PaloAltoNetworks.PCNSE.v2022-09-01.q323

Exam Code:	PCNSE
Exam Name:	Palo Alto Networks Certified Network Security Engineer Exam
Certification Provider:	Palo Alto Networks
Free Question Number:	323
Version:	v2022-09-01
# of views:	13019
# of Questions views:	3220
https://www.freepdfdumps.com/PaloAltoNetworks.PCNSE.v2022-09-01.q323.html	

NEW QUESTION: 1
The firewall identifies a popular application as an unknown-tcp.
Which two options are available to identify the application? (Choose two.)
A. Create a custom object for the custom application server to identify the custom application.
B. Create a custom application.
C. Create a Security policy to identify the custom application.
D. Submit an Apple-ID request to Palo Alto Networks.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which CLI command displays the current management plane memory utilization?
A. > debug management-server show
B. > show running resource-monitor
C. > show system info
D. > show system resources
Answer: D (LEAVE A REPLY)
https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364
"The command show system resources gives a snapshot of Management Plane (MP) resource utilization including memory and CPU. This is similar to the 'top' command in Linux."
https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364

NEW QUESTION: 3
Which command can be used to validate a Captive Portal policy?
A. eval captive-portal policy <criteria>
B. test cp-policy-match <criteria>

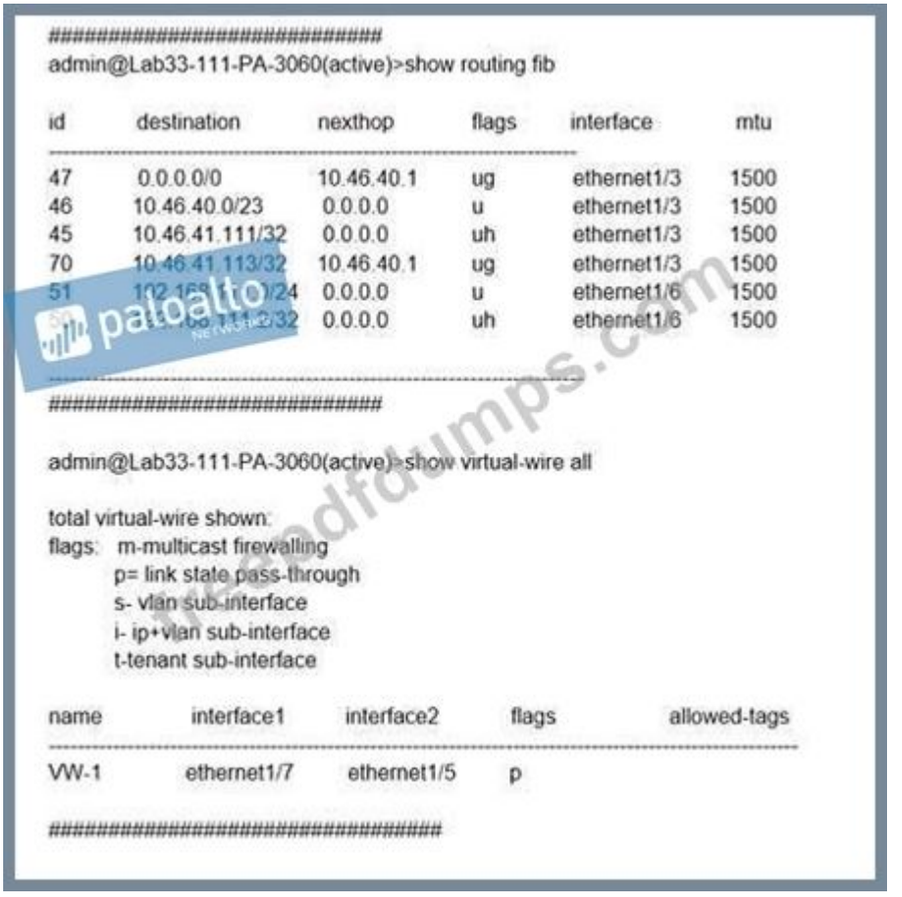
C. debug cp-policy <criteria>

D. request cp-policy-eval <criteria>

Answer: B (LEAVE A REPLY)

NEW QUESTION: 4

Refer to the exhibit.



```
##############################
admin@Lab33-111-PA-3060(active)>show routing fib

id      destination       nexthop      flags   interface      mtu
------------------------------------------------------------------
47      0.0.0.0/0         10.46.40.1   ug      ethernet1/3    1500
46      10.46.40.0/23     0.0.0.0      u       ethernet1/3    1500
45      10.46.41.111/32   0.0.0.0      uh      ethernet1/3    1500
70      10.46.41.113/32   10.46.40.1   ug      ethernet1/3    1500
51      192.168.[illegible]/24  0.0.0.0  u     ethernet1/6    1500
        192.168.[illegible]/32  0.0.0.0  uh    ethernet1/6    1500
------------------------------------------------------------------
##############################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p= link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name      interface1    interface2    flags    allowed-tags
------------------------------------------------------------
VW-1      ethernet1/7   ethernet1/5   p

##################################
```

Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

A. ethernet1/5

B. ethernet1/7

C. ethernet1/6

D. ethernet1/3

Answer: A (LEAVE A REPLY)

NEW QUESTION: 5

An administrator wants to upgrade an NGFW from PAN-OS® 9.0 to PAN-OS® 10.0. The firewall is not a part of an HA pair. What needs to be updated first?

A. XML Agent

B. Applications and Threats

C. WildFire

D. PAN-OS® Upgrade Agent

Answer: B (LEAVE A REPLY)

https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-the-firewall-to-pan-os-80/upgrade-a-firewall-to-pan-os-80

NEW QUESTION: 6
Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)
A. Verify AutoFocus status using CLI.
B. Check the WebUI Dashboard AutoFocus widget.
C. Check for WildFire forwarding logs.
D. Check the license
E. Verify AutoFocus is enabled below Device Management tab.
Answer: B,D (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-inte

NEW QUESTION: 7
An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing and preemption is disabled.
What must be verified to upgrade the firewalls to the most recent version of PAN-OS software?
A. Wildfire update package
B. User-ID agent
C. Anti virus update package
D. Application and Threats update package
Answer: D (LEAVE A REPLY)
Dependencies : Before upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS Upgrade.
Reference:
https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS-Upgrade/ta-p/111045

NEW QUESTION: 8
An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs.
The administrator assigns priority 100 to the active firewall.
Which priority is correct for the passive firewall?
A. 0
B. 99
C. 1
D. 255
Answer: D (LEAVE A REPLY)
Reference:

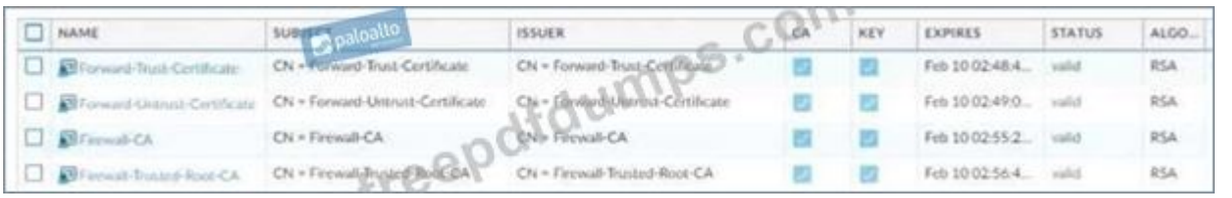
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5.p (page 9)
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pd page 315

NEW QUESTION: 9
If a template stack is assigned to a device and the stack includes three templates with overlapping
settings, which settings are published to the device when the template stack is pushed?
A. All the settings configured in all templates.
B. The administrator will be promoted to choose the settings for that chosen firewall.
C. The settings assigned to the template that is on top of the stack.
D. Depending on the firewall location, Panorama decides with settings to send.
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which protection feature is available only in a Zone Protection Profile?
A. SYN Flood Protection using SYN Flood Cookies
B. ICMP Flood Protection
C. Port Scan Protection
D. UDP Flood Protections
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 11
An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.
How would the administrator establish the chain of trust?
A. Use custom certificates
B. Enable LDAP or RADIUS integration
C. Set up multi-factor authentication
D. Configure strong password authentication
Answer: A (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/plan panorama-deployment

NEW QUESTION: 12
The SSL Forward Proxy decryption policy is configured. The following four certificate authority (CA) certificates are installed on the firewall.



An end-user visits the untrusted website https //www firewall-do-not-trust-website com.
Which certificate authority (CA) certificate will be used to sign the untrusted webserver certificate?

A. Forward-Untrust-Certificate
B. Forward-Trust-Certificate
C. Firewall-CA
D. Firewall-Trusted-Root-CA

Answer: B (LEAVE A REPLY)

Since Forward Trust Certificate isn't configured, then the Forward Trust Certificate will be used also for untrusted webserver.

NEW QUESTION: 13

Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?

A. Session Browser
B. Application Command Center
C. TCP Dump
D. Packet Capture

Answer: B (LEAVE A REPLY)

Reference:
https://live.paloaltonetworks.com/t5/Management-Articles/Tips-amp-Tricks-How-to-Use-the-Application-Comm ACC/ta-p/67342 The Application Command Center (ACC) page visually depicts trends and a historic view of traffic on your network. It displays the overall risk level for all network traffic, the risk levels and number of threats detected for the most active and highest-risk applications on your network, and the number of threats detected from the busiest application categories and from all applications at each risk level. The ACC can be viewed for the past hour, day, week, month, or any custom-defined time frame.

NEW QUESTION: 14

What can missing SSL packets when performing a packet capture on dataplane interfaces?

A. The packets are hardware offloaded to the offloaded processor on the dataplane
B. There is a hardware problem with offloading FPGA on the management plane
C. The missing packets are offloaded to the management plane CPU
D. The packets are not captured because they are encrypted

Answer: (SHOW ANSWER)

NEW QUESTION: 15

What are two common reasons to use a "No Decrypt" action to exclude traffic from SSL decryption? (Choose two.)

A. the website matches a category that is not allowed for most users

B. the website matches a high-risk category

C. the web server requires mutual authentication

D. the website matches a sensitive category

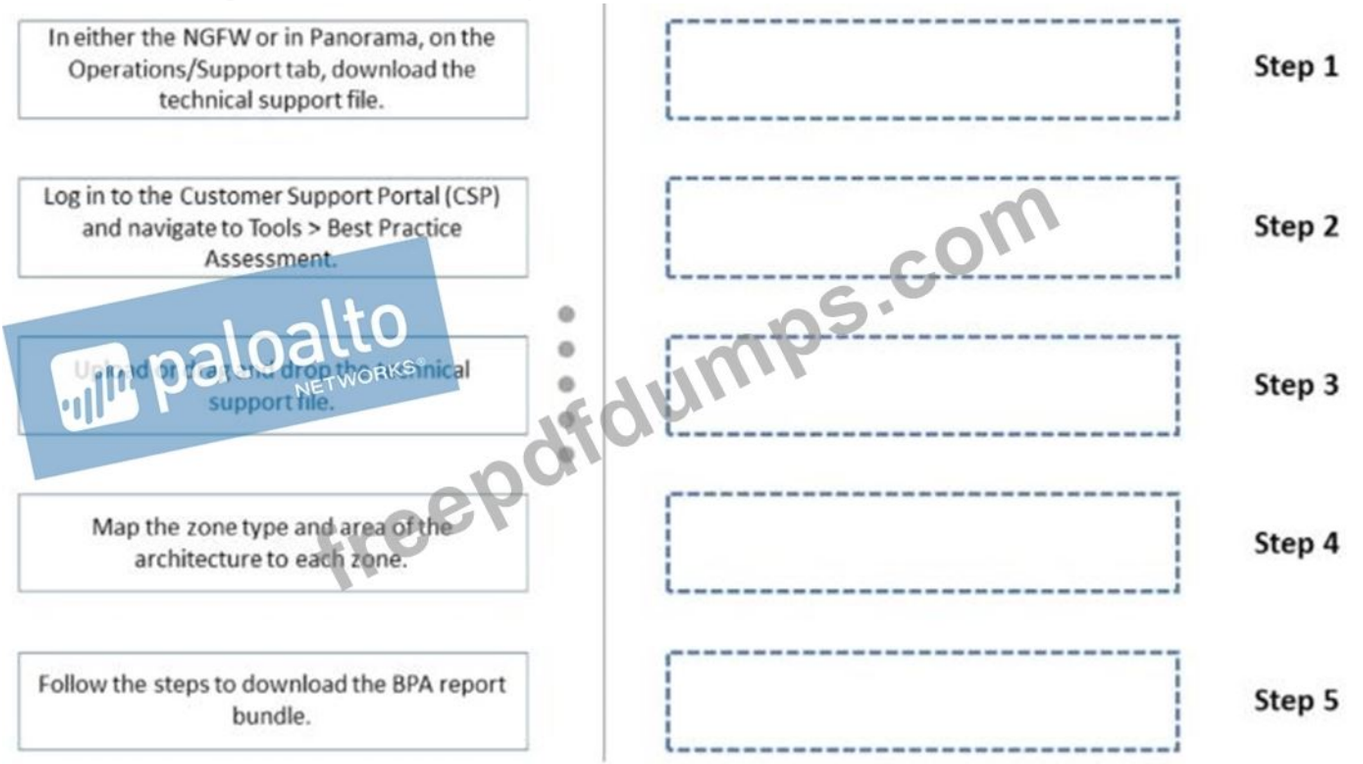
Answer: A,D (LEAVE A REPLY)

