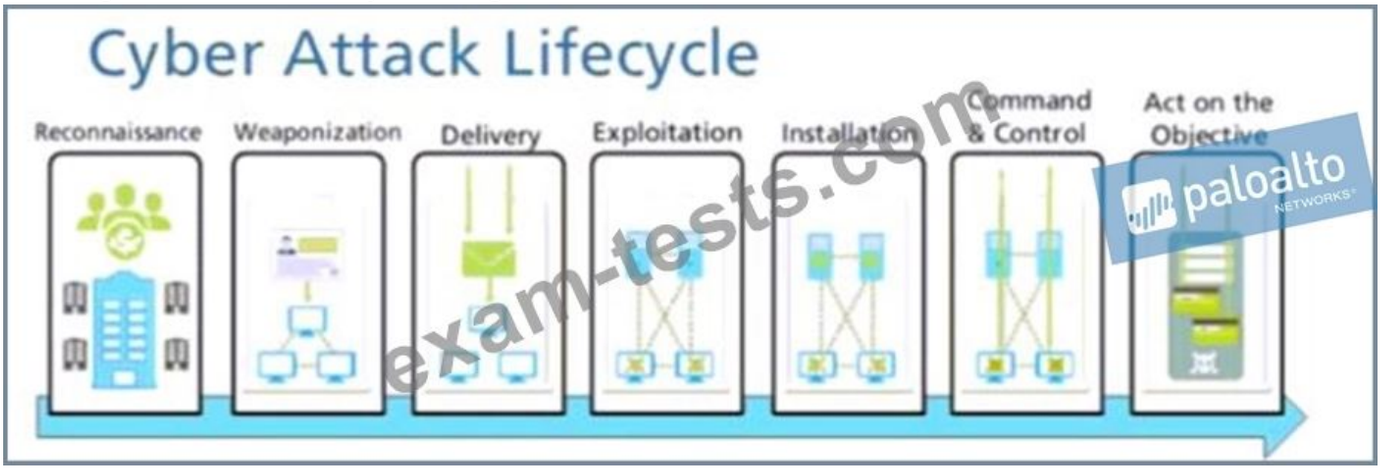
B. Enable Probing

C. Server Log Monitor Frequency (sec)

D. Enable Session

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 5
Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.



A. Installation
B. Reconnaissance
C. Exploitation
D. Act on the Objective
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which statement best describes the use of Policy Optimizer?
A. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications
B. Policy Optimizer can add or change a Log Forwarding profile for each Secunty policy selected
C. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists Admins can then manually enable policies they want to keep and delete ones they want to remove
D. Policy Optimizer can display which Security policies have not been used in the last 90 days
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
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
Answer: D (LEAVE A REPLY)

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

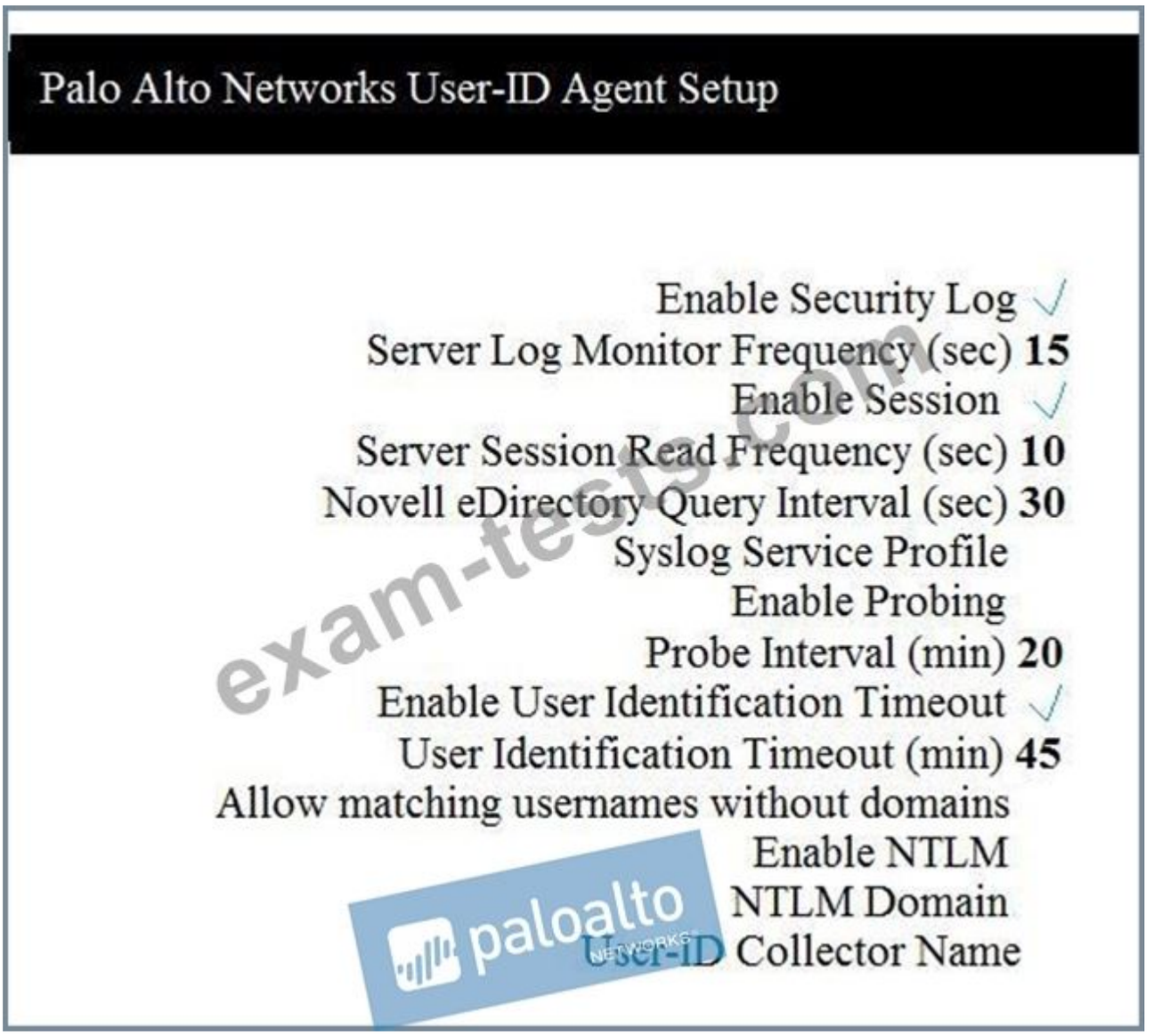
NEW QUESTION: 8
Which administrative management services can be configured to access a management interface?
A. HTTP, CLI, SNMP, HTTPS
B. HTTPS, SSH telnet SNMP
C. SSH: telnet HTTP, HTTPS
D. HTTPS, HTTP. CLI, API
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfaces You can use the following user interfaces to manage the Palo Alto Networks firewall: Use the Web Interface to perform configuration and monitoring tasks with relative ease. This graphical interface allows you to access the firewall using HTTPS (recommended) or HTTP and it is the best way to perform administrative tasks.
Use the Command Line Interface (CLI) to perform a series of tasks by entering commands in rapid succession over SSH (recommended), Telnet, or the console port. The CLI is a no-frills interface that supports two command modes, operational and configure, each with a distinct hierarchy of commands and statements. When you become familiar with the nesting structure and syntax of the commands, the CLI provides quick response times and administrative efficiency.
Use the XML API to streamline your operations and integrate with existing, internally developed applications and repositories. The XML API is a web service implemented using HTTP/HTTPS requests and responses.
Use Panorama to perform web-based management, reporting, and log collection for multiple firewalls. The Panorama web interface resembles the firewall web interface but with additional functions for centralized management.

NEW QUESTION: 9
Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?
A. global
B. intrazone
C. interzone
D. universal
Answer: D (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

NEW QUESTION: 10

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 over any service and add an application filter with the evasive characteristic.
B. 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
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 select evasive as the application
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 11
Which two configuration settings shown are not the default? (Choose two.)



A. Enable Probing

B. Server Log Monitor Frequency (sec)

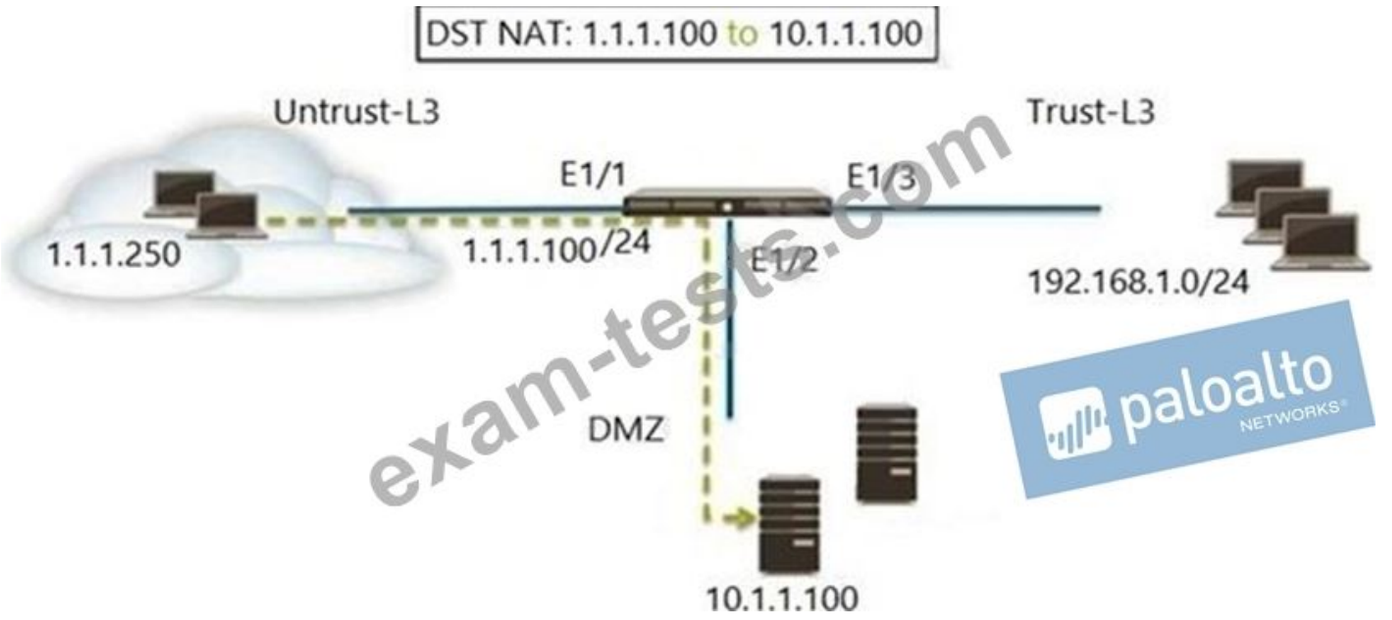
C. Enable Security Log

D. Enable Session

Answer: (SHOW ANSWER)

NEW QUESTION: 12

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 Untrust (10.1.1.100), web browsing -Allow

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

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

D. Untrust (any) to Untrust (1.1.1.100), web browsing - Allow

Answer: (SHOW ANSWER)

NEW QUESTION: 13

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

Answer: D (LEAVE A REPLY)

Service = layer 4, Application = layer 7

NEW QUESTION: 14

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

A. Check the action for the decoder in the antivirus profile

B. Check the action for the Security policy matching that traffic

C. View the application details in beacon paloaltonetworks.com

D. View the application details in Objects > Applications

Answer: D (LEAVE A REPLY)

NEW QUESTION: 15

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

A. decryption

C application override
B. authentication
C. NAT
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 16
Which dynamic update type includes updated anti-spyware signatures?
A. PAN-DB
B. Applications and Threats
C. GlobalProtect Data File
D. Antivirus
Answer: (SHOW ANSWER)
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnsa-study-guide.pdf Applications and Threats: Includes new and updated application and threat signatures, including those that detect spyware and vulnerabilities.

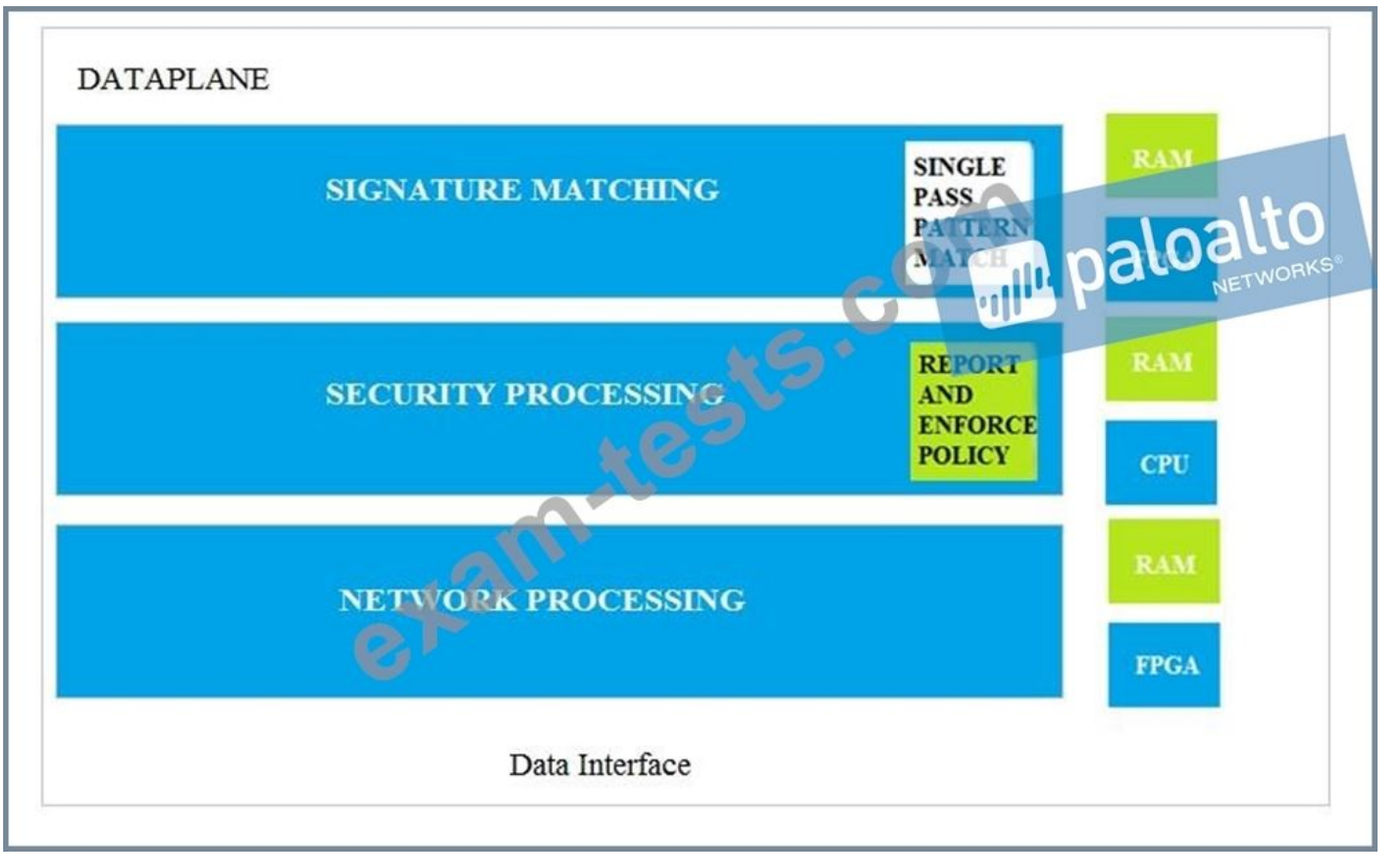
NEW QUESTION: 17
Which interface type can use virtual routers and routing protocols?
A. Virtual Wire
B. Layer3
C. Layer2
D. Tap
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
What are three DNS policy actions? (Choose three.)
A. Allow
B. Alert
C. Strict
D. Sinkhole
E. Block
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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
Answer: D (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-configuration-backups/revert-firewall-configuration-changes.html

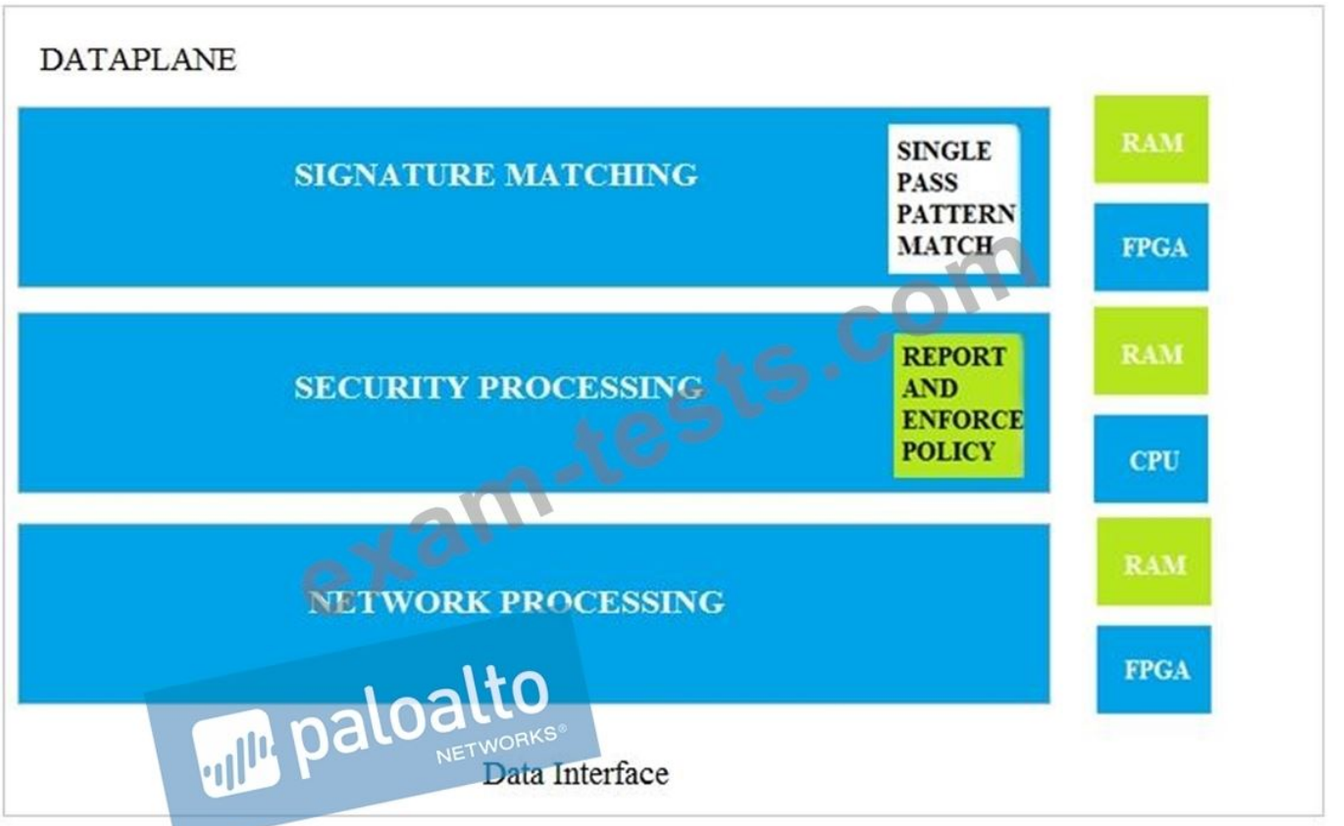
NEW QUESTION: 20
Which Palo Alto Networks component provides consolidated policy creation and centralized management?
A. GlobalProtect
B. Panorama
C. Aperture
D. AutoFocus
Answer: B (LEAVE A REPLY)
https://www.paloaltonetworks.com/resources/datasheets/panorama-centralized-management-datasheet

NEW QUESTION: 21
Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



A. Network Processing
B. Signature Matching
C. Security Processing
D. Security Matching
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



A. Security Matching
B. Security Processing
C. Network Processing
D. Signature Matching
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?
A. Root
B. Dynamic
C. Role-based
D. Superuser
Answer: C (LEAVE A REPLY)
Role Based profile roles: These are custom roles you can configure for more granular access control over the functional areas of the web interface, CLI, and XML API. For example, you can create an Admin Role profile role for your operations staff that provides access to the firewall and network configuration areas of the web interface and a separate profile for your security administrators that provides access to security policy definitions, logs, and reports. On a firewall with multiple virtual systems, you can select whether the role defines access for all virtual systems or specific virtual systems. After new features are added to the product, you must update the roles with corresponding access privileges; the firewall does not automatically add new features to custom role definitions.

NEW QUESTION: 24
An administrator would like to override the default deny action for a given application, and instead would like to block the traffic and send the ICMP code
"communication with the destination is administratively prohibited".
Which security policy action causes this?
A. Drop
B. Drop, send ICMP Unreachable
C. Reset both
D. Reset server
Answer: B (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy/security-policy-actions.html

NEW QUESTION: 25
The firewall sends employees an application block page when they try to access Youtube.
Which Security policy rule is blocking the youtube application?

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

A. intrazone-default
B. Deny Google
C. interzone-default
D. allowed-security services
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
Given the image, which two options are true about the Security policy rules. (Choose two.)

				Source				Destination		Rule Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

A. In the Allow FTP to web server rule, FTP is allowed using App-ID
B. The Allow Office Programs rule is using an Application Group

C. The Allow Office Programs rule is using an Application Filter
D. In the Allow Social Networking rule, allows all of Facebook's functions
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 27
Which action column is available to edit in the Action tab of an Antivirus security profile?
A. Virus
B. Signature
C. Spyware
D. Trojan
Answer: B (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/objects/objects-security-profiles-antivirus

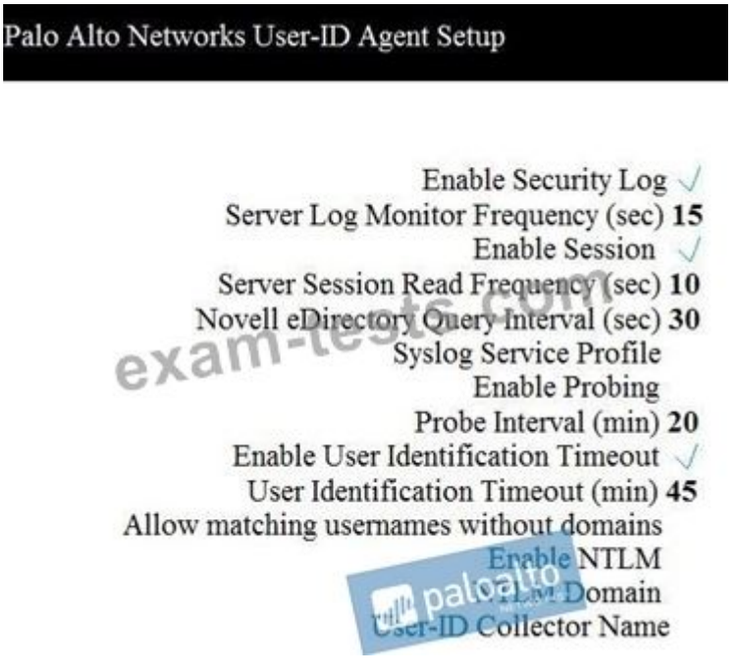
NEW QUESTION: 28
What do dynamic user groups you to do?
A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity
B. create a policy that provides auto-sizing for anomalous user behavior and malicious activity
C. create a policy that provides auto-remediation for anomalous user behavior and malicious activity
D. create a dynamic list of firewall administrators
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:text=Dynamic%20user%20groups%20help%20you,activity%20while%20maintaining%20user%20visibility.

NEW QUESTION: 29
What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)
A. SAML
B. TACACS+
C. LDAP
D. Kerberos
Answer: A,B (LEAVE A REPLY)
Reference:
The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

NEW QUESTION: 30
What in the minimum frequency for which you can configure the firewall too check for new wildfire antivirus signatures?
A. every 5 minutes
B. every 1 minute
C. every 24 hours
D. every 30 minutes
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 31
Which two configuration settings shown are not the default? (Choose two.)



A. Enable Security Log
B. Server Log Monitor Frequency (sec)
C. Enable Session
D. Enable Probing
Answer: (SHOW ANSWER)
Explanation
References:

NEW QUESTION: 32
Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?
A. Palo Alto Networks Bulletproof IP Addresses
B. Palo Alto Networks C&C IP Addresses
C. Palo Alto Networks Known Malicious IP Addresses
D. Palo Alto Networks High-Risk IP Addresses
Answer: A (LEAVE A REPLY)
To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.

