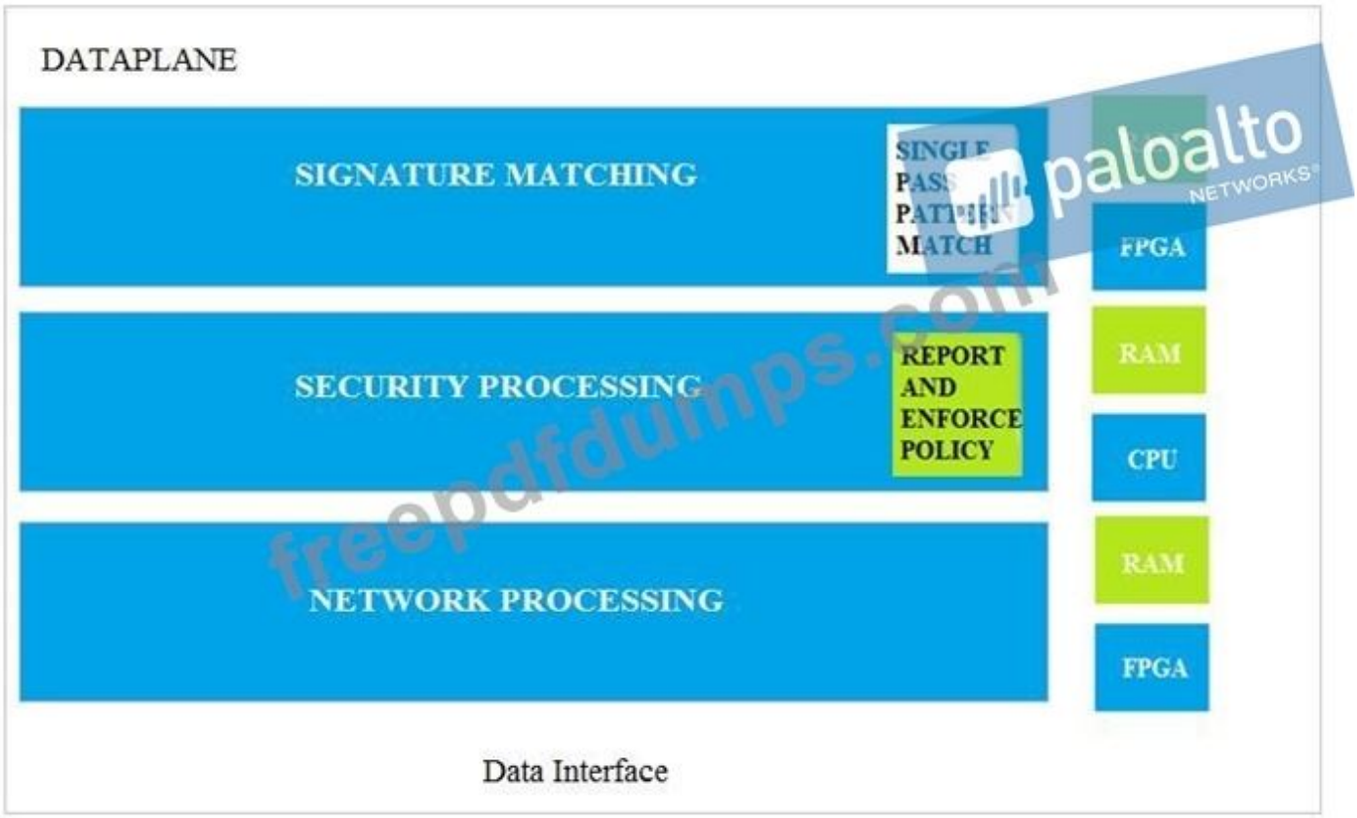
PaloAltoNetworks.NetSec-Analyst.v2026-03-30.q149

Exam Code:	NetSec-Analyst
Exam Name:	Palo Alto Networks Network Security Analyst
Certification Provider:	Palo Alto Networks
Free Question Number:	149
Version:	v2026-03-30
# of views:	209
# of Questions views:	1490
https://www.freepdfdumps.com/PaloAltoNetworks.NetSec-Analyst.v2026-03-30.q149.html	

NEW QUESTION: 1
Which CLI command will help confirm if FQDN objects are resolved in the event there is a shadow rule?
A. >show system fqdn
B. >request fqdn show system
C. >request show system fqdn
D. >request system fqdn show
Answer: A (LEAVE A REPLY)
The show system fqdn command displays the FQDN objects configured on the firewall and their resolved IP addresses. This can help confirm if the FQDN objects are resolved correctly and if they match the expected traffic. A shadow rule is a rule that is never matched because a preceding rule covers the same traffic. If a shadow rule uses FQDN objects, it is possible that the FQDN objects are not resolved or have different IP addresses than the traffic, causing the rule to be ineffective.

NEW QUESTION: 2
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. Signature Matching
D. Network Processing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
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. Reset server
B. Reset both
C. Drop, send ICMP Unreachable
D. Drop
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Which two types of profiles are needed to create an authentication sequence? (Choose two.)
A. Server profile
B. Authentication profile
C. Security profile
D. Interface Management profile
Answer: A,B (LEAVE A REPLY)

In the FW you define an Auth sequence which specifies the Auth Profile. If you click add on an Auth Profile and define one named TACACS for example, the Auth Profile calls in the TACACS+ Server Profile.

NEW QUESTION: 5
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. Name
C. Apps Seen
D. Apps Allowed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
An administrator would like to see the traffic that matches the interzone-default rule in the traffic logs.
What is the correct process to enable this logging1?
A. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session End and click OK
B. This rule has traffic logging enabled by default no further action is required
C. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session Start and click OK
D. Select the interzone-default rule and click Override on the Actions tab select Log at Session End and click OK
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?
A. Aggregation
B. Aggregate
C. High Availability
D. Management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
What is the correct process tor creating a custom URL category?
A. Objects > Security Profiles > URL Filtering > Add
B. Objects > Security Profiles > URL Category > Add
C. Objects > Custom Objects > URL Category > Add
D. Objects > Custom Objects > URL Filtering > Add
Answer: C (LEAVE A REPLY)

NEW QUESTION: 9
The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop.
Which security profile feature could have been used to prevent the communication with the CnC server?
A. Create an anti-spyware profile and enable DNS Sinkhole
B. Create an antivirus profile and enable DNS Sinkhole
C. Create a URL filtering profile and block the DNS Sinkhole category
D. Create a security policy and enable DNS Sinkhole
Answer: A (LEAVE A REPLY)
References:

NEW QUESTION: 10
An organization has some applications that are restricted for access by the Human Resources Department only, and other applications that are available for any known user in the organization.
What object is best suited for this configuration?
A. Application Filter
B. Application Group
C. Tag
D. External Dynamic List
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
Your company occupies one floor in a single building you have two active directory domain controllers on a single networks the firewall s management plane is only slightly utilized.
Which user-ID agent sufficient in your network?
A. PAN-OS integrated agent deployed on the firewall
B. Windows-based agent deployed on the internal network a domain member
C. Citrix terminal server agent deployed on the network
D. Windows-based agent deployed on each domain controller
Answer: D (LEAVE A REPLY)

Explanation/Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configureuser- mapping-using-the-windows-user-id- agent/configure-the-windows-based-user-id- agent-for-usermapping.
html

NEW QUESTION: 12
Which option lists the attributes that are selectable when setting up an Application filters?
A. Category, Subcategory, Technology, and Characteristic
B. Category, Subcategory, Technology, Risk, and Characteristic
C. Name, Category, Technology, Risk, and Characteristic
D. Category, Subcategory, Risk, Standard Ports, and Technology
Answer: B (LEAVE A REPLY)
Explanation/Reference:
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-application- filters

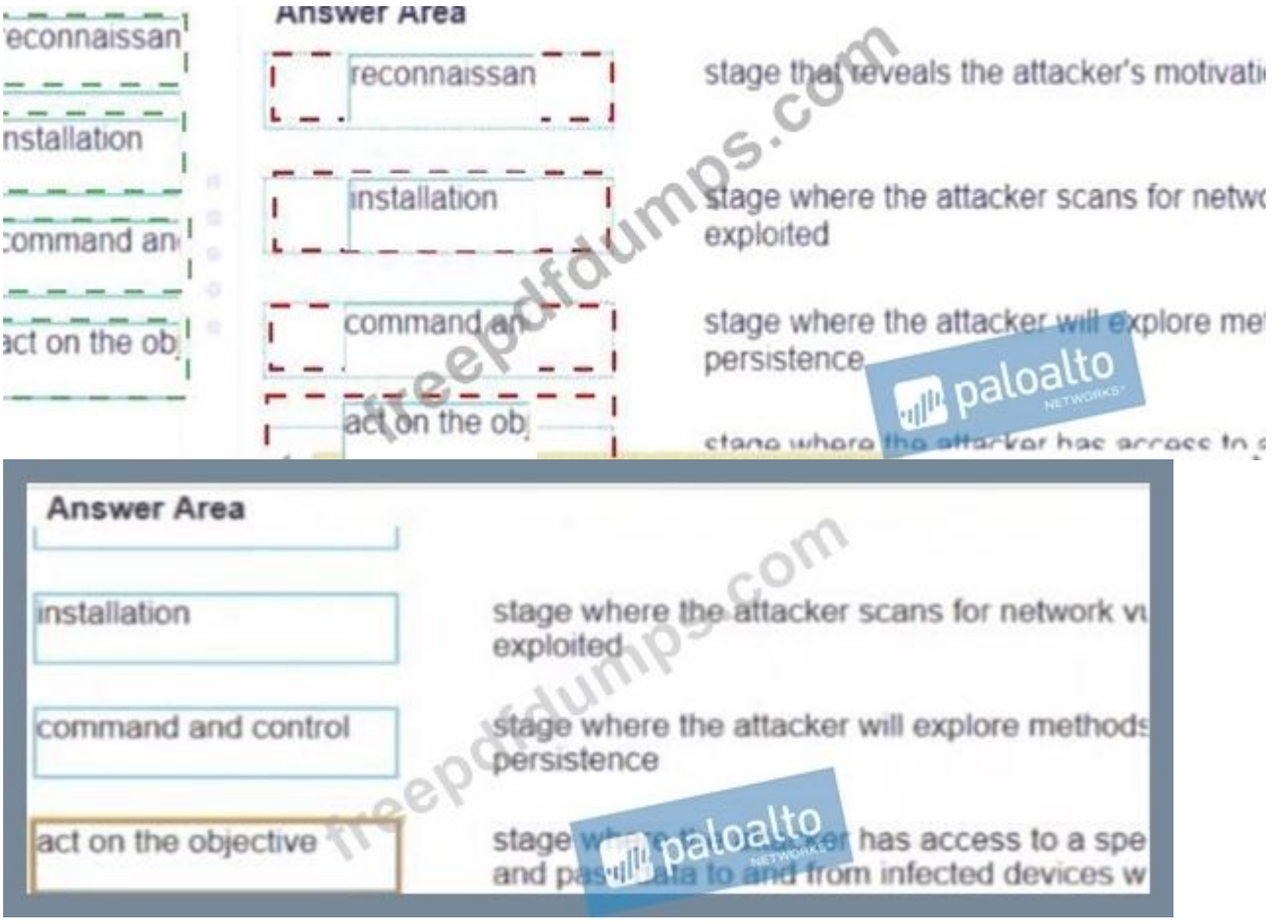
NEW QUESTION: 13
A network administrator creates an intrazone security policy rule on a NGFW. The source zones are set to IT.
Finance, and HR.
To which two types of traffic will the rule apply? (Choose two.)
A. Within zone HR
B. Within zone IT
C. Between zone IT and zone HR
D. Between zone IT and zone Finance
Answer: A,B (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTHCA0

NEW QUESTION: 14
Which three configuration settings are required on a Palo Alto networks firewall management interface?
A. default gateway
B. netmask
C. IP address
D. hostname
E. auto-negotiation
Answer: A,B,C (LEAVE A REPLY)
Explanation/Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIN7CAK

NEW QUESTION: 15
Which three Ethernet interface types are configurable on the Palo Alto Networks firewall? (Choose three.)
A. Virtual Wire
B. Tap
C. Dynamic
D. Layer 3
E. Static
Answer: (SHOW ANSWER)
Palo Alto Networks firewalls support three types of Ethernet interfaces that can be configured on the firewall:
virtual wire, tap, and layer 31. These interface types determine how the firewall processes traffic and applies security policies. Some of the characteristics of these interface types are:
Virtual Wire: A virtual wire interface allows the firewall to transparently pass traffic between two network segments without modifying the packets or affecting the routing. The firewall can still apply security policies and inspect the traffic based on the source and destination zones of the virtual wire2.
Tap: A tap interface allows the firewall to passively monitor traffic from a network switch or router without affecting the traffic flow. The firewall can only receive traffic from a tap interface and cannot send traffic out of it. The firewall can apply security policies and inspect the traffic based on the source and destination zones of the tap interface3.
Layer 3: A layer 3 interface allows the firewall to act as a router and participate in the network routing. The firewall can send and receive traffic from a layer 3 interface and apply security policies and inspect the traffic based on the source and destination IP addresses and zones of the interface4.
References: Ethernet Interface Types, Virtual Wire Interfaces, Tap Interfaces, Layer 3 Interfaces, Updated Certifications for PAN-OS 10.1, [Palo Alto Networks Certified Network Security Administrator (PAN-OS
10.0)] or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

NEW QUESTION: 16
Match the cyber-attack lifecycle stage to its correct description.

Answer:



NEW QUESTION: 17
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: (SHOW ANSWER)
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: 18
The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering "gambling" category.
Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the "gambling" URL category?
A. Add *.powerball.com to the URL Filtering allow list.
B. Manually remove powerball.com from the gambling URL category.
C. Create a custom URL category, add *.powerball.com to it and allow it in the Security Profile.
D. Add just the URL www.powerball.com to a Security policy allow rule.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 19
In which section of the PAN-OS GUI does an administrator configure URL Filtering profiles?
A. Policies
B. Network
C. Objects
D. Device
Answer: (SHOW ANSWER)
An administrator can configure URL Filtering profiles in the Objects section of the PAN-OS GUI. A URL Filtering profile is a collection of URL filtering controls that you can apply to individual Security policy rules that allow access to the internet1. You can set site access for URL categories, allow or disallow user credential submissions, enable safe search enforcement, and various other settings1.
To create a URL Filtering profile, go to Objects > Security Profiles > URL Filtering and click Add. You can then specify the profile name, description, and settings for each URL category and action2. You can also configure other options such as User Credential Detection, HTTP Header Insertion, and URL Filtering Inline ML2. After creating the profile, you can attach it to a Security policy rule that allows web traffic2.

NEW QUESTION: 20
Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choices to block the sameURL then which choice would be the last to block access to the URL?
A. EDL in URL Filtering Profile.
B. Custom URL category in Security Policy rule.
C. Custom URL category in URL Filtering Profile.
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: 21
Which table for NAT and NPTv6 (IPv6-to-IPv6 Network Prefix Translation) settings is available only on Panorama?
A. NAT Target Tab
B. NAT Active/Active HA Binding Tab
C. NAT Translated Packet Tab
D. NAT Policies General Tab
Answer: (SHOW ANSWER)
The NAT Target tab is a table that allows you to specify the target firewalls or device groups for each NAT policy rule on Panorama. This tab is available only on Panorama and not on individual firewalls. The NAT Target tab enables you to create a single NAT policy rulebase on Panorama and then selectively push the rules to the firewalls or device groups that require them. This reduces the complexity and duplication of managing NAT policies across multiple firewalls1. References: NAT Target Tab, NAT Policy Overview, NPTv6 Overview, Updated Certifications for PAN-OS 10.1.