Explanation

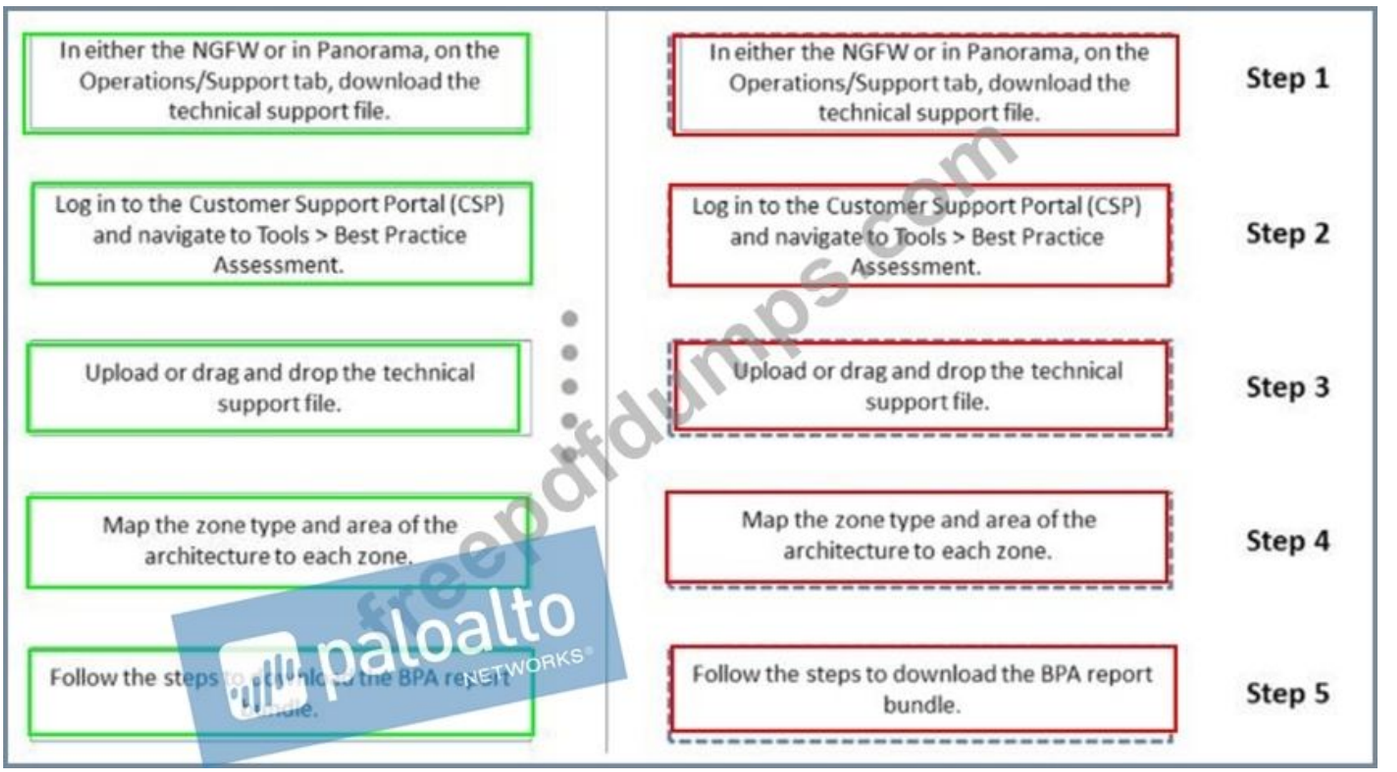
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-exclusions/palo-alto-networ The firewall provides a predefined SSL Decryption Exclusion list to exclude from decryption commonly used sites that break decryption because of technical reasons such as pinned certificates and mutual authentication.

NEW QUESTION: 16

Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.



Answer:



Reference:
https://www.paloaltonetworks.com/resources/videos/how-to-run-a-bpa

NEW QUESTION: 17
A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured.
What can be the cause of this problem?
A. Interface Ethernet 1/1 is in Virtual Wire Mode.
B. No Zone has been configured on Ethernet 1/4.
C. DNS has not been properly configured on the host.
D. DNS has not been properly configured on the firewall.
Answer: B (LEAVE A REPLY)