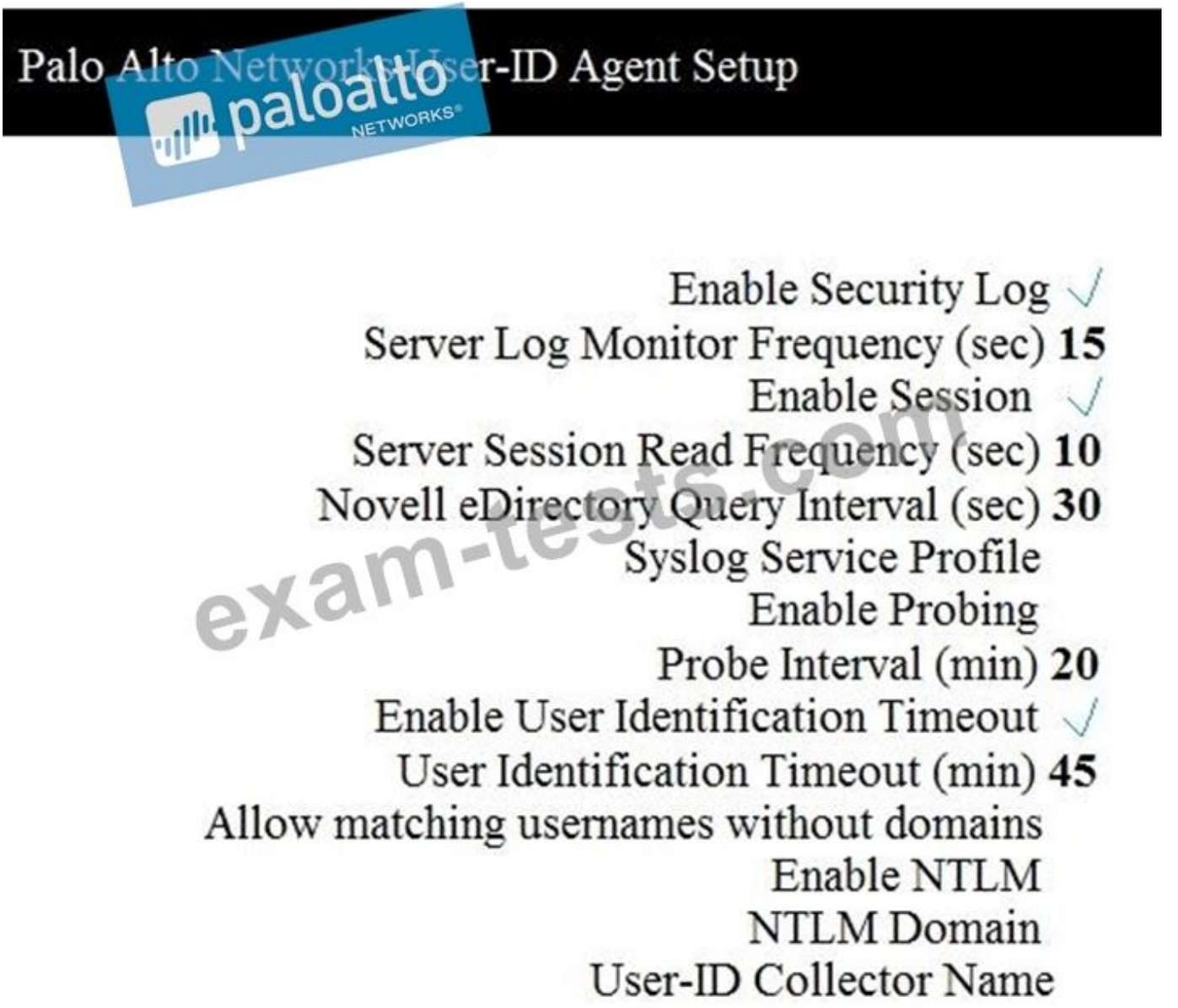
NEW QUESTION: 33
What are three valid information sources that can be used when tagging users to dynamic user groups? (Choose three.)
A. firewall logs
B. custom API scripts
C. Security Information and Event Management Systems (SIEMS), such as Splunk
D. biometric scanning results from iOS devices
E. DNS Security service
Answer: A,B,C (LEAVE A REPLY)
https://docs.paloaltonetworks.com/best-practices/10-1/user-id-best-practices/user-id-best-practices/user-id-best-practices-for-dynamic-user-groups Identity the user information sources for the tags:
Firewall logs
For Authentication, Data, Threat, Traffic, Tunnel Inspection, URL, and WildFire logs, create a log forwarding profile and use the Built-In Actions.
For User-ID, HIP Match, GlobalProtect, and IP-Tag logs, configure the log settings.
Cortex XSOAR
Security Information and Event Management Systems (SIEMS), such as Splunk Custom API scripts

NEW QUESTION: 34
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.
Answer: D (LEAVE A REPLY)
https://live.paloaltonetworks.com/t5/best-practice-assessment-blogs/the-best-practice-assessment-bpa-tool-for-ngfw-and-panorama/ba-p/248343

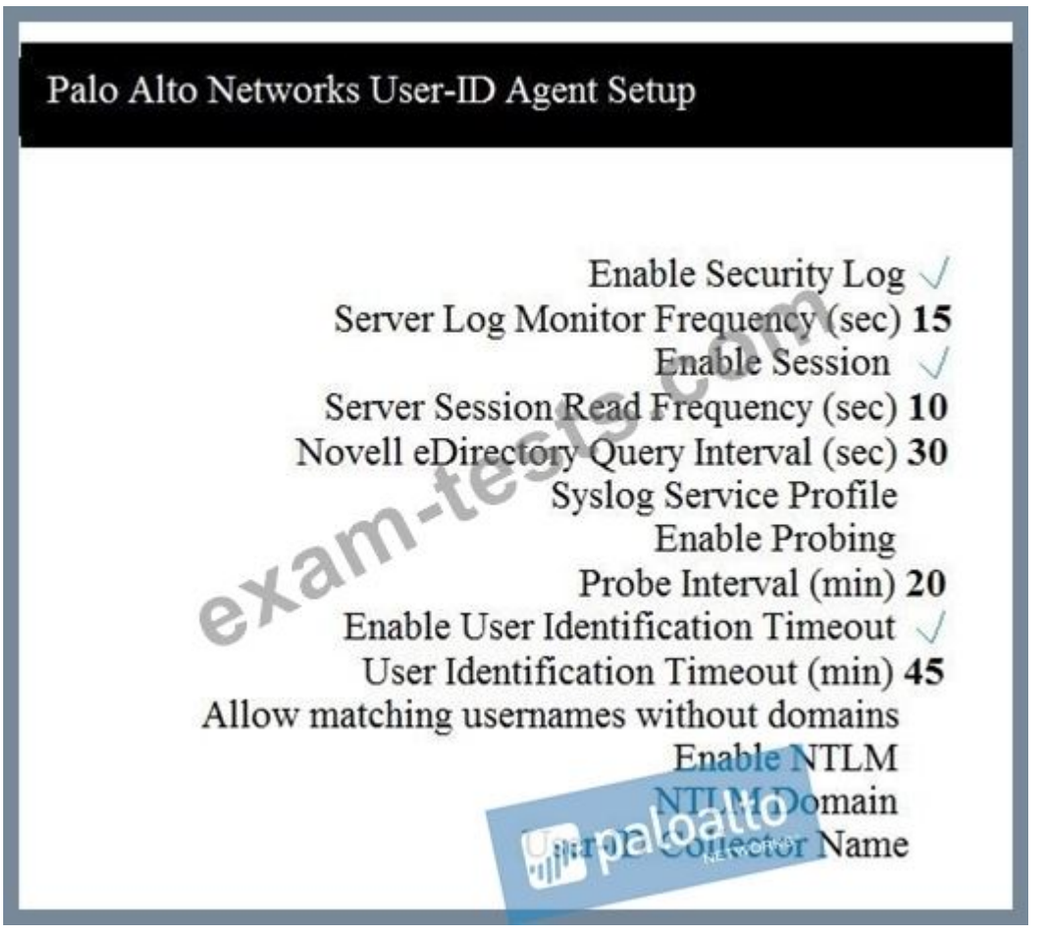
NEW QUESTION: 35
Which statement is true regarding NAT rules?
A. Static NAT rules have precedence over other forms of NAT.
B. Translation of the IP address and port occurs before security processing.
C. NAT rules are processed in order from top to bottom.
D. Firewall supports NAT on Layer 3 interfaces only.
Answer: C (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-policy-rules/nat-policy-overview

NEW QUESTION: 36
Which two configuration settings shown are not the default? (Choose two.)



A. Enable Security Log
B. Server Log Monitor Frequency (sec)
C. Enable Session
D. Enable Probing
Answer: (SHOW ANSWER)
By default - Server Log Monitor Frequency (sec) - 2
By default - Enable Session - disabled

NEW QUESTION: 37
Which two configuration settings shown are not the default? (Choose two.)



A. Enable Security Log

B. Server Log Monitor Frequency (sec)

C. Enable Session

D. Enable Probing

Answer: B,C (LEAVE A REPLY)

https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/user-identification/device-user-identification-user-mapping/enable-server-monitoring

NEW QUESTION: 38

An administrator wants to prevent users from submitting corporate credentials in a phishing attack.

Which Security profile should be applied?

A. antivirus

B. anti-spyware

C. URL-filtering

D. vulnerability protection

Answer: C (LEAVE A REPLY)

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up-credential-phishing-prevention.html#idc77030dc-6022-4458-8c50-1dc0fe7cffe4

NEW QUESTION: 39
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 decrypted.
B. The traffic was denied by security profile.
C. The traffic was denied by URL filtering.
D. The web session was unsuccessfully decrypted.
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which two rule types allow the administrator to modify the destination zone? (Choose two.)
A. interzone
B. shadowed
C. intrazone
D. universal
Answer: A,D (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

NEW QUESTION: 41
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.
Answer: D (LEAVE A REPLY)
Security Profiles are added to the end of Security policy rules. After a packet has been allowed by the Security policy.

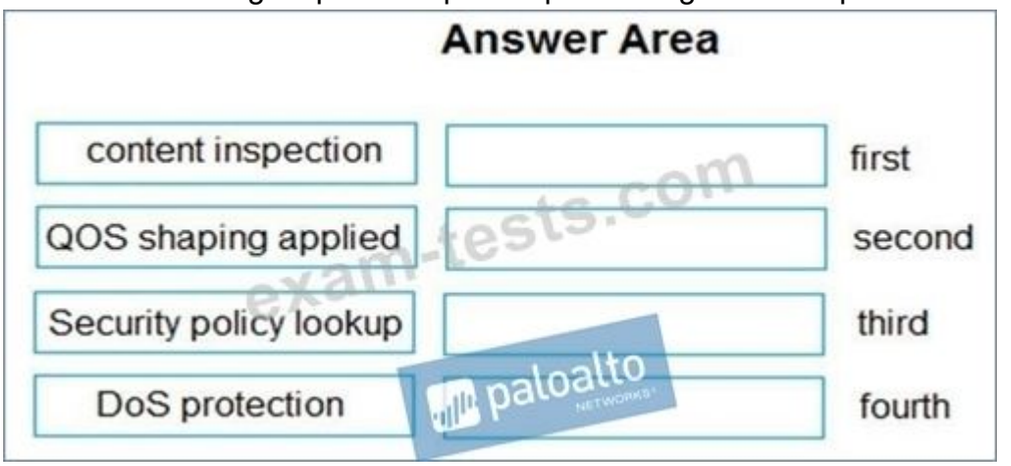
NEW QUESTION: 42
A NetSec manager was asked to create a new firewall administrator profile with customized privileges. The new firewall administrator must be able to download TSF File and Starts Dump File but must not be able to reboot the device.
Where does the NetSec manager go to configure the new firewall administrator role profile?
A. Device > Admin Roles > Add > XML API > Operational Request
B. Device > Admin Roles > Add > XML API > Configuration
C. Device > Admin Roles > Add > Web UI > Support
D. Device > Admin Roles > Add > Web UI > Operations

Answer: (SHOW ANSWER)

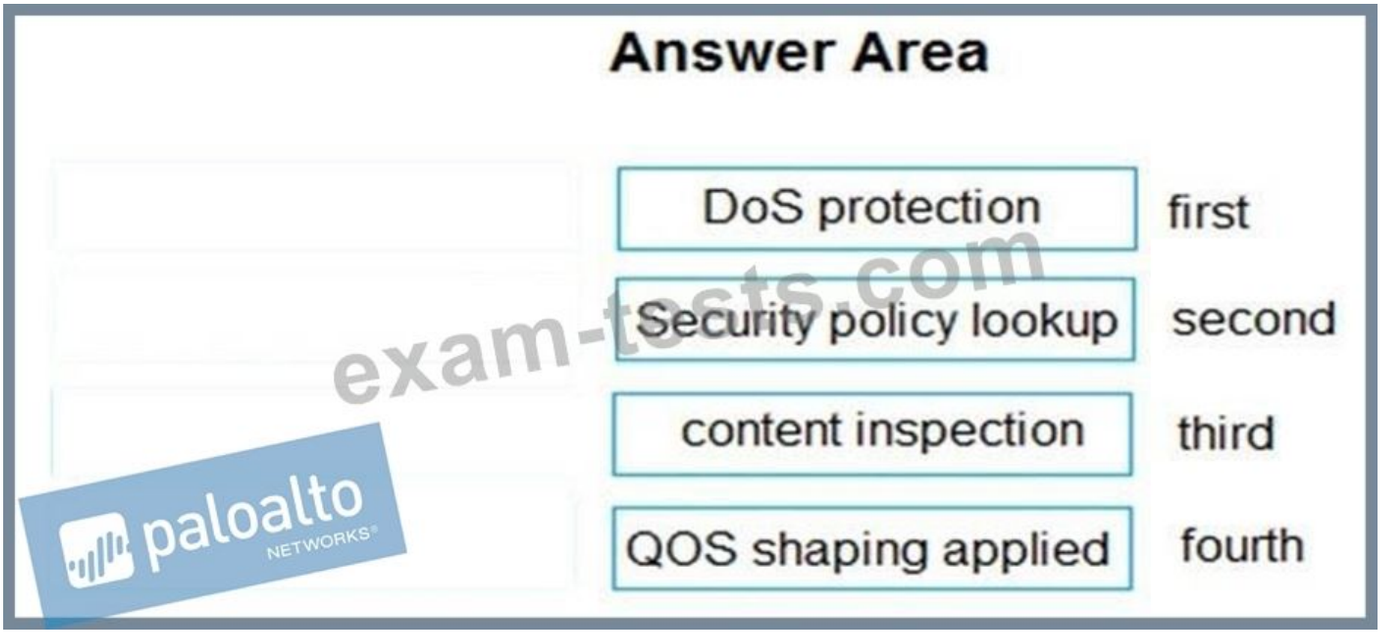
NEW QUESTION: 43

Drag and Drop Question

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



Answer:



Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0

NEW QUESTION: 44

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

A. Dynamic

B. Superuser

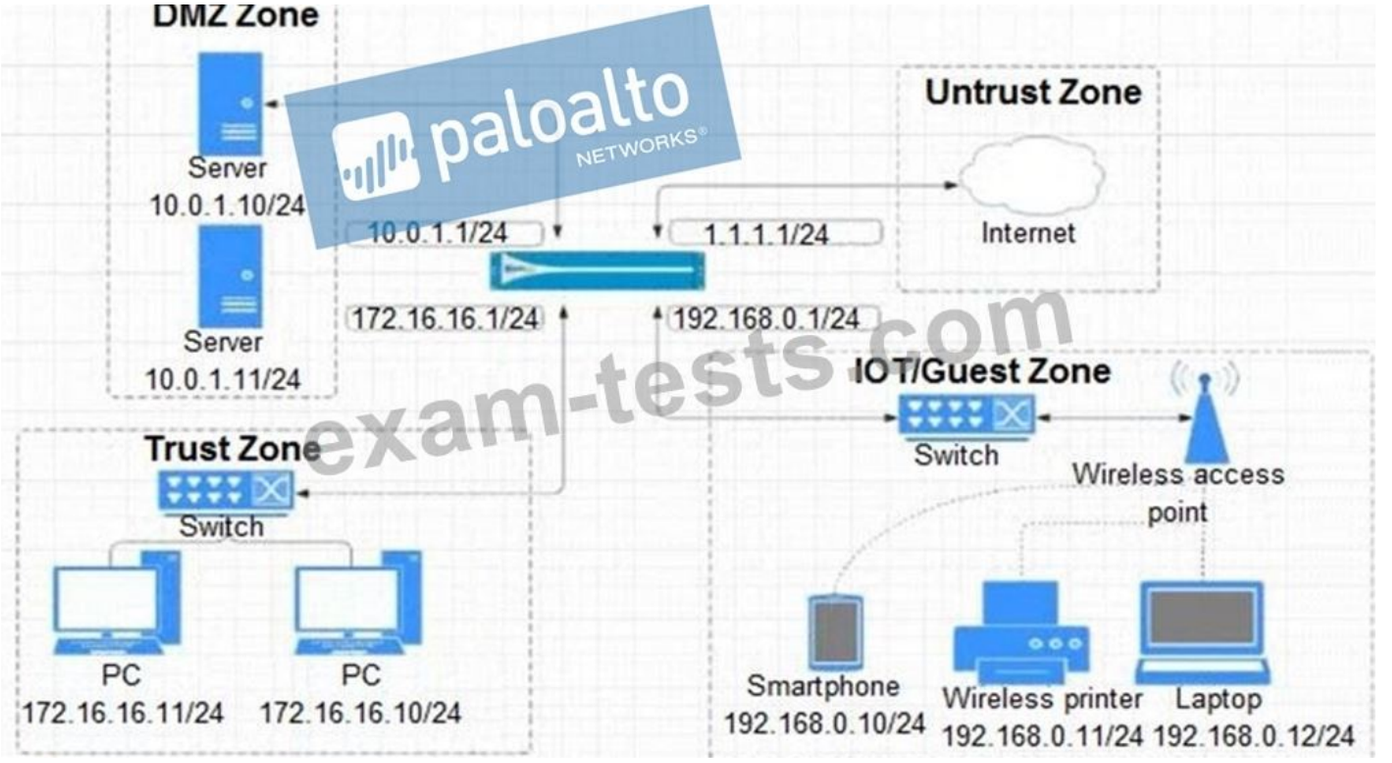
C. Root

D. Role-based

Answer: D (LEAVE A REPLY)

NEW QUESTION: 45

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 ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	S
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	

B.

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE
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 ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE
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 ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
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

Answer: (SHOW ANSWER)

NEW QUESTION: 46

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. The Log Forwarding profile is not configured on the policy.
C. Logging on the interzone-default policy is disabled
D. Traffic is being denied on the interzone-default policy.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 47
Which interface does not require a MAC or IP address?
A. Layer2
B. Virtual Wire
C. Layer3
D. Loopback
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
Which data flow direction is protected in a zero trust firewall deployment that is not protected in a perimeter-only firewall deployment?
A. east west
B. north south
C. outbound
D. inbound
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which two statements are correct about App-ID content updates? (Choose two.)
A. After an application content update, new applications are automatically identified and classified
B. Existing security policy rules are not affected by application content updates
C. Updated application content may change how security policy rules are enforced

D. After an application content update, new applications must be manually classified prior to use
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 50
Which two statements are true for the DNS Security service introduced in PAN-OS version 10.0? (Choose two.)
A. It removes the 100K limit for DNS entries for the downloaded DNS updates.
B. It eliminates the need for dynamic DNS updates.
C. It functions like PAN-DB and requires activation through the app portal.
D. It is automatically enabled and configured.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 51
Which administrative management services can be configured to access a management interface?
A. HTTP, CLI, SNMP, HTTPS
B. HTTPS, SSH, telnet, SNMP
C. SSH, telnet, HTTP, HTTPS
D. HTTPS, HTTP, CLI, API
Answer: (SHOW ANSWER)
The administrative management services are http, https, telnet and ssh.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/management-interfaces

NEW QUESTION: 52
Which verdict may be assigned to a WildFire sample?
A. Phishing
B. Spyware
C. PUP
D. Malware
Answer: A (LEAVE A REPLY)
https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts

NEW QUESTION: 53
Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

A. engress outside
B. internal-inside-dmz
C. inside-portal
D. intercone-default
Answer: D (LEAVE A REPLY)

NEW QUESTION: 54
An administrator configured a Security policy rule with an Antivirus Security profile. The administrator did not change the action for the profile.
If a virus gets detected, how will the firewall handle the traffic?
A. It allows the traffic but generates an entry in the Threat logs.
B. It drops the traffic because the profile was not set to explicitly allow the traffic.
C. It uses the default action assigned to the virus signature.
D. It allows the traffic because the profile was not set the explicitly deny the traffic.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
Which profile must be applied to the Security policy rule to block spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers?
A. Anti-spyware
B. File blocking
C. WildFire
D. URL filtering
Answer: A (LEAVE A REPLY)
Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients.
https://docs.paloaltonetworks.com/network-security/security-policy/security-profiles/security-profile-anti-spyware

NEW QUESTION: 56

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

A. Threat Implementation License

B. Threat Environment License

C. Threat Prevention License

D. Threat Protection License

Answer: C (LEAVE A REPLY)

NEW QUESTION: 57

An administrator would like to override the default deny action for a given application, and instead would like to block the traffic and send the ICMP code "communication with the destination is administratively prohibited".

Which security policy action causes this?

A. Drop

B. Drop, send ICMP Unreachable

C. Reset both

D. Reset server

Answer: B (LEAVE A REPLY)

Silently drops the traffic; for an application, it overrides the default deny action. A TCP reset is not sent to the host/application.

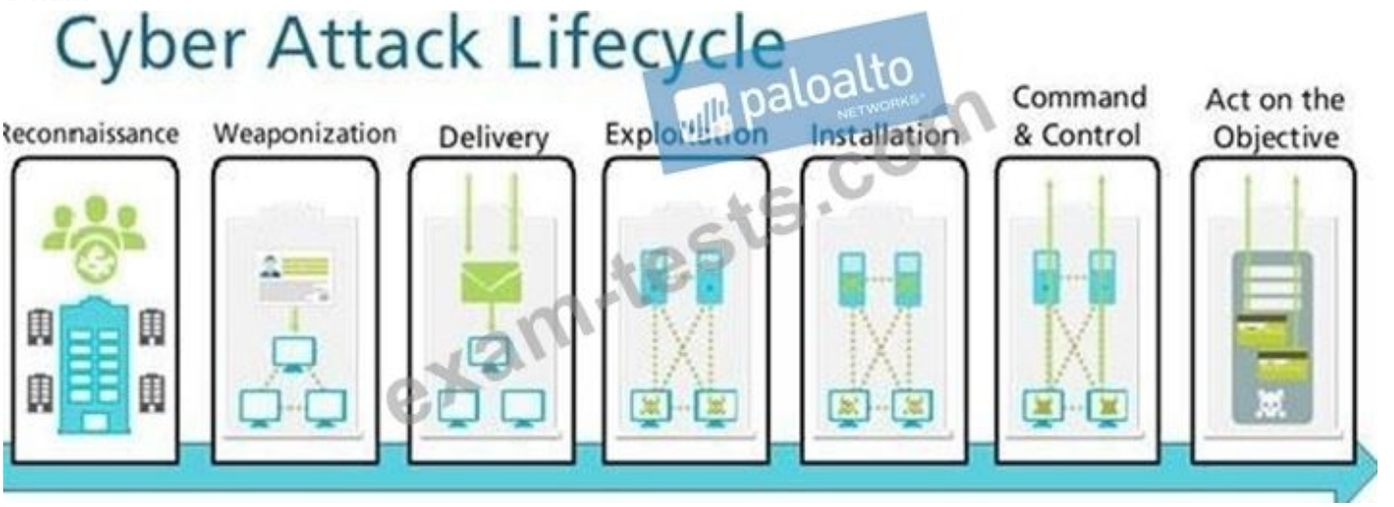
For Layer 3 interfaces, to optionally send an ICMP unreachable response to the client, set Action: Drop and enable the Send ICMP Unreachable

check box. When enabled, the firewall sends the ICMP code for communication with the destination is administratively prohibited--ICMPv4: Type 3, Code 13; ICMPv6: Type 1, Code 1.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClltCAC#:~:text=The% 20Deny%20action%20will%20tear,packets%20will%20be%20silently%20discarded.

NEW QUESTION: 58

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



A. delivery
B. command and control
C. exploitation
D. reinsurance
E. installation
Answer: (SHOW ANSWER)
Delivery: This stage marks the transition from the attacker working outside of an organization's network to working within an organization's network. Malware delivered during this stage is designed to exploit existing software vulnerabilities. To deliver its initial malware, the attacker might choose to embed malicious code within seemingly innocuous PDF or Word files, or within an email message.

NEW QUESTION: 59
Which User-ID agent would be appropriate in a network with multiple WAN links, limited network bandwidth, and limited firewall management plane resources?
A. Windows-based agent deployed on the internal network
B. PAN-OS integrated agent deployed on the internal network
C. Citrix terminal server deployed on the internal network
D. Windows-based agent deployed on each of the WAN Links
Answer: A (LEAVE A REPLY)
Explanation
Another reason to choose the Windows agent over the integrated PAN-OS agent is to save processing cycles on the firewall's management plane.

NEW QUESTION: 60
Where within the firewall GUI can all existing tags be viewed?
A. Monitor > Tags
B. Objects > Tags
C. Policies > Tags
D. Network > Tags
Answer: B (LEAVE A REPLY)

NEW QUESTION: 61
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
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/dns-security/enable-dns-security.html

NEW QUESTION: 62
Which three factors can be used to create malware based on domain generation algorithms? (Choose three.)
A. Time of day
B. URL custom categories
C. Other unique values
D. Cryptographic keys
E. IP address
Answer: A,C,D (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/dns-security/domain-generation-algorithm-detection

NEW QUESTION: 63
Why should a company have a File Blocking profile that is attached to a Security policy?
A. To detonate files in a sandbox environment
B. To analyze file types
C. To block uploading and downloading of specific types of files
D. To block uploading and downloading of any type of files
Answer: C (LEAVE A REPLY)

NEW QUESTION: 64
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. USER-ID = `Allow users in Trusted'
C. Application = `Telnet'
D. Log Forwarding
Answer: C (LEAVE A REPLY)

NEW QUESTION: 65

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
Answer: B (LEAVE A REPLY)
Which User-ID agent should I use?
Use agentless (PAN-OS)
If you have a small to medium deployment with 10 or fewer Domain controllers or Exchange servers If you wish to share PAN-OS sourced mappings from AD, Captive portal or Global Protect with other PA devices (max 255 devices) Use User-ID Agent (Windows) If you have medium to large deployment with more than 10 domain controllers If you have multi-domain setup with large number of servers to monitor

NEW QUESTION: 66
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
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

NEW QUESTION: 67
In which threat profile object would you configure the DNS Security service?
A. WildFire
B. URL Filtering
C. Anti-Spyware
D. Antivirus
Answer: C (LEAVE A REPLY)

NEW QUESTION: 68
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
Answer: (SHOW ANSWER)

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/activate-licenses-and-subscriptions.html

NEW QUESTION: 69
Given the detailed log information above, what was the result of the firewall traffic inspection?

A. It was blocked by the Security policy action.
B. It was blocked by the Anti-Virus Security profile action.
C. It was blocked by the Anti-Spyware Profile action.
D. It was blocked by the Vulnerability Protection profile action.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 70
Which two security profile types can be attached to a security policy? (Choose two.)
A. threat
B. DDoS protection
C. vulnerability
D. antivirus
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 71
Which dynamic update type includes updated anti-spyware signatures?
A. Antivirus
B. PAN-DB
C. Applications and Threats
D. GlobalProtect Data File
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72

Which two configurations does an administrator need to compare in order to see differences between the active configuration and potential changes if committed? (Choose two.)

A. Active

B. Running

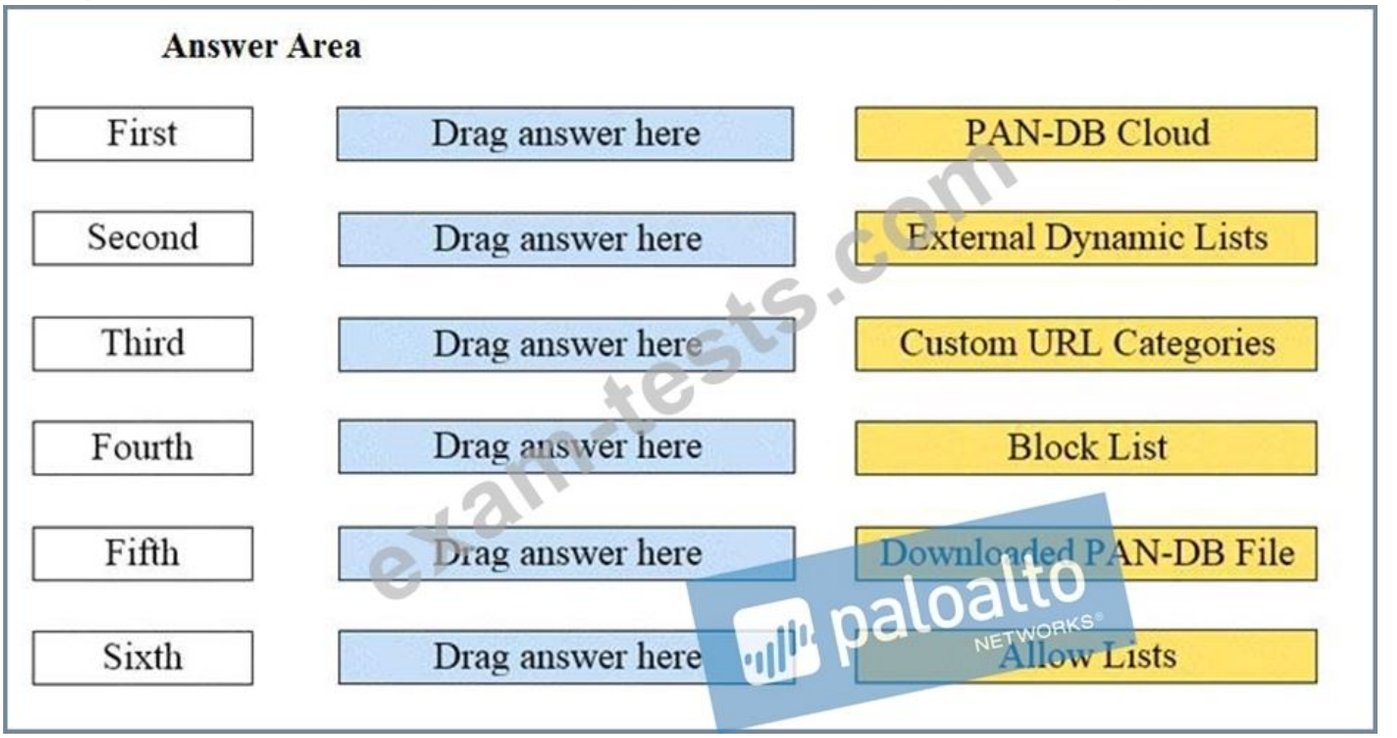
C. Device state

D. Candidate

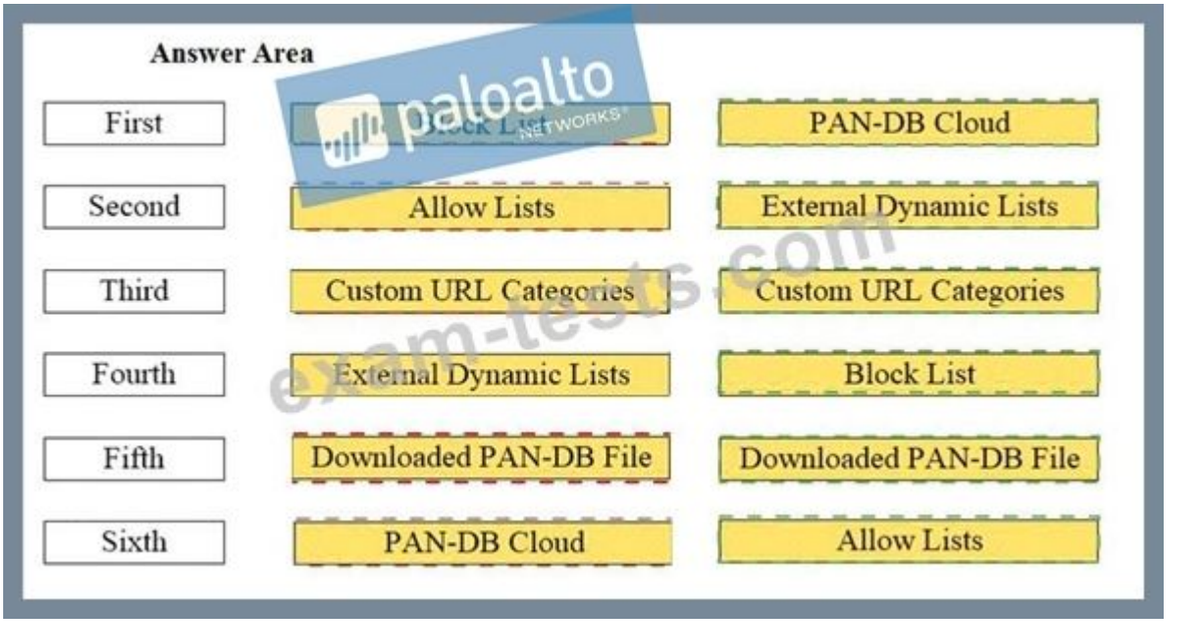
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 73

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



Answer:



Explanation

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

NEW QUESTION: 74
Based on the screenshot what is the purpose of the group in User labelled "it"?