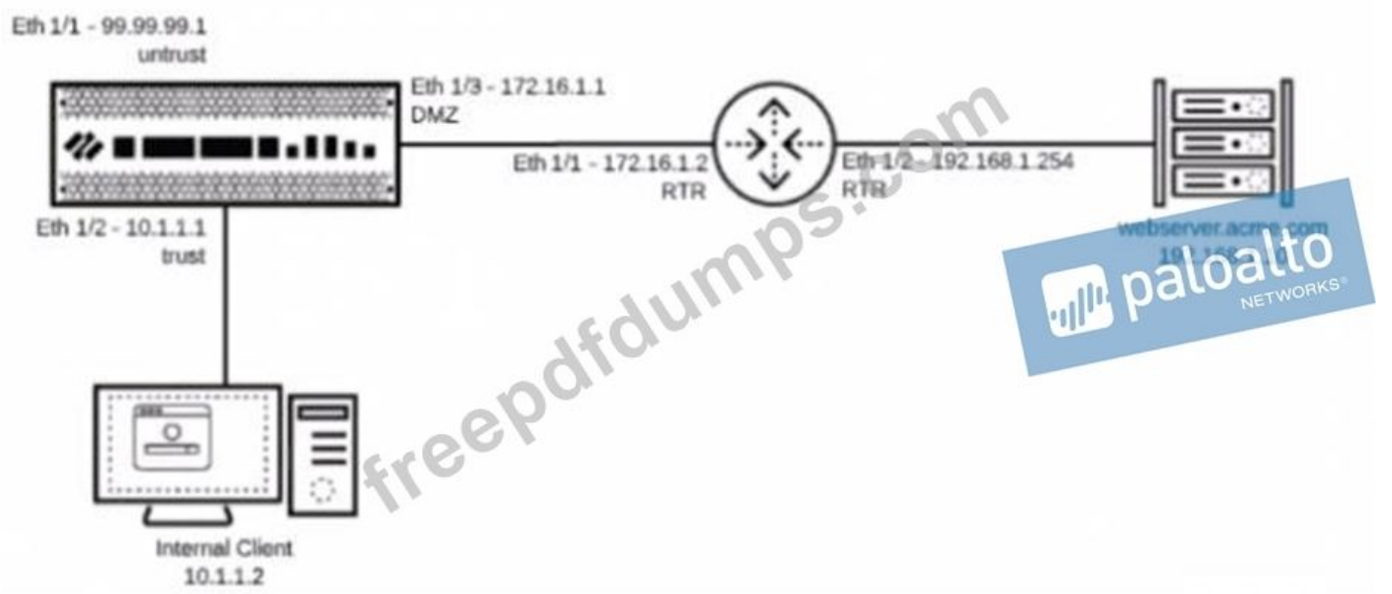
NEW QUESTION: 22
What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?
A. every 30 minutes
B. every 5 minutes
C. once every 24 hours
D. every 1 minute
Answer: (SHOW ANSWER)
Because new WildFire signatures are now available every five minutes, it is a best practice to use this setting to ensure the firewall retrieves these signatures within a minute of availability.

NEW QUESTION: 23
Which Security policy action will message a user's browser that their web session has been terminated?
A. Drop
B. Deny
C. Reset client
D. Reset server
Answer: C (LEAVE A REPLY)

Sending a reset only to the client would ensure, for example, internal hosts receive a notification the session was reset and the browser is not left spinning or the application can close the established session while the remote server is left unaware.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClltCAC

NEW QUESTION: 24
Which prevention technique will prevent attacks based on packet count?
A. antivirus profile
B. zone protection profile
C. vulnerability profile
D. URL filtering profile
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
You have been tasked to configure access to a new web server located in the DMZ Based on the diagram what configuration changes are required in the NGFW virtual router to route traffic from the 10 1 1 0/24 network to 192 168 1 0/24?

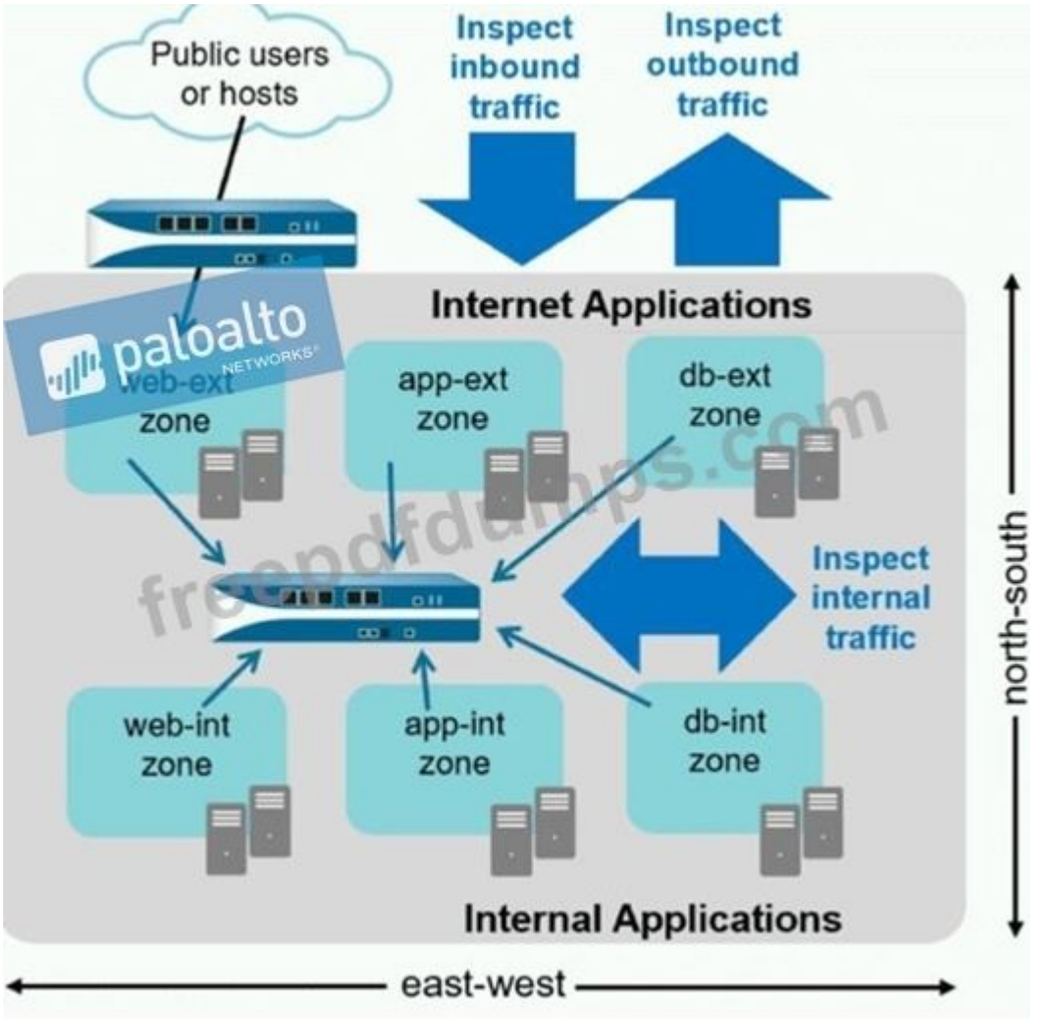


A. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next-hop of 192.168
1.10
B. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/2 with a next-hop of 172.16.1.2
C. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with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

NEW QUESTION: 26
Where does a user assign a tag group to a policy rule in the policy creation window?
A. Application tab
B. General tab
C. Actions tab
D. Usage tab
Answer: B (LEAVE A REPLY)
A user can assign a tag group to a policy rule in the policy creation window by selecting the General tab. A tag group is a collection of tags that can be used to identify and filter policy rules based on different criteria, such as function, location, or priority. A user can create a tag group on Panorama and assign it to a policy rule to apply the same set of tags to multiple firewalls or device groups1. To assign a tag group to a policy rule, the user needs to:
Select the General tab in the policy creation window.
Click the Tag Group drop-down menu and select the tag group that the user wants to assign to the policy rule.
Click OK to save the changes. The policy rule will inherit the tags from the tag group and display them in the Tag column.
References: Assign a Tag Group to a Policy Rule, Policy, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

NEW QUESTION: 27
Which administrator type utilizes predefined roles for a local administrator account?
A. Superuser
B. Role-based
C. Dynamic
D. Device administrator
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 28
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



A. north-south traffic
B. branch office traffic
C. perimeter traffic
D. east-west traffic
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.
Why doesn't the administrator see the traffic?
A. The interzone-default policy is disabled by default.
B. Traffic is being denied on the interzone-default policy.
C. The Log Forwarding profile is not configured on the policy.
D. Logging on the interzone-default policy is disabled.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 30

What are three valid source or D=destination conditions available as Security policy qualifiers? (Choose three.)

A. Service

B. User

C. Application

D. Address

E. Zone ab

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

Three valid source or destination conditions available as Security policy qualifiers are User, Application, and Zone. These qualifiers allow you to define the match criteria for a Security policy rule based on the identity of the user, the application used, and the zone where the traffic originates or terminates. You can use these qualifiers to enforce granular security policies that control access to network resources and prevent threats1.

Some of the characteristics of these qualifiers are:

User: The User qualifier allows you to specify the source or destination user or user group for a Security policy rule. The firewall can identify users based on various methods, such as User-ID, Captive Portal, or GlobalProtect. You can use the User qualifier to apply different security policies for different users or user groups, such as allowing access to certain applications or resources based on user roles or privileges2.

Application: The Application qualifier allows you to specify the application or application group for a Security policy rule. The firewall can identify applications based on App-ID, which is a technology that classifies applications based on multiple attributes, such as signatures, protocol decoders, heuristics, and SSL decryption. You can use the Application qualifier to allow or deny access to specific applications or application groups, such as enabling web browsing but blocking social networking or file sharing3.

Zone: The Zone qualifier allows you to specify the source or destination zone for a Security policy rule. A zone is a logical grouping of one or more interfaces that have similar functions or security requirements. The firewall can apply security policies based on the zones where the traffic originates or terminates, such as intrazone, interzone, or universal. You can use the Zone qualifier to segment your network and isolate traffic based on different trust levels or network functions4.

References: Security Policy, Zones, User-ID, App-ID, Certifications - Palo Alto Networks, [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

NEW QUESTION: 31

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: 32

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. Send a TCP reset packet to the client- and server-side devices
D. Perform the default deny action as defined in the App-ID database for the application
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which two security profile types can be attached to a security policy? (Choose two.)
A. antivirus
B. DDoS protection
C. threat
D. vulnerability
Answer: A,D (LEAVE A REPLY)
References:

NEW QUESTION: 34
Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?
A. Active Directory monitoring
B. domain controller monitoring
C. Windows session monitoring
D. Windows client probing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
You need to allow users to access the office-suite application of their choice. How should you configure the firewall to allow access to any office-suite application?
A. Create an Application Filter and name it Office Programs then filter on the business-systems category.
B. Create an Application Group and add Office 365, Evernote Google Docs and Libre Office
C. Create an Application Filter and name it Office Programs, then filter it on the office programs subcategory.
D. Create an Application Group and add business-systems to it.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
Which license is required to use the Palo Alto Networks built-in IP address EDLs?
A. DNS Security

B. Threat Prevention
C. WildFire
D. SD-Wan
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in- policy
/builtin-edls.html#:~:text=With%20an%

NEW QUESTION: 37
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)
References:

NEW QUESTION: 38
Which URL Filtering Profile action does not generate a log entry when a user attempts to access a URL?
A. override
B. continue
C. block
D. allow
Answer: (SHOW ANSWER)

NEW QUESTION: 39
An administrator is troubleshooting an issue with traffic that matches the intrazone-default rule, which is set to default configuration.
What should the administrator do?
A. change the logging action on the rule
B. refresh the Traffic Log
C. tune your Traffic Log filter to include the dates
D. review the System Log
Answer: A (LEAVE A REPLY)

NEW QUESTION: 40

A network has 10 domain controllers, multiple WAN links, and a network infrastructure with bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?
A. Windows-based agent on a domain controller
B. Captive Portal
C. Citrix terminal server with adequate data-plane resources
D. PAN-OS integrated agent
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?
A. SAML
B. Multi-Factor Authentication
C. Role-based
D. Dynamic
Answer: (SHOW ANSWER)
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage- firewall-administrators/administrative-role-types.html

NEW QUESTION: 42
What are the requirements for using Palo Alto Networks EDL Hosting Sen/ice?
A. any supported Palo Alto Networks firewall or Prisma Access firewall
B. an additional subscription free of charge
C. an additional paid subscription
D. a firewall device running with a minimum version of PAN-OS 10.1
Answer: A (LEAVE A REPLY)

NEW QUESTION: 43
When creating a Panorama administrator type of Device Group and Template Admin, which two things must you create first? (Choose two.)
A. access domain
B. admin rote
C. server profile
D. password profile
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 44
Based on the graphic which statement accurately describes the output shown in the server monitoring panel?

A. The User-ID agent is connected to a domain controller labeled lab-client.
B. The host lab-client has been found by the User-ID agent.
C. The host lab-client has been found by a domain controller.
D. The User-ID agent is connected to the firewall labeled lab-client.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which two features implement one-to-one translation of a source IP address while allowing the source port to change? (Choose two.)
A. Static IP
B. Dynamic IP / Port Fallback
C. Dynamic IP
D. Dynamic IP and Port (DIPP)
Answer: A,D (LEAVE A REPLY)
Static IP and Dynamic IP and Port (DIPP) are two features that implement one-to-one translation of a source IP address while allowing the source port to change. Static IP translates a single source address to a specific public address, and allows the source port to change dynamically1. Dynamic IP and Port (DIPP) translates the source IP address or range to a single IP address, and uses the source port to differentiate between multiple source IPs that share the same translated address2. Both of these features provide a one-to-one translation of IP addresses, but do not restrict the source port. References:
* Static IP - Palo Alto Networks
* Dynamic IP and Port - Palo Alto Networks

NEW QUESTION: 46

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 HR
B. traffic between zone IT and zone Finance
C. traffic between zone Finance and zone HR
D. traffic within zone IT
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 47
Which three statement describe the operation of Security Policy rules or Security Profiles? (Choose three)
A. Security Policy rules are attached to Security Profiles.
B. Security Policy rules can block or allow traffic.
C. Security Profile should be used only on allowed traffic.
D. Security policy rules inspect but do not block traffic.
E. Security Profile are attached to security policy rules.
Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 48
All users from the internal zone must be allowed only HTTP access to a server in the DMZ zone.
Complete the empty field in the Security policy using an application object to permit only this type of access.
Source Zone: Internal -
Destination Zone: DMZ Zone -
Application: _____
Service: application-default -
Action: allow
A. Application = "any"
B. Application = "http"
C. Application = "ssl"
D. Application = "web-browsing"

Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which the app-ID application will you need to allow in your security policy to use facebook-chat?
A. facebook-email
B. facebook-chat
C. facebook-base
D. facebook
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 50
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 performs over 200 security checks on Panorama/firewall for the assessment
D. It provides a percentage of adoption for each assessment area
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?
A. Tap
B. Layer 2
C. Layer 3
D. Virtual Wire
Answer: A (LEAVE A REPLY)

NEW QUESTION: 52
How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?
A. Automatically "download and install" but with the "disable new applications" option used
B. Configure the option for "Threshold"
C. Disable automatic updates during weekdays
D. Automatically "download only" and then install Applications and Threats later, after the administrator approves the update
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
An administrator would like to use App-ID's deny action for an application and would like that action updated with dynamic updates as new content becomes available.

Which security policy action causes this?
A. Reset server
B. Reset both
C. Deny
D. Drop
Answer: C (LEAVE A REPLY)
Explanation/Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-configuration backups/revert-firewall-configuration- changes.html

NEW QUESTION: 54
An administrator creates a new Security policy rule to allow DNS traffic from the LAN to the DMZ zones.
The administrator does not change the rule type from its default value.
What type of Security policy rule is created?
A. Tagged
B. Universal
C. Interzone
D. Intrazone
Answer: (SHOW ANSWER)

NEW QUESTION: 55
In which two types of NAT can oversubscription be used? (Choose two.)
A. Static IP
B. Destination NAT
C. Dynamic IP and Port (DIPP)
D. Dynamic IP
Answer: C,D (LEAVE A REPLY)
Oversubscription is a feature that allows you to use more private IP addresses than public IP addresses for NAT. This means that multiple private IP addresses can share the same public IP address, as long as they use different ports. Oversubscription can be used in two types of NAT: Dynamic IP and Port (DIPP) and Dynamic IP. DIPP NAT translates both the source IP address and the source port number of the outgoing packets, and can have an oversubscription rate greater than 1. Dynamic IP NAT translates only the source IP address of the outgoing packets, and can have an oversubscription rate of 1 or less. Static IP and Destination NAT do not support oversubscription, as they require a one-to-one mapping between the private and public IP addresses. References: Source NAT, Configure NAT, NAT

NEW QUESTION: 56
Which statements is true regarding a Heatmap report?