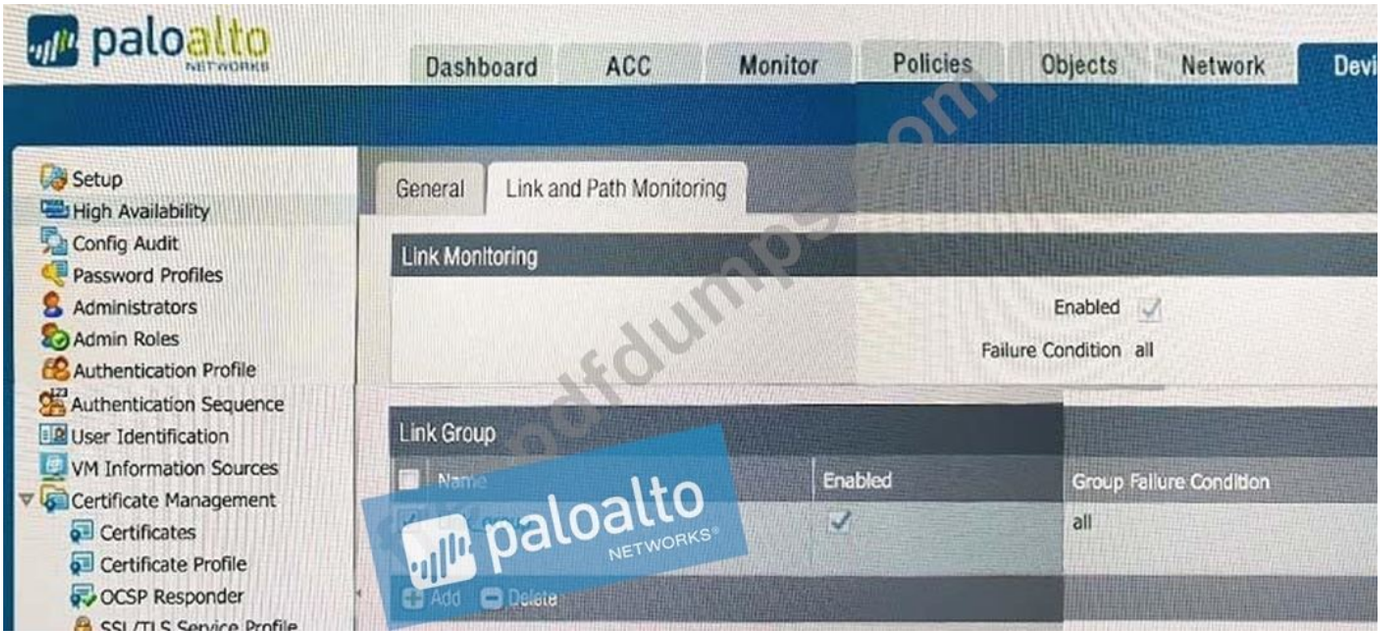
NEW QUESTION: 18

An administrator needs to build Security rules in a Device Group that allow traffic to specific users and groups defined in Active Directory What must be configured in order to select users and groups for those rules from Panorama?
A. A master device with Group Mapping configured must be set in the device group where the Security rules are configured
B. The Security rules must be targeted to a firewall in the device group and have Group Mapping configured
C. User-ID Redistribution must be configured on Panorama to ensure that all firewalls have the same mappings
D. A User-ID Certificate profile must be configured on Panorama
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are form external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this traffic as their accounting application and to scan this traffic for threats.
Which option would achieve this result?
A. Create a custom App-ID and enable scanning on the advanced tab.
B. Create an Application Override policy.
C. Create a custom App-ID and use the "ordered conditions" check box.
D. Create an Application Override policy and custom threat signature for the application.
Answer: (SHOW ANSWER)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRoCAK

NEW QUESTION: 20
Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x-enabled wireless network device that has no native integration with PAN-OS software?
A. XML API
B. Port Mapping
C. Client Probing
D. Server Monitoring
Answer: A (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api.htm
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/server-monit

NEW QUESTION: 21
If the firewall has the link monitoring configuration, what will cause a failover?



A. ethernet1/6 going down
B. ethernet1/3 going down
C. ethernet1/3 or Ethernet1/6 going down
D. ethernet1/3 and ethernet1/6 going down
Answer: (SHOW ANSWER)

NEW QUESTION: 22
What are two best practices for incorporating new and modified App-IDs? (Choose two.)
A. Run the latest PAN-OS version in a supported release tree to have the best performance for the new App-IDs
B. Configure a security policy rule to allow new App-IDs that might have network-wide impact
C. Perform a Best Practice Assessment to evaluate the impact of the new or modified App-IDs
D. Study the release notes and install new App-IDs if they are determined to have low impact
Answer: B,D (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/app-id-updates-workflow.html

NEW QUESTION: 23
Which three statements accurately describe Decryption Mirror? (Choose three.)
A. Decryption Mirror requires a tap interface on the firewall
B. Decryption, storage, inspection and use of SSL traffic are regulated in certain countries
C. Only management consent is required to use the Decryption Mirror feature
D. You should consult with your corporate counsel before activating and using Decryption Mirror in a production environment
E. Use of Decryption Mirror might enable malicious users with administrative access to the firewall to harvest sensitive information that is submitted via an encrypted channel
Answer: B,D,E (LEAVE A REPLY)

Explanation
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-concepts/decryption-mirrori
"Keep in mind that the decryption, storage, inspection, and/or use of SSL traffic is governed in certain countries and user consent might be required in order to use the decryption mirror feature. Additionally, use of this feature could enable malicious users with administrative access to the firewall to harvest usernames, passwords, social security numbers, credit card numbers, or other sensitive information submitted using an encrypted channel. Palo Alto Networks recommends that you consult with your corporate counsel before activating and using this feature in a production environment."

NEW QUESTION: 24
A session in the Traffic log is reporting the application as "incomplete." What does "incomplete" mean?
A. The three-way TCP handshake was observed, but the application could not be identified.
B. The three-way TCP handshake did not complete.
C. The traffic is coming across UDP, and the application could not be identified.
D. Data was received but was instantly discarded because of a Deny policy was applied before App-ID could be applied.
Answer: B (LEAVE A REPLY)
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

NEW QUESTION: 25
The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?
A. 6-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Protocol, and Source Security Zone
B. 5-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Protocol
C. 7-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Source User, URL Category, and Source Security Zone
D. 9-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Source User, Source Security Zone,
Answer: A (LEAVE A REPLY)
Destination Security Zone, Application, and URL Category
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVECA0

NEW QUESTION: 26
A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects. How would an administrator configure the interface to 1Gbps?
A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
B. set deviceconfig system speed-duplex 1Gbps-duplex
C. set deviceconfig system speed-duplex 1Gbps-full-duplex
D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex
Answer: C (LEAVE A REPLY)
Reference:
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Management- Port/ta-p/59034 user@PA# set deviceconfig system speed-duplex 100Mbps-full-duplex 100Mbps-full-duplex 100Mbps-half-duplex 100Mbps-half-duplex 10Mbps-full-duplex 10Mbps-full-duplex 10Mbps-half-duplex 10Mbps-half-duplex 1Gbps-full-duplex 1Gbps-full-duplex 1Gbps-half-duplex 1Gbps-half-duplex auto-negotiate auto-negotiate

NEW QUESTION: 27
In a Panorama template which three types of objects are configurable? (Choose three)
A. HIP objects
B. security profiles
C. interface management profiles
D. certificate profiles
E. QoS profiles
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which CLI command enables an administrator to check the CPU utilization of the dataplane?
A. show running resource-monitor
B. show system resources
C. debug running resources
D. debug data-plane dp-cpu
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
In a security-first network what is the recommended threshold value for content updates to be dynamically updated?
A. 1 to 4 hours
B. 6 to 12 hours
C. 24 hours
D. 36 hours
Answer: B (LEAVE A REPLY)

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-threat-content-updates/best-practices-security-first.html
Schedule content updates so that they download-and-install automatically. Then, set a Threshold that determines the amount of time the firewall waits before installing the latest content. In a security-first network, schedule a six to twelve hour threshold.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-threat-content-updates/best-practices-security-first.html#id184AH00F06E

NEW QUESTION: 30
An administrator wants to upgrade an NGFW from PAN-OS 7.1.2 to PAN-OS 8.1.0. The firewall is not a part of an HA pair.
What needs to be updated first?
A. WildFire
B. XML Agent
C. Applications and Threats
D. PAN-OS Upgrade Agent
Answer: (SHOW ANSWER)

NEW QUESTION: 31
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?
A. Use the debug dataplane packet-diag set capture stage firewall file command.
B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
C. Use the debug dataplane packet-diag set capture stage management file command.
D. Use the topdump command.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta- p/62390

NEW QUESTION: 32
When performing the "ping" test shown in this CLI output:

What will be the source address in the ICMP packet?