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

A. Allows "any" users to access servers in the DMZ zone
B. Allows users in group "DMZ" lo access IT applications
C. Allows users in group "it" to access IT applications
D. Allows users to access IT applications on all ports
Answer: C (LEAVE A REPLY)

NEW QUESTION: 75
In which profile should you configure the DNS Security feature?
A. URL Filtering Profile
B. Anti-Spyware Profile
C. Zone Protection Profile
D. Antivirus Profile
Answer: B (LEAVE A REPLY)
Reference:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/dns-security/enable- dnssecurity.html

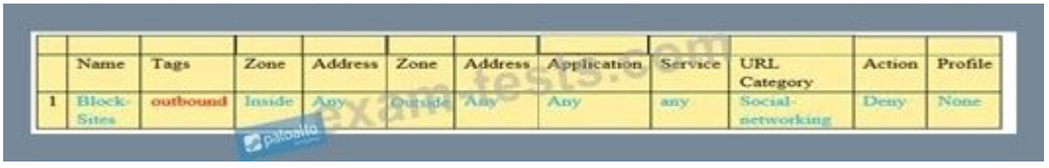
NEW QUESTION: 76
Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)

A. Path monitoring determines if route is useable

B. Route with highest metric is actively used
C. Path monitoring does not determine if route is useable
D. Route with lowest metric is actively used
Answer: (SHOW ANSWER)

NEW QUESTION: 77
A Panorama administrator would like to create an address object for the DNS server located in the New York City office, but does not want this object added to the other Panorama managed firewalls.
Which configuration action should the administrator take when creating the address object?
A. Tag the address object with the New York Office tag.
B. Ensure that Disable Override is cleared.
C. Ensure that the Shared option is checked.
D. Ensure that the Shared option is cleared.
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-device-groups/manage-unused-shared-objects

NEW QUESTION: 78
In the example security policy shown, which two websites fcked? (Choose two.)



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

A. Amazon
B. LinkedIn
C. YouTube
D. Facebook
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 79

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

A. Drop

B. Deny

C. Reset server

D. Reset client

Answer: B (LEAVE A REPLY)

NEW QUESTION: 80

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. EIGRP

B. BGP

C. RIP

D. IS-IS

E. OSPF

Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 81

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

A. Captive Portal

B. Windows session monitoring via a domain controller

C. passive server monitoring using a PAN-OS integrated User-ID agent

D. passive server monitoring using the Windows-based agent

Answer: A (LEAVE A REPLY)

NEW QUESTION: 82

Which option is part of the content inspection process?

A. SSL Proxy re-encrypt

B. Packet forwarding process

C. Packet egress process

D. IPsec tunnel encryption

Answer: A (LEAVE A REPLY)

NEW QUESTION: 83

Which action results in the firewall blocking network traffic with out notifying the sender?

A. Reset Client

B. Deny

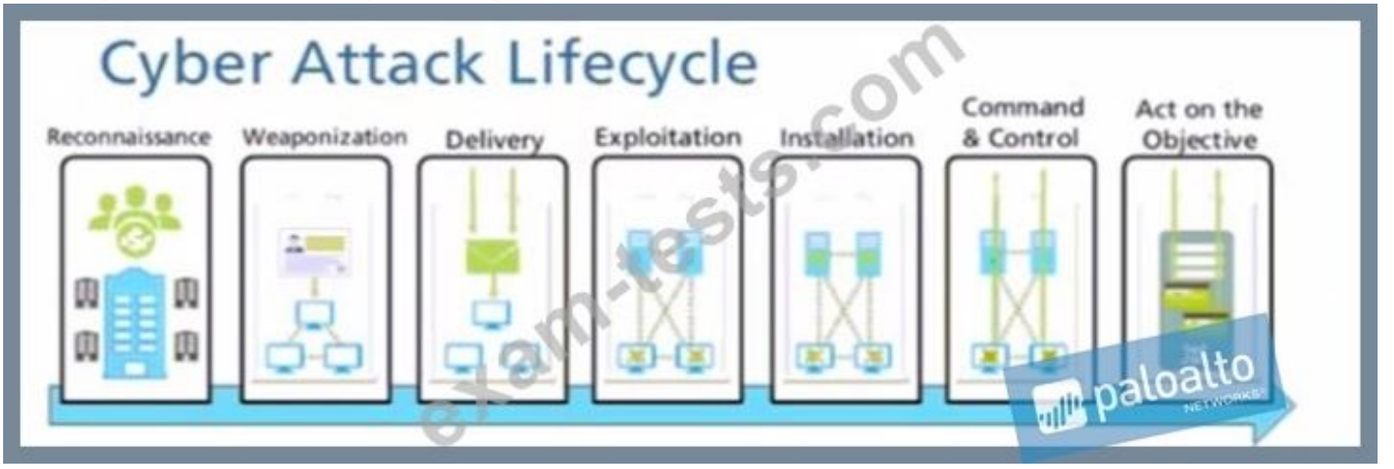
C. Reset Server

D. Drop

Answer: (SHOW ANSWER)

NEW QUESTION: 84

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



A. Exploitation

B. Reconnaissance

C. Installation

D. Act on the Objective

Answer: A (LEAVE A REPLY)

NEW QUESTION: 85

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

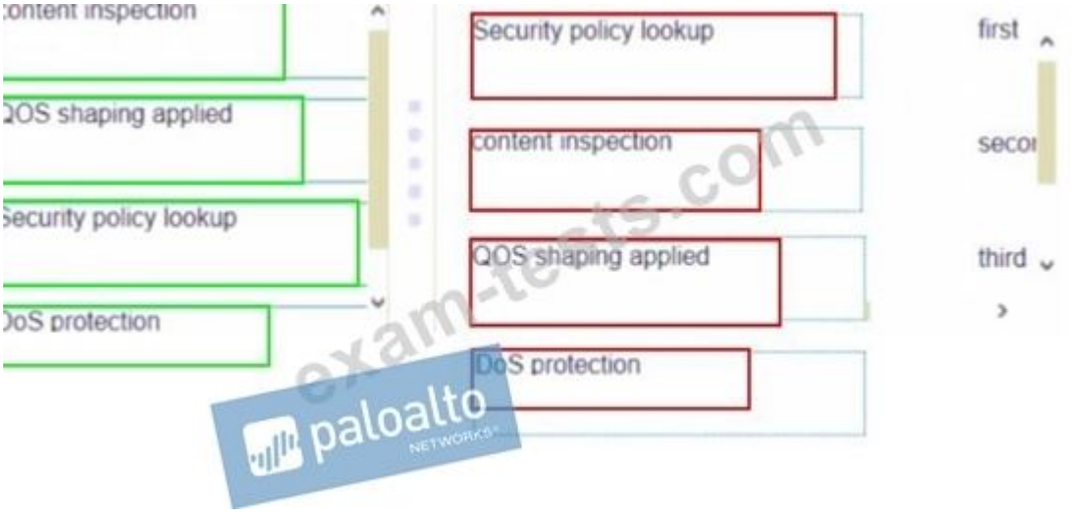
Answer: A,D (LEAVE A REPLY)

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-an-admin-role-profile

NEW QUESTION: 86

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

Answer:



NEW QUESTION: 87
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 groups applications based on application attributes such as category and subcategory.
C. It dynamically filters applications based on critical, high, medium, low. or informational severity.
D. It dynamically provides application statistics based on network, threat, and blocked activity,
Answer: B (LEAVE A REPLY)

NEW QUESTION: 88
Based on the screenshot what is the purpose of the group in User labelled "it"?

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

A. Allows users in group "it" to access IT applications
B. Allows users to access IT applications on all ports

C. Allows "any" users to access servers in the DMZ zone
D. Allows users in group "DMZ" lo access IT applications
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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.
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 90
Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?
A. GlobalProtect
B. AutoFocus
C. Aperture
D. Panorama
Answer: A (LEAVE A REPLY)
GlobalProtect: GlobalProtect safeguards your mobile workforce by inspecting all traffic using your next-generation firewalls deployed as internet gateways, whether at the perimeter, in the Demilitarized Zone (DMZ), or in the cloud.

NEW QUESTION: 91
Drag and Drop Question
Place the steps in the correct packet-processing order of operations.

Answer:

NEW QUESTION: 92

Based on the Security policy rules shown, SSH will be allowed on which port?

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

A. the default port

B. only ephemeral ports

C. any port

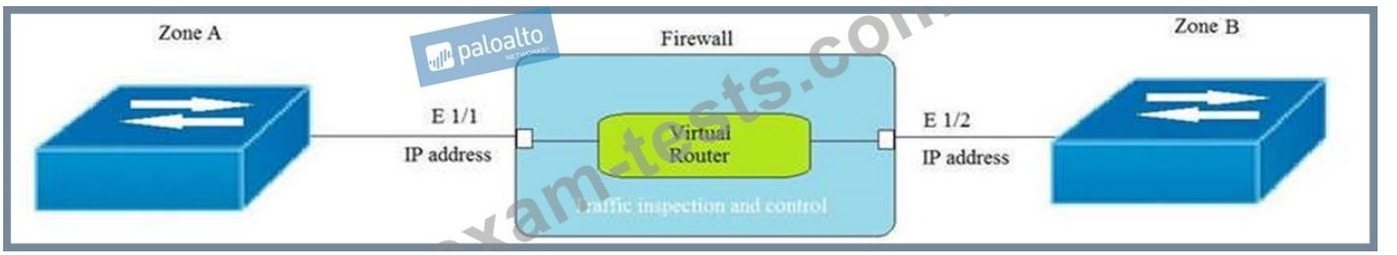
D. same port as ssl and snmpv3

Answer: A (LEAVE A REPLY)

Application-default means the default port will be used. In this case for SSH port 22.

NEW QUESTION: 93

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



A. Layer2

B. Tap

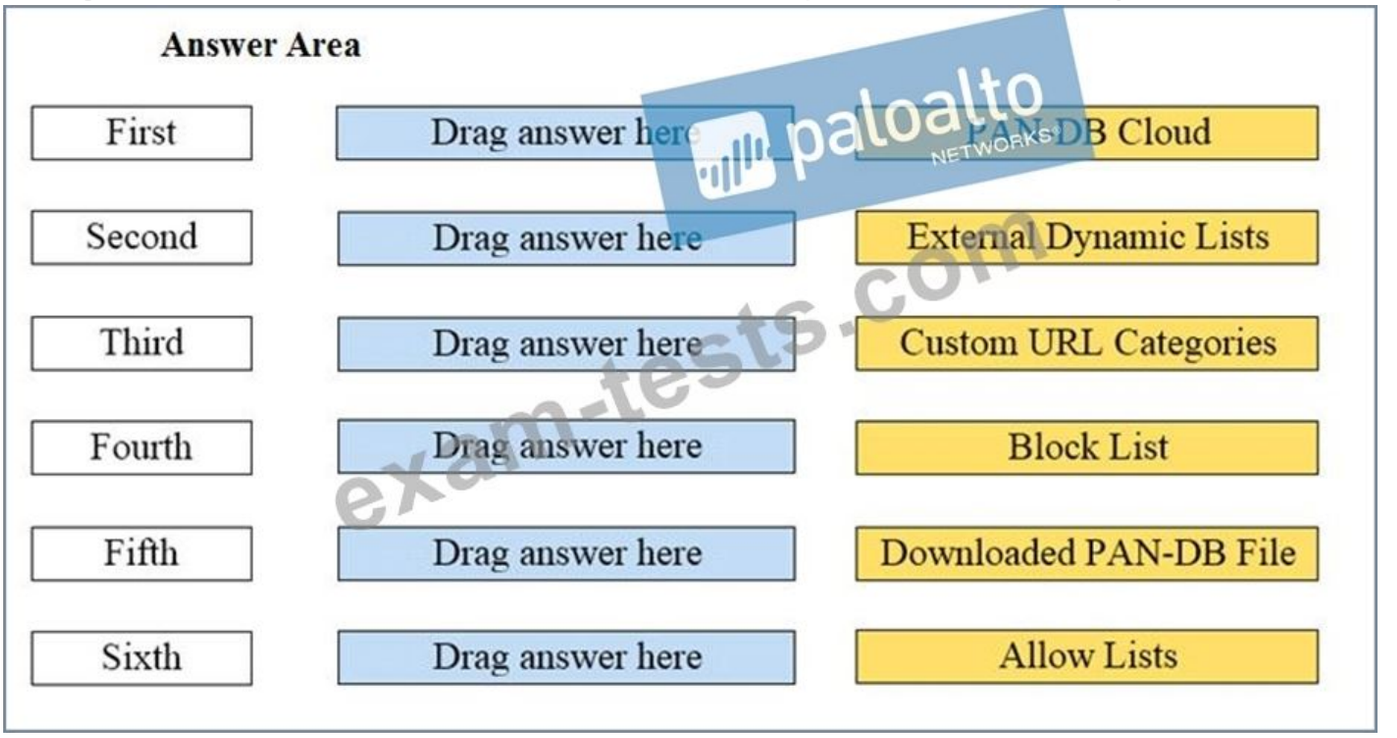
C. Virtual Wire

D. Layer3

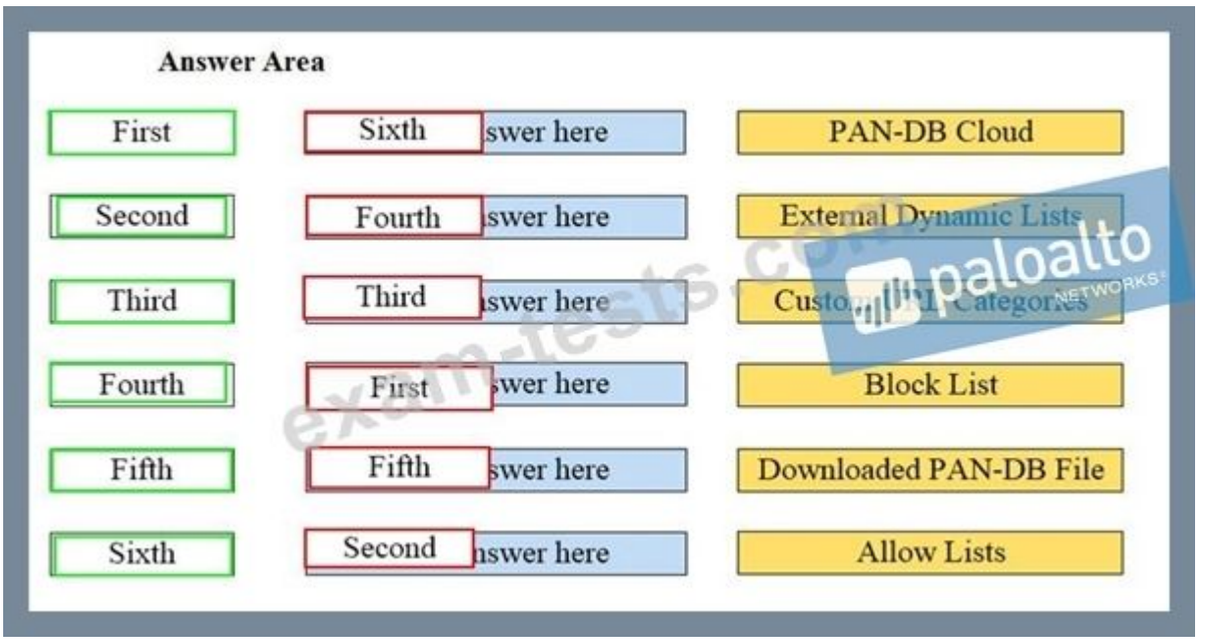
Answer: D (LEAVE A REPLY)

NEW QUESTION: 94

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



Answer:



NEW QUESTION: 95

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

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

A. Facebook

B. LinkedIn

C. YouTube

D. Amazon

Answer: (SHOW ANSWER)

NEW QUESTION: 96

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

A. Device>Setup>Services

B. Device>Setup>Management

C. Device>Setup>Operations

D. Device>Setup>Interfaces

Answer: (SHOW ANSWER)

NEW QUESTION: 97

By default, which action is assigned to the intrazone-default rule?

A. Reset-server

B. Reset-client

C. Deny

D. Allow

Answer: D (LEAVE A REPLY)

NEW QUESTION: 98
Which statement is true regarding a Prevention Posture Assessment?
A. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
C. It provides a percentage of adoption for each assessment area
D. It performs over 200 security checks on Panorama/firewall for the assessment
Answer: B (LEAVE A REPLY)
Prevention Posture Assessment (PPA) - The PPA is a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture. The PPA not only helps to identify all security risks, it also provides detailed suggestions on how to prevent the risks and close the gaps. The assessment, guided by an experienced Palo Alto Networks sales engineer, helps determine the areas of greatest risk where you should focus prevention activities. You can run the PPA on firewalls and on Panorama.
https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best-practice-security-policy/use-palo-alto-networks-assessment-and-review-tools

NEW QUESTION: 99
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
Answer: (SHOW ANSWER)
Explanation/Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClN7CAK

NEW QUESTION: 100
How frequently can wildfire updates be made available to firewalls?
A. every 5 minutes
B. every 60 minutes
C. every 30 minutes
D. every 15 minutes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 101
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. universal
B. intrazone
C. interzone
D. default
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Based on the screenshot, what is the purpose of the group in User labelled "it"?

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

A. Allows users to access IT applications on all ports.
B. Allow users in group "DMZ" to access IT applications.
C. Allows "any" users to access servers in the DMZ zone.
D. Allow users in group "it" to access IT applications.
Answer: D (LEAVE A REPLY)

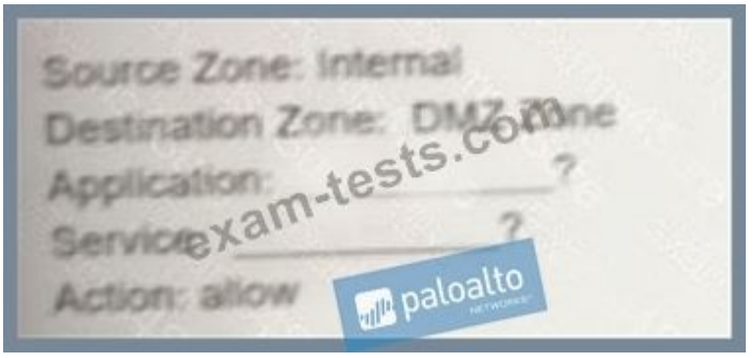
NEW QUESTION: 103
Which two App-ID applications will need to be allowed to use Facebook-chat? (Choose two.)
A. facebook
B. facebook-chat
C. facebook-base
D. facebook-email
Answer: (SHOW ANSWER)
If you wanted to chat, then facebook-base and facebook-chat would need to be allowed in the same rule.

NEW QUESTION: 104
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
Answer: B,C,E (LEAVE A REPLY)

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIN7CAK

NEW QUESTION: 105
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. destination zone
C. source address
D. source zone
Answer: (SHOW ANSWER)

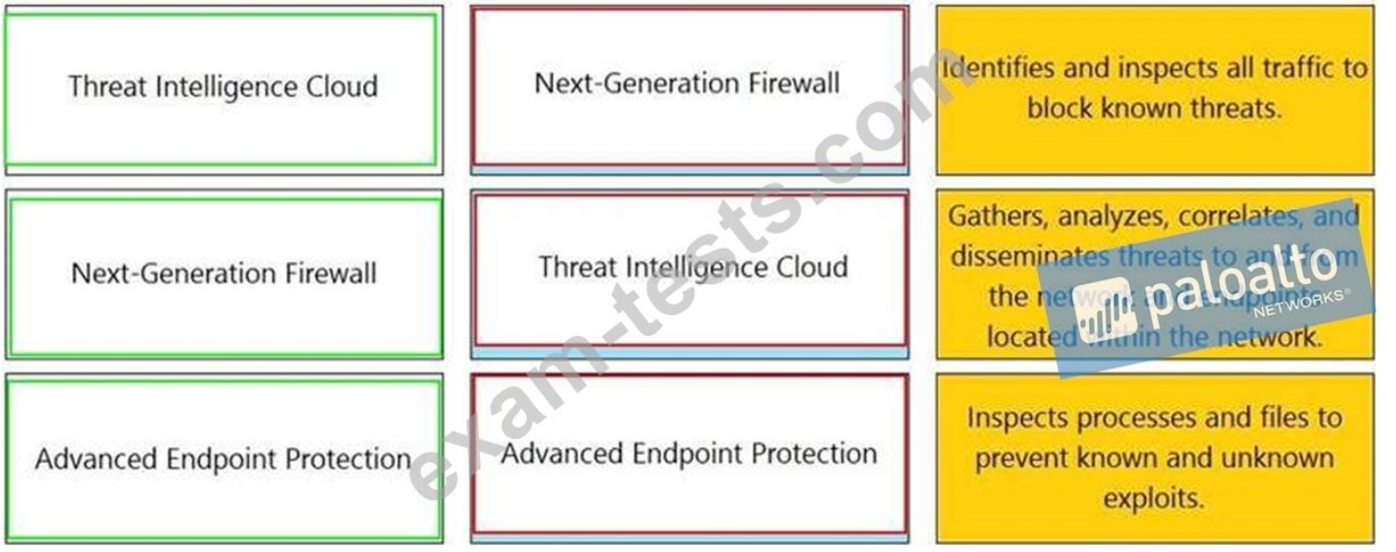
NEW QUESTION: 106
All users from the internal zone must be allowed only Telnet access to a server in the DMZ zone.
Complete the two empty fields in the Security Policy rules that permits only this type of access.



Choose two.
A. Application = "Telnet"
B. Application = "any"
C. Service - "application-default"
D. Service = "any"
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 107
Match each feature to the DoS Protection Policy or the DoS Protection Profile.

Answer:



NEW QUESTION: 108

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

A. Override

B. Allow

C. Block

D. Continue

Answer: (SHOW ANSWER)

References:

NEW QUESTION: 109

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

A. on either the data place 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.
Answer: B (LEAVE A REPLY)
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html

NEW QUESTION: 110
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, the 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
Answer: A (LEAVE A REPLY)
An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the Subcategory office-programs. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes you defined for the filter.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in -policy/create-an-application-filter.html

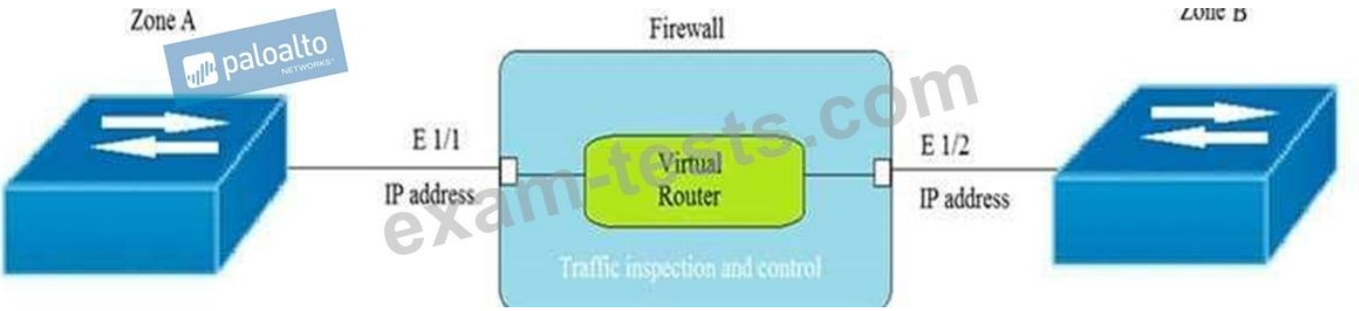
NEW QUESTION: 111
An administrator would like to apply a more restrictive Security profile to traffic for file sharing applications. The administrator does not want to update the Security policy or object when new applications are released.
Which object should the administrator use as a match condition in the Security policy?
A. the Content Delivery Networks URL category
B. the Online Storage and Backup URL category
C. an application group containing all of the file-sharing App-IDs reported in the traffic logs
D. an application filter for applications whose subcategory is file-sharing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
Which URL profiling action does not generate a log entry when a user attempts to access that URL?
A. Override
B. Allow
C. Block
D. Continue
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/url-filtering/url-filtering-concepts/url- filtering-profile-actions

NEW QUESTION: 113
An administrator needs to create a Security policy rule that matches DNS traffic within the LAN zone, and also needs to match DNS traffic within the DMZ zone.
The administrator does not want to allow traffic between the DMZ and LAN zones.
Which Security policy rule type should they use?
A. default
B. universal
C. intrazone
D. interzone
Answer: A (LEAVE A REPLY)
Explanation/Reference:

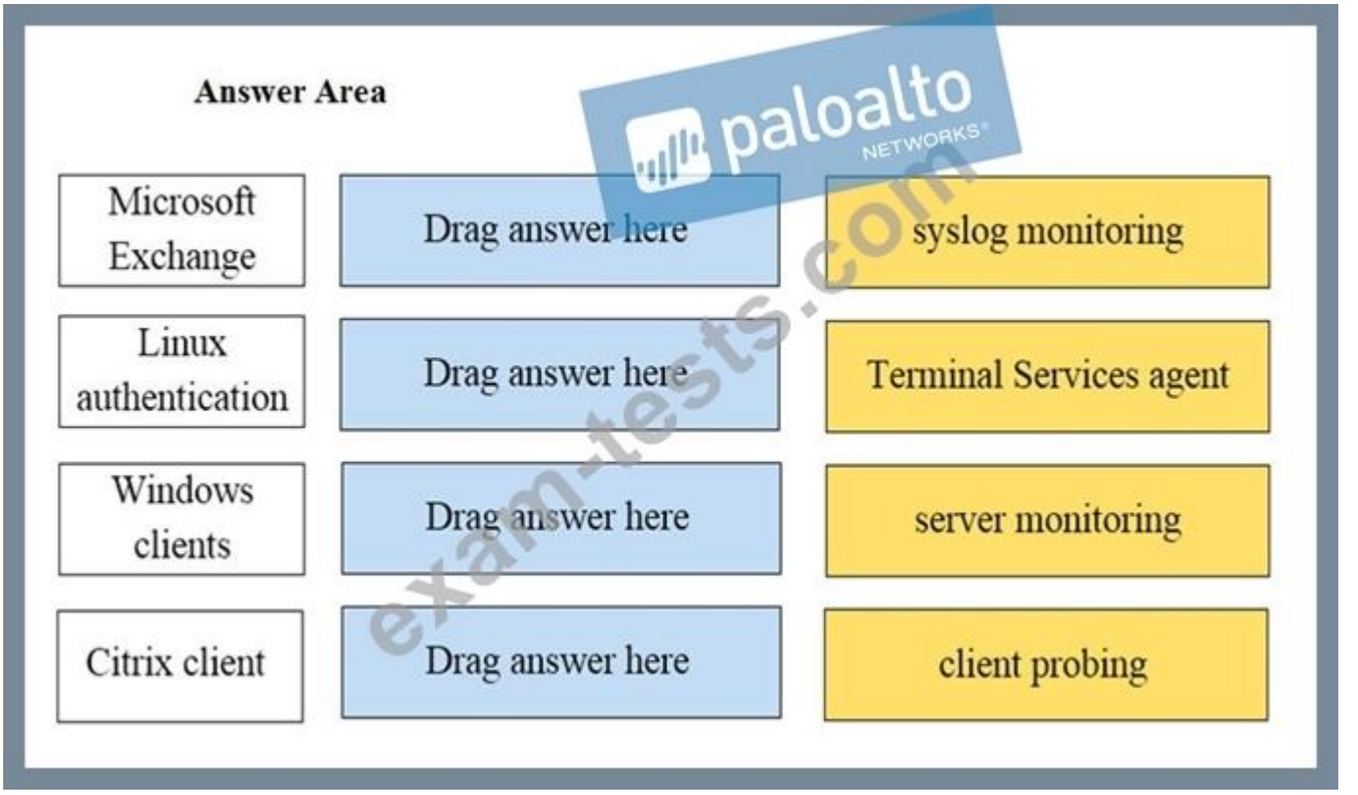
NEW QUESTION: 114
Which interface type requires no routing or switching but applies Security or NAT policy rules before passing allowed traffic?
A. Tap
B. Virtual Wire
C. Layer 2
D. Layer 3
Answer: (SHOW ANSWER)
A virtual wire logically binds two Ethernet interfaces together, allowing for all traffic to pass between the interfaces, or just traffic with selected VLAN tags (no other switching or routing services are available). You can create virtual wire subinterfaces to classify traffic according to an IP address, IP range, or subnet. A virtual wire requires no changes to adjacent network devices. A virtual wire can bind two Ethernet interfaces of the same medium (both copper or both fiber optic), or bind a copper interface to a fiber optic interface.