A. When guided by authorized sales engineer, it helps determine te areas of greatest security risk.
B. It provides a percentage of adoption for each assessment area.
C. It runs only on firewall.
D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture.
Answer: B (LEAVE A REPLY)
Reference: https://live.paloaltonetworks.com/t5/best-practice-assessment-blogs/the-best-practice-assessment- bpa-tool-for-ngfw-and-panorama/ba-p/248343

NEW QUESTION: 57
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: 58
Identify the correct order to configure the PAN-OS integrated USER-ID agent.
3. add the service account to monitor the server(s)
2. define the address of the servers to be monitored on the firewall
4. commit the configuration, and verify agent connection status
1. create a service account on the Domain Controller with sufficient permissions to execute the User- ID agent

A. 1-3-2-4
B. 1-4-3-2
C. 3-1-2-4
D. 2-3-4-1
Answer: A (LEAVE A REPLY)

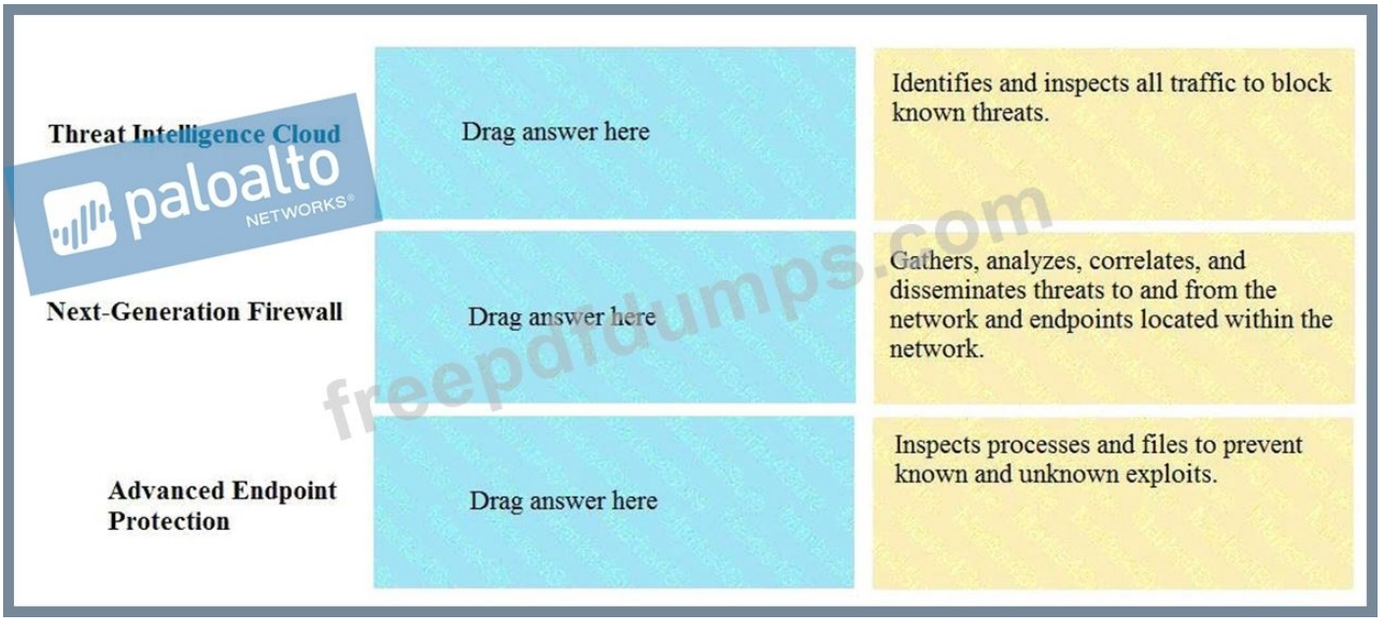
NEW QUESTION: 59
During the packet flow process, which two processes are performed in application identification? (Choose two.)
A. pattern based application identification
B. application override policy match
C. session application identified
D. application changed from content inspection
Answer: A,B (LEAVE A REPLY)
Reference: http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309

NEW QUESTION: 60
An engineer at a managed services provider is updating an application that allows its customers to request firewall changes to also manage SD-WAN. The application will be able to make any approved changes directly to devices via API.
What is a requirement for the application to create SD-WAN interfaces?
A. REST API's "sdwanInterfaceprofiles" parameter on a Panorama device
B. REST API's "sdwanInterfaces" parameter on a firewall device
C. XML API's "sdwanprofiles/interfaces" parameter on a Panorama device
D. XML API's "InterfaceProfiles/sdwan" parameter on a firewall device
Answer: B (LEAVE A REPLY)
To create SD-WAN interfaces through an API, the correct approach is to use the REST API's "sdwanInterfaces" parameter on a firewall device. This parameter allows you to configure SD-WAN interfaces directly on the firewall devices via API, ensuring that the required interfaces are set up and managed for SD-WAN functionality.

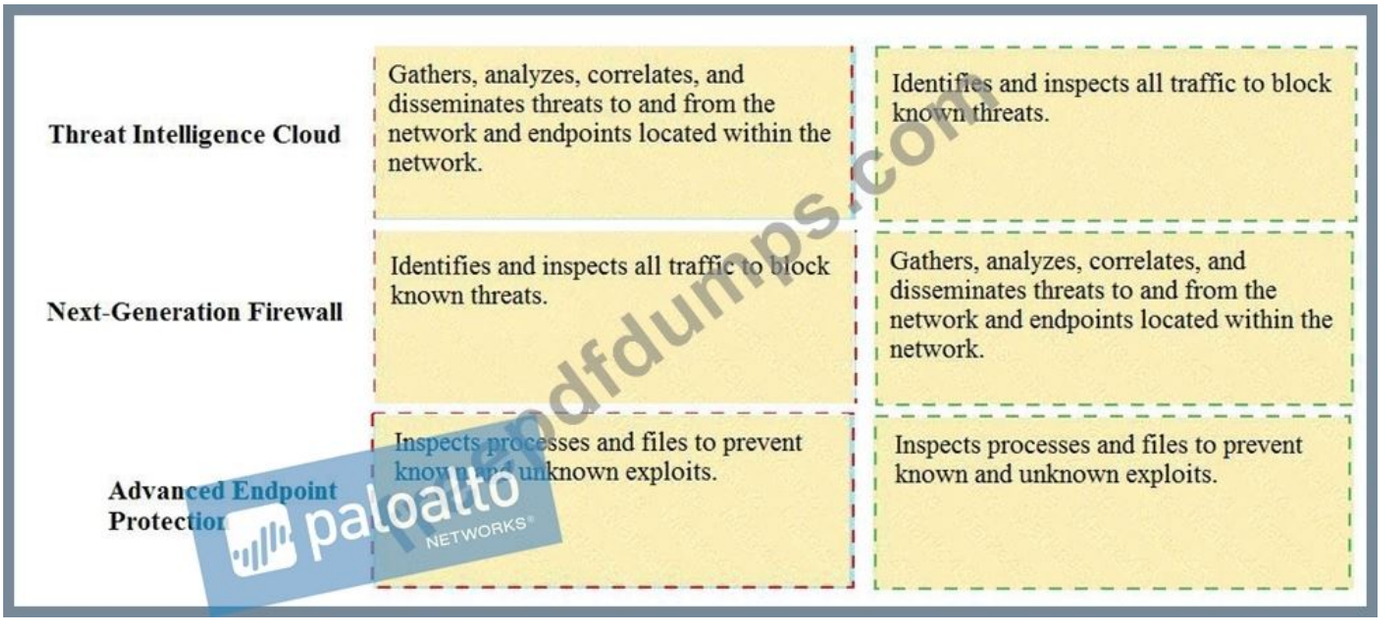
NEW QUESTION: 61
What is used to monitor Security policy applications and usage?
A. Policy Optimizer
B. App-ID
C. Security profile
D. Policy-based forwarding
Answer: A (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/policies/policies-security/applications-and-usage

NEW QUESTION: 62

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: 63
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. 22
B. 80
C. 23
D. 53
Answer: (SHOW ANSWER)

NEW QUESTION: 64
An administrator plans to upgrade a pair of active/passive firewalls to a new PAN-OS release. The environment is highly sensitive, and downtime must be minimized.
What is the recommended upgrade process for minimal disruption in this high availability (HA) scenario?
A. Suspend the active firewall to trigger a failover to the passive firewall. With traffic now running on the former passive unit, upgrade the suspended (now passive) firewall and confirm proper operation. Then fail traffic back and upgrade the remaining firewall.
B. Shut down the currently active firewall and upgrade it offline, allowing the passive firewall to handle all traffic. Once the active firewall finishes upgrading, bring it back online and rejoin the HA cluster.
Finally, upgrade the passive firewall while the newly upgraded unit remains active.
C. Isolate both firewalls from the production environment and upgrade them in a separate, offline setup.
Reconnect them only after validating the new software version, resuming HA functionality once both units are fully upgraded and tested.
D. Push the new PAN-OS version simultaneously to both firewalls, having them upgrade and reboot in parallel. Rely on automated HA reconvergence to restore normal operations without manually failing over traffic.
Answer: A (LEAVE A REPLY)

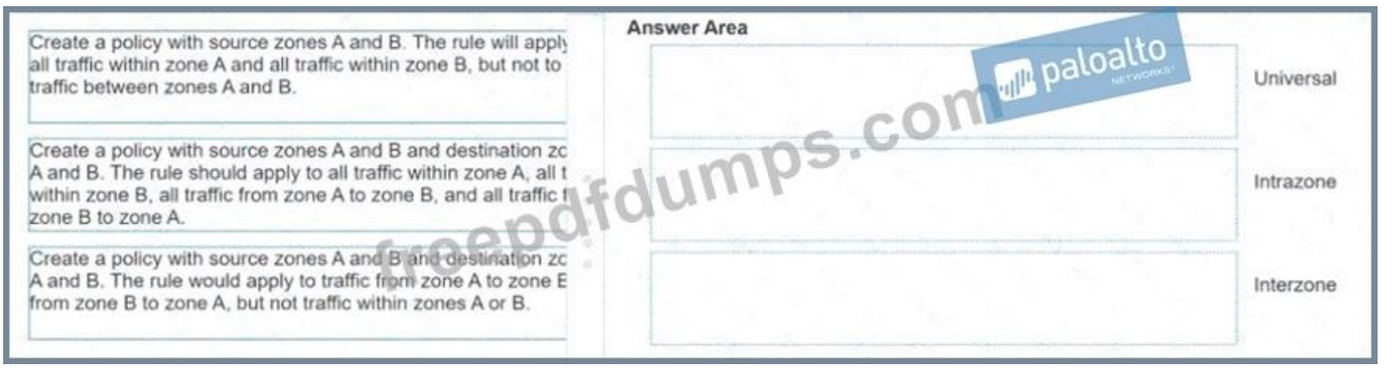
In an active/passive HA setup, the recommended process for upgrading involves minimizing downtime and ensuring traffic continuity by using the failover process:
Suspend the active firewall: This triggers a failover to the passive unit, making it the active unit.
Upgrade the former passive (now active) unit: With traffic now running on the previously passive unit, upgrade the suspended unit while the active unit continues handling traffic.
Confirm proper operation: Once the upgrade is complete, verify that the upgraded unit is functioning properly.
Fail traffic back: Once the upgraded firewall is confirmed to be working, fail the traffic back to the original active unit and upgrade the remaining firewall.

NEW QUESTION: 65
According to a customer's CIO, who is upgrading PAN-OS versions, "Finding issues and then engaging with your support people requires expertise that our operations team can better utilize elsewhere on more valuable tasks for the business." The upgrade project was initiated in a rush because the company did not have the appropriate tools to indicate that their current NGFWs were reaching capacity.
Which two actions by the Palo Alto Networks team offer a long-term solution for the customer? (Choose two.)
A. Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.
B. Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.
C. Inform the CIO that the new enhanced security features they will gain from the PAN-OS upgrades will fix any future problems with upgrading and capacity.
D. Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.
Answer: B,D (LEAVE A REPLY)
The customer's CIO highlights two key pain points: (1) the operations team lacks expertise to efficiently manage PAN-OS upgrades and support interactions, diverting focus from valuable tasks, and (2) the company lacked tools to monitor NGFW capacity, leading to a rushed upgrade. The goal is to recommend long-term solutions leveraging Palo Alto Networks' offerings for Strata Hardware Firewalls. Options B and D-training and AIOps Premium within Strata Cloud Manager (SCM)- address these issues by enhancing team capability and providing proactive management tools. Below is a detailed explanation, verified against official documentation.
Step 1: Analyzing the Customer's Challenges
* Expertise Gap: The CIO notes that identifying issues and engaging support requires expertise the operations team doesn't fully have or can't prioritize. Upgrading PAN-OS on Strata NGFWs involves tasks like version compatibility checks, pre-upgrade validation, and troubleshooting, which demand familiarity with PAN-OS tools and processes.

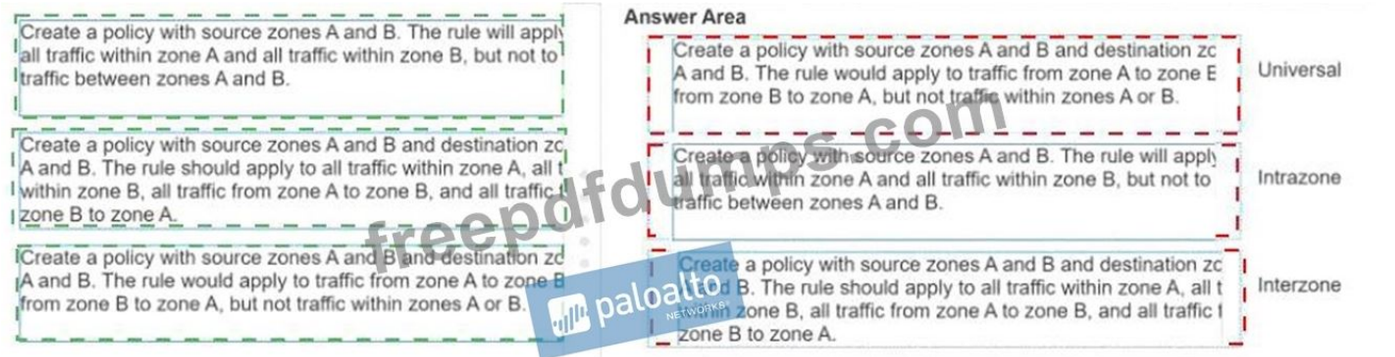
* Capacity Visibility: The rushed upgrade stemmed from not knowing the NGFWs were nearing capacity (e.g., CPU, memory, session limits), indicating a lack of monitoring or predictive analytics.
Long-term solutions must address both operational efficiency and proactive capacity management, aligning with Palo Alto Networks' ecosystem for Strata firewalls.
Reference: PAN-OS Administrator's Guide (11.1) - Upgrade Overview
"Successful upgrades require planning, validation, and monitoring to avoid disruptions and ensure capacity is sufficient." Step 2: Evaluating the Recommended Actions Option A: Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.
Analysis: AIOps for NGFW (free version) is a cloud-based tool that uses machine learning to monitor firewall health, detect anomalies, and provide upgrade recommendations. It offers basic telemetry (e.g., CPU usage, session counts) and alerts, which could have flagged capacity issues earlier. However, it lacks advanced features like automated remediation, detailed capacity planning, or integration with Strata Cloud Manager, limiting its long-term impact. Additionally, it doesn't address the expertise gap, as the team still needs knowledge to interpret and act on insights.
Conclusion: Helpful but not a comprehensive long-term solution.
Reference: AIOps for NGFW Documentation
"The free version provides basic health monitoring and ML-driven insights but lacks premium features for proactive management." Option B: Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.
Analysis: Palo Alto Networks offers training through the Palo Alto Networks Authorized Training Partners and Cybersecurity Academy, covering PAN-OS administration, upgrades, and troubleshooting. For Strata NGFWs, courses like "Firewall Essentials: Configuration and Management (EDU-210)" teach upgrade best practices, capacity monitoring (e.g., via Device > High Availability > Resources), and support engagement.
How It Solves the Issue:
Reduces reliance on external expertise by upskilling the team.
Enables efficient upgrade planning (e.g., using Best Practice Assessment (BPA) tool).
Frees the team for higher-value tasks by minimizing support escalations.
Long-Term Benefit: A trained team can proactively manage upgrades and capacity, addressing the CIO's concern about expertise allocation.
Conclusion: A strong long-term solution.
Reference: Palo Alto Networks Training Catalog
"Training empowers operations teams to confidently manage NGFWs, including upgrades and capacity planning." Option C: Inform the CIO that the new enhanced security features they will gain from the PAN-OS upgrades will fix any future problems with upgrading and capacity.
Analysis: New PAN-OS versions (e.g., 11.1) bring features like enhanced App-ID, decryption, or ML- based threat detection, improving security. However, these don't inherently solve upgrade complexity or capacity visibility. Capacity issues depend on hardware limits (e.g., PA-5200 Series