A. 10.46.72.93

B. 10.46.64.94

C. 10.30.0.93

D. 192.168.93.1

Answer: B (LEAVE A REPLY)

NEW QUESTION: 33

A company.com wants to enable Application Override. Given the following screenshot:

Which two statements are true if Source and Destination traffic match the Application Override policy? (Choose two)

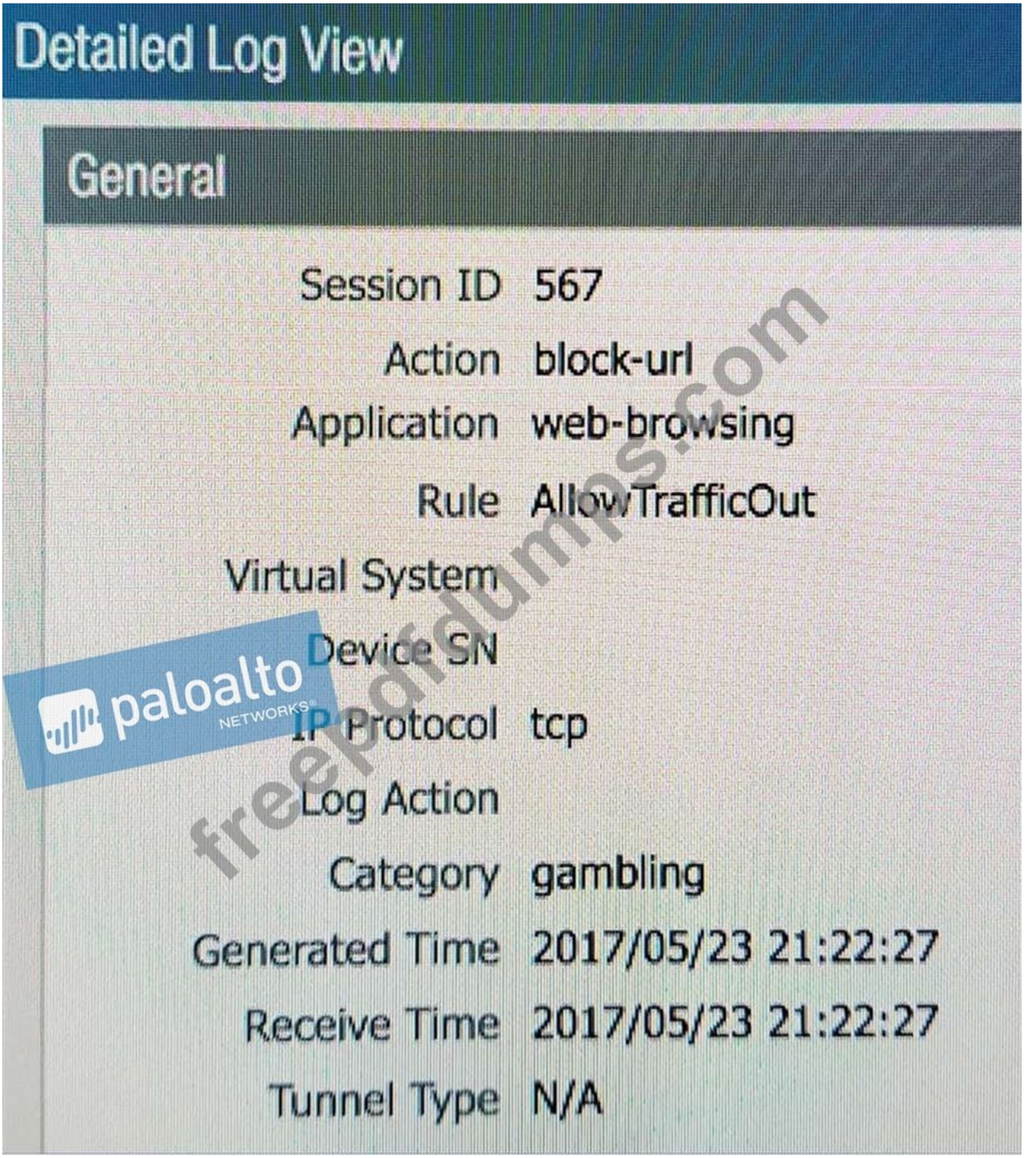
A. Traffic that matches "rtp-base" will bypass the App-ID and Content-ID engines.
B. Traffic will be forced to operate over UDP Port 16384.
C. Traffic utilizing UDP Port 16384 will now be identified as "rtp-base".
D. Traffic utilizing UDP Port 16384 will bypass the App-ID and Content-ID engines.
Answer: C,D (LEAVE A REPLY)
An application override policy is changes how the Palo Alto Networks firewall classifies network traffic into applications. An application override with a custom application prevents the session from being processed by the App-ID engine, which is a Layer-7 inspection.
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Create-an-Application-Override-Policy/ta-p/60044

NEW QUESTION: 34
A network security engineer has a requirement to allow an external server to access an internal web server. The internal web server must also initiate connections with the external server.
What can be done to simplify the NAT policy?
A. Configure ECMP to handle matching NAT traffic
B. Configure a NAT Policy rule with Dynamic IP and Port
C. Create a new Source NAT Policy rule that matches the existing traffic and enable the Bi-directional option
D. Create a new Destination NAT Policy rule that matches the existing traffic and enable the Bi-directional option
Answer: C (LEAVE A REPLY)
Explanation: https://www.paloaltonetworks.com/documentation/70/pan-os/pan- os/networking/nat-configuration-examples

NEW QUESTION: 35

An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image. Which configuration change should the administrator make?