NEW QUESTION: 115
Given the topology, which zone type should zone A and zone B to be configured with?



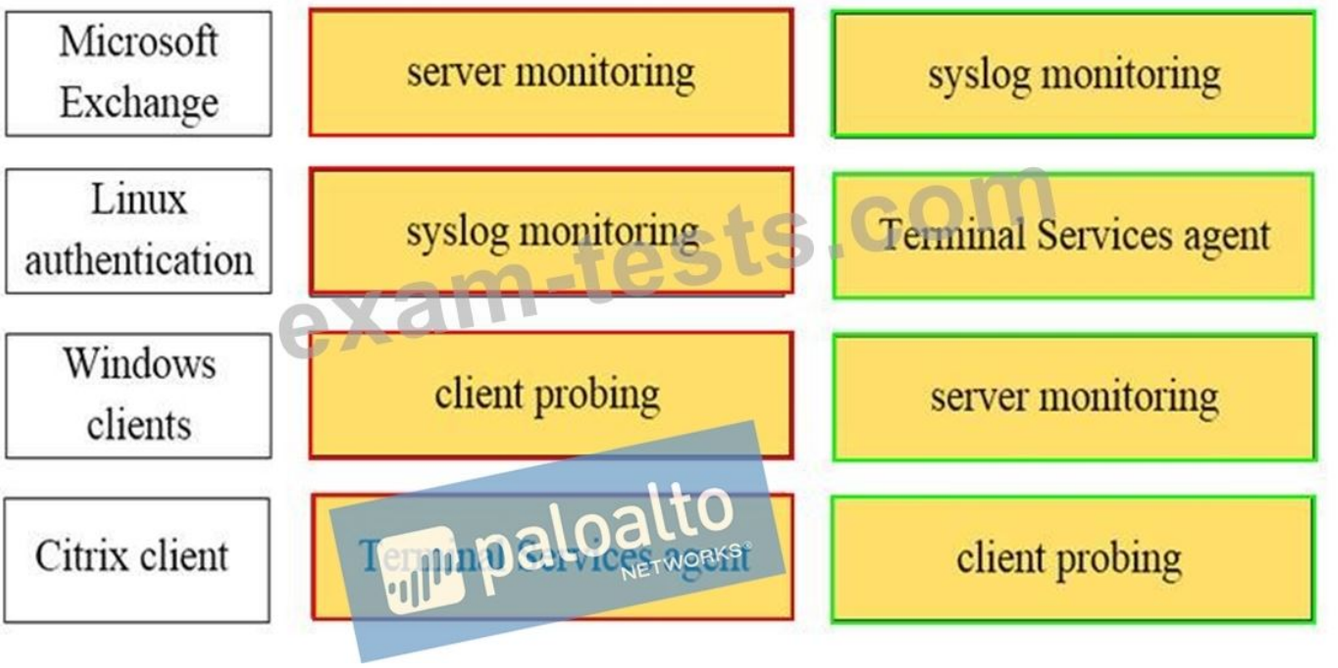
A. Layer2
B. Virtual Wire
C. Layer3
D. Tap
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Match the network device with the correct User-ID technology.



Answer:

Answer Area



NEW QUESTION: 117
During the packet flow process, which two processes are performed in application identification? (Choose two.)
A. application changed from content inspection
B. pattern based application identification
C. session application identified
D. application override policy match
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Which administrator type utilizes predefined roles for a local administrator account?
A. Superuser
B. Role-based
C. Dynamic
D. Device administrator
Answer: (SHOW ANSWER)
Dynamic roles: These are built-in or predefined roles that provide access to the firewall. When new features are added, the firewall automatically updates the definitions of Dynamic roles; you never need to manually update them.

NEW QUESTION: 119
In which profile should you configure the DNS Security feature?
A. URL Filtering Profile

B. Zone Protection Profile
C. Antivirus Profile
D. Anti-Spyware Profile
Answer: D (LEAVE A REPLY)

NEW QUESTION: 120
Which type security policy rule would match traffic flowing between the inside zone and outside zone within the inside zone and within the outside zone?
A. interzone
B. global
C. intrazone
D. universal
Answer: (SHOW ANSWER)

NEW QUESTION: 121
What must be configured for the firewall to access multiple authentication profiles for external services to authenticate a non-local account?
A. authentication sequence
B. LDAP server profile
C. authentication server list
D. authentication list profile
Answer: A (LEAVE A REPLY)
Explanation/Reference:
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/framemaker/pan-os/7-1/pan-os-admin.pdf page 144

NEW QUESTION: 122
Which objects would be useful for combining several services that are often defined together?
A. service groups
B. shared service objects
C. application groups
D. application filters

Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
Which profile should be used to obtain a verdict regarding analyzed files?
A. WildFire analysis
B. Vulnerability profile
C. Content-ID
D. Advanced threat prevention
Answer: A (LEAVE A REPLY)
A profile is a set of rules or settings that defines how the firewall performs a specific function, such as detecting and preventing threats, filtering URLs, or decrypting traffic1.
There are different types of profiles that can be applied to different types of traffic or scenarios, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, Decryption, or WildFire Analysis1.
The WildFire Analysis profile is a profile that enables the firewall to submit unknown files or email links to the cloud-based WildFire service for analysis and verdict determination2. WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware3. WildFire uses a variety of malware detection techniques, such as static analysis, dynamic analysis, machine learning, and intelligent run-time memory analysis, to identify and protect against unknown threats34.
The Vulnerability Protection profile is a profile that protects the network from exploits that target known software vulnerabilities. It allows the administrator to configure the actions and log settings for each vulnerability severity level, such as critical, high, medium, low, or informational5.
Content-ID is not a profile, but a feature of the firewall that performs multiple functions to identify and control applications, users, content, and threats on the network. Content-ID consists of four components: App-ID, User-ID, Content Inspection, and Threat Prevention.
Advanced Threat Prevention is not a profile, but a term that refers to the comprehensive approach of Palo Alto Networks to prevent sophisticated and unknown threats. Advanced Threat Prevention includes WildFire, but also other products and services, such as DNS Security, Cortex XDR, Cortex XSOAR, and AutoFocus.
Therefore, the profile that should be used to obtain a verdict regarding analyzed files is the WildFire Analysis profile.
References:
1: Security Profiles - Palo Alto Networks 2: WildFire Analysis Profile - Palo Alto Networks 3: WildFire - Palo Alto Networks 4: Advanced Wildfire as an ICAP Alternative | Palo Alto Networks 5: Vulnerability Protection Profile - Palo Alto Networks : [Content-ID - Palo Alto Networks] : [Advanced Threat Prevention - Palo Alto Networks]

NEW QUESTION: 124
Complete the statement. A security profile can block or allow traffic
A. on unknown-tcp or unknown-udp traffic

B. after it is evaluated by a security policy that allows traffic
C. before it is evaluated by a security policy
D. after it is evaluated by a security policy that allows or blocks traffic
Answer: B (LEAVE A REPLY)
Security profiles are objects added to policy rules that are configured with an action of allow.

NEW QUESTION: 125
Which statement is true regarding a Best Practice Assessment?
A. The BPA tool can be run only on firewalls
B. It provides a percentage of adoption for each assessment 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
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best- practice-security-policy/use-palo-alto-networks-assessment-and-review-tools

NEW QUESTION: 126
Access to which feature requires PAN-OS Filtering licens?
A. Custom URL categories
B. DNS Security
C. PAN-DB database
D. URL external dynamic lists
Answer: (SHOW ANSWER)

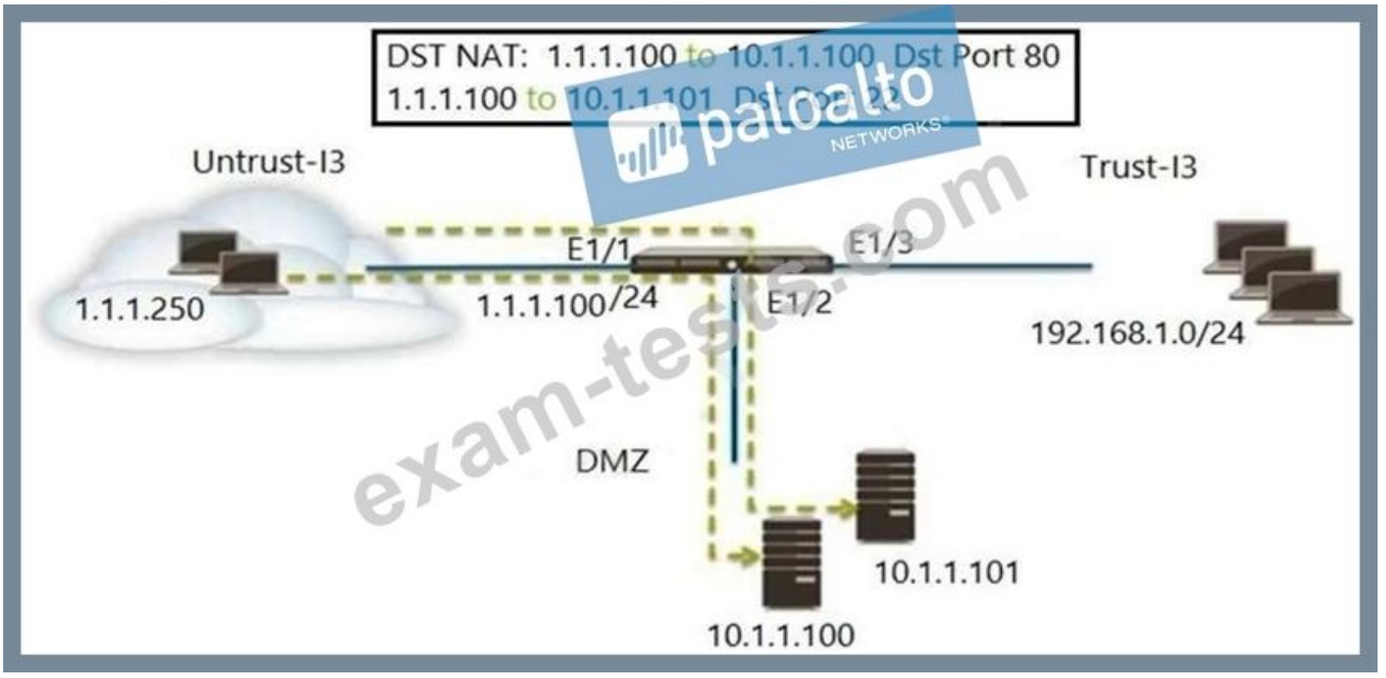
NEW QUESTION: 127
A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago. Which utility should the company use to identify out-of-date or unused rules on the firewall?
A. Rule Usage Filter > Unused Apps
B. Rule Usage Filter > No App Specified
C. Rule Usage Filter >Hit Count > Unused in 30 days
D. Rule Usage Filter > Hit Count > Unused in 90 days
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
An interface can belong to how many Security Zones?
A. 2
B. 4
C. 3

D. 1
Answer: D (LEAVE A REPLY)

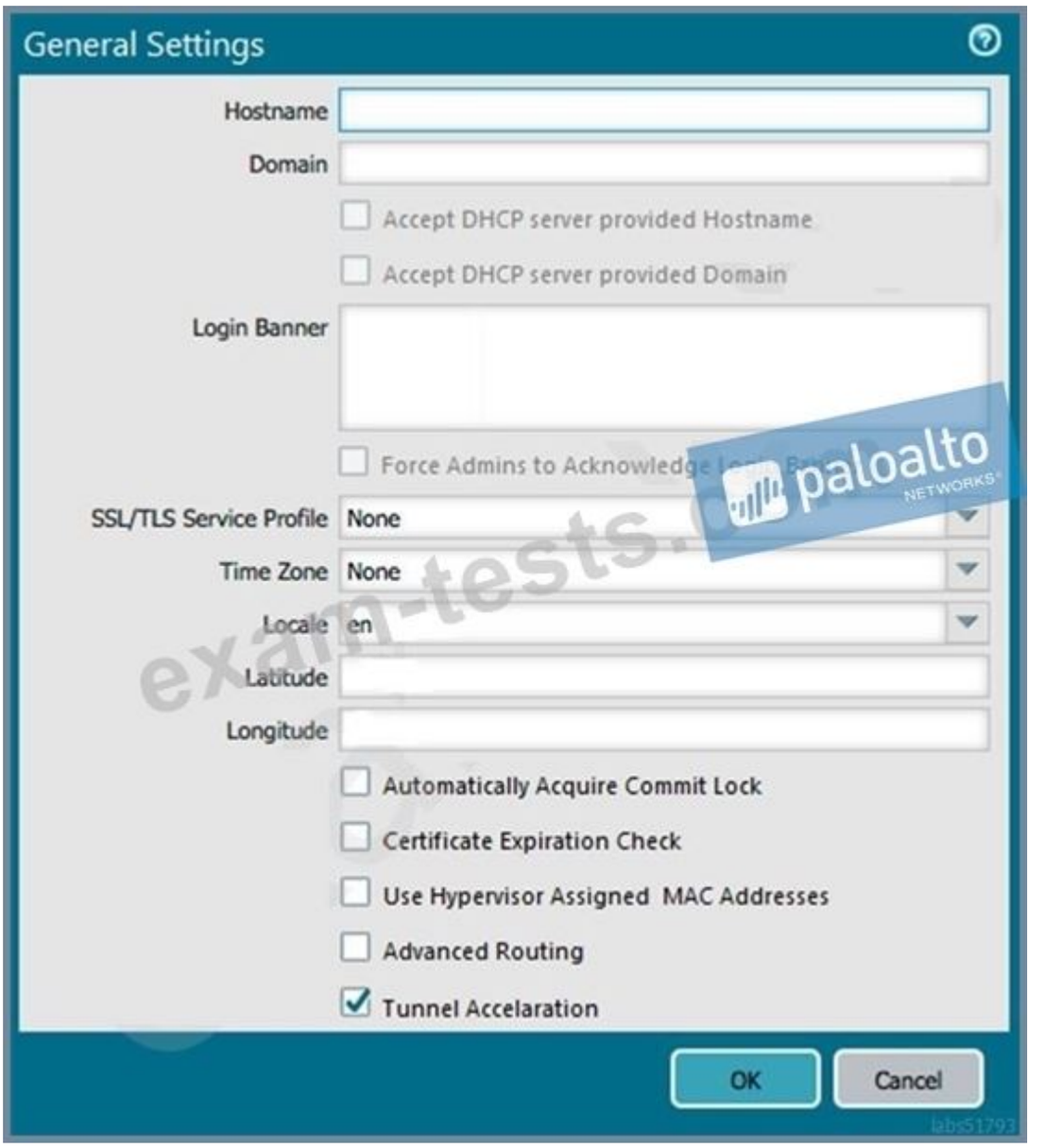
NEW QUESTION: 129
Which Security profile must be added to Security policies to enable DNS Signatures to be checked?
A. Antivirus
B. URL Filtering
C. Vulnerability Protection
D. Anti-Spyware
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Refer to the exhibit. An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.



Which two Security policy rules will accomplish this configuration? (Choose two.)
A. Untrust (Any) to DMZ (1.1.1.100), web-browsing - 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), ssh - Allow
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 131
Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?



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.
Answer: D (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFGCA0

NEW QUESTION: 132
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, send ICMP Unreachable
B. Reset server
C. Reset both
D. Drop

Answer: C (LEAVE A REPLY)

NEW QUESTION: 133
What is the default action for the SYN Flood option within the DoS Protection profile?
A. Reset-client
B. Alert
C. Sinkhole
D. Random Early Drop
Answer: (SHOW ANSWER)
DoS Protection Profiles and Policy Rules work together to provide protection against flooding of many incoming SYN, UDP, ICMP, and ICMPv6 packets, and other types of IP packets. You determine what thresholds constitute flooding. In general, the DoS Protection profile sets the thresholds at which the firewall generates a DoS alarm, takes action such as Random Early Drop, and drops additional incoming connections. A DoS Protection policy rule configured to protect (rather than to allow or deny packets) determines the criteria for packets to match (such as source address) in order to be counted toward the thresholds. This flexibility allows you to block certain traffic, or allow certain traffic and treat other traffic as DoS traffic. When the incoming rate exceeds your maximum threshold, the firewall blocks incoming traffic from the source address.

NEW QUESTION: 134
What are two differences between an application group and an application filter? (Choose two.)
A. Application groups dynamically group applications based on attributes, while application filters contain applications that are statically grouped.
B. Application groups can be added to application filters, while application filters cannot be added to application groups.
C. Application groups enable access to sanctioned applications explicitly, while application filters enable access to sanctioned applications implicitly.
D. Application groups are static, while application filters are dynamic.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 135
Which User Credential Detection method should be applied within a URL Filtering Security profile to check for the submission of a valid corporate username and the associated password?
A. Valid Username Detected Log Severity
B. IP User
C. Group Mapping
D. Domain Credential
Answer: C (LEAVE A REPLY)

NEW QUESTION: 136
Based on the security policy rules shown, ssh will be allowed on which port?

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

A. 80
B. 22
C. 53
D. 23
Answer: (SHOW ANSWER)

NEW QUESTION: 137
In the example security policy shown, which two websites would be blocked? (Choose two.)

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

A. Facebook
B. Amazon
C. LinkedIn
D. YouTube
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

	Name	Type	Source Zone	Source Address	Destination Zone	Destination Address	Application	Service	Action
1	inside-portal	universal	inside	any	outside	203.0.113.20	any	any	Allow
2	internal-inside-dmz	universal	inside	any	dmz	any	ftp ssh ssl web-browsing	application-default	Allow
3	egress-outside	universal	inside	any	outside	any	any	application-default	Allow
4	egress-outside-content-id	universal	inside	any	outside	any	any	application-default	Allow
5	[illegible]	universal	danger	any	danger	any	any	application-default	Allow
6	[illegible]-default	intrazone	any	any	(intrazone)	any	any	any	Allow
7	intrazone-default	intrazone	any	any	any	any	any	any	Deny

A. internal-inside-dmz
B. inside-portal
C. intercone-default
D. engress outside
Answer: (SHOW ANSWER)

NEW QUESTION: 139
An administrator would like to block access to a web server, while also preserving resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)
A. Reset server
B. Reset both
C. Drop
D. Deny
Answer: (SHOW ANSWER)
Palo Alto Networks firewall protection is based on application intelligence, so in the case of TCP, a TCP session must be established before the application can be discovered. However, after a TCP session has been established, silent dropping of packets without sending a TCP reset can be dangerous. The "drop" action could break the application and cause it to misbehave. An application might hang, continue to send packets, or unnecessarily hold system resources open. Therefore, the default "deny" action defined for more than half of the applications recognized by the firewall is to send a TCP reset.

NEW QUESTION: 140
How many levels can there be in a device-group hierarchy, below the shared level?
A. 2
B. 3
C. 4
D. 5
Answer: (SHOW ANSWER)

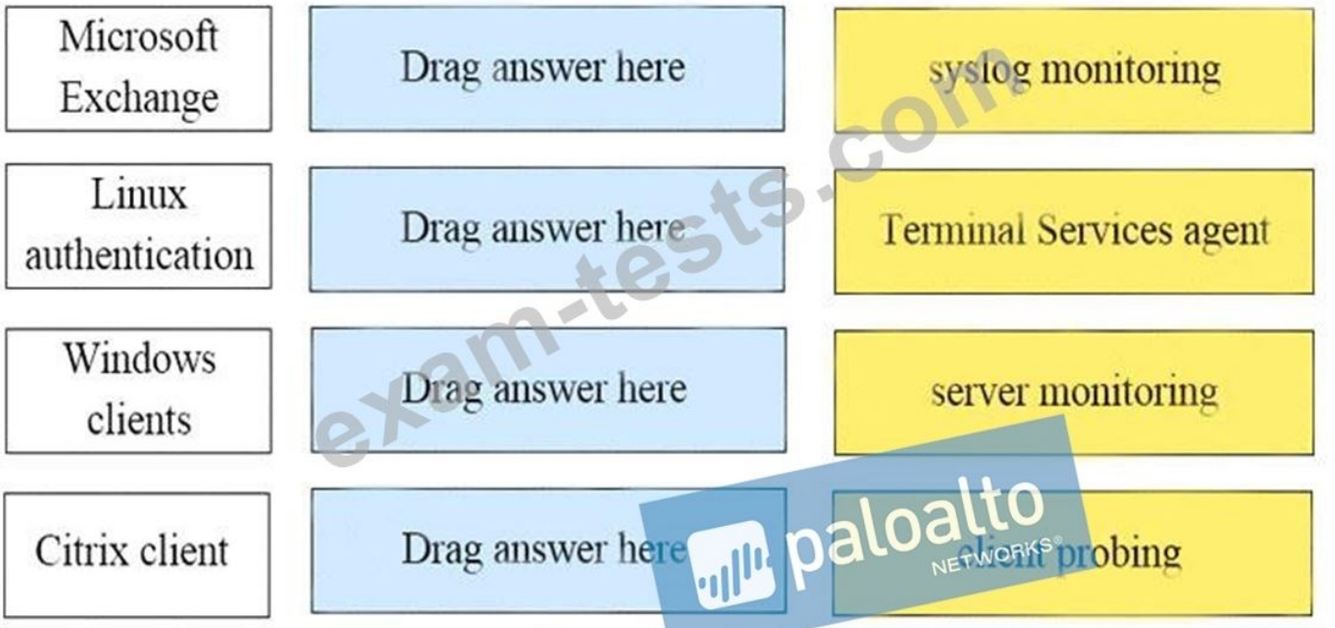
You can Create a Device Group Hierarchy to nest device groups in a tree hierarchy of up to four levels, with lower-level groups inheriting the settings (policy rules and objects) of higher-level groups.
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/device-groups/device-group-hierarchy

NEW QUESTION: 141
What are two predefined AntiSpyware profiles? (Choose two.)
A. Strict
B. Default
C. Standard
D. Secure
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Which two App-ID applications will need to be allowed to use Facebook-chat? (Choose two.)
A. facebook
B. facebook-chat
C. facebook-base
D. facebook-email
Answer: B,C (LEAVE A REPLY)
Explanation/Reference:
Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClV0CAK

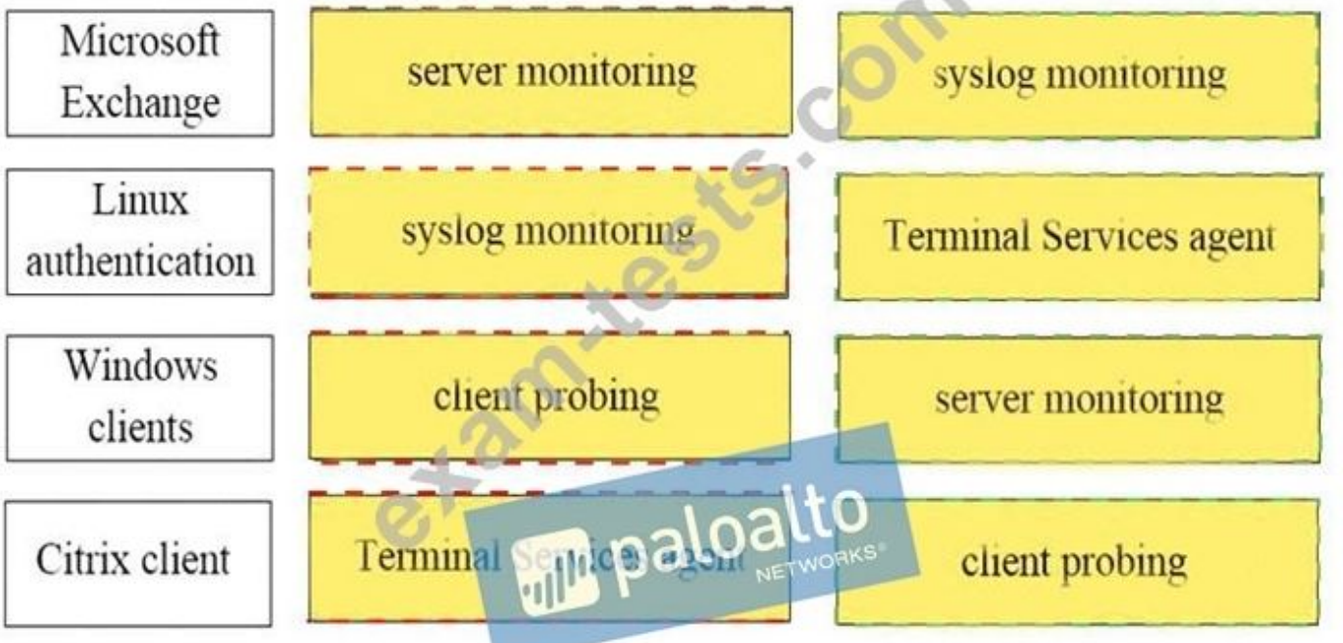
NEW QUESTION: 143
Match the network device with the correct User-ID technology.