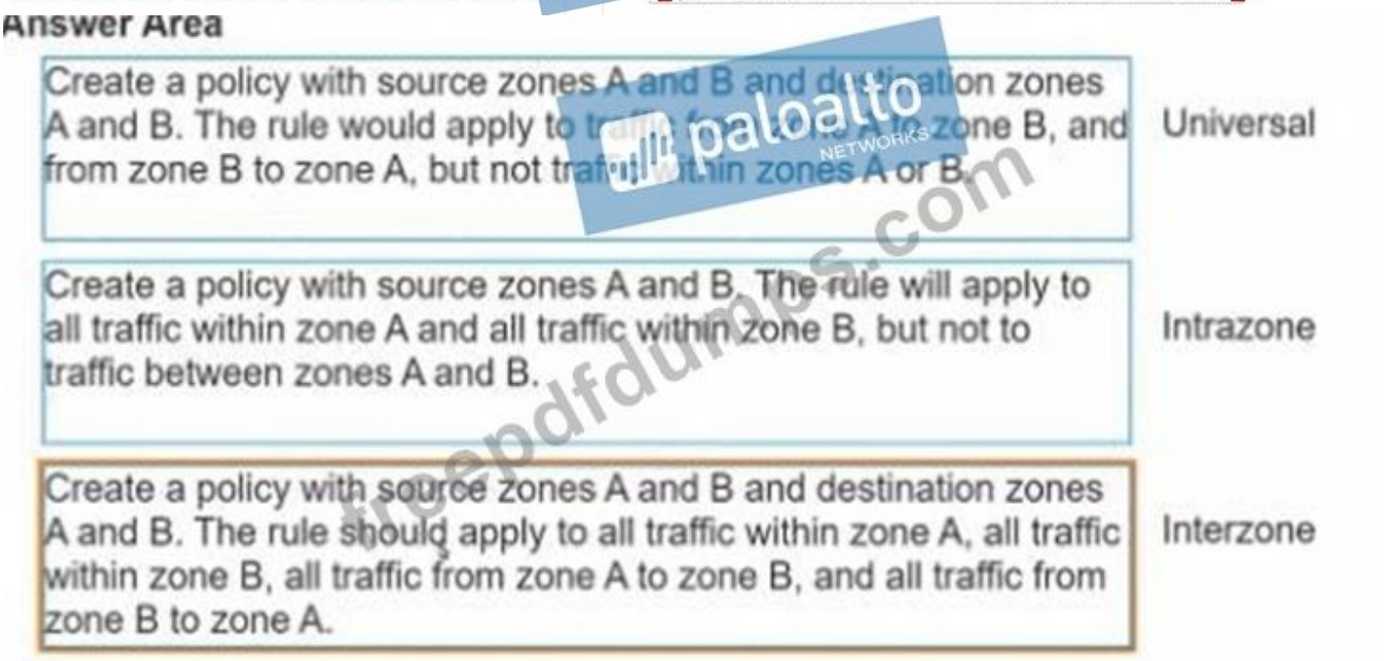
max sessions), not software features, and upgrades still require expertise. This response oversells benefits without addressing root causes.
Conclusion: Not a valid long-term solution.
Reference: PAN-OS 11.1 Release Notes
"New features enhance security but do not automate upgrade processes or capacity monitoring."
Option D: Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.
Analysis: AIOps Premium, integrated with Strata Cloud Manager (SCM), is a subscription-based service for managing Strata NGFWs. It provides:
Predictive Analytics: Forecasts capacity needs (e.g., CPU, memory, sessions) using ML.
Upgrade Planning: Recommends optimal upgrade paths and validates configurations.
Proactive Alerts: Identifies issues before they escalate, reducing support calls.
Centralized Management: Monitors all firewalls from SCM, integrating with existing PAN-OS deployments.
How It Solves the Issue:
Prevents rushed upgrades by predicting capacity limits (e.g., via Capacity Saturation Reports).
Simplifies upgrade preparation with automated insights, reducing expertise demands.
Aligns with existing Strata technology, enhancing ROI.
Long-Term Benefit: Offers a scalable, proactive toolset to manage NGFWs, addressing both capacity and operational efficiency.
Conclusion: A robust long-term solution.
Reference: Strata Cloud Manager AIOps Premium Documentation
"AIOps Premium provides advanced capacity planning and upgrade readiness, minimizing operational burden." Step 3: Why B and D Are the Best Choices B (Training): Directly tackles the expertise gap, empowering the team to handle upgrades and capacity monitoring independently. It's a foundational fix, ensuring long-term self-sufficiency.
D (AIOps Premium in SCM): Provides a technological solution to preempt capacity issues and streamline upgrades, reducing the need for deep expertise and support escalations. It complements training by automating complex tasks.
Synergy: Together, they address both human (expertise) and systemic (tools) challenges, aligning with the CIO's goals of operational efficiency and business value.
Step 4: How These Actions Integrate with Strata NGFWs
Training: Teaches use of PAN-OS tools like System Resources (CLI: show system resources) and Dynamic Updates for capacity and upgrade prep.
AIOps Premium: Enhances Strata NGFW management via SCM, pulling telemetry (e.g., from Device > Setup > Telemetry) to predict and resolve issues.
Reference: PAN-OS Administrator's Guide (11.1) - Monitoring
"Combine training and tools like AIOps to optimize NGFW performance and upgrades."

NEW QUESTION: 66
Match each rule type with its example



Answer:





NEW QUESTION: 67

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

A. Allow

B. Reset-server

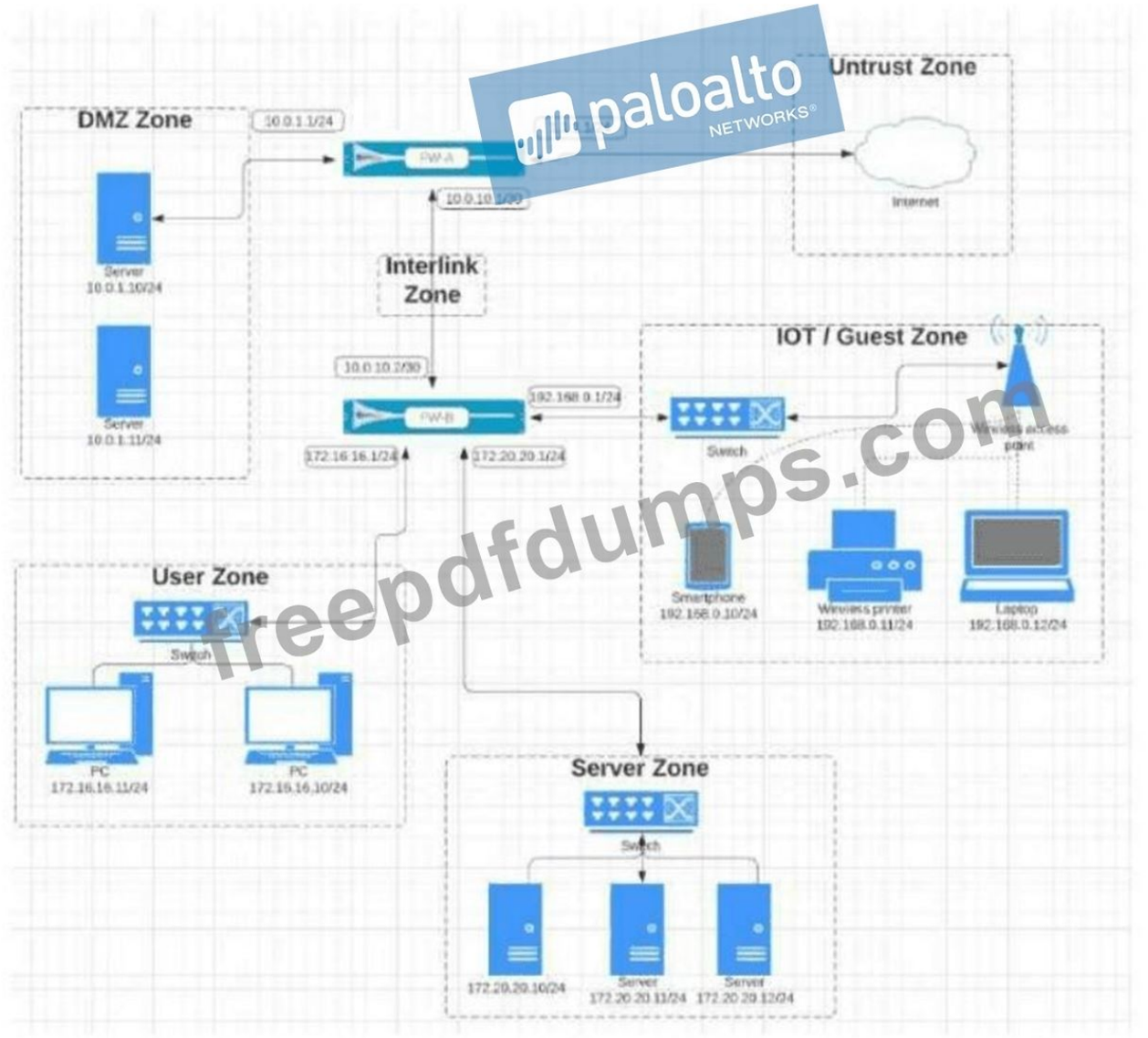
C. Reset-client

D. Deny

Answer: (SHOW ANSWER)

NEW QUESTION: 68

Review the Screenshot:



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

Which rule group enables the required traffic?

A.

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

B.

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

C.

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

D.

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
FW-A_RuleGroup-01-W	FW-A	universal	DMZ	10.0.1.0/24	any	InterLink	10.0.20.0/30	any	mysql ssh	application-default	any	Allow
FW-B_RuleGroup-01-X	FW-B	universal	InterLink	10.0.10.0/30	any	Server	172.20.20.0/24	any	mysql ssh	application-default	any	Allow
FW-A_RuleGroup-01-Y	FW-A	universal	InterLink	10.0.10.0/30	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow
FW-B_RuleGroup-01-Z	FW-B	universal	Server	172.20.20.0/24	any	InterLink	10.0.10.0/30	any	ssh	application-default	any	Allow

Answer: B (LEAVE A REPLY)

Option B enables the required traffic by allowing SSL and web-browsing from UNTRUST to DMZ, denying SSH from UNTRUST to DMZ, allowing MYSQL from DMZ to SERVER, and allowing SSH from SERVER to DMZ. Option A allows SSH from UNTRUST to DMZ, which is not required. Option C denies all the required traffic. Option D denies all traffic from UNTRUST to TRUST, which is irrelevant to the question

https://www.paloaltonetworks.com/services/education/palo-alto-networks-certified-network-security- administrator

NEW QUESTION: 69

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

A. Installation

B. Weaponization

C. Command and Control

D. Reconnaissance

E. Exploitation

Answer: B (LEAVE A REPLY)

NEW QUESTION: 70

Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping.

What is the quickest way to reset the hit counter to zero in all the security policy rules?

A. At the CLI enter the command reset rules and press Enter

B. Highlight a rule and use the Reset Rule Hit Counter > Selected Rules for each rule

C. Reboot the firewall

D. Use the Reset Rule Hit Counter > All Rules option

Answer: D (LEAVE A REPLY)

References:

NEW QUESTION: 71

For the firewall to use Active Directory to authenticate users, which Server Profile is required in the Authentication Profile?
A. TACACS+
B. RADIUS
C. LDAP
D. SAML
Answer: C (LEAVE A REPLY)
Explanation/Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/configure-an-authenticationprofile-and-sequence

NEW QUESTION: 72
Which two compliance frameworks are included with the Premium version of Strata Cloud Manager (SCM)? (Choose two)
A. Payment Card Industry (PCI)
B. National Institute of Standards and Technology (NIST)
C. Center for Internet Security (CIS)
D. Health Insurance Portability and Accountability Act (HIPAA)
Answer: A,B (LEAVE A REPLY)
Step 1: Understanding Strata Cloud Manager (SCM) Premium
Strata Cloud Manager is a unified management interface for Strata NGFWs, Prisma Access, and other Palo Alto Networks solutions. The Premium version (subscription-based) includes advanced features like:
* AIOps Premium: Predictive analytics, capacity planning, and compliance reporting.
* Compliance Posture Management: Pre-built dashboards and reports for specific regulatory frameworks.
Compliance frameworks in SCM Premium provide visibility into adherence to standards like PCI DSS and NIST, generating actionable insights and audit-ready reports based on firewall configurations, logs, and traffic data.
Reference: Strata Cloud Manager Documentation
"SCM Premium delivers compliance reporting for industry standards, integrating with NGFW telemetry to ensure regulatory alignment." Step 2: Evaluating the Compliance Frameworks Option A: Payment Card Industry (PCI) Analysis: The Payment Card Industry Data Security Standard (PCI DSS) is a mandatory framework for organizations handling cardholder data. SCM Premium includes a PCI DSS Compliance Dashboard that maps NGFW configurations (e.g., security policies, decryption, Threat Prevention) to PCI DSS requirements (e.g., Requirement 1: Firewall protection, Requirement 6: Vulnerability protection). It tracks compliance with controls like network segmentation, encryption, and monitoring, critical for Strata NGFW deployments in payment environments.
Evidence: Palo Alto Networks emphasizes PCI DSS support in SCM Premium for retail, financial, and e- commerce customers, providing pre-configured reports for audits.

Conclusion: Included in SCM Premium.
Reference: Strata Cloud Manager Premium Features Overview
"PCI DSS compliance reporting ensures cardholder data protection with automated insights."
Option B: National Institute of Standards and Technology (NIST) Analysis: NIST frameworks, notably the NIST Cybersecurity Framework (CSF) and NIST SP 800-53, are widely adopted for cybersecurity risk management, especially in government and critical infrastructure sectors. SCM Premium offers a NIST Compliance Dashboard, aligning NGFW settings (e.g., App-ID, User- ID, logging) with NIST controls (e.g., Identify, Protect, Detect, Respond, Recover). This is key for Strata customers needing federal compliance or a risk-based approach.
Evidence: Palo Alto Networks documentation highlights NIST CSF and 800-53 mapping in SCM Premium, reflecting its broad applicability.
Conclusion: Included in SCM Premium.
Reference: Strata Cloud Manager AIOps Premium Datasheet
"NIST compliance reporting supports risk management and regulatory adherence." Option C: Center for Internet Security (CIS) Analysis: The CIS Controls and Benchmarks provide practical cybersecurity guidelines (e.g., CIS Controls v8, CIS Benchmarks for OS hardening). While Palo Alto Networks supports CIS principles (e.g., via Best Practice Assessments), SCM Premium documentation does not explicitly list a dedicated CIS Compliance Dashboard. CIS alignment is often manual or supplementary, not a pre-built feature like PCI or NIST.
Evidence: No direct evidence in SCM Premium feature sets confirms CIS as a standard inclusion; it's more commonly referenced in standalone tools like CIS-CAT or Expedition.
Conclusion: Not included in SCM Premium.
Reference: PAN-OS Administrator's Guide (11.1) - Best Practices
"CIS alignment is supported but not a native SCM Premium framework."
Option D: Health Insurance Portability and Accountability Act (HIPAA)
Analysis: HIPAA governs protected health information (PHI) security in healthcare. While Strata NGFWs can enforce HIPAA-compliant policies (e.g., encryption, access control), SCM Premium does not feature a dedicated HIPAA Compliance Dashboard. HIPAA compliance is typically achieved through custom configurations and external audits, not a pre-configured SCM framework.
Evidence: Palo Alto Networks documentation lacks mention of HIPAA as a standard SCM Premium offering, unlike PCI and NIST.
Conclusion: Not included in SCM Premium.
Reference: Strata Cloud Manager Documentation
"HIPAA compliance is supported via NGFW capabilities, not SCM Premium dashboards." Step 3: Why A and B Are Correct A (PCI): Directly addresses a common Strata NGFW use case (payment security) with a tailored dashboard, reflecting SCM Premium's focus on industry-specific compliance.
B (NIST): Provides a flexible, widely adopted framework for cybersecurity, integrated into SCM Premium for broad applicability across sectors.

Exclusion of C and D: CIS and HIPAA, while relevant to NGFW deployments, lack dedicated, pre-built compliance reporting in SCM Premium, making them supplementary rather than core inclusions.
Step 4: Verification Against SCM Premium Features
SCM Premium's compliance posture management explicitly lists PCI DSS and NIST (e.g., CSF, 800-53) as supported frameworks, leveraging NGFW telemetry (e.g., Monitor > Logs > Traffic) and AIOps analytics.
This aligns with Palo Alto Networks' focus on high-demand regulations as of PAN-OS 11.1 and SCM updates through March 08, 2025.
Reference: Strata Cloud Manager Release Notes (March 2025)
"Premium version includes PCI DSS and NIST compliance dashboards for automated reporting."
Conclusion The two compliance frameworks included with the Premium version of Strata Cloud Manager are A.
Payment Card Industry (PCI) and B. National Institute of Standards and Technology (NIST).
These are verified by SCM Premium's documented capabilities, ensuring Strata NGFW customers can meet regulatory requirements efficiently.

NEW QUESTION: 73
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: 74
You receive notification about new malware that is being used to attack hosts The malware exploits a software bug in a common application Which Security Profile detects and blocks access to this threat after you update the firewall's threat signature database?
A. Vulnerability Profile applied to inbound Security policy rules
B. Antivirus Profile applied to outbound Security policy rules
C. Data Filtering Profile applied to inbound Security policy rules
D. Data Filtering Profile applied to outbound Security policy rules
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which five Zero Trust concepts does a Palo Alto Networks firewall apply to achieve an integrated approach to prevent threats? (Choose five.)
A. Application identification
B. Filtration protection
C. Antivirus
D. User identification
E. Vulnerability protection
F. Anti-spyware
Answer: A,C,D,E,F (LEAVE A REPLY)

NEW QUESTION: 76
An address object of type IP Wildcard Mask can be referenced in which part of the configuration?
A. Security policy rule
B. ACC global filter
C. external dynamic list
D. NAT address pool
Answer: (SHOW ANSWER)
You can use an address object of type IP Wildcard Mask only in a Security policy rule.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-addresses IP Wildcard Mask
-Enter an IP wildcard address in the format of an IPv4 address followed by a slash and a mask (which must begin with a zero); for example, 10.182.1.1/0.127.248.0. In the wildcard mask, a zero (0) bit indicates that the bit being compared must match the bit in the IP address that is covered by the 0. A one (1) bit in the mask is a wildcard bit, meaning the bit being compared need not match the bit in the IP address that is covered by the 1.
Convert the IP address and the wildcard mask to binary. To illustrate the matching: on binary snippet 0011, a wildcard mask of 1010 results in four matches (0001, 0011, 1001, and 1011).

NEW QUESTION: 77
What is the best-practice approach to logging traffic that traverses the firewall?
A. Enable both log at session start and log at session end.