A)

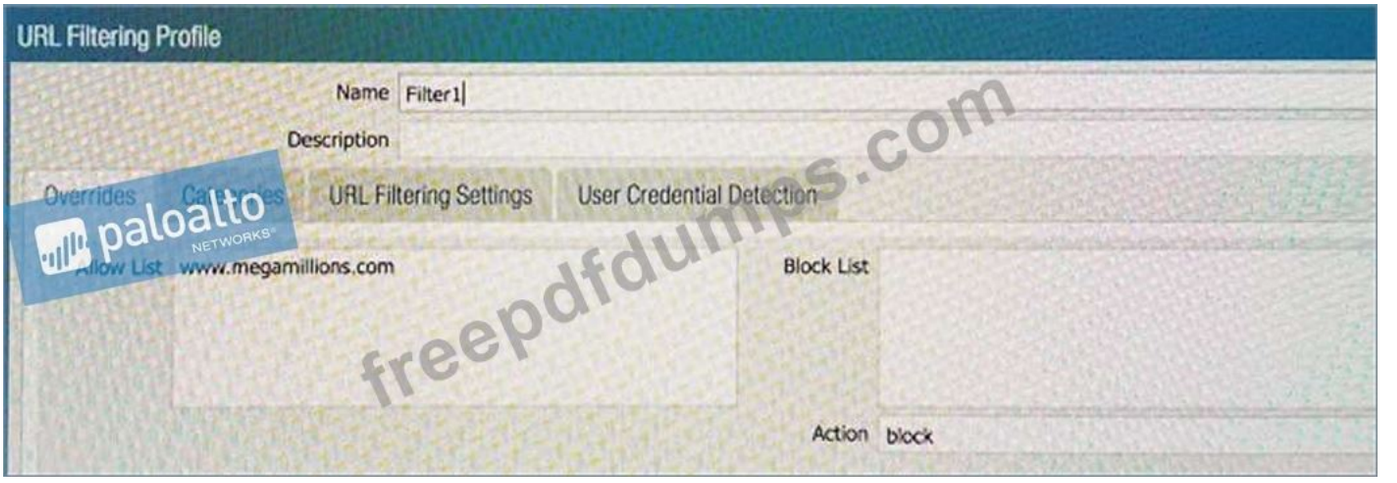


B)

C)

D)

E)



A. Option C

B. Option E

C. Option A

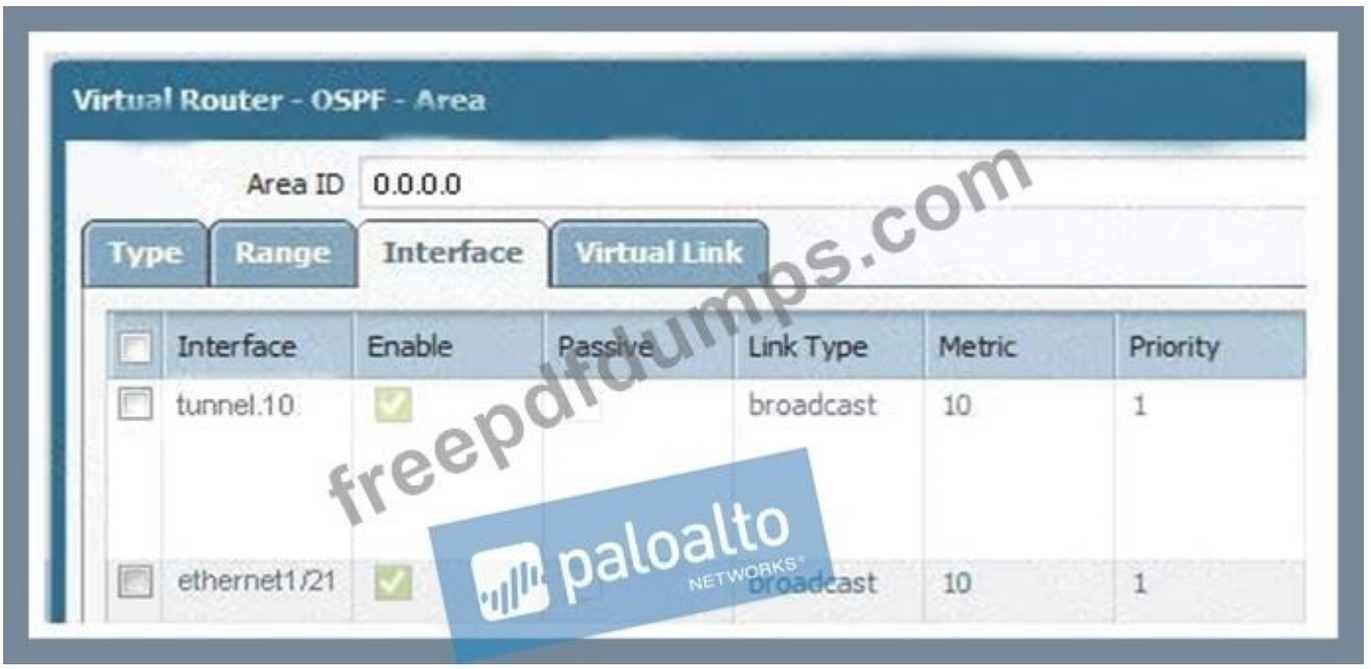
D. Option D

E. Option B
Answer: (SHOW ANSWER)

NEW QUESTION: 36
If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto networks NGFW to inspect when users browse to HTTP(S) websites?
A. SSL Forward Proxy
B. SSL Inbound Inspection
C. TLS Bidirectional proxy
D. SSL Outbound Inspection
Answer: (SHOW ANSWER)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClV8CAK
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html

NEW QUESTION: 37
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW. The update contains an application that matches the same traffic signatures as the custom application.
Which application should be used to identify traffic traversing the NGFW?
A. System logs show an application error and neither signature is used.
B. Downloaded application
C. Custom application
D. Custom and downloaded application signature files are merged and both are used
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunner is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.



Which Link Type setting will correct the error?

A. Set tunnel. 1 to p2mp

B. Set Ethernet 1/1 to p2p

C. Set tunnel. 1 to p2p

D. Set Ethernet 1/1 to p2mp

Answer: C (LEAVE A REPLY)

NEW QUESTION: 39

A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server.

Which solution in PAN-OS® software would help in this case?

A. application override

B. Virtual Wire mode

C. content inspection

D. redistribution of user mappings

Answer: (SHOW ANSWER)

Explanation/Reference:

Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/deploy-user-id-in- a-large-scale-network

NEW QUESTION: 40

A logging infrastructure may need to handle more than 10,000 logs per second.