Answer Area



Answer:

Answer Area



Explanation

Microsoft Exchange - Server monitoring

Linux authentication - syslog monitoring

Windows Client - client probing

Citrix client - Terminal Services agent

NEW QUESTION: 144
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 connecting the firewall configuration
B. after downloading the update
C. after installing the update
D. after clicking Check New in the Dynamic Update window
Answer: A (LEAVE A REPLY)

NEW QUESTION: 145
Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?

A. It defines the firewall's global SSL/TLS timeout values.

B. It defines the SSUTLS encryption strength used to protect the management interface.

C. It defines the certificate to send to the client's browser from the management interface.

D. It defines the CA certificate used to verify the client's browser.

Answer: C (LEAVE A REPLY)

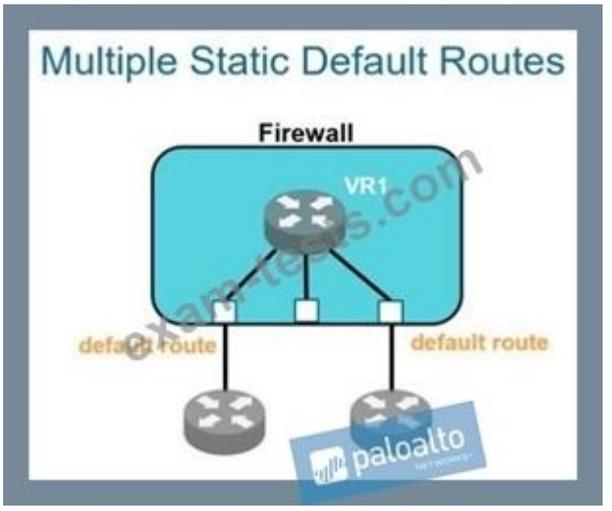
NEW QUESTION: 146
Which two components are utilized within the Single-Pass Parallel Processing architecture on a Palo Alto Networks Firewall? (Choose two.)
A. Layer-ID
B. User-ID
C. App-ID
D. QoS-ID
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 147
In the example security policy shown, which two websites would be blocked? (Choose two.)

	Name	Tags	Zone	Address	Zone	Address	Application	Service	URL Category
1	Block-Sites	outbound	Inside	Any	Outside	Any	Any	any	Social-networking

A. Facebook
B. YouTube
C. Amazon
D. LinkedIn
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 148
Which two statements are correct regarding multiple static default routes when they are configured as shown in the image? (Choose two.)



A. Route with lowest metric is actively used
B. Route with highest metric is actively used

C. Path monitoring does not determine if route is useable

D. Path monitoring determines if route is useable

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 149

How often does WildFire release dynamic updates?

A. every 5 minutes

B. every 15 minutes

C. every 60 minutes

D. every 30 minutes

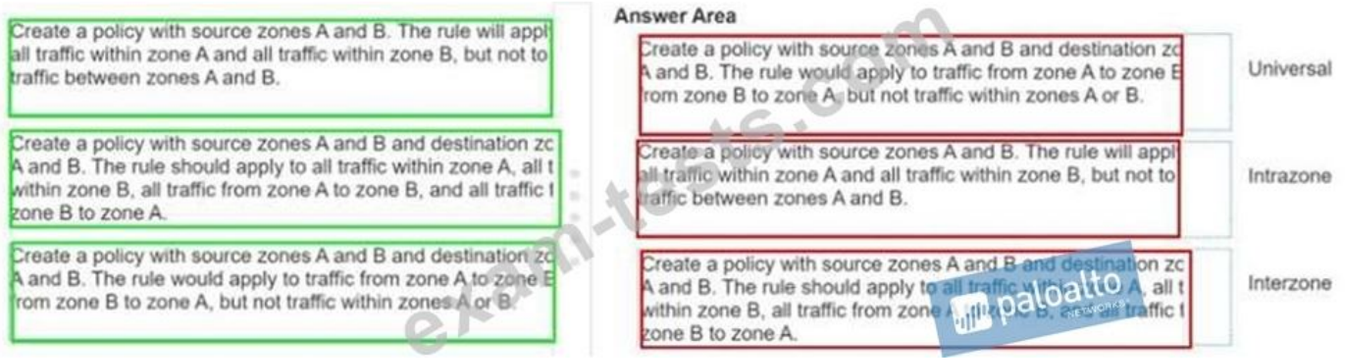
Answer: (SHOW ANSWER)

Explanation/Reference: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-new-features/wildfire-features/five-minute- wildfire-updates

NEW QUESTION: 150

Match each rule type with its example

Answer:



NEW QUESTION: 151

Which statement is true regarding a Best Practice Assessment?

A. The BPA tool can be run only on firewalls

B. It provides a percentage of adoption for each assessment data

C. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities

D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Answer: (SHOW ANSWER)

Best Practice Assessment (BPA) Tool -The BPA for next-generation firewalls and Panorama evaluates a device's configuration by measuring the adoption of capabilities, validating whether the policies adhere to best practices, and providing recommendations and instructions for how to remediate failed best practice checks.

The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories. The results include trending data, which shows the rate of security improvement as you adopt new capabilities, fix gaps, and progress toward a Zero-Trust network.

The BPA component performs more than 200 security checks on a firewall or Panorama configuration and provides a pass/fail score for each check. Each check is a best practice identified by Palo Alto Networks security experts. If a check returns a failing score, the tool provides the justification for the failing score and how to fix the issue.

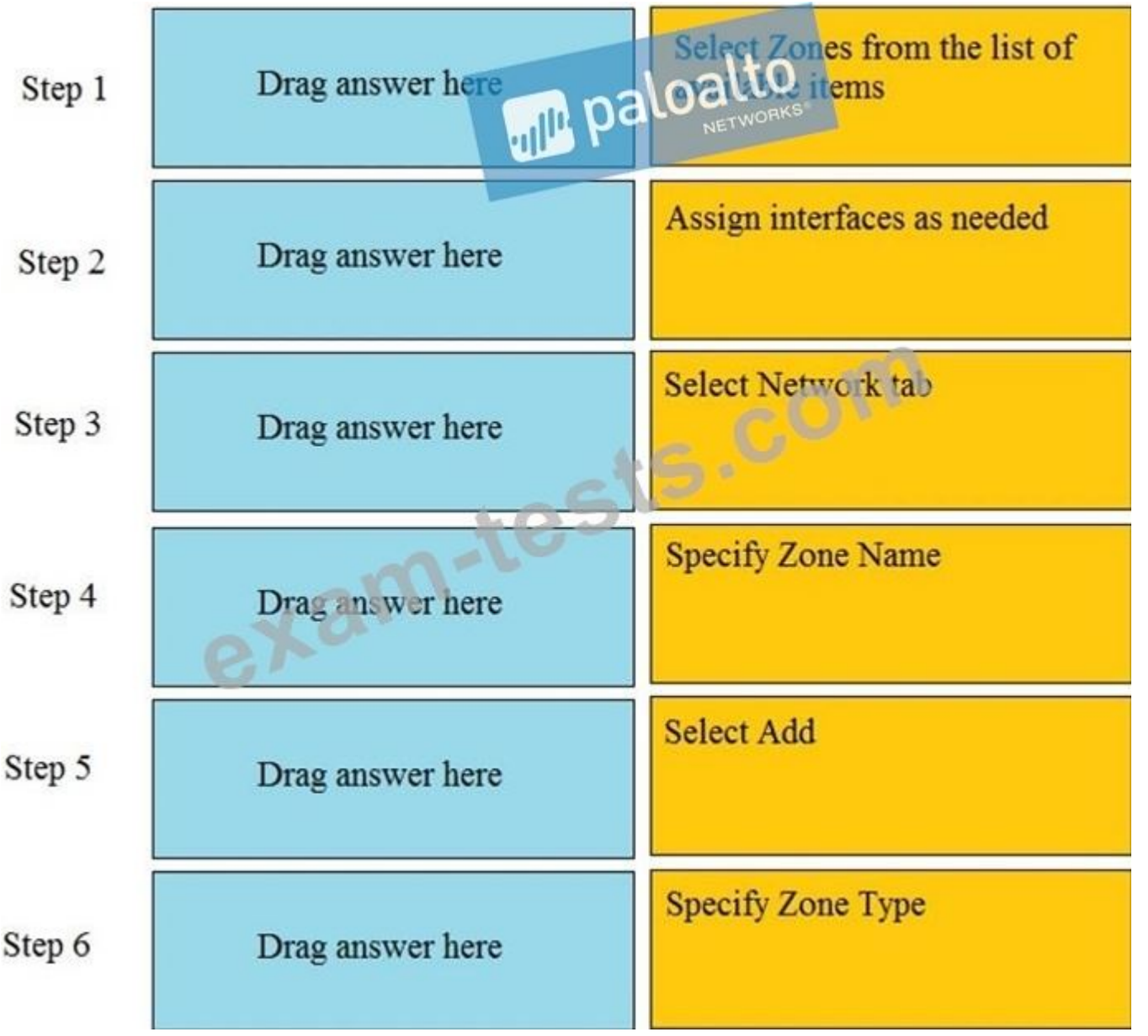
https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best-practice-security-policy/use-palo-alto-networks-assessment-and-review-tools

NEW QUESTION: 152

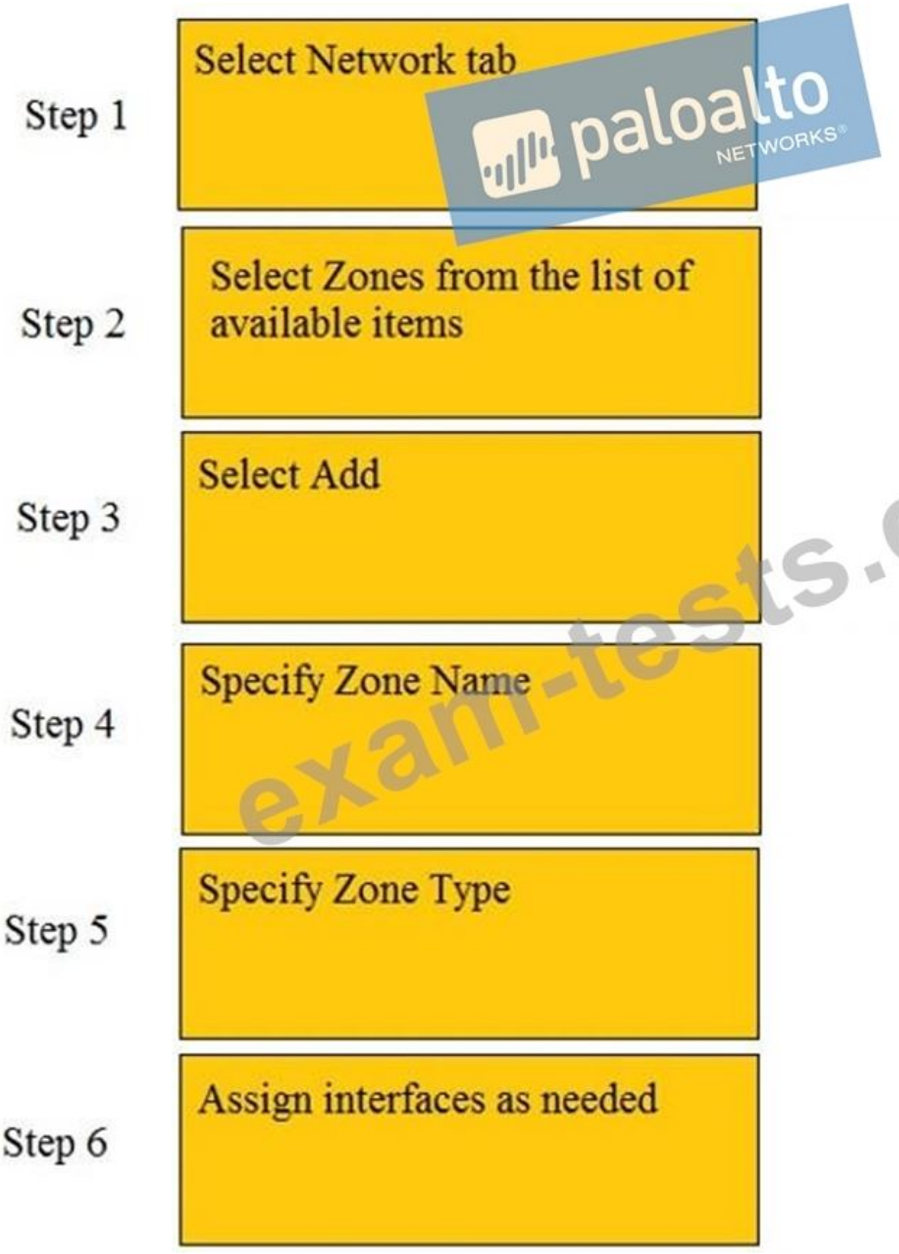
Drag and Drop Question

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

Select and Place:

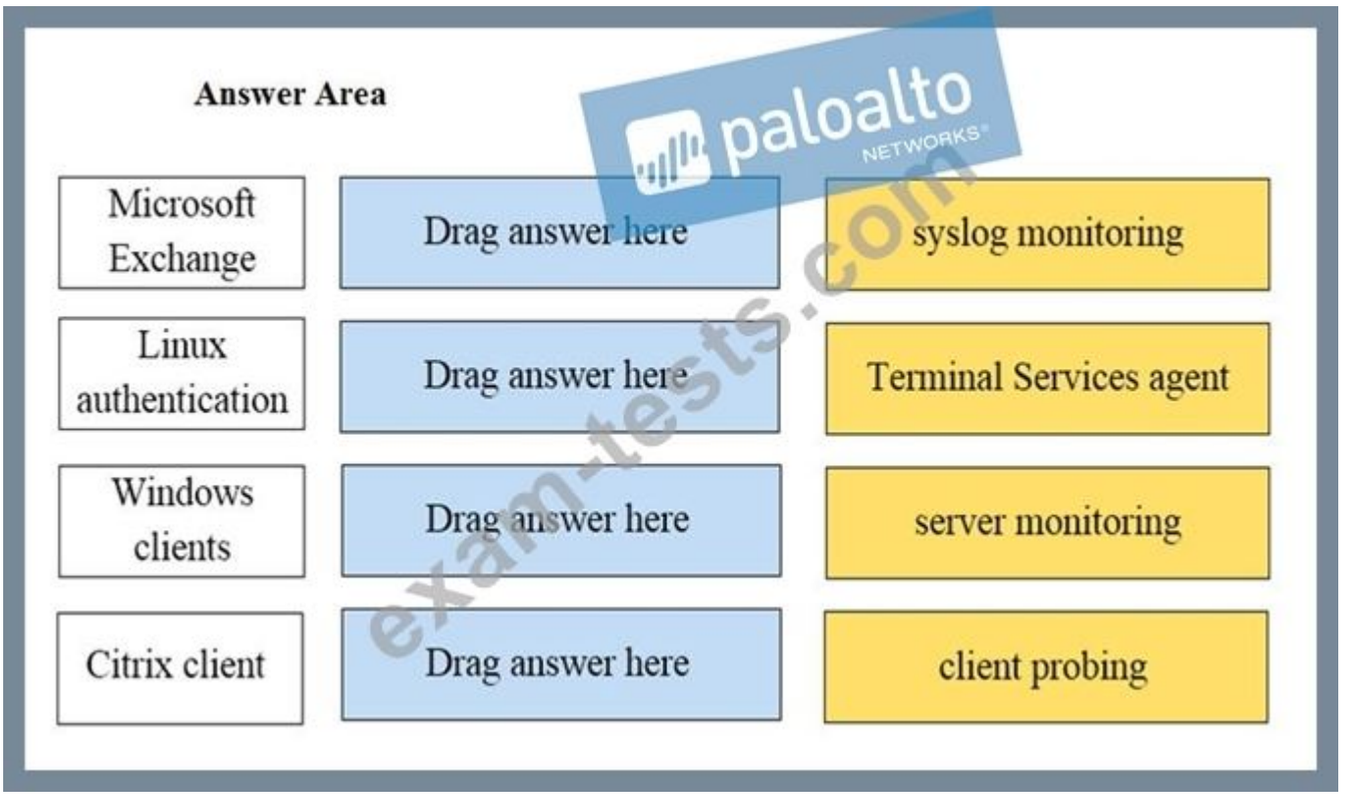


Answer:

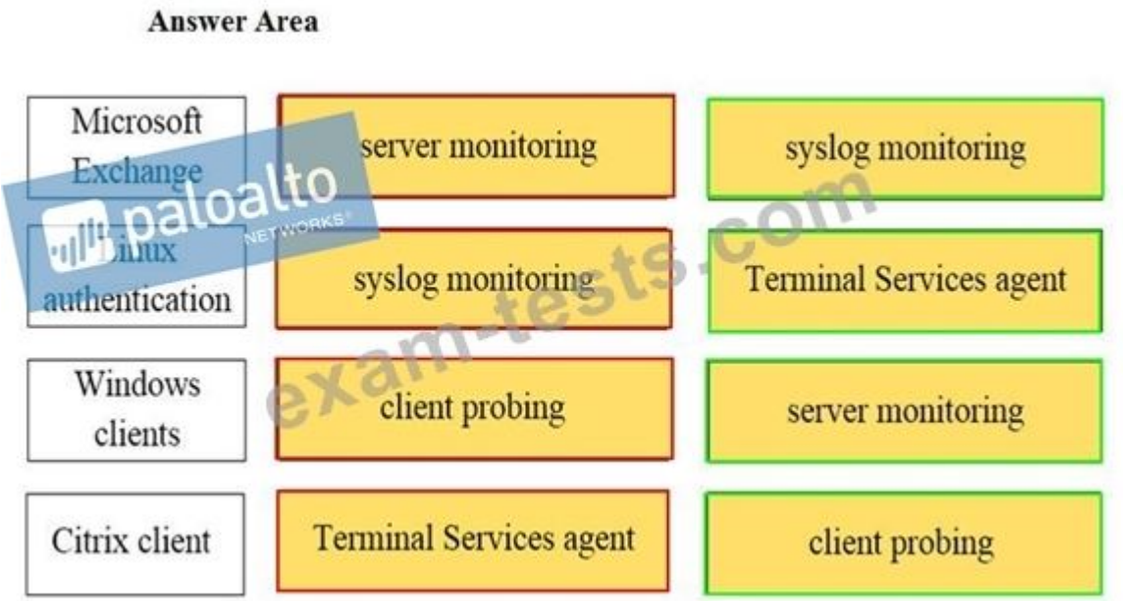


NEW QUESTION: 153

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

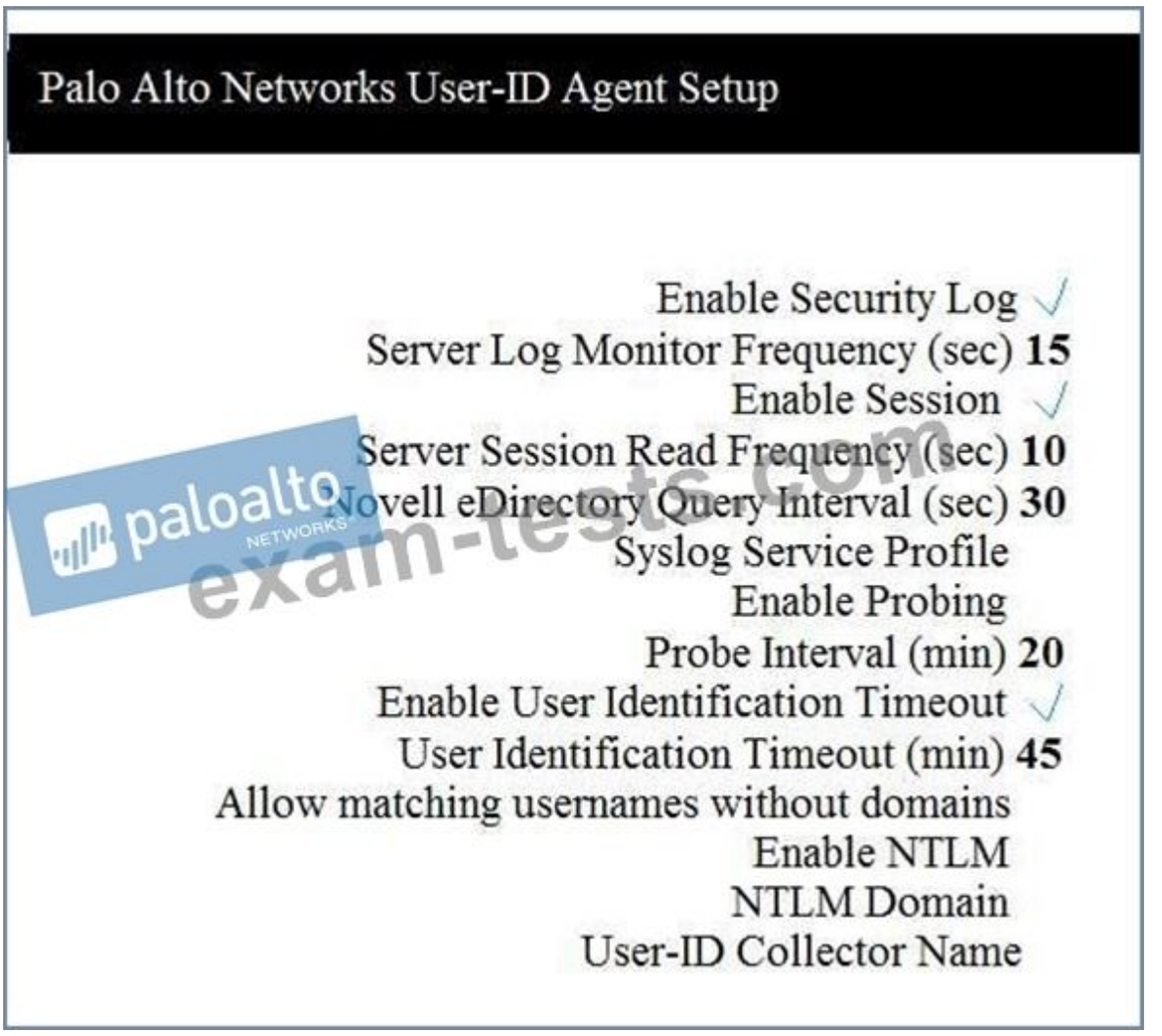


Answer:



NEW QUESTION: 154

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



A. Enable Security Log

B. Server Log Monitor Frequency (sec)

C. Enable Session

D. Enable Probing

Answer: B,C (LEAVE A REPLY)

Explanation/Reference: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/user-identification/device- user-identification-user-mapping/enable-server-monitoring

NEW QUESTION: 155

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

A. Reconnaissance

B. Exploitation

C. Act on Objective

D. Installation

Answer: B (LEAVE A REPLY)

NEW QUESTION: 156

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

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security	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

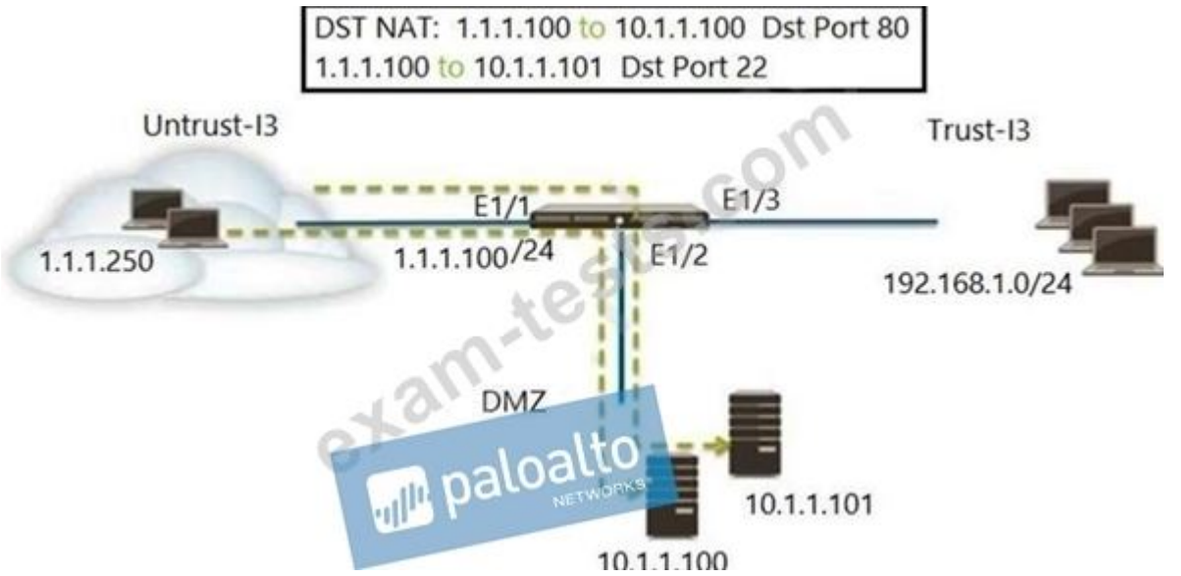
C. 23

D. 22

Answer: D (LEAVE A REPLY)

NEW QUESTION: 157

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



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

A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow

B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow

C. Untrust (Any) to DMZ (1.1.1.100), ssh -Allow

D. Untrust (Any) to DMZ (10.1.1.100, 10.1.1.101), ssh, web-browsing -Allow

E. Untrust (Any) to DMZ (1.1.1.100), web-browsing -Allow

Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 158

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

A. Windows session monitoring via a domain controller

B. passive server monitoring using the Windows-based agent

C. Captive Portal

D. passive server monitoring using a PAN-OS integrated User-ID agent

Answer: C (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresse

NEW QUESTION: 159

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

A. Device>Setup>Services

B. Device>Setup>Management

C. Device>Setup>Operations

D. Device>Setup>Interfaces

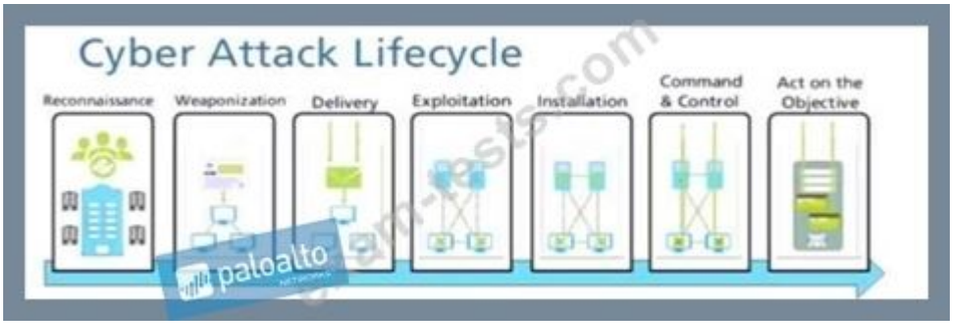
Answer: (SHOW ANSWER)

Explanation/Reference:

NEW QUESTION: 160
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?

A. Service
B. Apps Seen
C. Apps Allowed
D. Name
Answer: B (LEAVE A REPLY)

NEW QUESTION: 161
Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.