B. Enable log at session start only.
C. Enable log at session end only.
D. Disable all logging options.
Answer: C (LEAVE A REPLY)
The best-practice approach to logging traffic that traverses the firewall is to enable log at session end only.
This option allows the firewall to generate a log entry only when a session ends, which reduces the load on the firewall and the log storage. The log entry contains information such as the source and destination IP addresses, ports, zones, application, user, bytes, packets, and duration of the session. The log at session end option also provides more accurate information about the session, such as the final application and user, the total bytes and packets, and the session end reason1. To enable log at session end only, you need to:
* Create or modify a Security policy rule that matches the traffic that you want to log.
* Select the Actions tab in the policy rule and check the Log at Session End option.
* Commit the changes to the firewall or Panorama and the managed firewalls.
References: View and Manage Logs, Log at Session End, Certifications - Palo Alto Networks, [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

NEW QUESTION: 78
An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact a command-and-control (C2) server. Which two security profile components will detect and prevent this threat after the firewall's signature database has been updated?
(Choose two.)
A. vulnerability protection profile applied to outbound security policies
B. anti-spyware profile applied to outbound security policies
C. antivirus profile applied to outbound security policies
D. URL filtering profile applied to outbound security policies
Answer: B,D (LEAVE A REPLY)
References:

NEW QUESTION: 79
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:
https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

NEW QUESTION: 80
Which two App-ID applications will need to be allowed to use Facebook-chat? (Choose two.)
A. facebook-base
B. facebook-email
C. facebook
D. facebook-chat
Answer: (SHOW ANSWER)

NEW QUESTION: 81
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 traffic was denied by security profile.
B. The traffic was denied by URL filtering.
C. The web session was unsuccessfully decrypted.
D. The web session was decrypted.
Answer: D (LEAVE A REPLY)

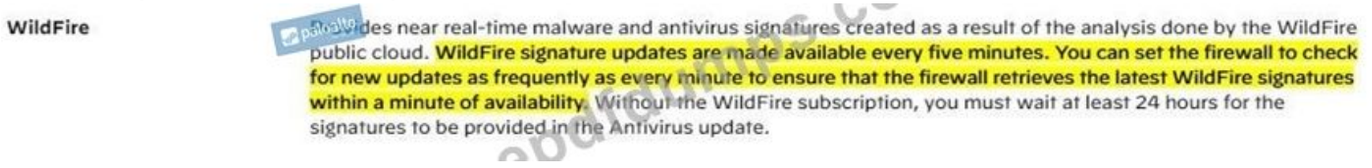
NEW QUESTION: 82
After making multiple changes to the candidate configuration of a firewall, the administrator would like to start over with a candidate configuration that matches the running configuration.
Which command in Device > Setup > Operations would provide the most operationally efficient way to accomplish this?
A. Revert to running configuration
B. Import named config snapshot
C. Revert to last saved configuration
D. Load named configuration snapshot
Answer: A (LEAVE A REPLY)

NEW QUESTION: 83
When is the content inspection performed in the packet flow process?
A. after the application has been identified
B. after the SSL Proxy re-encrypts the packet
C. before the packet forwarding process
D. before session lookup
Answer: A (LEAVE A REPLY)
Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0

NEW QUESTION: 84
Which two firewall components enable you to configure SYN flood protection thresholds? (Choose two.)
A. QoS profile
B. DoS Protection profile
C. Zone Protection profile
D. DoS Protection policy
Answer: B,C (LEAVE A REPLY)
Explanation/Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

NEW QUESTION: 85
To what must an interface be assigned before it can process traffic?
A. Security profile
B. Security Zone
C. Security Protection
D. Security policy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 86
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: (SHOW ANSWER)



NEW QUESTION: 87
Which two features can be used to tag a user name so that it is included in a dynamic user group? (Choose two)
A. XML API
B. log forwarding auto-tagging
C. GlobalProtect agent
D. User-ID Windows-based agent
Answer: A,D (LEAVE A REPLY)

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions

NEW QUESTION: 88
Which three types of Source NAT are available to users inside a NGFW? (Choose three.)
A. Static IP
B. Static IP and Port (SIPP)
C. Static Port
D. Dynamic IP and Port (DIPP)
E. Dynamic IP
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 89
Which action results in the firewall blocking network traffic without notifying the sender?
A. Deny
B. Drop
C. No notification
D. Reset Client
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90
Which administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server.
Which security profile components will detect and prevent this threat after the firewall`s signature database has been updated?
A. data filtering profile applied to outbound security policies
B. vulnerability profile applied to inbound security policies
C. data filtering profile applied to inbound security policies
D. antivirus profile applied to outbound security policies
Answer: (SHOW ANSWER)

NEW QUESTION: 91
In which three places on the PAN-OS interface can the application characteristics be found? (Choose three.)
A. Objects tab > Application Filters
B. Policies tab > Security
C. ACC tab > Global Filters
D. Objects tab > Application Groups
E. Objects tab > Applications
Answer: A,D,E (LEAVE A REPLY)

The application characteristics can be found in three places on the PAN-OS interface: Objects tab > Application Filters, Objects tab > Application Groups, and Objects tab > Applications. These places allow you to view and manage the applications and application groups that are used in your Security policy rules. You can also create custom applications and application filters based on various attributes, such as category, subcategory, technology, risk, and behavior1. Some of the characteristics of these places are:
Objects tab > Application Filters: An application filter is a dynamic object that groups applications based on specific criteria. You can use an application filter to match multiple applications in a Security policy rule without having to list them individually. For example, you can create an application filter that includes all applications that have a high risk level or use peer-to-peer technology.
Objects tab > Application Groups: An application group is a static object that groups applications based on your custom requirements. You can use an application group to match multiple applications in a Security policy rule without having to list them individually. For example, you can create an application group that includes all applications that are related to a specific business function or project.
Objects tab > Applications: An application is an object that identifies and classifies network traffic based on App-ID, which is a technology that uses multiple attributes to identify applications. You can use an application to match a specific application in a Security policy rule and control its access and behavior. For example, you can use an application to allow web browsing but block file sharing or social networking.
References: Objects, [Application Filters], [Application Groups], [Applications], Updated Certifications for PAN-OS 10.1, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

NEW QUESTION: 92
Which Security policy action will message a user's browser thai their web session has been terminated?
A. Drop
B. Reset server
C. Reset client
D. Deny

Answer: D (LEAVE A REPLY)

NEW QUESTION: 93
Which stage of the cyber-attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?
A. reconnaissance
B. delivery
C. exploitation
D. installation
Answer: (SHOW ANSWER)
Weaponization and Delivery: Attackers will then determine which methods to use in order to deliver malicious payloads. Some of the methods they might utilize are automated tools, such as exploit kits, spear phishing attacks with malicious links, or attachments and malvertizing.
Gain full visibility into all traffic, including SSL, and block high-risk applications. Extend those protections to remote and mobile devices.
Protect against perimeter breaches by blocking malicious or risky websites through URL filtering.
Block known exploits, malware and inbound command-and-control communications using multiple threat prevention disciplines, including IPS, anti-malware, anti-CnC, DNS monitoring and sinkholing, and file and content blocking.
Detect unknown malware and automatically deliver protections globally to thwart new attacks.
Provide ongoing education to users on spear phishing links, unknown emails, risky websites, etc.
https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

NEW QUESTION: 94
Which rule type is appropriate for matching traffic both within and between the source and destination zones?
A. universal
B. intrazone
C. shadowed
D. interzone
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95
Which rule type is appropriate for matching traffic occurring within a specified zone?
A. Interzone
B. Intrazone
C. Universal
D. Shadowed
Answer: B (LEAVE A REPLY)

NEW QUESTION: 96

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

A. The entry matches a list entry.

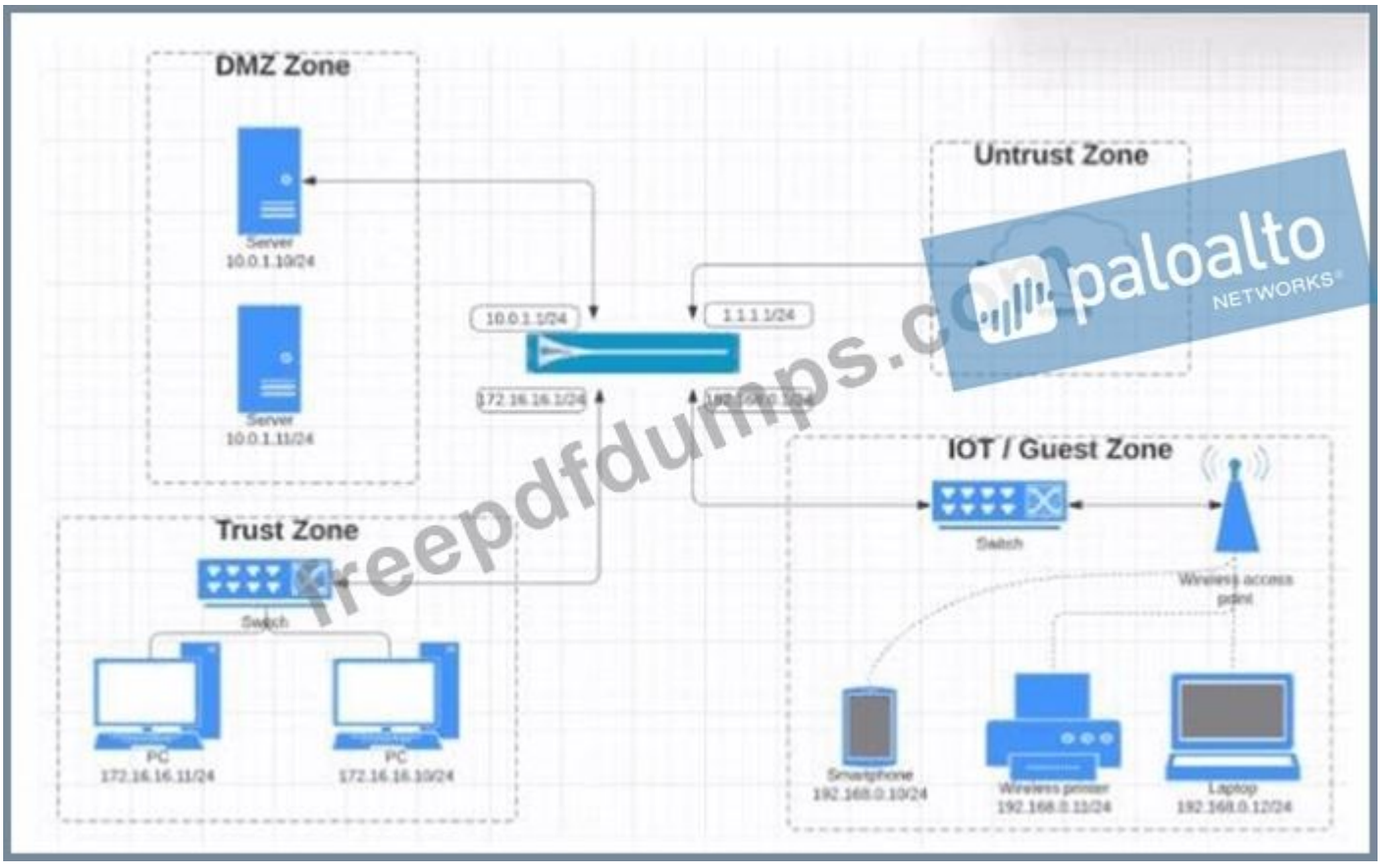
B. The entry doesn't match a list entry.

C. The entry is duplicated.

D. The entry contains wildcards.

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 97



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.

B.

C.

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

D.

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
Where in Panorama Would Zone Protection profiles be configured?
A. Shared
B. Templates
C. Device Groups
D. Panorama tab
Answer: B (LEAVE A REPLY)
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewalls-using-panorama/set-up-your-centralized-configuration-and-policies/use-templates-to-administer-a-base-configuration

NEW QUESTION: 99
URL categories can be used as match criteria on which two policy types? (Choose two.)
A. authentication
B. decryption
C application override
C. NAT
Answer: (SHOW ANSWER)
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url- category-as-policy-match-criteria.html

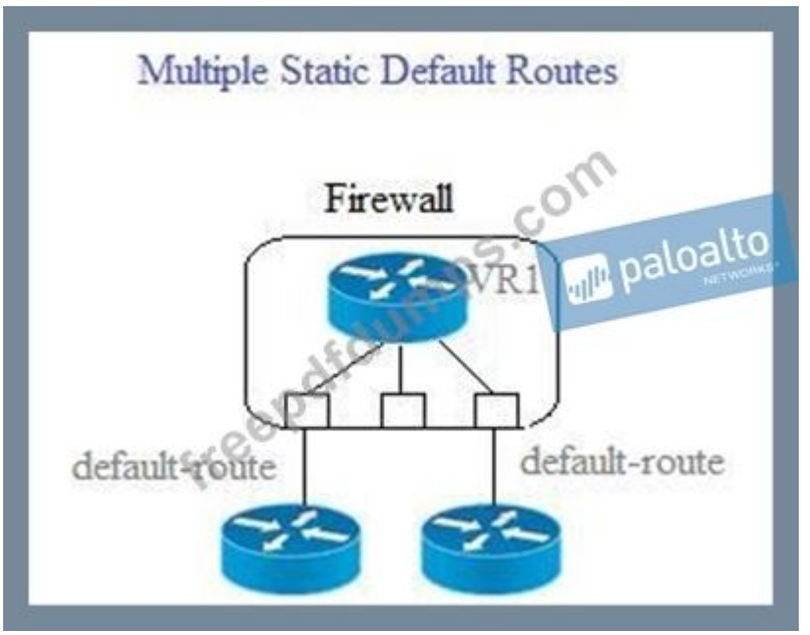
NEW QUESTION: 100
Which security profile should be used to classify malicious web content?
A. URL Filtering
B. Antivirus
C. Web Content
D. Vulnerability Protection
Answer: A (LEAVE A REPLY)
URL Filtering is a security profile that allows you to classify web content based on the URL category and reputation of the website. URL Filtering can help you block access to malicious web content, such as phishing, malware, or command and control sites, as well as enforce acceptable

use policies for web browsing. URL Filtering uses the PAN-DB cloud service to provide up-to-date information on the URL categories and reputations of millions of websites. You can configure URL Filtering policies to allow, block, alert, continue, or override web requests based on the URL category and reputation, as well as customize the response pages and exceptions for different user groups. References: URL Filtering, Set Up a Basic Security Policy, Updated Certifications for PAN-OS 10.1

NEW QUESTION: 101
What Policy Optimizer policy view differ from the Security policy do?
A. It shows rules that are missing Security profile configurations.
B. It indicates rules with App-ID that are not configured as port-based.
C. It shows rules with the same Source Zones and Destination Zones.
D. It indicates that a broader rule matching the criteria is configured above a more specific rule.
Answer: (SHOW ANSWER)
Policy Optimizer policy view differs from the Security policy view in several ways. One of them is that it indicates rules with App-ID that are not configured as port-based. These are rules that have the application set to "any" instead of a specific application or group of applications. These rules are overly permissive and can introduce security gaps, as they allow any application traffic on the specified ports. Policy Optimizer helps you convert these rules to application-based rules that follow the principle of least privilege access12. You can use Policy Optimizer to discover and convert port-based rules to application-based rules, and also to remove unused applications, eliminate unused rules, and discover new applications that match your policy criteria3.
References:
* Policy Optimizer Best Practices - Palo Alto Networks
* Manage: Policy Optimizer - Palo Alto Networks | TechDocs
* Why use Security Policy Optimizer and what are the benefits?

NEW QUESTION: 102
What can be achieved by selecting a policy target prior to pushing policy rules from Panorama?
A. Doing so provides audit information prior to making changes for selected policy rules
B. You specify the location as pre can - or post-rules to push policy rules
C. You can specify the firewalls m a device group to which to push policy rules
D. Doing so limits the templates that receive the policy rules
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
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 lowest metric is actively used
C. Path monitoring does not determine if route is useable
D. Route with highest metric is actively used
Answer: (SHOW ANSWER)

NEW QUESTION: 104
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)
Explanation/Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html After a packet has been allowed by the Security policy, Security Profiles are used to scan packets for threats, vulnerabilities, viruses, spyware, malicious URLs, data exfiltration, and exploitation software.