Which two options support a dedicated log collector function? (Choose two)

A. Panorama virtual appliance on ESX(i) only

B. M-500

C. M-100 with Panorama installed

D. M-100

Answer: B,C (LEAVE A REPLY)
(https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/ta-p/72181)

NEW QUESTION: 41
A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port to which it connects.
How would an administrator configure the interface to 1Gbps?
A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
B. set deviceconfig system speed-duplex 1Gbps-duplex
C. set deviceconfig system speed-duplex 1Gbps-full-duplex
D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex- of-the-Management-Port/ta-p/59034

NEW QUESTION: 42
An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing and preemption is disabled.
What must be verified to upgrade the firewalls to the most recent version of PAN-OS software?
A. Wildfire update package
B. User-ID agent
C. Anti virus update package
D. Application and Threats update package
Answer: D (LEAVE A REPLY)
Before upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS Upgrade.
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/upgrade-to-pan-os-90/upgrade-the-firewall-to-pan-os-90/upgrade-an-ha-firewall-pair-to-pan-os-90.html#idab14f5f2-f662-4e5c-ba5b-2cc35993e2ec

NEW QUESTION: 43
Which three user authentication services can be modified to provide the Palo Alto Networks NGFW with both usernames and role names? (Choose three.)
A. RADIUS
B. SAML
C. Kerberos
D. TACACS+
E. PAP
F. LDAP

Answer: (SHOW ANSWER)

NEW QUESTION: 44
What are the main benefits of WildFire? (Select the three correct answers.)
A. WildFire gathers information from possible threats detected by both NGFWs and Endpoints.
B. By using Palo Alto Networks' proprietary cloud-based architecture, quarantine holds on suspicious files are typically reduced to less than 30 seconds.
C. By collecting and distributing malware signatures from every major anti-virus vendor, WildFire can provide comprehensive protection.
D. It's a sandboxing environment that can detect malware by observing the behavior of unknown files.
E. Signatures for identified malware are quickly distributed globally to all Palo Alto Networks' customers' firewalls.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)
A. Create a no-decrypt Decryption Policy rule.
B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
C. Create a Dynamic Address Group for untrusted sites
D. Create a Security Policy rule with vulnerability Security Profile attached.
E. Enable the "Block sessions with untrusted issuers" setting.
Answer: A,D (LEAVE A REPLY)
Explanation/Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects- decryption-profile

NEW QUESTION: 46
Which CLI command enables an administrator to check the CPU utilization of the dataplane?
A. show running resource-monitor
B. debug data-plane dp-cpu
C. show system resources
D. debug running resources
Answer: A (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXwCAK

NEW QUESTION: 47
An administrator needs to evaluate a recent policy change that was committed and pushed to a firewall device group.
How should the administrator identify the configuration changes?
A. review the configuration logs on the Monitor tab
B. click Preview Changes under Push Scope
C. use Test Policy Match to review the policies in Panorama
D. context-switch to the affected firewall and use the configuration audit tool
Answer: B (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-com

NEW QUESTION: 48
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of reconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.
Which VPN configuration would adapt to changes when deployed to the future site?
A. Preconfigured GlobalProtect client
B. Preconfigured PIsec tunnels
C. Preconfigured GlobalProtect satellite
D. Preconfigured PPTP Tunnels
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
Decrypted packets from the website https://www.microsoft.com will appear as which application and service within the Traffic log?
A. web-browsing and 443
B. SSL and 80
C. SSL and 443
D. web-browsing and 80
Answer: (SHOW ANSWER)
Explanation
We know that SSL decryption is supposed to give us visibility of traffic that would otherwise be encrypted.
Therefore, we'd expect decrypted traffic to be identified as the underlying applications, such as web-browsing, facebook-base or other, but not as SSL.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS

NEW QUESTION: 50
Which three rule types are available when defining policies in Panorama? (Choose three.)
A. Pre Rules
B. Post Rules
C. Default Rules
D. Stealth Rules
E. Clean Up Rules
Answer: A,B,C (LEAVE A REPLY)
Explanation
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama-web-interface/definin

NEW QUESTION: 51
An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.
Which Security Profile type will prevent this attack?
A. Vulnerability Protection
B. Anti-Spyware
C. URL Filtering
D. Antivirus
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/ objects-security-profiles-vulnerability-protection

NEW QUESTION: 52
A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg txt. The firewall is currently running PAN-OS 10.0 and using a lab config The contents of init-cfg txi in the USB flash drive are as follows:

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsys,jumbo-frame
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command:> request resort system Upon restart, the firewall fails to begin the bootstrapping process The failure is caused because

A. PANOS version must be 91.x at a minimum but the firewall is running 10.0.x

B. The bootstrap.xml file is a required file but it is missing

C. The hostname is a required parameter, but it is missing in imt-cfg txt

D. The USB must be formatted using the ext3 file system, FAT32 is not supported

E. Firewall must be m factory default state or have all private data deleted for bootstrapping

Answer: (SHOW ANSWER)

NEW QUESTION: 53

Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

A. HA1 IP Address

B. Network Interface Type

C. Master Key

D. Zone Protection Profile

Answer: (SHOW ANSWER)

https://docs.paloaltonetworks.com/panorama/7-1/panorama-admin/manage-firewalls/template-capabilities-and-exceptions.html# You can use Templates and Template Stacks to define a wide array of settings but you can perform the following tasks only locally on each managed firewall:

Configure a device block list.

Clear logs.

Enable operational modes such as normal mode, multi-vsys mode, or FIPS-CC mode.

Configure the IP addresses of firewalls in an HA pair.

Configure a master key and diagnostics.