A. Act on the Objective
B. Installation
C. Exploitation
D. Reconnaissance
Answer: C (LEAVE A REPLY)

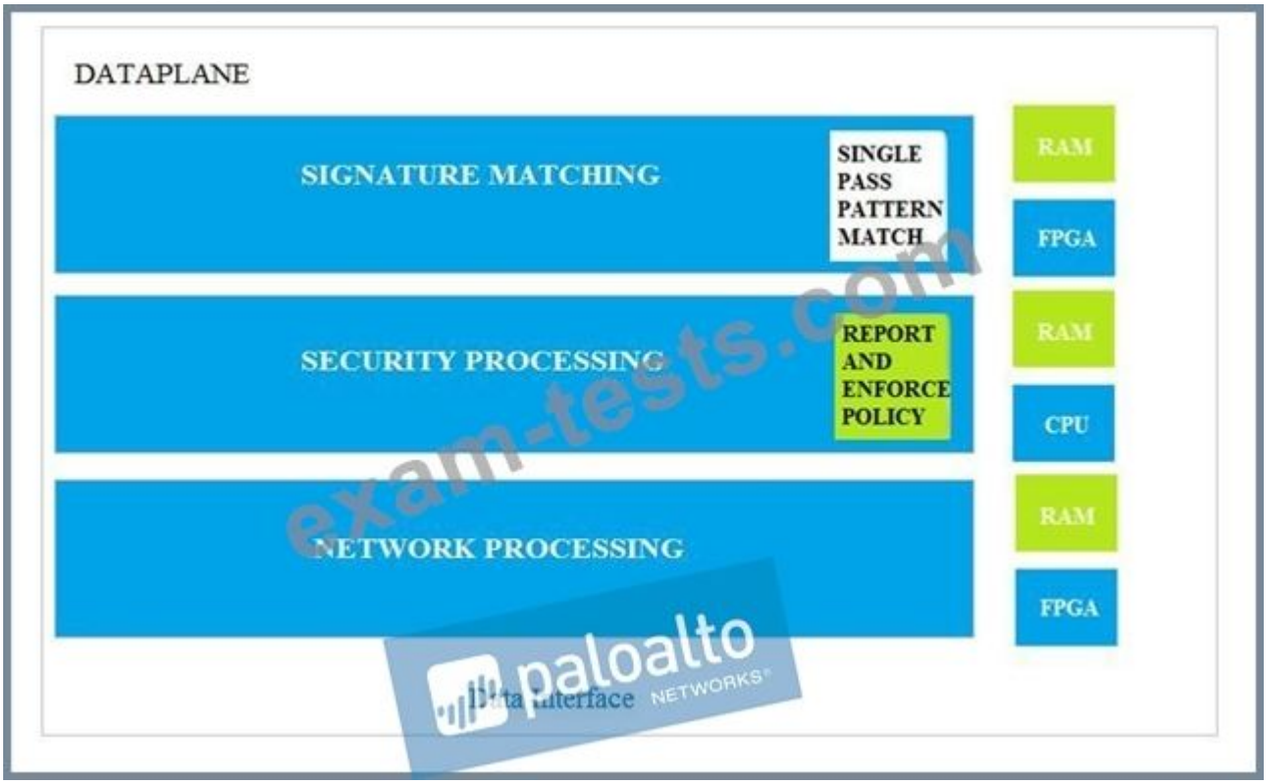
NEW QUESTION: 162
A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT. Finance, and HR.
Which two types of traffic will the rule apply to? (Choose two)
A. traffic within zone IT
B. traffic between zone IT and zone Finance
C. traffic between zone Finance and zone HR
D. traffic within zone HR
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 163
Employees are shown an application block page when they try to access YouTube.
Which security policy is blocking the YouTube application?

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

A. intrazone-default
B. Deny Google
C. allowed-security services
D. interzone-default
Answer: D (LEAVE A REPLY)
You can check application categories on:
https://applipedia.paloaltonetworks.com/

NEW QUESTION: 164
Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 165
Based on the security policy rules shown, ssh will be allowed on which port?

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

A. the default port
B. any port
C. only ephemeral ports
D. same port as ssl and snmpv3
Answer: A (LEAVE A REPLY)

NEW QUESTION: 166
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. Pre-analyze
C. Review App Matches
D. Review Apps
Answer: (SHOW ANSWER)

NEW QUESTION: 167
Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP-to-user mappings as soon

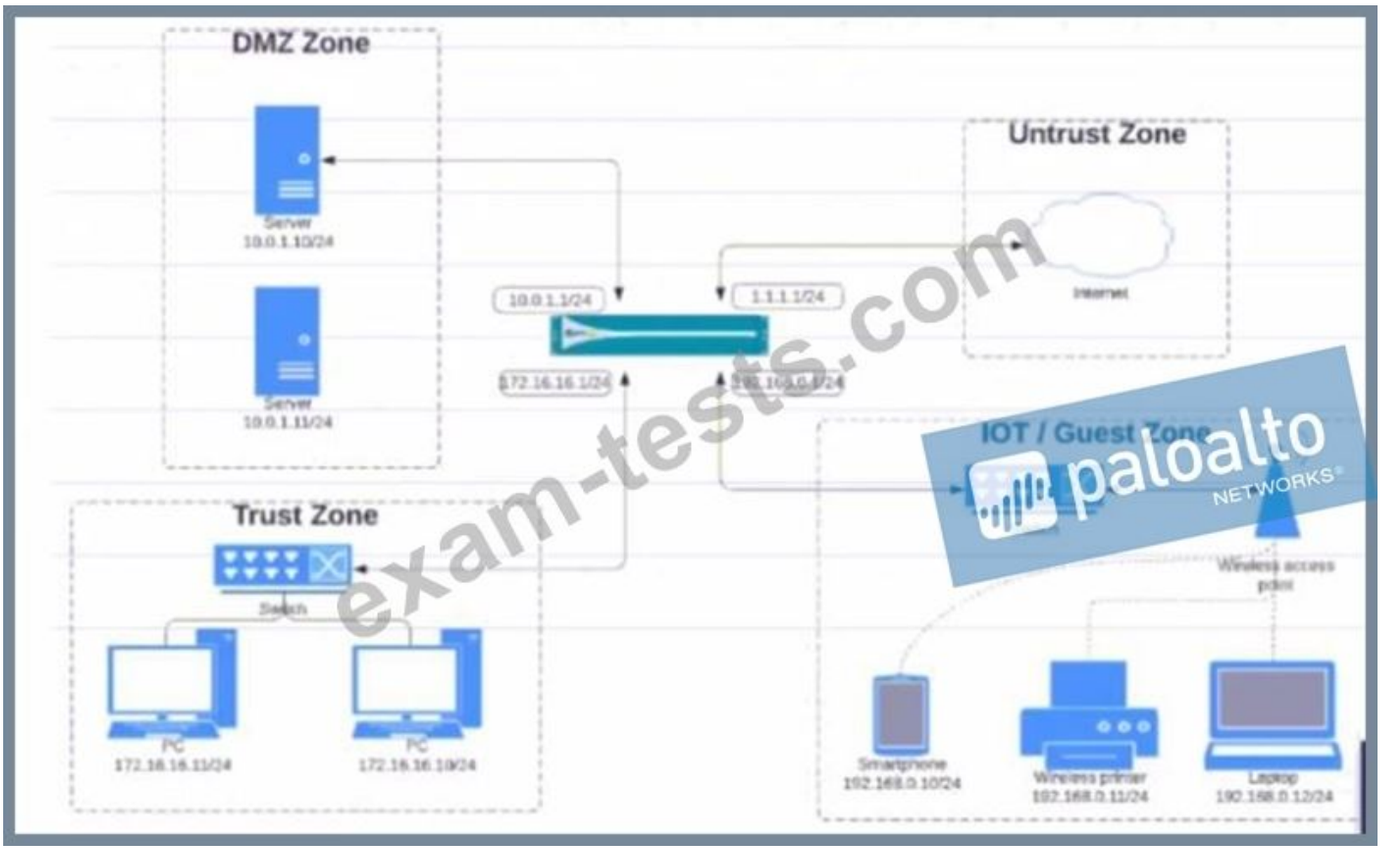
as possible with minimal downtime and minimal configuration changes to the wireless devices themselves. The wireless devices are from various manufactures.
Given the scenario, choose the option for sending IP-to-user mappings to the NGFW.
A. syslog
B. RADIUS
C. UID redistribution
D. XFF headers
Answer: A (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-id-to-monitor-syslog-senders-for-user-mapping

NEW QUESTION: 168
Which rule type is appropriate for matching traffic both within and between the source and destination zones?
A. interzone
B. shadowed
C. intrazone
D. universal
Answer: D (LEAVE A REPLY)
Universal -By default, all the traffic destined between two zones, regardless of whether it is from the same zone or different zone. Universal rule types apply to all matching interzone and intrazone traffic in the specified source and destination zones.

NEW QUESTION: 169
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
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 170
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
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 171



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)

B)

C)

D)

A. Option
B. Option
C. Option
D. Option
Answer: D (LEAVE A REPLY)

NEW QUESTION: 172
Which URL profiling action does not generate a log entry when a user attempts to access that URL?
A. Override
B. Allow
C. Block
D. Continue
Answer: B (LEAVE A REPLY)
Allow traffic destined for that URL category; allowed traffic is not logged.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/url-filtering/configure-url-filtering.html

NEW QUESTION: 173
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
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/ configure-user-mapping-using-the-windows-user-id-agent/configure-the-windows-based-user-id-agent-for-user- mapping.html

NEW QUESTION: 174

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

A. Tunnel

B. Virtual Wire

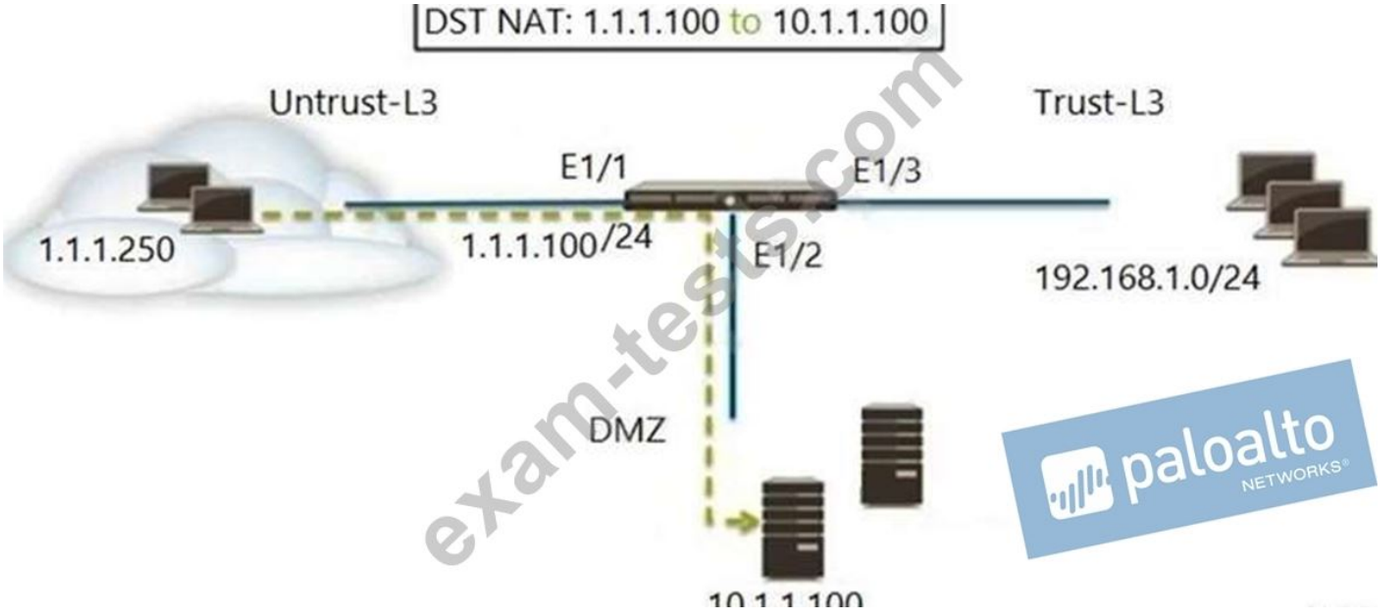
C. Tap

D. Layer3

Answer: (SHOW ANSWER)

NEW QUESTION: 175

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



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

A. Untrust (any) to DMZ (10.1.1.100), web browsing -Allow

B. Untrust (any) to Untrust (1.1.1.100), web browsing -Allow

C. Untrust (any) to Untrust (10.1.1.100), web browsing -Allow

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

Answer: D (LEAVE A REPLY)

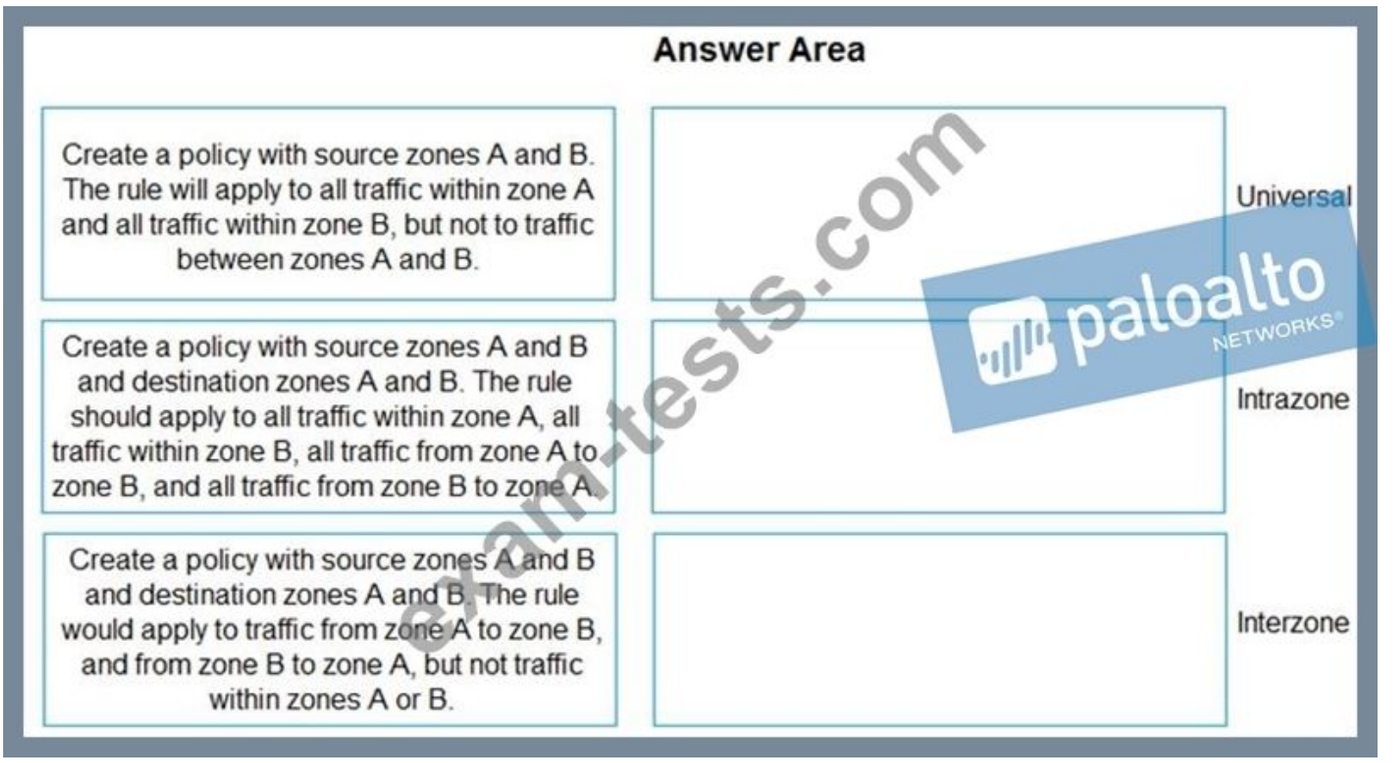
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping

NEW QUESTION: 176

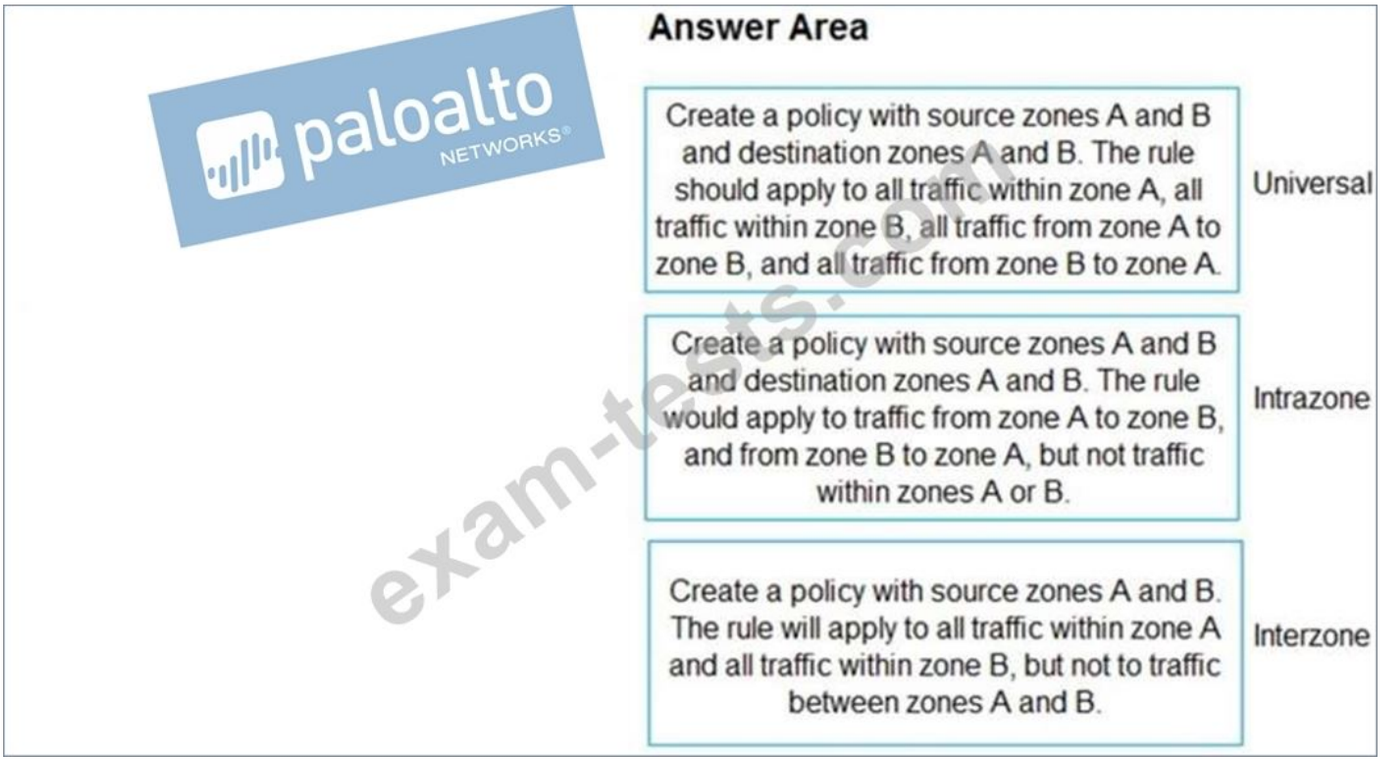
An administrator configured a Security policy rule where the matching condition includes a single application and the action is set to deny.
What deny action will the firewall perform?
A. Discard the session's packets and send a TCP reset packet to let the client know the session has been terminated
B. Drop the traffic silently
C. Perform the default deny action as defined in the App-ID database for the application
D. Send a TCP reset packet to the client- and server-side devices
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-policy/security-policy-actions

NEW QUESTION: 177
What is the main function of Policy Optimizer?
A. reduce load on the management plane by highlighting combinable security rules
B. migrate other firewall vendors' security rules to Palo Alto Networks configuration
C. eliminate "Log at Session Start" security rules
D. convert port-based security rules to application-based security rules
Answer: D (LEAVE A REPLY)
Policy Optimizer provides a simple workflow to migrate your legacy Security policy rulebase to an App-ID-based rulebase, which improves your security by reducing the attack surface and offering visibility into applications so you can safely enable them. Policy Optimizer identifies port-based rules so you can convert them to application-based whitelist rules or add applications from a port-based rule to an existing application-based rule without compromising application availability. It also identifies over-provisioned App-ID-based rules (App-ID rules configured with unused applications). Policy Optimizer helps you prioritize which port-based rules to migrate first, identify application-based rules that allow applications you do not use, and analyze rule usage characteristics such as hit count.

NEW QUESTION: 178
Drag and Drop Question
Match each rule type with its example.



Answer:



NEW QUESTION: 179

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

Answer: (SHOW ANSWER)

To enable DNS security, domain queries using DNS security that are found to be threats are remediated with an Anti-Spyware Security Profile. Edit an existing or open a new Anti-Spyware Profile using Objects > Security Profiles > Anti-Spyware.

NEW QUESTION: 180
How would a Security policy need to be written to allow outbound traffic using Secure Shell (SSH) to destination ports tcp/22 and tcp/4422?
A. The admin creates a custom service object named "tcp-4422" with port tcp/4422.
The admin then creates a Security policy allowing application "ssh" and service "tcp-4422".
B. The admin creates a custom service object named "tcp-4422" with port tcp/4422.
The admin then creates a Security policy allowing application "ssh", service "tcp-4422", and service "application-default".
C. The admin creates a custom service object named "tcp-4422" with port tcp/4422.
The admin also creates a custom service object named "tcp-22" with port tcp/22.
The admin then creates a Security policy allowing application "ssh", service "tcp-4422", and service "tcp-22".
D. The admin creates a Security policy allowing application "ssh" and service "application-default".
Answer: (SHOW ANSWER)
If you select application default, you will not add other service.

NEW QUESTION: 181
The Port Mapping user mapping method can monitor which two types of environments? (Choose two.)
A. Microsoft terminal servers
B. Linux servers
C. Exchange Servers
D. Citrix
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 182

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

A. create the service object in the specific template

B. uncheck the shared option

C. ensure that disable override is selected

D. ensure that disable override is cleared

Answer: B (LEAVE A REPLY)

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-services

NEW QUESTION: 183

Which two statements are true for the DNS Security service introduced in PAN-OS version 10.0? (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.

Answer: B,D (LEAVE A REPLY)

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/dns-security/cloud-delivered-dns-signatures

1) Locally available, downloadable DNS signature sets (packaged with the antivirus and WildFire updates) come with a hard-coded capacity limitation of 100k signatures and do not include signatures generated through advanced analysis.

2) To better accommodate the influx of new DNS signatures being produced on a daily basis, the cloud-based signature database provides users with instant access to newly added DNS signatures without the need to download updates.

NEW QUESTION: 184

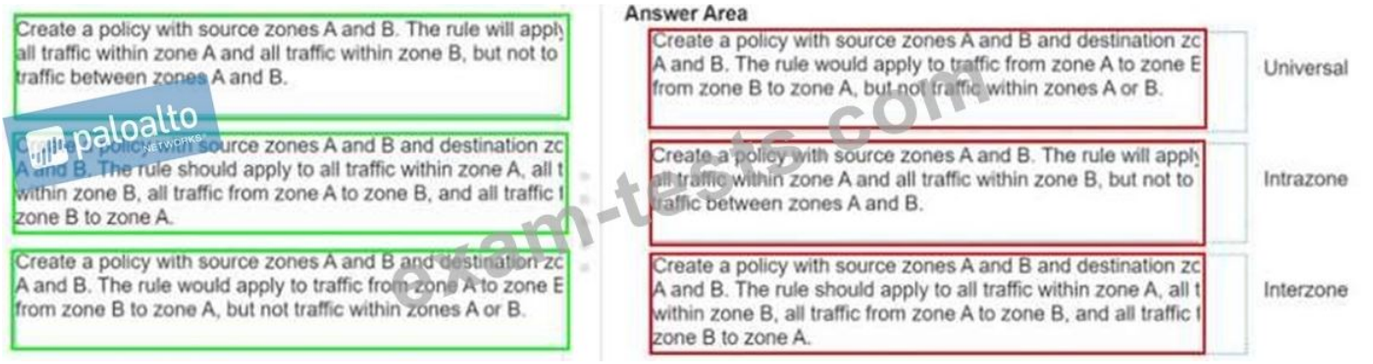
Given the detailed log information above, what was the result of the firewall traffic inspection?

A. It was blocked by the Anti-Virus Security profile action.
B. It was blocked by the Anti-Spyware Profile action.
C. It was blocked by the Security policy action.
D. It was blocked by the Vulnerability Protection profile action.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 185
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 phishing category to override.
B. Set the malware category to block.
C. Set the Command and Control category to block.
D. Set the hacking category to continue.
Answer: B (LEAVE A REPLY)

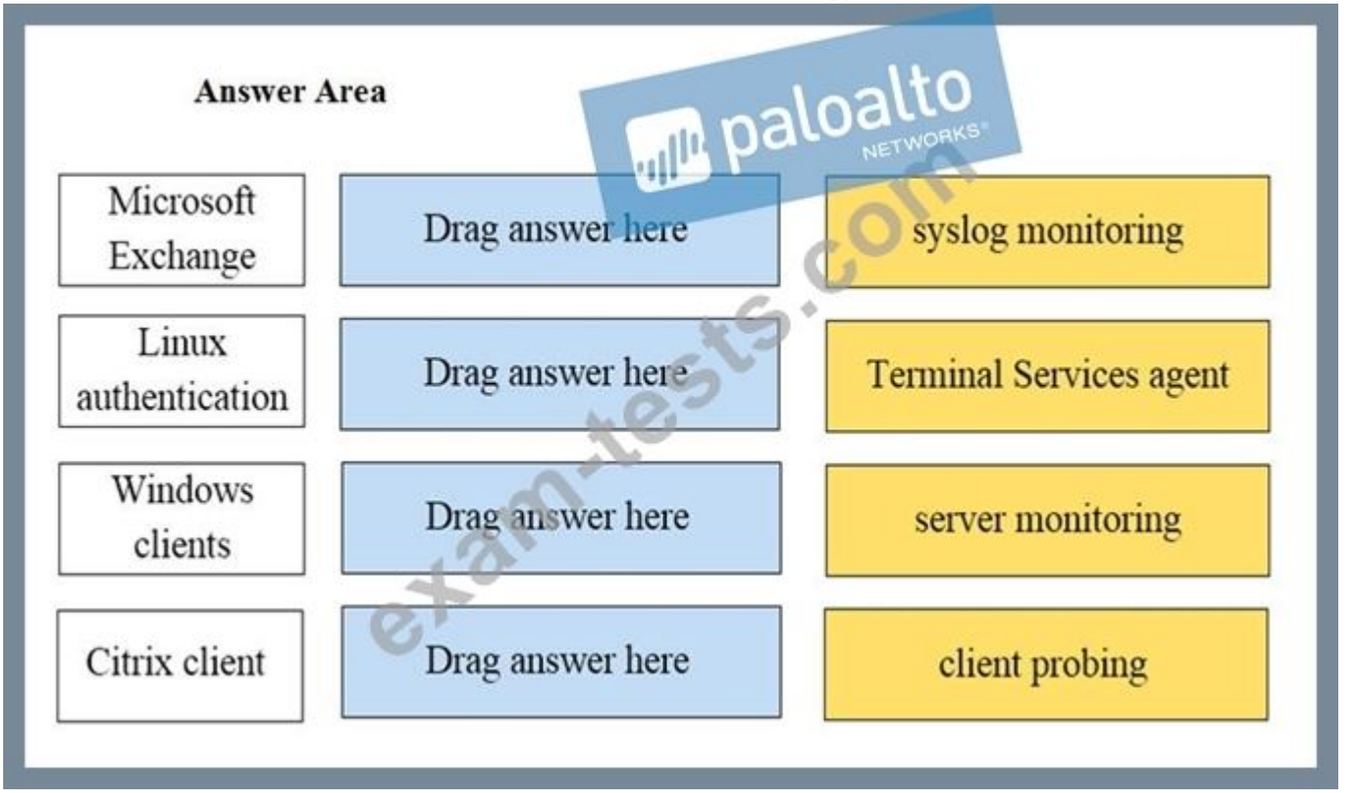
NEW QUESTION: 186
Match each rule type with its example

Answer:

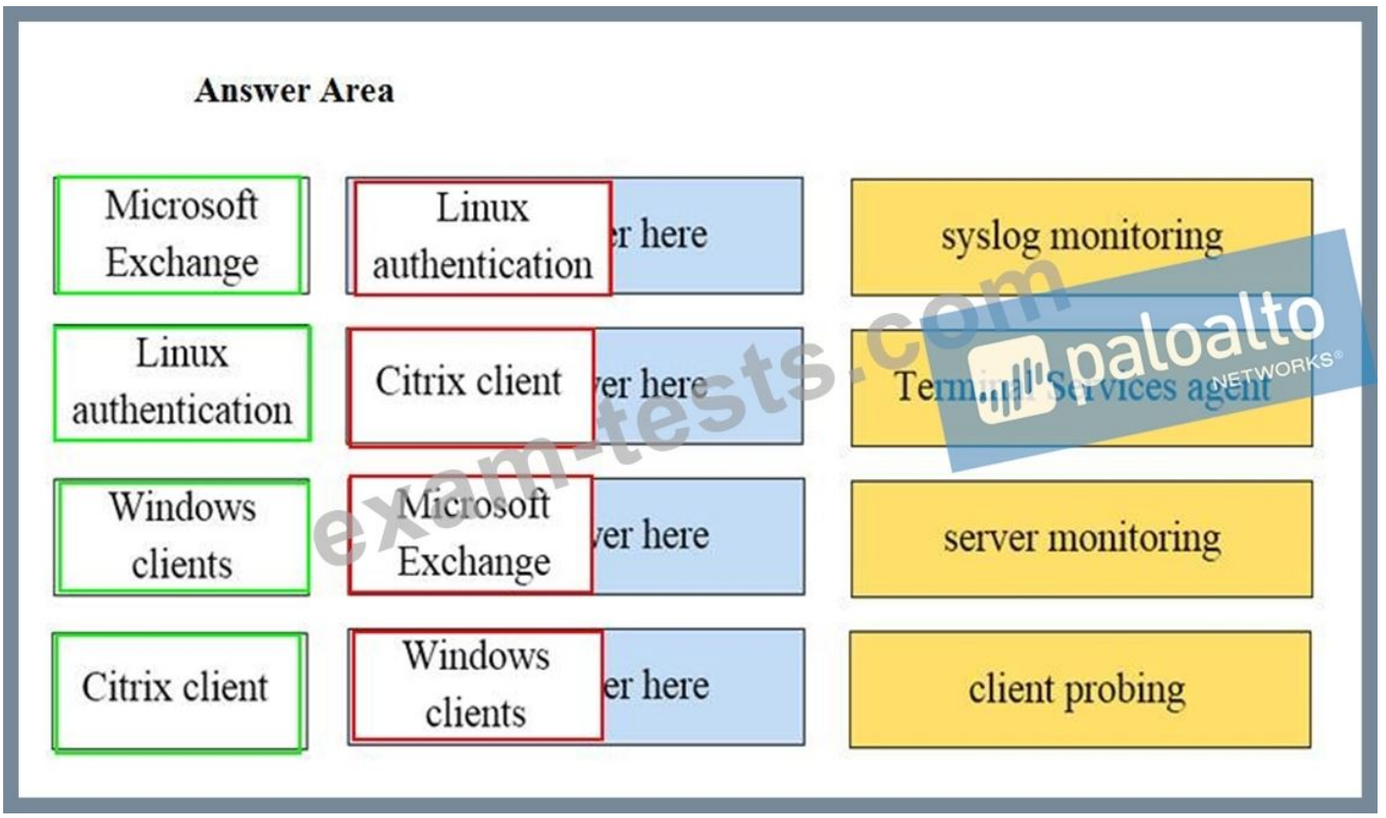


NEW QUESTION: 187

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



Answer:



NEW QUESTION: 188
Which parameter is used to view the Security policy rulebase as groups?
A. Tags
B. Service
C. Type
D. Action
Answer: (SHOW ANSWER)
You must create a tag before you can group rules using that tag. After you assign grouped rules by a tag, View Rulebase as Groups to see a visual representation of your policy rulebase based on the assigned tags. While viewing your rulebase as groups, the policy order and priority is maintained. In this view, select the group tag to view all rules grouped by that tag.
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/objects/objects-tags

NEW QUESTION: 189
Based on the screenshot what is the purpose of the included groups?