NEW QUESTION: 105
Which interface does not require a MAC or IP address?
A. Virtual Wire
B. Loopback
C. Layer2
D. Layer3

Answer: A (LEAVE A REPLY)

NEW QUESTION: 106
Which order of steps is the correct way to create a static route?
A. 1) Enter the route and netmask
2) Enter the IP address for the specific next hop
3) Specify the outgoing interface for packets to use to go to the next hop
4) Add an IPv4 or IPv6 route by name
B. 1) Enter the route and netmask
2) Specify the outgoing interface for packets to use to go to the next hop
3) Enter the IP address for the specific next hop
4) Add an IPv4 or IPv6 route by name
C. 1) Enter the IP address for the specific next hop
2) Enter the route and netmask
3) Add an IPv4 or IPv6 route by name
4) Specify the outgoing interface for packets to use to go to the next hop
D. 1) Enter the IP address for the specific next hop
2) Add an IPv4 or IPv6 route by name
3) Enter the route and netmask
4) Specify the outgoing interface for packets to use to go to the next hop
Answer: A (LEAVE A REPLY)
* Enter the route and netmask
* Enter the IP address for the specific next hop
* Specify the outgoing interface for packets to use to go to the next hop
* Add an IPv4 or IPv6 route by name Comprehensive Explanation: This is the correct order of steps to create a static route in a virtual router on the firewall. The first step is to enter the route and netmask for the destination network, such as 192.168.2.2/24 for an IPv4 address or 2001:db8:123:1::1/64 for an IPv6 address. The second step is to enter the IP address for the specific next hop, such as 192.168.56.1 or 2001:db8:49e:1::1. The third step is to specify the outgoing interface for packets to use to go to the next hop, such as ethernet1/1. The fourth step is to add an IPv4 or IPv6 route by name, such as route11. References:
* Configure a Static Route - Palo Alto Networks

NEW QUESTION: 107
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)
Explanation/Reference:https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy- optimizer.html

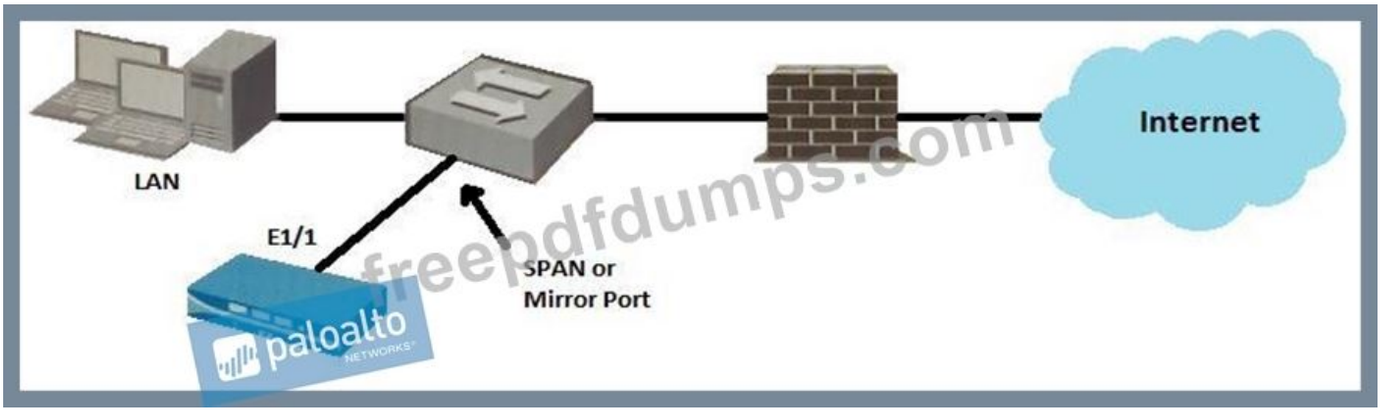
NEW QUESTION: 108
An internal host wants to connect to servers of the internet through using source NAT.
Which policy is required to enable source NAT on the firewall?
A. NAT policy with no source of destination zone selected
B. NAT policy with source zone and destination zone specified
C. post-NAT policy with external source and any destination address
D. pre-NAT policy with external source and any destination address
Answer: B (LEAVE A REPLY)

NEW QUESTION: 109
Selecting the option to revert firewall changes will replace what settings?
A. dynamic update scheduler settings
B. the device state with settings from another configuration
C. the running configuration with settings from the candidate configuration
D. the candidate configuration with settings from the running configuration
Answer: D (LEAVE A REPLY)

NEW QUESTION: 110
Which two actions in the IKE Gateways will allow implementation of post-quantum cryptography when building VPNs between multiple Palo Alto Networks NGFWs? (Choose two.)
A. Select IKE v2, enable the Advanced Options * PQ PPK, then set a 64+ character string for the post- quantum pre shared key.
B. Ensure Authentication is set to "certificate," then import a post-quantum derived certificate.
C. Select IKE v2 Preferred, enable the Advanced Options * PQ KEM, then add one or more "Rounds."
D. Select IKE v2, enable the Advanced Options * PQ KEM, then create an IKE Crypto Profile with Advanced Options adding one or more "Rounds."
Answer: C,D (LEAVE A REPLY)

To implement post-quantum cryptography (PQC) in VPNs between Palo Alto Networks NGFWs, you would enable the PQ KEM (Post-Quantum Key Encapsulation Mechanism) in the IKE gateway configuration. This enables the firewall to use quantum-resistant encryption for key exchange, which is an essential part of securing communications against the potential future threats posed by quantum computing.
By selecting IKE v2 Preferred and enabling the PQ KEM option under Advanced Options, you can add specific Rounds for the post-quantum cryptography process, which will help in implementing quantum- resistant key exchange methods.
This option similarly selects IKE v2 and enables PQ KEM while also creating a dedicated IKE Crypto Profile with the necessary Rounds configured for post-quantum cryptography.

NEW QUESTION: 111
How does the Policy Optimizer policy view differ from the Security policy view?
A. It provides sorting options that do not affect rule order.
B. It displays rule utilization.
C. It details associated zones.
D. It specifies applications seen by rules.
Answer: (SHOW ANSWER)
You can't filter or sort rules in PoliciesSecurity because that would change the order of the policy rules in the rulebase. Filtering and sorting PoliciesSecurityPolicy OptimizerNo App Specified, PoliciesSecurityPolicy OptimizerUnused Apps, and PoliciesSecurityPolicy OptimizerNew App Viewer (if you have a SaaS Inline Security subscription) does not change the order of the rules in the rulebase. https://docs.paloaltonetworks.com
/pan-os/11-0/pan-os-admin/app-id/security-policy-rule-optimization/policy-optimizer-concepts/sorting-and- filtering-security-policy-rules

NEW QUESTION: 112


Given the topology, which zone type should interface E1/1 be configured with?
A. Layer3
B. Tap
C. Virtual Wire
D. Tunnel

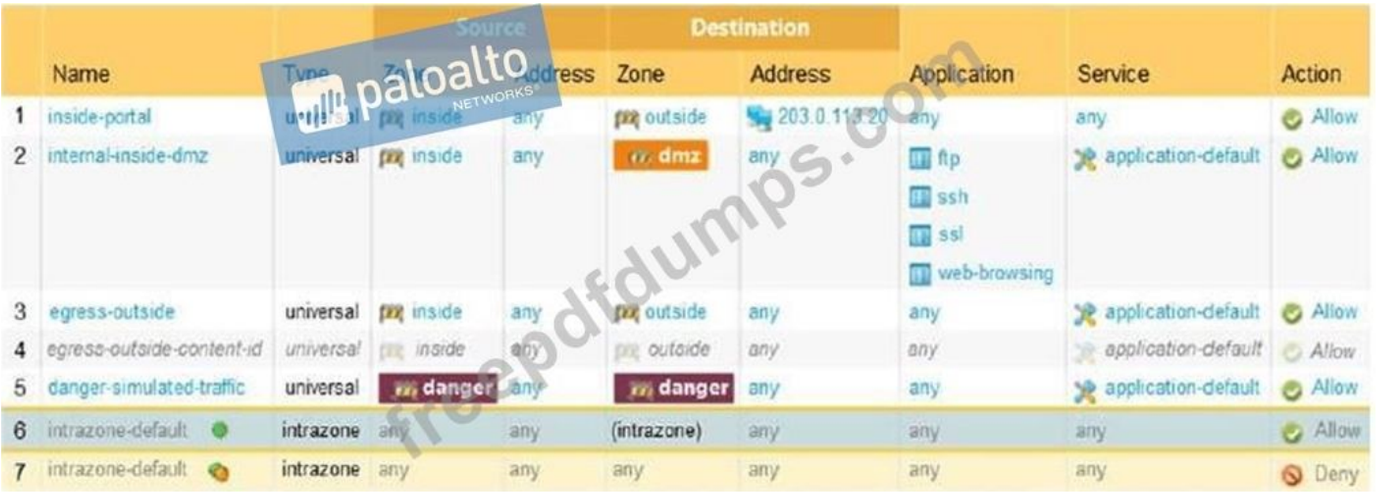
Answer: B (LEAVE A REPLY)

NEW QUESTION: 113
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 the Security policy rule 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 Security Profile action is applied last
D. If it is an allowed rule, then the Security Profile action is applied last
Answer: D (LEAVE A REPLY)

NEW QUESTION: 114
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)
References: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

NEW QUESTION: 115
Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?
A. GlobalProtect
B. Parisma SaaS
C. AutoFocus
D. Aperture
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?



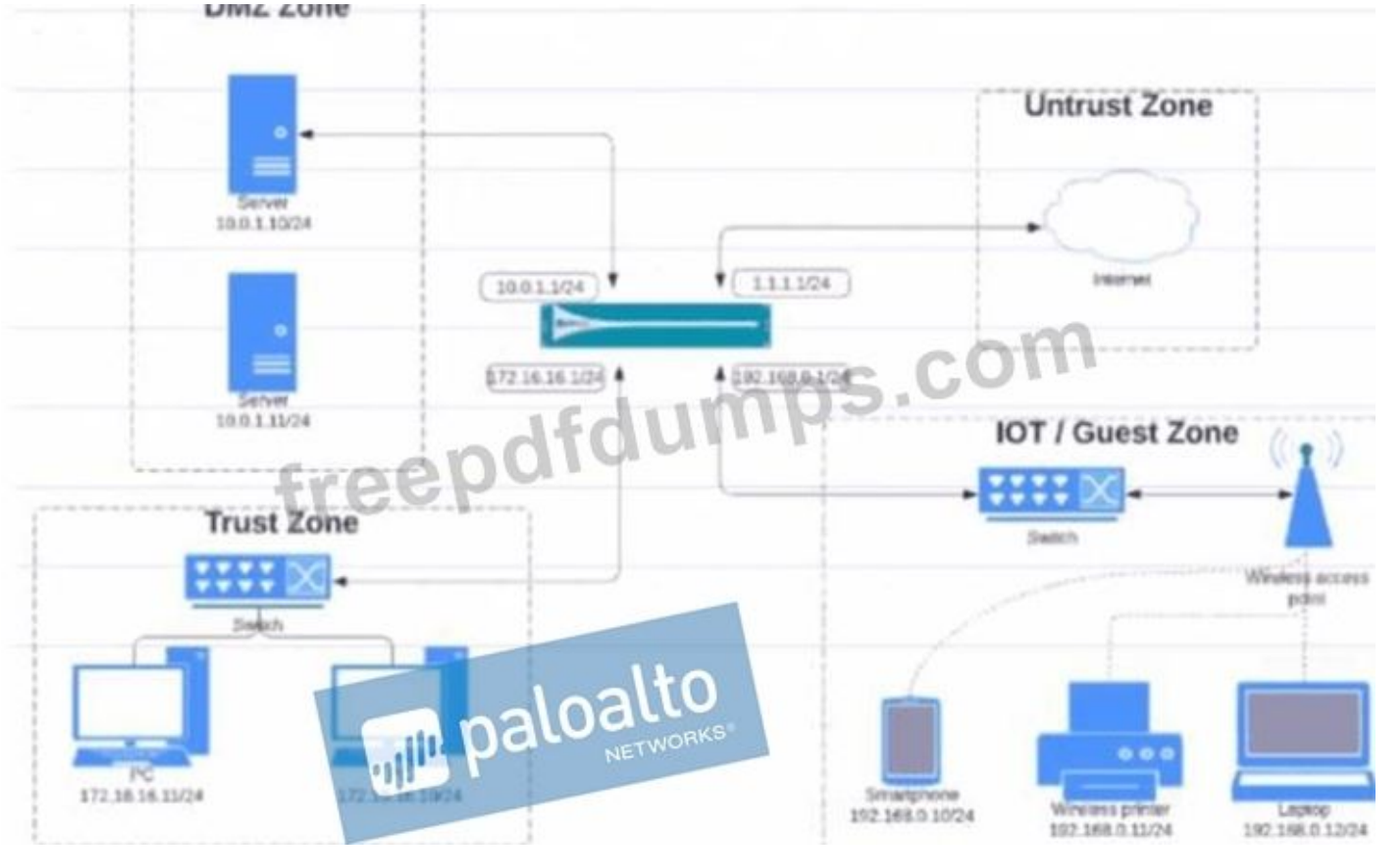
	Name	Type	Source Zone	Source Address	Destination Zone	Destination Address	Application	Service	Action
1	inside-portal		inside	any	outside	203.0.113.20	any	any	Allow
2	internal-inside-dmz	universal	inside	any	dmz	any	ftp ssh ssl web-browsing	application-default	Allow
3	egress-outside	universal	inside	any	outside	any	any	application-default	Allow
4	egress-outside-content-id	universal	inside	any	outside	any	any	application-default	Allow
5	danger-simulated-traffic	universal	danger	any	danger	any	any	application-default	Allow
6	intrazone-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. engress outside
D. intercone-default
Answer: (SHOW ANSWER)

NEW QUESTION: 117
When creating a Source NAT policy, which entry in the Translated Packet tab will display the options Dynamic IP and Port, Dynamic, Static IP, and None?

A. IP Address
B. Address Type
C. Translation Type
D. Interface
Answer: C (LEAVE A REPLY)

NEW QUESTION: 118



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.

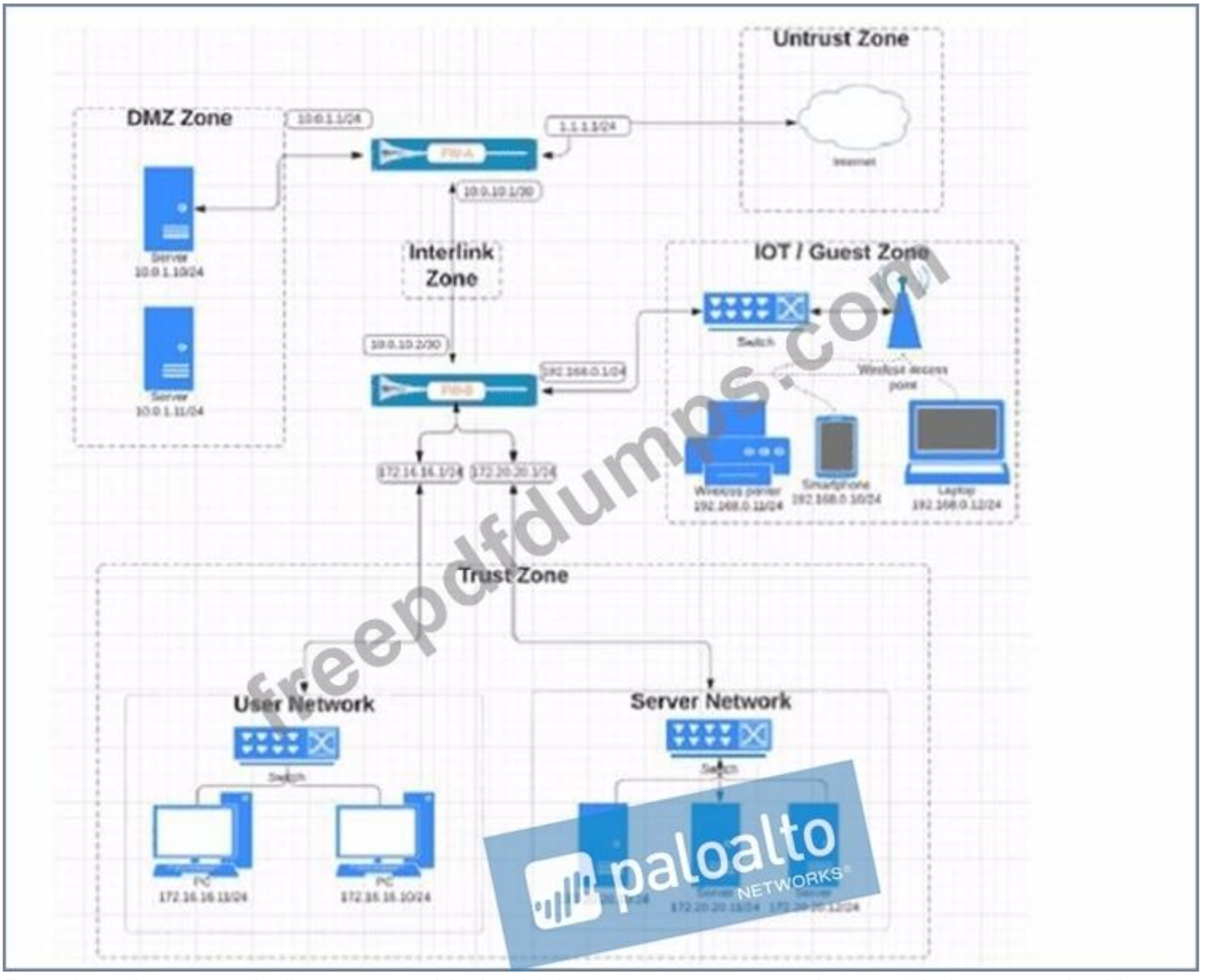
B.

C.

D.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 119



Based on the network diagram provided, which two statements apply to traffic between the User and Server networks? (Choose two.)