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

A. They are only groups visible based on the firewall's credentials.
B. They are used to map usernames to group names.
C. They are groups that are imported from RADIUS authentication servers.
D. They contain only the users you allow to manage the firewall.
Answer: (SHOW ANSWER)

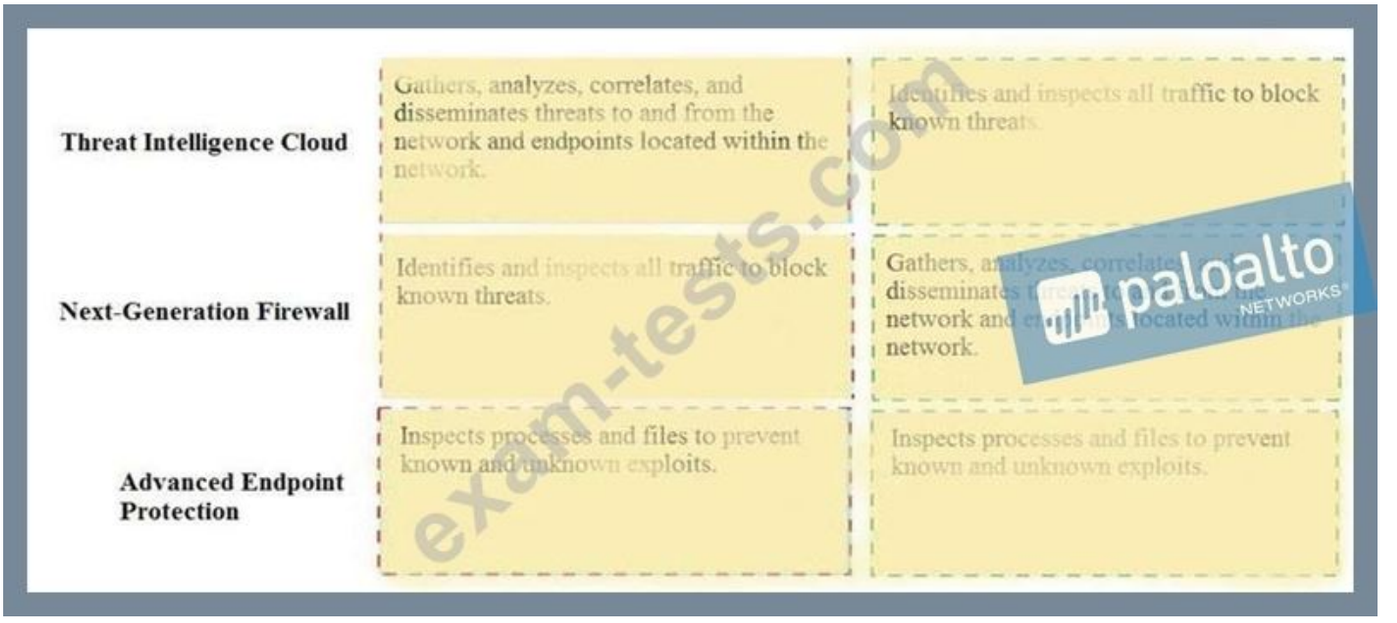
NEW QUESTION: 190
The External zone type is used to pass traffic between which type of objects?
A. Layer 3 interfaces
B. virtual systems
C. Layer 2 interfaces
D. virtual routers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 191
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
Answer: D (LEAVE A REPLY)
https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

NEW QUESTION: 192
Which definition describes the guiding principle of the zero-trust architecture?
A. never trust, never connect
B. always connect and verify
C. never trust, always verify
D. trust, but verity
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

NEW QUESTION: 193
Match the Palo Alto Networks Security Operating Platform architecture to its description.

Answer:



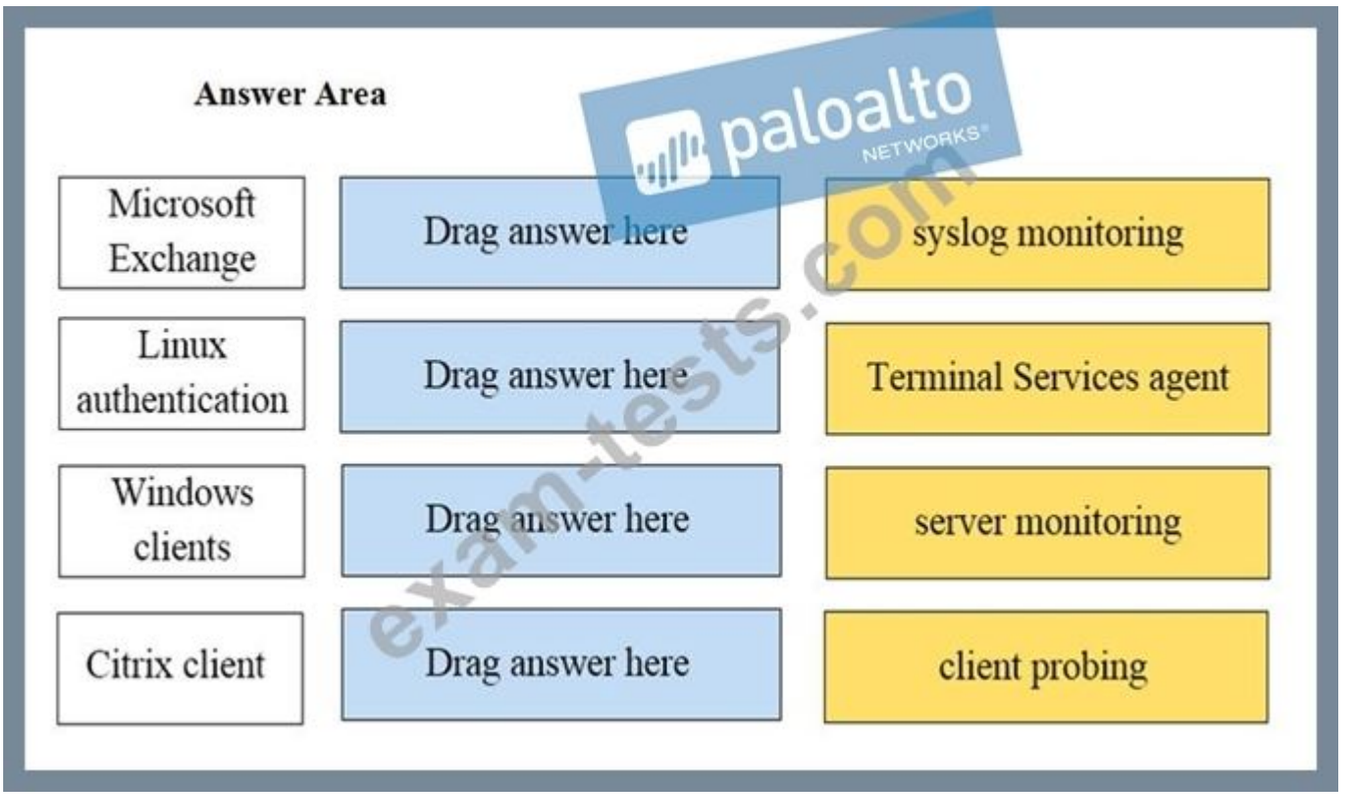
Explanation

Threat Intelligence Cloud - Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.

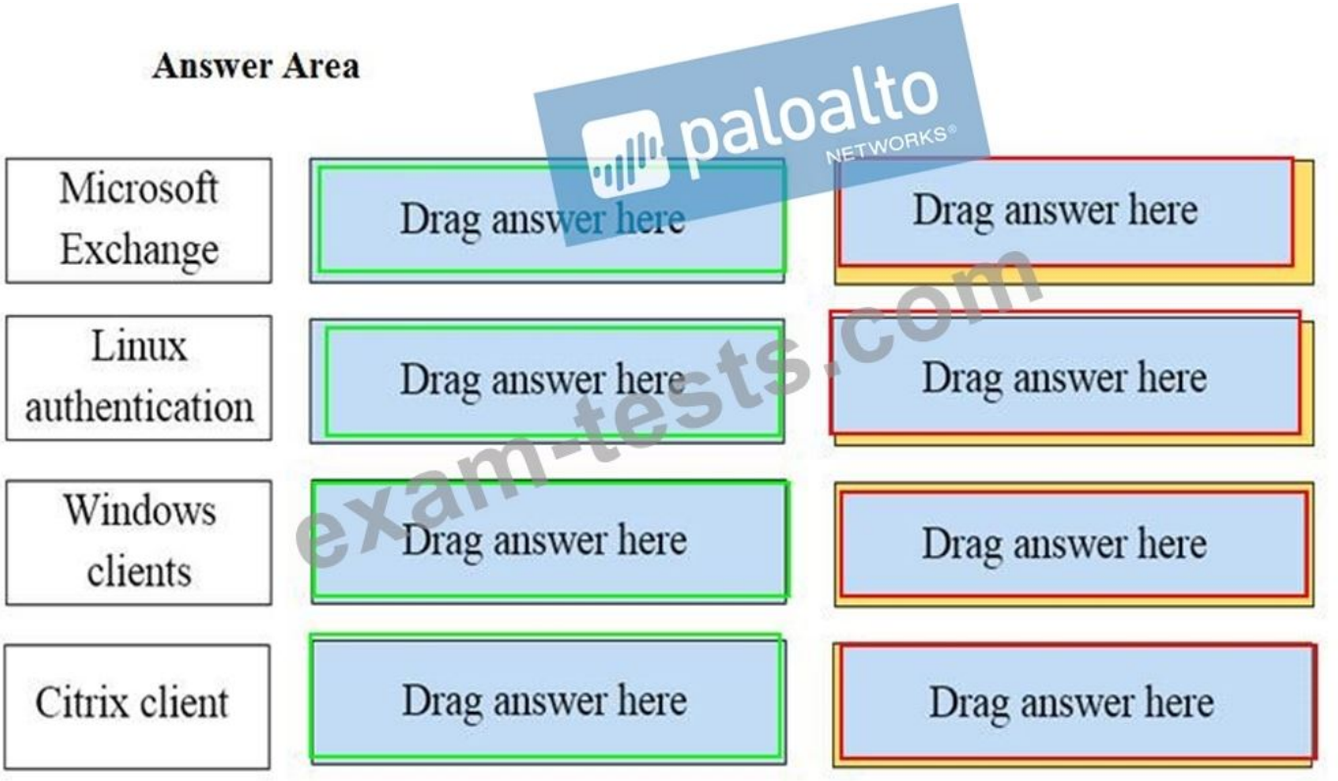
Next-Generation Firewall - Identifies and inspects all traffic to block known threats Advanced Endpoint Protection - Inspects processes and files to prevent known and unknown exploits

NEW QUESTION: 194

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



Answer:



NEW QUESTION: 195

What is the purpose of the automated commit recovery feature?

A. It reverts the firewall configuration if the firewall recognizes a loss of connectivity to Panorama after the change.

B. It reverts the Panorama configuration.

C. It generates a config log after the Panorama configuration successfully reverts to the last running configuration.
D. It causes HA synchronization to occur automatically between the HA peers after a push from Panorama.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 196
You receive notification about a new malware that infects hosts An infection results in the infected host attempting to contact a command-and-control server Which Security Profile when applied to outbound Security policy rules detects and prevents this threat from establishing a command-and-control connection?
A. Antivirus Profile
B. Data Filtering Profile
C. Vulnerability Protection Profile
D. Anti-Spyware Profile
Answer: D (LEAVE A REPLY)
Anti-Spyware Security Profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients.

NEW QUESTION: 197
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. Log Forwarding
B. Destination IP: 192.168.1.123/24
C. Application = 'Telnet'
D. USER-ID = 'Allow users in Trusted'
Answer: C (LEAVE A REPLY)

NEW QUESTION: 198

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. Layer 3

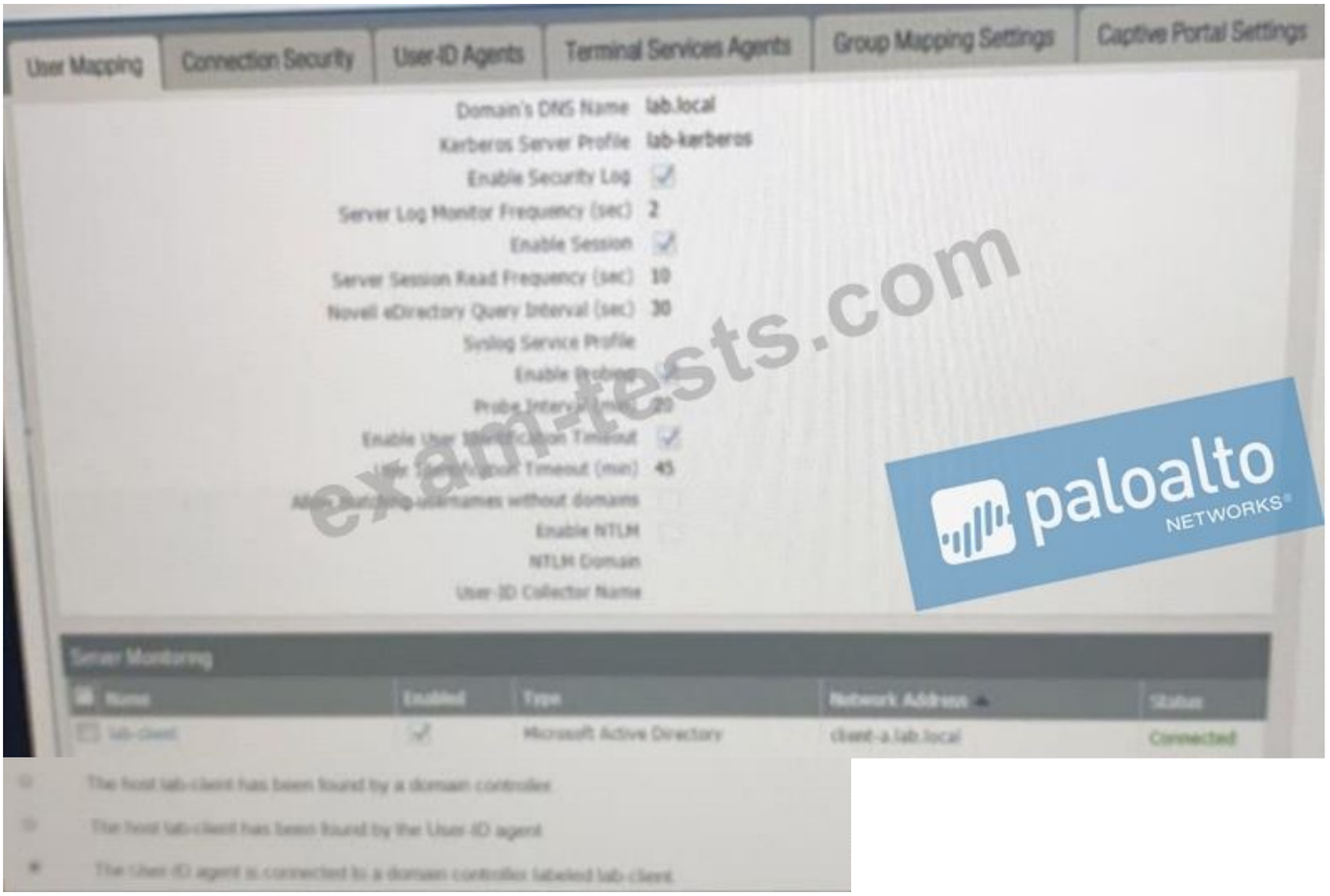
C. Layer 2

D. Virtual Wire

Answer: A (LEAVE A REPLY)

NEW QUESTION: 199

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



A. The host lab-client has been by the User-ID agent.

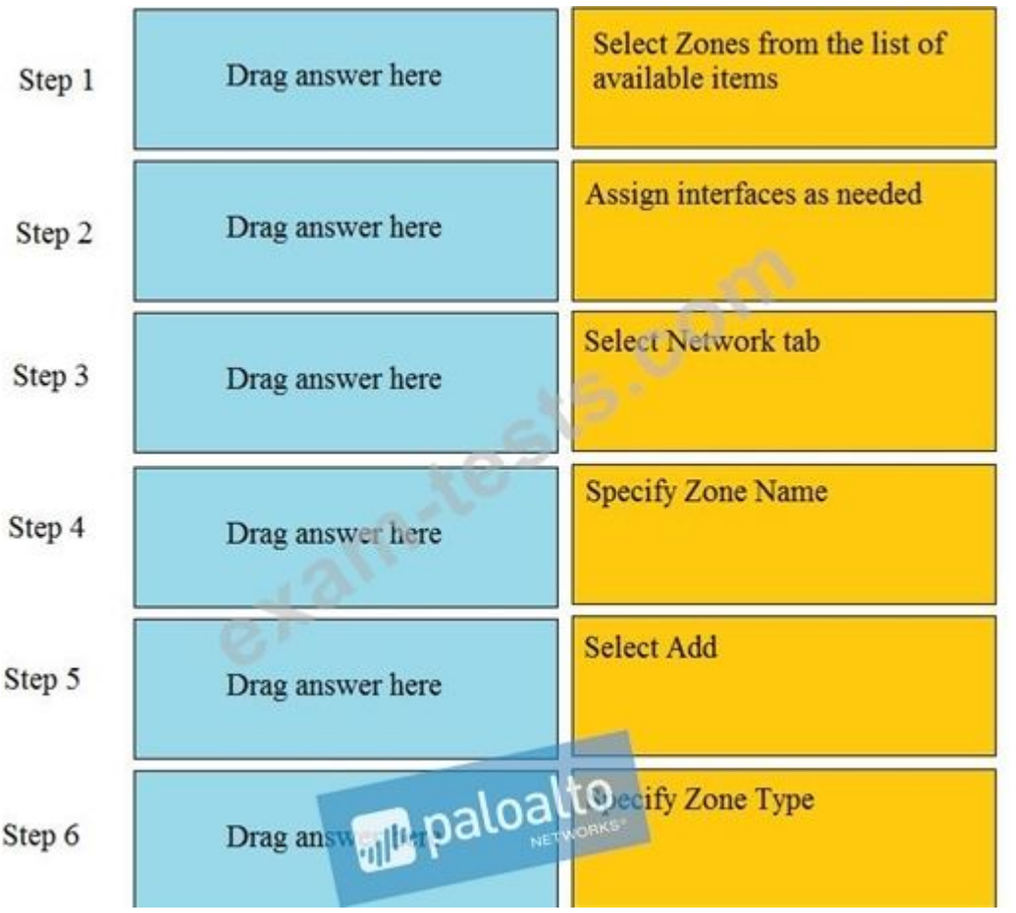
B. The host lab-client has been found by a domain controller.

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

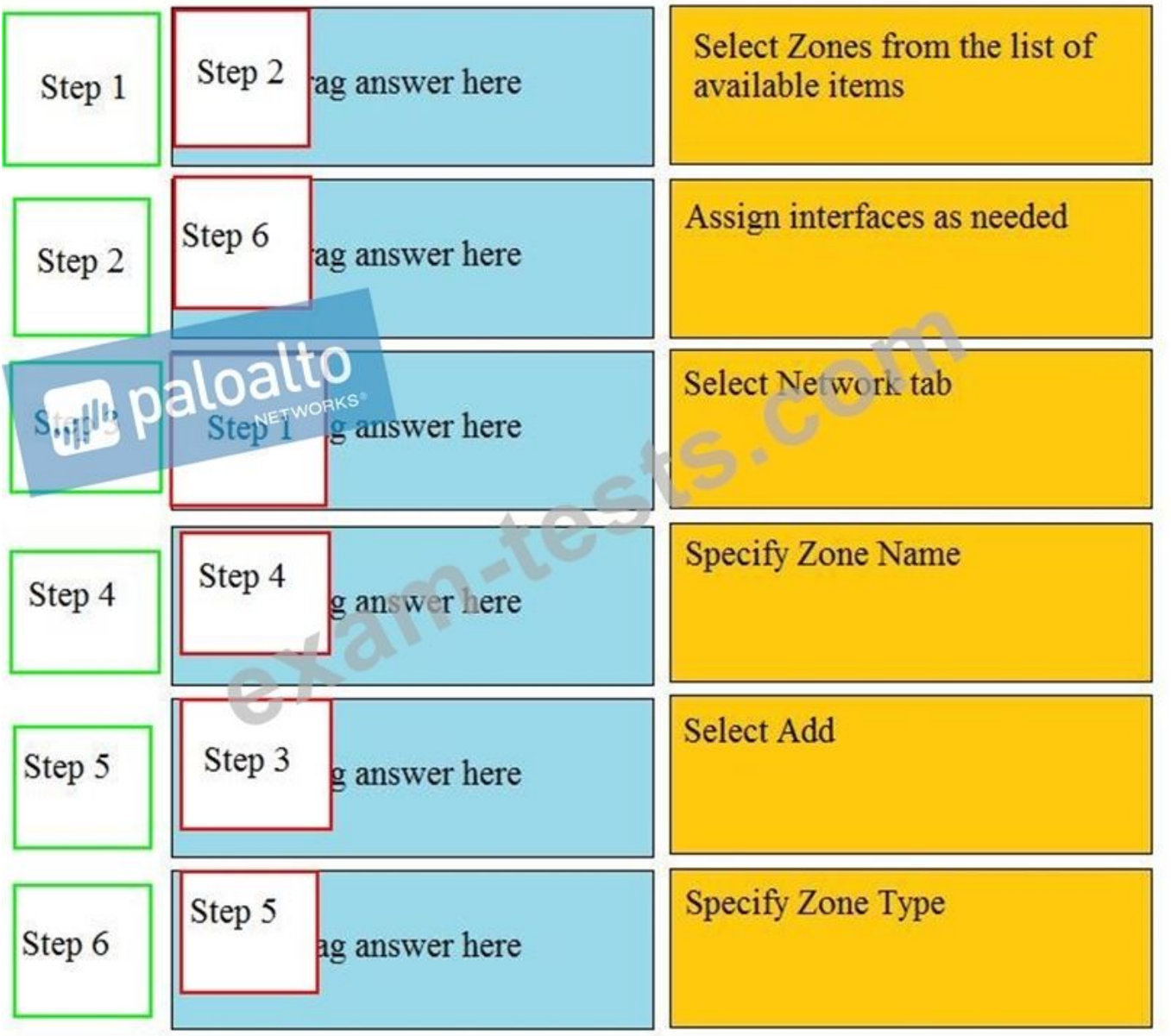
Answer: C (LEAVE A REPLY)

NEW QUESTION: 200

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


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

Answer:



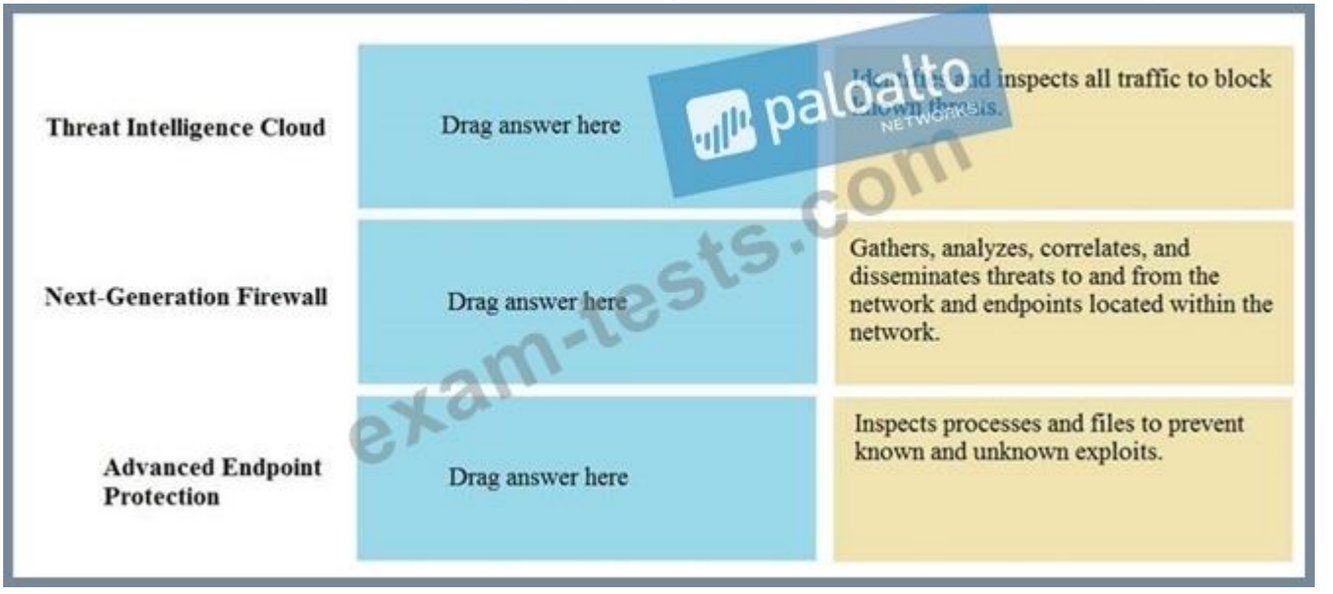
NEW QUESTION: 201
Which type firewall configuration contains in-progress configuration changes?
A. candidate
B. backup
C. running
D. committed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 202
Which statement is true regarding a Best Practice Assessment?
A. When guided by an authorized sales engineer, it helps determine the areas of greatest risk where you should focus prevention activities.
B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture.

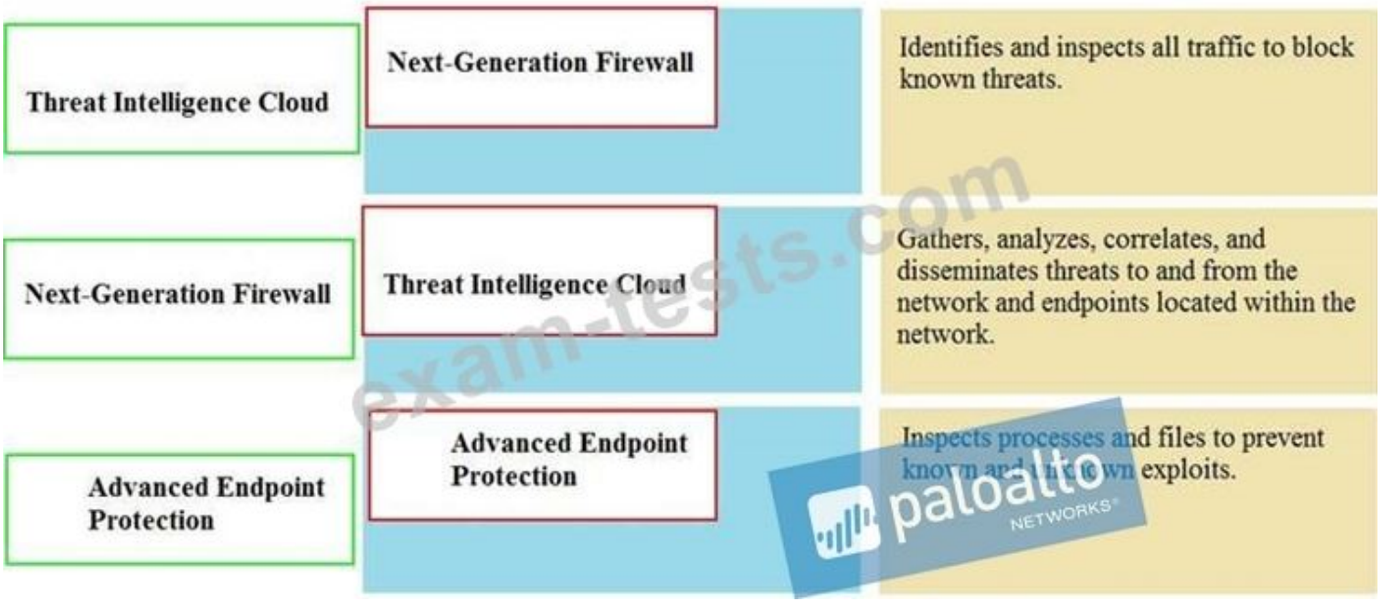
C. It shows how current configuration compares to Palo Alto Networks recommendations.
D. It runs only on firewalls.
Answer: (SHOW ANSWER)

NEW QUESTION: 203
Which path in PAN-OS 10.2 is used to schedule a content update to managed devices using Panorama?
A. Panorama > Device Deployment > Dynamic Updates > Schedules > Add
B. Panorama > Device Deployment > Content Updates > Schedules > Add
C. Panorama > Dynamic Updates > Device Deployment > Schedules > Add
D. Panorama > Content Updates > Device Deployment > Schedules > Add
Answer: A (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/upgrade-panorama/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/schedule-a-content-update-using-panorama

NEW QUESTION: 204
Match the Palo Alto Networks Security Operating Platform architecture to its description.

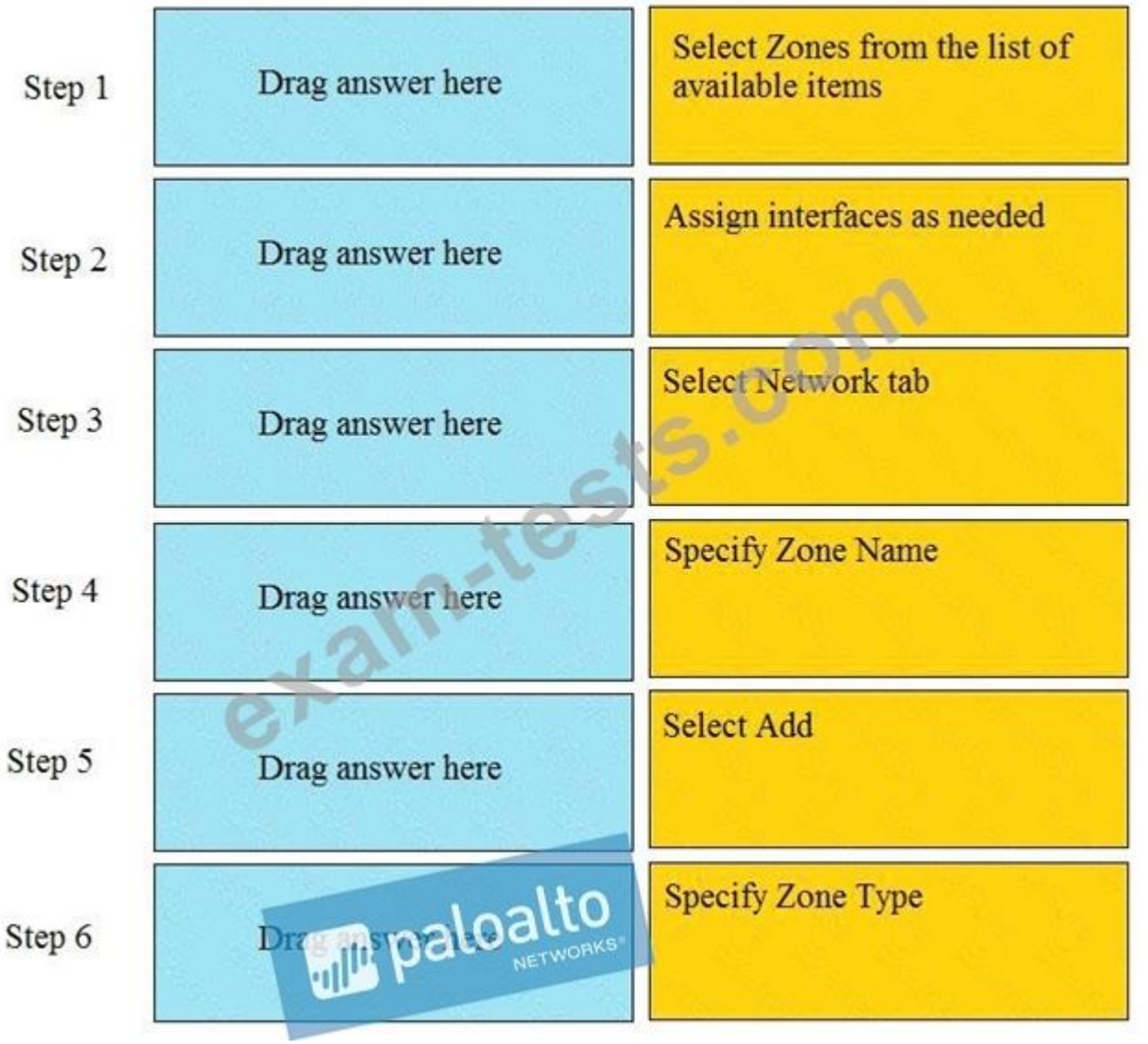


Answer:

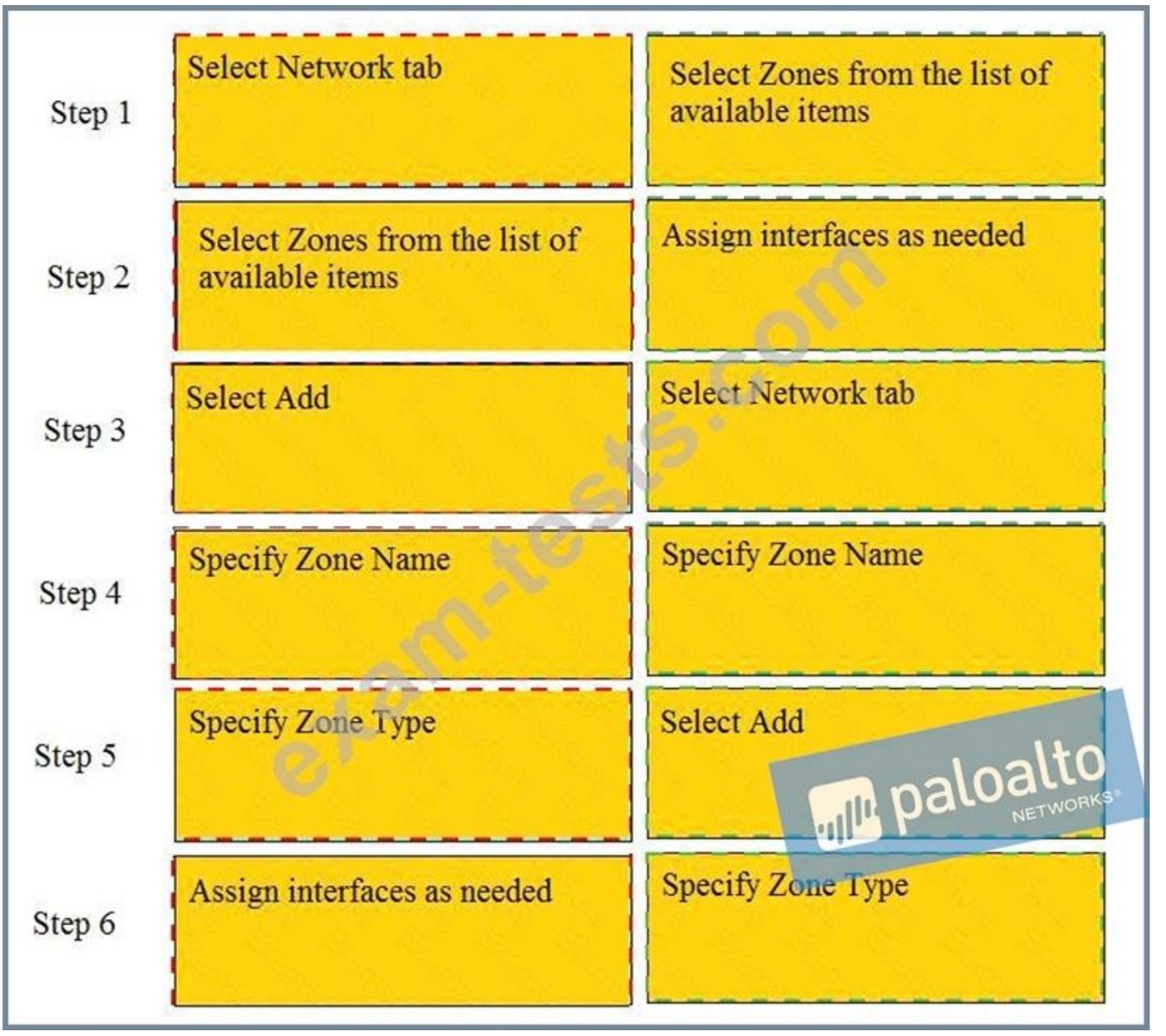


NEW QUESTION: 205

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



Answer:



Explanation

Step 1 - Select network tab

Step 2 - Select zones from the list of available items

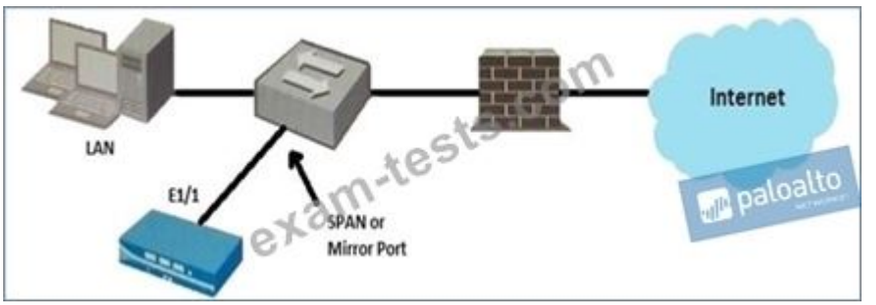
Step 3 - Select Add

Step 4 - Specify Zone Name

Step 5 - Specify Zone Type

Step 6 - Assign interfaces as needed

NEW QUESTION: 206



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

A. Layer3

B. Tunnel

C. Virtual Wire

D. Tap

Answer: D (LEAVE A REPLY)

NEW QUESTION: 207

Which statement best describes the 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 exists Admins can then manually enable policies they want to keep and delete ones they want to remove

B. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications

C. Policy Optimizer can add or change a Log Forwarding profile for each Secunty policy selected

D. Policy Optimizer can display which Security policies have not been used in the last 90 days

Answer: B (LEAVE A REPLY)

NEW QUESTION: 208

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

	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Rule Usage Hit Count	Rule Usage Last Hit	Rule Usage First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

A. The Allow Office Programs rule is using an Application Filter

B. In the Allow Social Networking rule, allows all of Facebook's functions

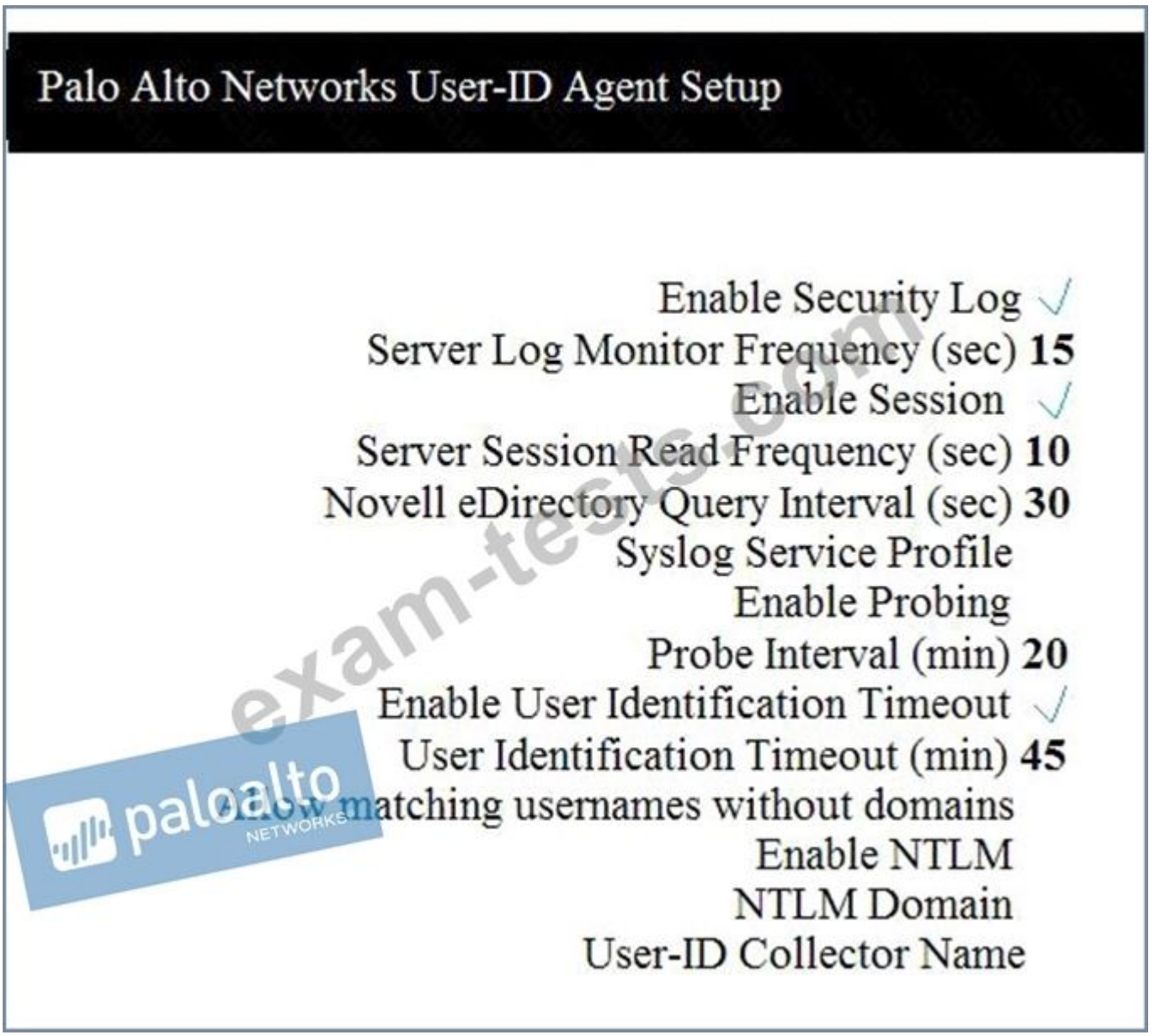
C. In the Allow FTP to web server rule, FTP is allowed using App-ID

D. The Allow Office Programs rule is using an Application Group

Answer: (SHOW ANSWER)

NEW QUESTION: 209

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



A. Enable Session
B. Enable Probing
C. Server Log Monitor Frequency (sec)
D. Enable Security Log
Answer: A,C (LEAVE A REPLY)

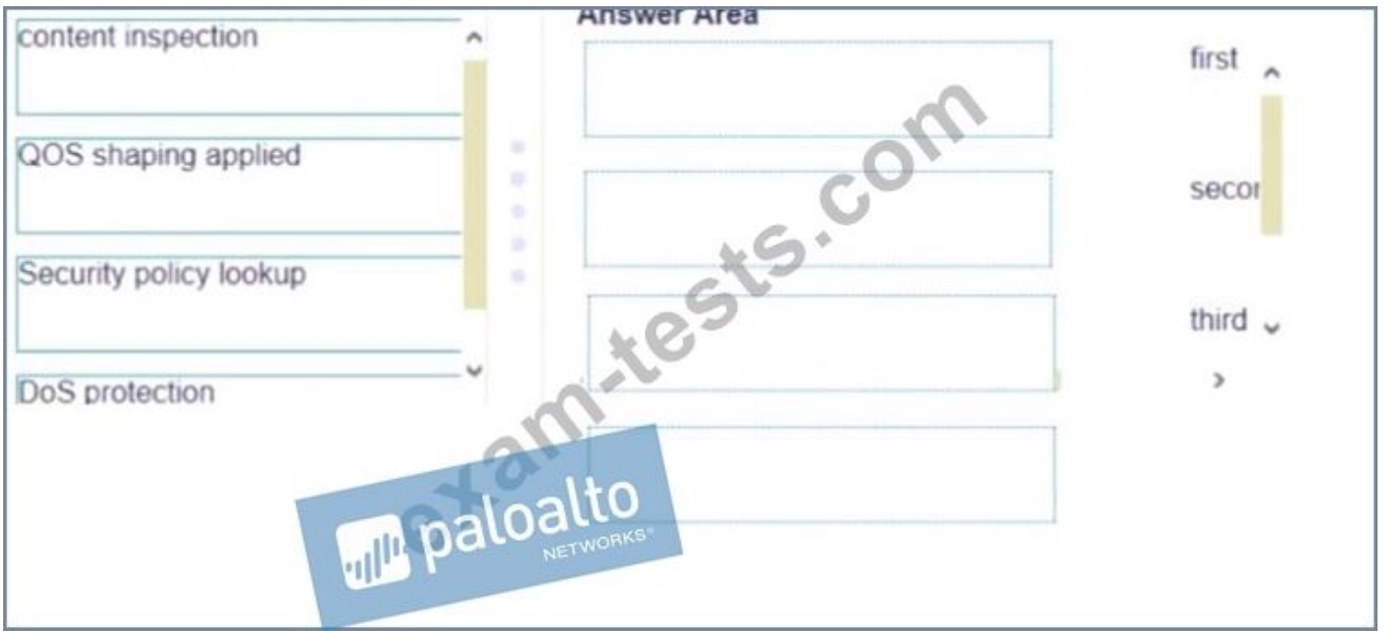
NEW QUESTION: 210
Which plane on a Palo Alto Networks Firewall provides configuration, logging, and reporting functions on a separate processor?
A. data
B. network processing
C. management
D. security processing
Answer: C (LEAVE A REPLY)
Management plane = Log, Report, Configure

Data Plane = AV, exploits, UF, Spyware, VPN, QoS, NAT, CC#, etc

NEW QUESTION: 211
Which type of address object is "10 5 1 1/0 127 248 2"?
A. IP range
B. IP netmask
C. IP subnet
D. IP wildcard mask
Answer: (SHOW ANSWER)

NEW QUESTION: 212
Which administrator type utilizes predefined roles for a local administrator account?
A. Dynamic
B. Device administrator
C. Role-based
D. Superuser
Answer: A (LEAVE A REPLY)

NEW QUESTION: 213
Place the following steps in the packet processing order of operations from first to last.



Answer:

NEW QUESTION: 214

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

A. vulnerability protection

B. antivirus

C. anti-spyware

D. data filtering

Answer: (SHOW ANSWER)

NEW QUESTION: 215

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
Answer: B (LEAVE A REPLY)
Routers know which subnets are physically connected to it and can route between them without any further configuration.

NEW QUESTION: 216
Which update option is not available to administrators?
A. New Spyware Notifications
B. New URLs
C. New Application Signatures
D. New Malicious Domains
E. New Antivirus Signatures
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 217
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
Answer: B (LEAVE A REPLY)
In PANOS10 you need to click a button "Show Technology Column" to see the technology tab.

NEW QUESTION: 218
Which type of security policy rule will match traffic that flows between the Outside zone and inside zone, but would not match traffic that flows within the zones?
A. global
B. intrazone
C. interzone
D. universal
Answer: C (LEAVE A REPLY)
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic- contentupdates.html#:~:text=WildFire%20signature%20updates%20are%20made,within%20a%20minute%20of %
20availability

NEW QUESTION: 219

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

A. save candidate config

B. export named configuration snapshot

C. export device state

D. save named configuration snapshot

Answer: D (LEAVE A REPLY)

NEW QUESTION: 220

Based on the screenshot, what is the purpose of the Included Groups?

			Source			Destination				
	Name	Type	Zone	Address	User	Zone	Address	Application	Service	Action
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.

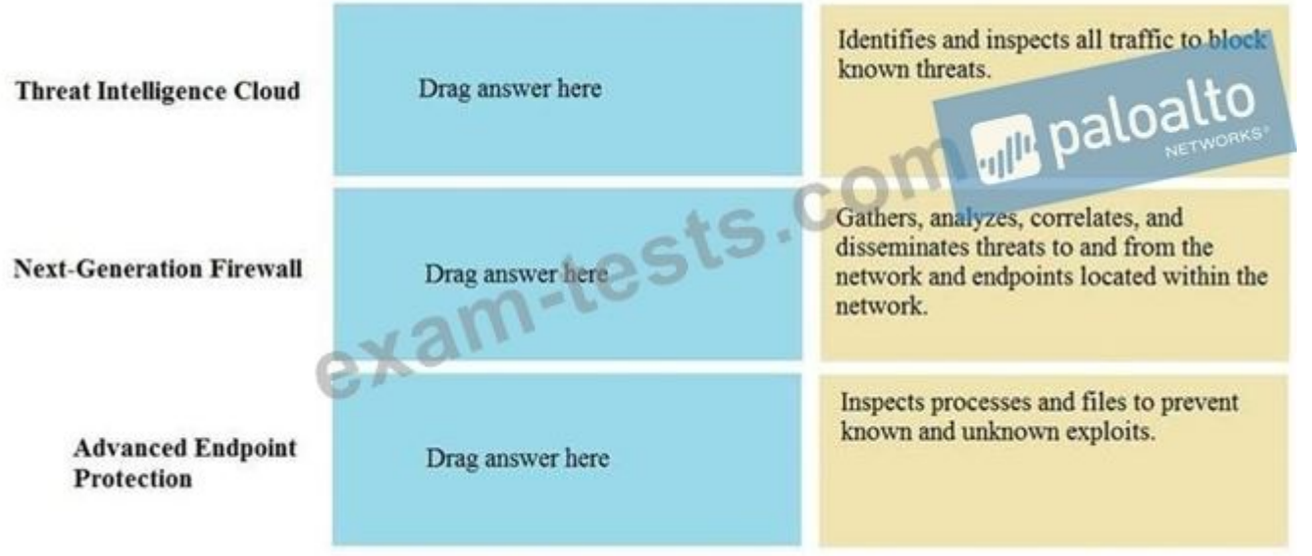
Answer: D (LEAVE A REPLY)

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

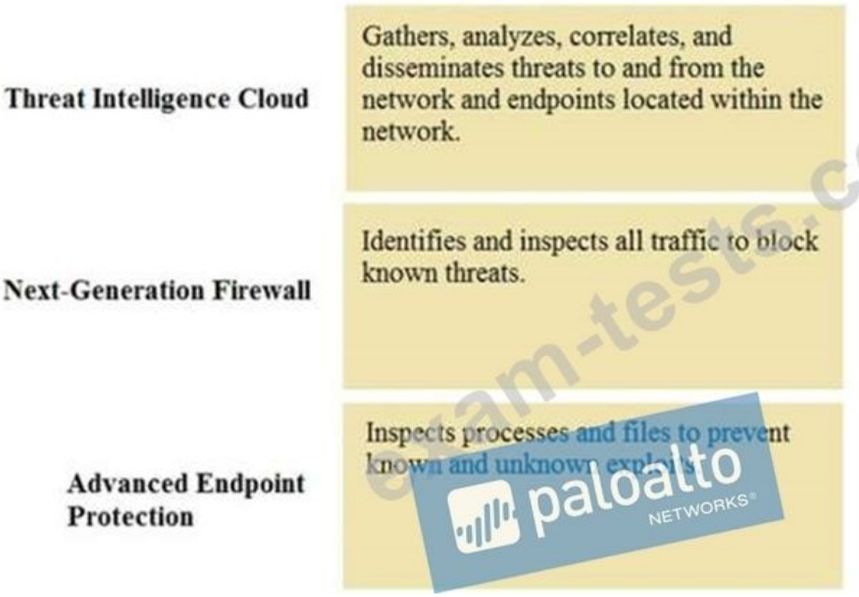
NEW QUESTION: 221

Drag and Drop Question

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



Answer:



NEW QUESTION: 222
What do dynamic user groups you to do?
A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity
B. create a policy that provides auto-remediation for anomalous user behavior and malicious activity
C. create a policy that provides auto-sizing for anomalous user behavior and malicious activity
D. create a dynamic list of firewall administrators
Answer: (SHOW ANSWER)