A. Traffic is permitted through the default intrazone "allow" rule.

B. Traffic restrictions are possible by modifying intrazone rules.

C. Traffic restrictions are not possible, because the networks are in the same zone.

D. Traffic is permitted through the default interzone "allow" rule.

Answer: A,B (LEAVE A REPLY)

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTHCA0&lang=es

NEW QUESTION: 120

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-Spyware Profile action.

C. It was blocked by the Anti-Virus Security profile action.

D. It was blocked by the Vulnerability Protection profile action.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 121

In which two Security Profiles can an action equal to the block IP feature be configured? (Choose two.)

A. URL Filtering

B. Vulnerability Protection

C. Antivirus b

D. Anti-spyware

Answer: B,D (LEAVE A REPLY)

The block IP feature can be configured in two Security Profiles: Vulnerability Protection and Anti-spyware.

The block IP feature allows the firewall to block traffic from a source IP address for a specified period of time after detecting a threat. This feature can help prevent further attacks from the same source and reduce the load on the firewall1. The block IP feature can be enabled in the following Security Profiles:

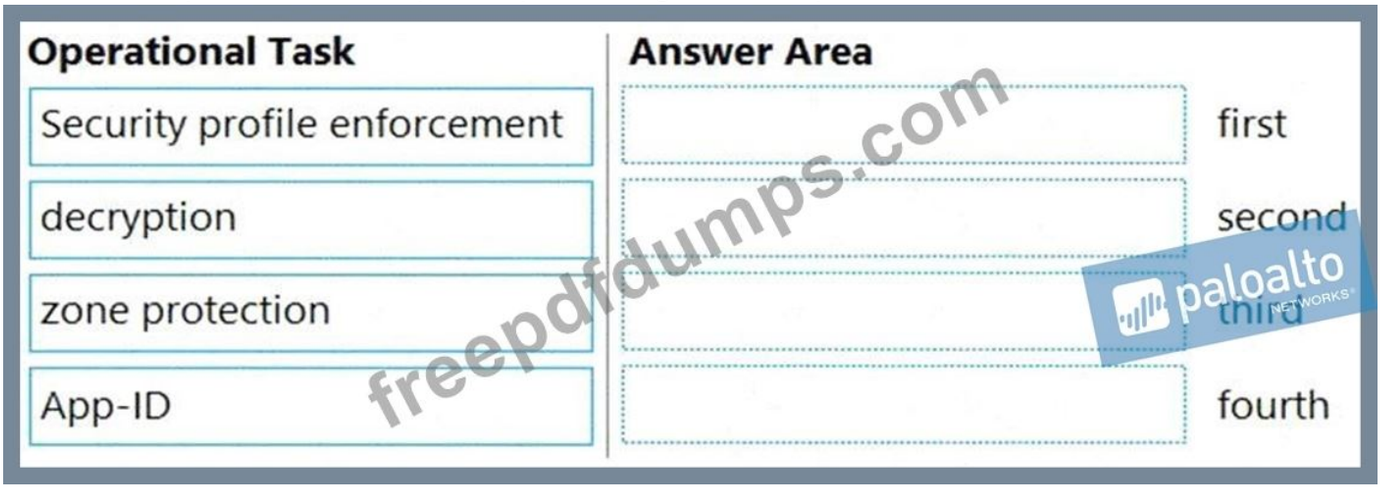
Vulnerability Protection: A Vulnerability Protection profile defines the actions that the firewall takes to protect against exploits and vulnerabilities in applications and protocols. You can configure a rule in the Vulnerability Protection profile to block IP connections for a specific threat or a group of threats2.

Anti-spyware: An Anti-spyware profile defines the actions that the firewall takes to protect against spyware and command-and-control (C2) traffic. You can configure a rule in the Anti-spyware profile to block IP addresses for a specific spyware or C2 signature.

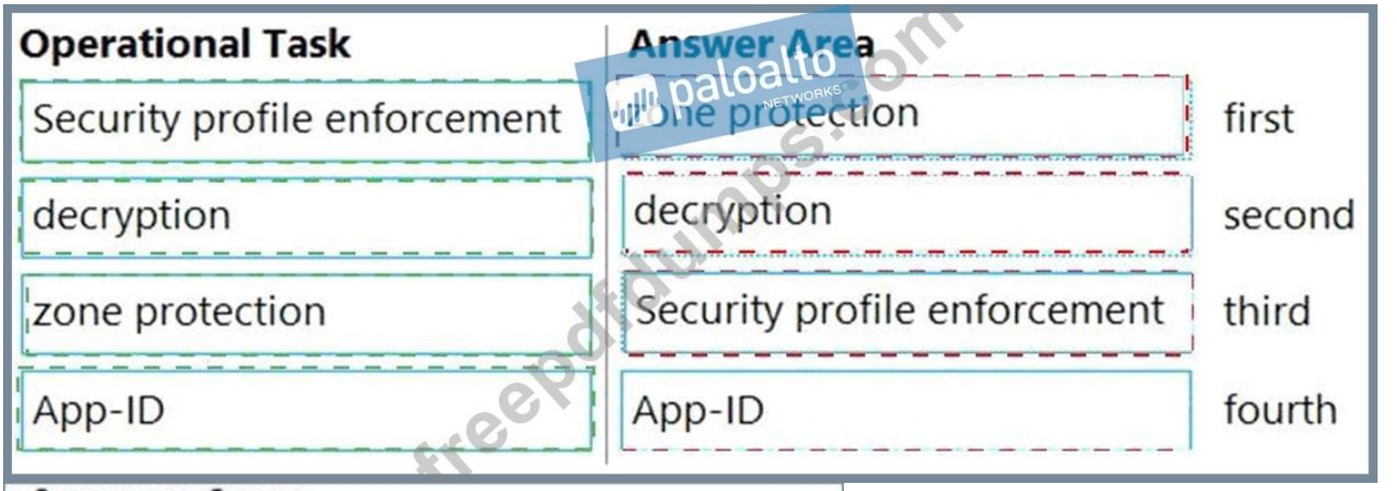
References: Monitor Blocked IP Addresses, Block IP Addresses, Vulnerability Protection Profile, [Anti- Spyware Profile], Certifications - Palo Alto Networks, [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PAN-OS
10.0)].

NEW QUESTION: 122

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



Answer:



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

NEW QUESTION: 123

In which two Security Profiles can an action equal to the block IP feature be configured? (Choose two.)

A. Antivirus

B. URL Filtering

C. Vulnerability Protection

D. Anti-spyware

Answer: C,D (LEAVE A REPLY)

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

/actions-in-security-profiles

NEW QUESTION: 124

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

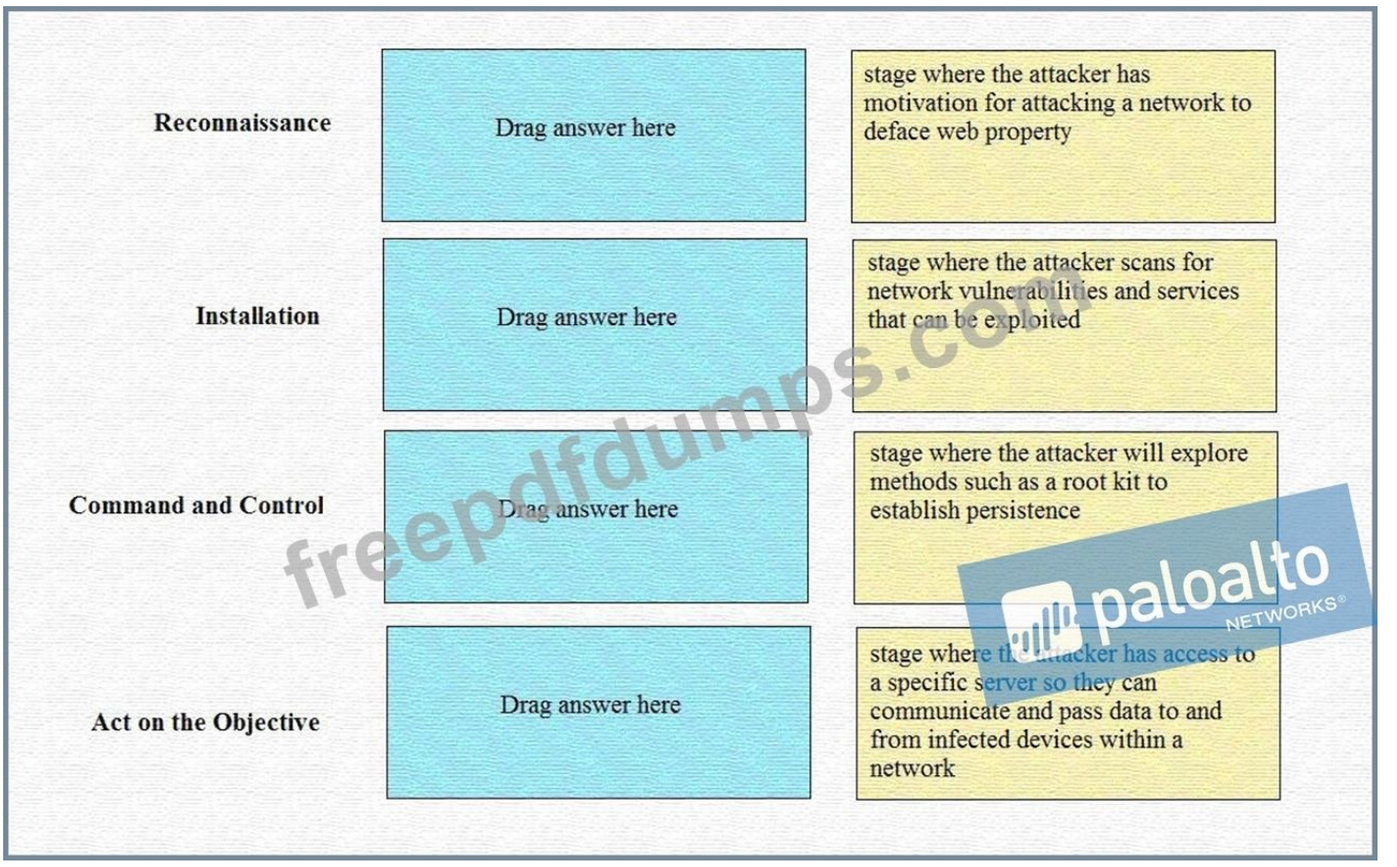
B. PAN-OS integrated agent deployed on the internal network
C. Citrix terminal server deployed on the internal network
D. Windows-based agent deployed on each of the WAN Links
Answer: A (LEAVE A REPLY)
Another reason to choose the Windows agent over the integrated PAN-OS agent is to save processing cycles on the firewall's management plane.

NEW QUESTION: 125
What are three ways application characteristics are used? (Choose three.)
A. As a setting to define a new custom application
B. As a global filter in the Application Command Center (ACC)
C. As an attribute to define an application group
D. As an Object to define Security policies
E. As an attribute to define an application filter
Answer: A,C,E (LEAVE A REPLY)

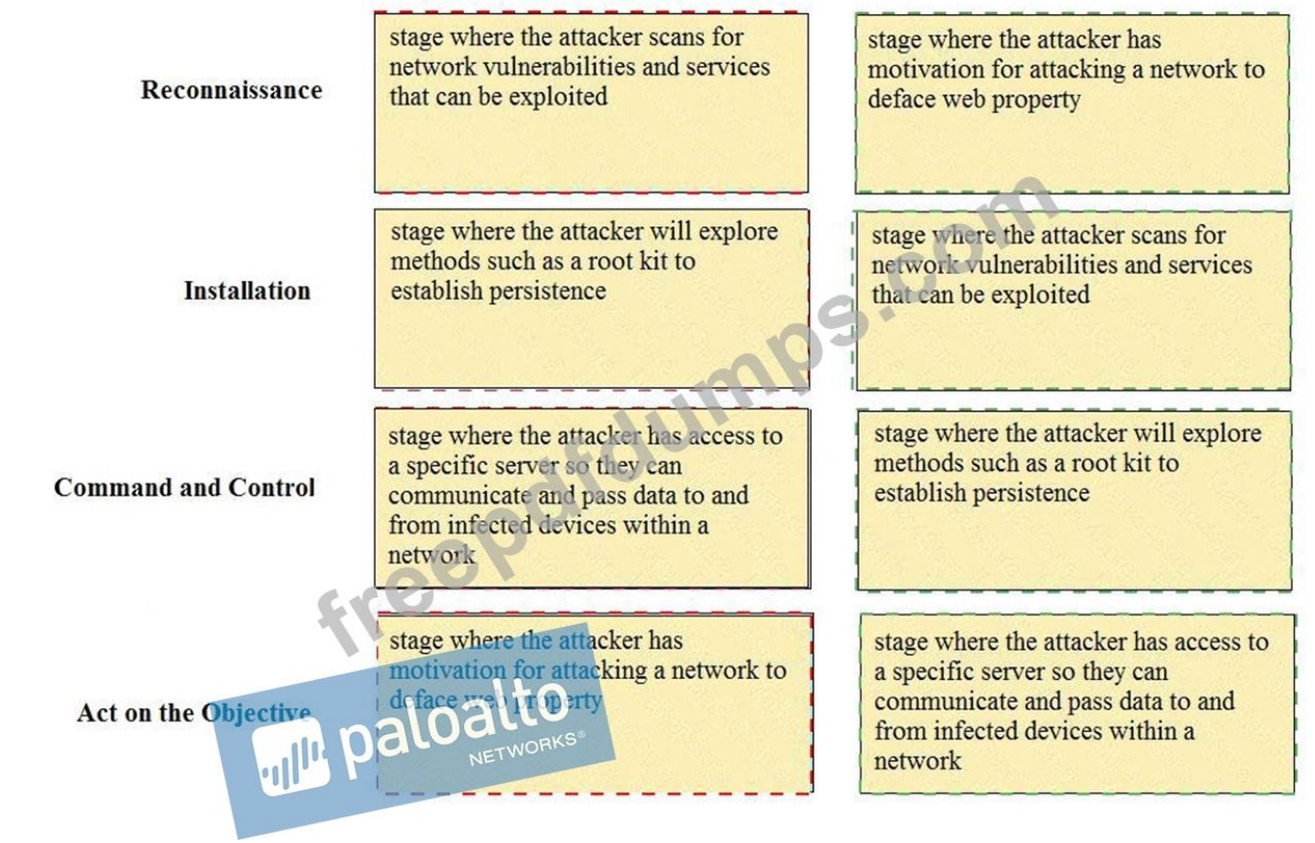
NEW QUESTION: 126
Which firewall feature do you need to configure to query Palo Alto Networks service updates over a data-plane interface instead of the management interface?
A. Data redistribution
B. SNMP setup
C. Dynamic updates
D. Service route
Answer: D (LEAVE A REPLY)

NEW QUESTION: 127
Which Palo Alto network security operating platform component provides consolidated policy creation and centralized management?
A. Panorama
B. Prisma SaaS
C. GlobalProtect
D. AutoFocus
Answer: A (LEAVE A REPLY)

NEW QUESTION: 128
Match the Cyber-Attack Lifecycle stage to its correct description.



Answer:



Explanation:

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

Installation - stage where the attacker will explore methods such as a root kit to establish persistence Command and Control - stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.
Act on the Objective - stage where an attacker has motivation for attacking a network to deface web property

NEW QUESTION: 129
Which statement best describes a common use of Policy Optimizer?
A. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected.
B. 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.
C. Policy Optimizer can display which Security policies have not been used in the last 90 days.
D. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 130
A systems engineer (SE) successfully demonstrates NGFW managed by Strata Cloud Manager (SCM) to a company. In the resulting planning phase of the proof of value (POV), the CISO requests a test that shows how the security policies are either meeting, or are progressing toward meeting, industry standards such as Critical Security Controls (CSC), and how the company can verify that it is effectively utilizing the functionality purchased.
During the POV testing timeline, how should the SE verify that the POV will meet the CISO's request?
A. Near the end, pull a Security Lifecycle Review (SLR) in the POV and create a report for the customer.
B. At the beginning, work with the customer to create custom dashboards and reports for any information required, so reports can be pulled as needed by the customer.
C. Near the end, the customer pulls information from these SCM dashboards: Best Practices, CDSS Adoption, and NGFW Feature Adoption.
D. At the beginning, use PANhandler golden images that are designed to align to compliance and to turning on the features for the CDSS subscription being tested.
Answer: B (LEAVE A REPLY)
The SE has demonstrated an NGFW managed by SCM, and the CISO now wants the POV to show progress toward industry standards (e.g., CSC) and verify effective use of purchased features (e.g., CDSS subscriptions like Advanced Threat Prevention). The SE must ensure the POV delivers measurable evidence during the testing timeline. Let's evaluate the options.
Step 1: Understand the CISO's Request

* Industry Standards (e.g., CSC): The Center for Internet Security's Critical Security Controls (e.g., CSC 1: Inventory of Devices, CSC 4: Secure Configuration) require visibility, threat prevention, and policy enforcement, which NGFW and SCM can address.
* Feature Utilization: Confirm that licensed functionalities (e.g., App-ID, Threat Prevention, URL Filtering) are active and effective.
* POV Goal: Provide verifiable progress and utilization metrics within the testing timeline.
Reference: Strata Cloud Manager Overview (docs.paloaltonetworks.com/strata-cloud-manager); CIS Critical Security Controls (www.cisecurity.org/controls).
Step 2: Define SCM Capabilities
Strata Cloud Manager (SCM): A cloud-based management platform for Palo Alto NGFWs, offering dashboards (e.g., Best Practices, Feature Adoption) and custom reporting to monitor security posture, policy compliance, and subscription usage.
Security Lifecycle Review (SLR): A report generated via the Customer Support Portal (not SCM) analyzing traffic logs for security gaps, not real-time POV progress.
Dashboards and Reports: SCM provides prebuilt and customizable views for real-time insights into policy effectiveness and feature adoption.
Reference: SCM Dashboards and Reports (docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and- reports).
Step 3: Evaluate Each Option
A). Near the end, pull a Security Lifecycle Review (SLR) in the POV and create a report for the customer.
Description: The SLR analyzes 7-30 days of traffic logs, providing a retrospective security posture assessment (e.g., threats blocked, policy gaps).
Process: Near POV end, upload logs to the Customer Support Portal (Support > Security Lifecycle Review), generate, and share the report.
Limitations:
SLR is a point-in-time analysis, not a real-time progress tracker during the POV timeline.
Requires post-POV log collection, delaying feedback.
Doesn't directly show feature utilization progress or CSC alignment in SCM.
Fit: Misses the "during the POV timeline" requirement; better for post-POV analysis.
Reference: Security Lifecycle Review Guide (support.paloaltonetworks.com, requires login).
B). At the beginning, work with the customer to create custom dashboards and reports for any information required, so reports can be pulled as needed by the customer.
Description: SCM allows custom dashboards and reports (Monitor > Dashboards or Reports) tailored to metrics like policy compliance (CSC alignment) and feature usage (e.g., Threat Prevention hits).
Process:
At POV start, collaborate with the CISO to define metrics (e.g., "Threats blocked by ATP" for CSC 6, "App- ID usage" for feature adoption).
Configure custom dashboards in SCM (Dashboards > Add Dashboard > Custom).
Set up scheduled or on-demand reports (Reports > Custom Reports).

Enable the customer to monitor progress throughout the POV.
Benefits:
Real-time visibility into policy effectiveness and feature use during the timeline.
Aligns with CSC (e.g., blocked malware events) and shows subscription ROI.
Empowers the customer to verify results independently.
Fit: Meets the CISO's request fully within the POV timeline.
Reference: SCM Custom Dashboards (docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and- reports/custom-dashboards).
C). Near the end, the customer pulls information from these SCM dashboards: Best Practices, CDSS Adoption, and NGFW Feature Adoption.
Description: SCM provides prebuilt dashboards:
Best Practices: Assesses policy alignment with security standards.
CDSS Adoption: Tracks subscription usage (e.g., ATP, URL Filtering).
NGFW Feature Adoption: Monitors features like App-ID or User-ID.
Limitations:
Waiting until "near the end" delays visibility, missing ongoing progress tracking.
Prebuilt dashboards may not fully align with CSC or specific customer needs without customization.
Fit: Useful but incomplete; lacks proactive setup and real-time monitoring throughout the POV.
Reference: SCM Prebuilt Dashboards (docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and- reports/prebuilt-dashboards).
D). At the beginning, use PANhandler golden images that are designed to align to compliance and to turning on the features for the CDSS subscription being tested.
Description: PANhandler is a tool for managing Skillets (configuration templates), including "golden images" for compliance (e.g., NIST, CIS benchmarks).
Process: Apply a Skillet at POV start to configure the NGFW with compliance settings and CDSS features.
Limitations:
Configures the NGFW but doesn't verify progress or utilization during the POV.
No reporting or dashboard integration for the CISO to track results.
Fit: Sets up the environment but doesn't meet the verification requirement.
Reference: PANhandler Skillets (github.com/PaloAltoNetworks/panhandler).
Step 4: Select the Best Approach
B is the strongest choice:
Proactive: Starts at the beginning, ensuring metrics are tracked throughout the POV.
Customizable: Tailors dashboards/reports to CSC (e.g., threat detection for CSC 6) and feature use (e.g., ATP events).
Verifiable: Enables the customer to pull reports as needed, meeting the CISO's request within the timeline.
Why not A, C, or D?
A: SLR is retrospective, not real-time, missing the "during" aspect.

C: Prebuilt dashboards are helpful but delayed and less flexible than custom options.
D: Golden images configure but don't verify progress or utilization.
Step 5: Verification with Palo Alto Documentation
SCM Custom Dashboards: Supports real-time, tailored monitoring (SCM Docs).
SLR: Post-analysis tool, not POV-progressive (Support Portal Docs).
Prebuilt Dashboards: Limited customization (SCM Docs).
PANhandler: Configuration-focused, not reporting-focused (PANhandler Docs).
Thus, the verified answer is B.

NEW QUESTION: 131
What are two valid selections within an Antivirus profile? (Choose two.)
A. block-ip
B. deny
C. default
D. drop
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 132
What must be considered with regards to content updates deployed from Panorama?
A. Content update schedulers need to be configured separately per device group.
B. Panorama can only install up to five content versions of the same type for potential rollback scenarios.
C. A PAN-OS upgrade resets all scheduler configurations for content updates.
D. Panorama can only download one content update at a time for content updates of the same type.
Answer: (SHOW ANSWER)
Reference: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-licenses-and-updates
/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/schedule-a-content- update-using-panorama.html

NEW QUESTION: 133
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: D (LEAVE A REPLY)
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-device-groups

/create-objects-for-use-in-shared-or-device-group-policy

NEW QUESTION: 134
An administrator manages a network with 300 addresses that require translation. The administrator configured NAT with an address pool of 240 addresses and found that connections from addresses that needed new translations were being dropped.
Which type of NAT was configured?
A. Static IP
B. Dynamic IP
C. Destination NAT
D. Dynamic IP and Port
Answer: B (LEAVE A REPLY)
The size of the NAT pool should be equal to the number of internal hosts that require address translations. By default, if the source address pool is larger than the NAT address pool and eventually all of the NAT addresses are allocated, new connections that need address translation are dropped. To override this default behavior, use Advanced (Dynamic IP/Port Fallback) to enable the use of DIPP addresses when necessary

NEW QUESTION: 135
At which point in the app-ID update process can you determine if an existing policy rule is affected by an app- ID update?
A. after clicking Check New in the Dynamic Update window
B. after connecting the firewall configuration
C. after downloading the update
D. after installing the update
Answer: (SHOW ANSWER)
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device- dynamicupdates

NEW QUESTION: 136
Which statement best describes the use of Policy Optimizer?
A. Policy Optimizer can add or change a Log Forwarding profile for each Secunty policy selected
B. 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
C. Policy Optimizer can display which Security policies have not been used in the last 90 days
D. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Which type of profile must be applied to the Security policy rule to protect against buffer overflows illegal code execution and other attempts to exploit system flaws?
A. anti-spyware
B. URL filtering
C. vulnerability protection
D. file blocking
Answer: C (LEAVE A REPLY)
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-security- profiles-vulnerability-protection.html Vulnerability Protection Security Profiles protect against threats entering the network. For example, Vulnerability Protection Security Profiles protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection Security Profile protects clients and servers from all known critical-, high-, and medium-severity threats. You also can create exceptions that enable you to change the response to a specific signature.

NEW QUESTION: 138
An administrator configured a Security policy rule with an Antivirus Security profile. The administrator did not change the action (or the profile. If a virus gets detected, how wilt the firewall handle the traffic?
A. It drops the traffic because the profile was not set to explicitly allow the traffic.
B. It allows the traffic but generates an entry in the Threat logs.
C. It allows the traffic because the profile was not set to explicitly deny the traffic.
D. It uses the default action assigned to the virus signature.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 139
Within an Anti-Spyware security profile, which tab is used to enable machine learning based engines?
A. Inline Cloud Analysis
B. Signature Exceptions
C. Machine Learning Policies
D. Signature Policies

Answer: A (LEAVE A REPLY)

* An Anti-Spyware security profile is a set of rules that defines how the firewall detects and prevents spyware from compromising hosts on the network. Spyware is a type of malware that collects information from the infected system, such as keystrokes, browsing history, or personal data, and sends it to an external command-and-control (C2) server1.
* An Anti-Spyware security profile consists of four tabs: Signature Policies, Signature Exceptions, Machine Learning Policies, and Inline Cloud Analysis1.
* The Signature Policies tab allows you to configure the actions and log settings for each spyware signature category, such as adware, botnet, keylogger, phishing, or worm. You can also enable DNS Security to block malicious DNS queries and responses1.
* The Signature Exceptions tab allows you to create exceptions for specific spyware signatures that you want to override the default action or log settings. For example, you can allow a signature that is normally blocked by the profile, or block a signature that is normally alerted by the profile1.
* The Machine Learning Policies tab allows you to configure the actions and log settings for machine learning based signatures that detect unknown spyware variants. You can also enable WildFire Analysis to submit unknown files to the cloud for further analysis1.
* The Inline Cloud Analysis tab allows you to enable machine learning based engines that detect unknown spyware variants in real time. These engines use cloud-based models to analyze the behavior and characteristics of network traffic and identify malicious patterns. You can enable inline cloud analysis for HTTP/HTTPS traffic, SMTP/SMTPS traffic, or IMAP/IMAPS traffic1.

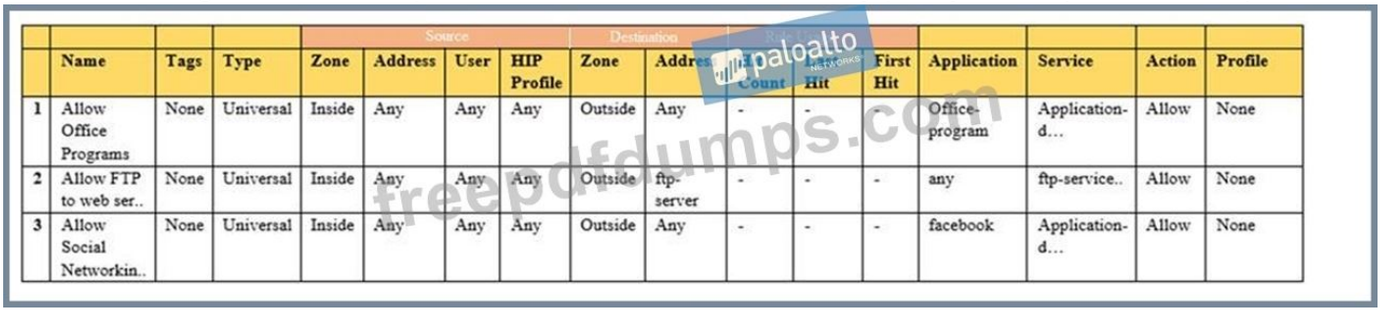
Therefore, the tab that is used to enable machine learning based engines is the Inline Cloud Analysis tab.

References:

1: Security Profile: Anti-Spyware - Palo Alto Networks

NEW QUESTION: 140

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 FTP to web server rule, FTP is allowed using App-ID

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

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

Answer: A,D (LEAVE A REPLY)

In the Allow FTP to web server rule, FTP is allowed using port based rule and not APP-ID.

NEW QUESTION: 141
What is considered best practice with regards to committing configuration changes?
A. Wait until all running and pending jobs are finished before committing
B. Export configuration after each single configuration change performed
C. Disable the automatic commit feature that prioritizes content database installations before committing
D. Validate configuration changes prior to committing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 142
How are service routes used in PAN-OS?
A. By the OSPF protocol, as part of Dijkstra's algorithm, to give access to the various services offered in the network
B. To statically route subnets so they are joinable from, and have access to, the Palo Alto Networks external services
C. For routing, because they are the shortest path selected by the BGP routing protocol
D. To route management plane services through data interfaces rather than the management interface
Answer: (SHOW ANSWER)
* Service routes are a feature of PAN-OS that allows the administrator to customize the interface that the firewall uses to send requests to external services, such as DNS, email, Palo Alto Networks updates, User-ID agent, syslog, Panorama, dynamic updates, URL updates, licenses, and AutoFocus1.
* By default, the firewall uses the management interface for all service routes, unless the packet destination IP address matches the configured destination service route, in which case the source IP address is set to the source address configured for the destination1.
* However, in some scenarios, the administrator may want to use a different interface for service routes, such as when the management interface does not have public internet access, or when the administrator wants to isolate or monitor the traffic for certain services23.
* To configure service routes, the administrator can select Device > Setup > Services > Service Route Configuration and customize each service with a source interface and a source address. The administrator can also configure destination service routes to specify a destination IP address and a gateway for each service1.
* Service routes are not related to routing protocols such as OSPF or BGP, which are used to exchange routing information between routers and determine the best path to reach a network destination. Service routes are only used to change the interface that the firewall uses to communicate with external services.
Therefore, service routes are used to route management plane services through data interfaces rather than the management interface.
References:

1: Configure Service Routes - Palo Alto Networks 2: Setting a Service Route for Services to Use a Dataplane' s Interface - Palo Alto Networks 3: How to Perform Updates when Management Interface does not have Public Internet Access - Palo Alto Networks

NEW QUESTION: 143
Palo Alto Networks firewall architecture accelerates content map minimizing latency using which two components'? (Choose two)
A. Single Stream-based Engine
B. Policy Engine
C. Network Processing Engine
D. Parallel Processing Hardware
Answer: (SHOW ANSWER)

NEW QUESTION: 144
Based on the image provided, which two statements apply to the Security policy rules? (Choose two.)

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

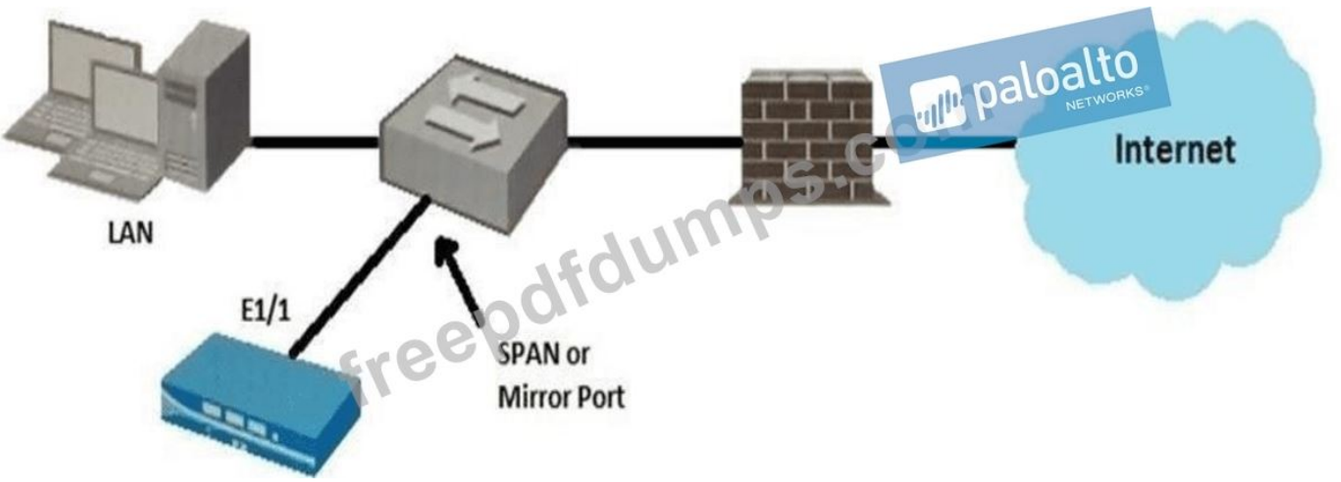
A. In the Allow-FTP policy, FTP is allowed using App-ID.
B. The Allow-Office-Programs rule is using an application group.
C. The Allow-Office-Programs rule is using an application filter.
D. The Allow-Social-Media rule allows all Facebook functions.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 145
An administrator needs to allow users to use only certain email applications.
How should the administrator configure the firewall to restrict users to specific email applications?
A. Create an application group and add the email applications to it.
B. Create an application group and add the email category to it.
C. Create an application filter and filter it on the collaboration category.
D. Create an application filter and filter it on the collaboration category, email subcategory.
Answer: (SHOW ANSWER)

NEW QUESTION: 146
Which two addresses should be reserved to enable DNS sinkholing? (Choose two.)
A. IPv6

B. Email
C. IPv4
D. MAC
Answer: A,C (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGECA0

NEW QUESTION: 147
Which statement is true regarding a Best Practice Assessment?
A. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities
B. The BPA tool can be run 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 data
Answer: (SHOW ANSWER)

NEW QUESTION: 148


Given the topology, which zone type should you configure for firewall interface E1/1?
A. Tunnel
B. Layer3
C. Tap
D. Virtual Wire
Answer: C (LEAVE A REPLY)

NEW QUESTION: 149
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 provides application statistics based on network, threat, and blocked activity,
C. It dynamically groups applications based on application attributes such as category and subcategory.

D. It dynamically filters applications based on critical, high, medium, low. or informational severity.
Answer: C (LEAVE A REPLY)