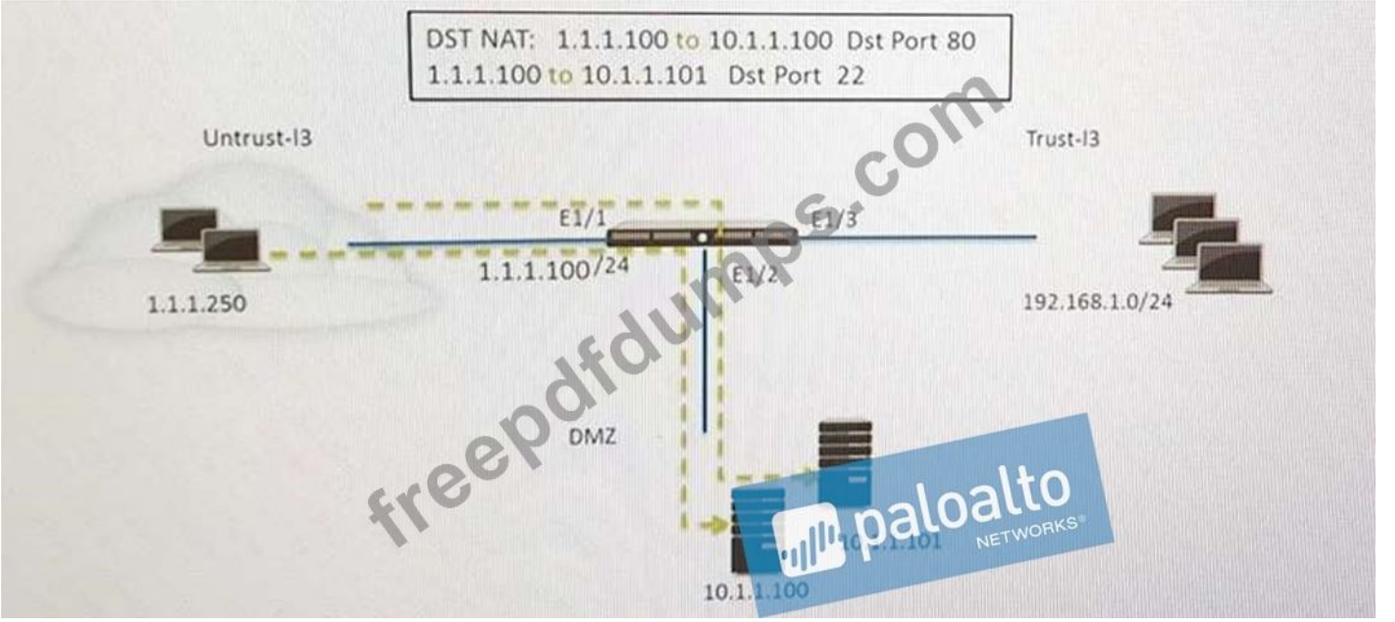
Compare configuration files (Config Audit).

Renaming a vsys on a multi-vsys firewall.

NEW QUESTION: 54
When you configure an active/active high availability pair which two links can you use? (Choose two)
A. HA2 backup
B. HA3
C. Console Backup
D. HSCI-C
Answer: A,B (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/set-up-activeactive-ha/configure-activeactive-ha.html

NEW QUESTION: 55
Which Panorama objects restrict administrative access to specific device-groups?
A. templates
B. admin roles
C. access domains
D. authentication profiles
Answer: C (LEAVE A REPLY)
Access domains control administrative access to specific Device Groups and templates, and also control the ability to switch context to the web interface of managed firewalls.
https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/panorama-overview/role-based-access-control/access-domains.html

NEW QUESTION: 56
Refer to the exhibit.

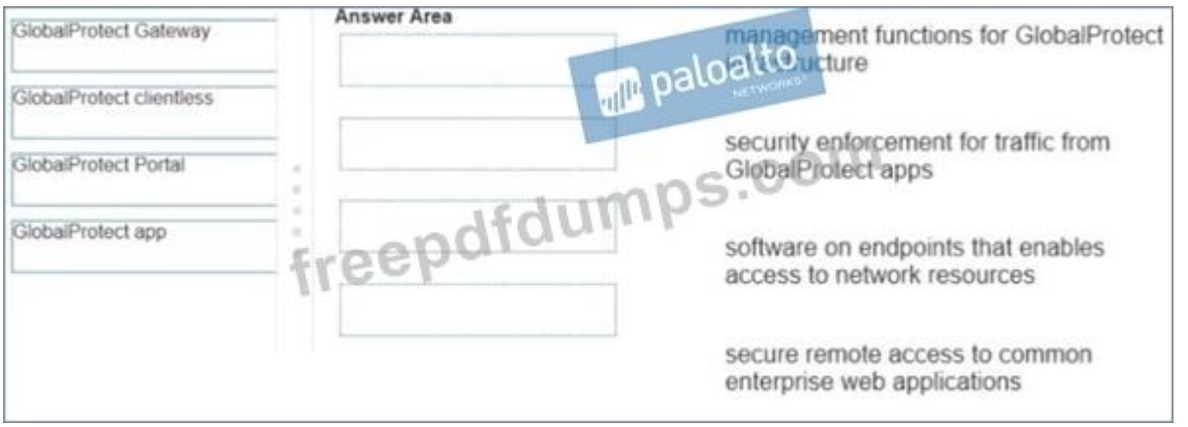


An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) received HTTP traffic and host B(10.1.1.101) receives SSH traffic.
Which two security policy rules will accomplish this configuration? (Choose two)
A. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
B. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
C. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow
D. Untrust (Any) to Untrust (10.1.1.1) Ssh-Allow
Answer: (SHOW ANSWER)

NEW QUESTION: 57
Refer to exhibit.

An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.
How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all existing monitoring platforms?
A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.
B. Any configuration on an M-500 would address the insufficient bandwidth concerns.
C. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.
D. Configure log compression and optimization features on all remote firewalls.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 58
Match each GlobalProtect component to the purpose of that component



Answer:

NEW QUESTION: 59

What are three valid actions in a File Blocking Profile? (Choose three)

A. Forward

B. Block

C. Alret

D. Upload

E. Reset-both

F. Continue

Answer: (SHOW ANSWER)

You can configure a file blocking profile with the following actions:

- Forward - When the specified file type is detected, the file is sent to WildFire for analysis. A log is also generated in the data filtering log.
- Block - When the specified file type is detected, the file is blocked and a customizable block page is presented to the user. A log is also generated in the data filtering log.
- Alert - When the specified file type is detected, a log is generated in the data filtering log.
- Continue - When the specified file type is detected, a customizable response page is presented to the user. The user can click through the page to download the file. A log is also generated in the data filtering log. Because this type of forwarding action requires user interaction, it is only applicable for web traffic.

Continue-and-forward - When the specified file type is detected, a customizable continuation page is presented to the user. The user can click through the page to download the file. If the user clicks through the continue page to download the file, the file is sent to WildFire for analysis. A log is also generated in the data filtering log.
https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/policy/file-blocking-profiles.html

NEW QUESTION: 60
A remote administrator needs firewall access on an untrusted interface Which two components are required on the firewall to configure certificate-based administrator authentication to the web UI? (Choose two)
A. client certificate
B. certificate profile
C. certificate authority (CA) certificate
D. server certificate
Answer: A,B (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface.html

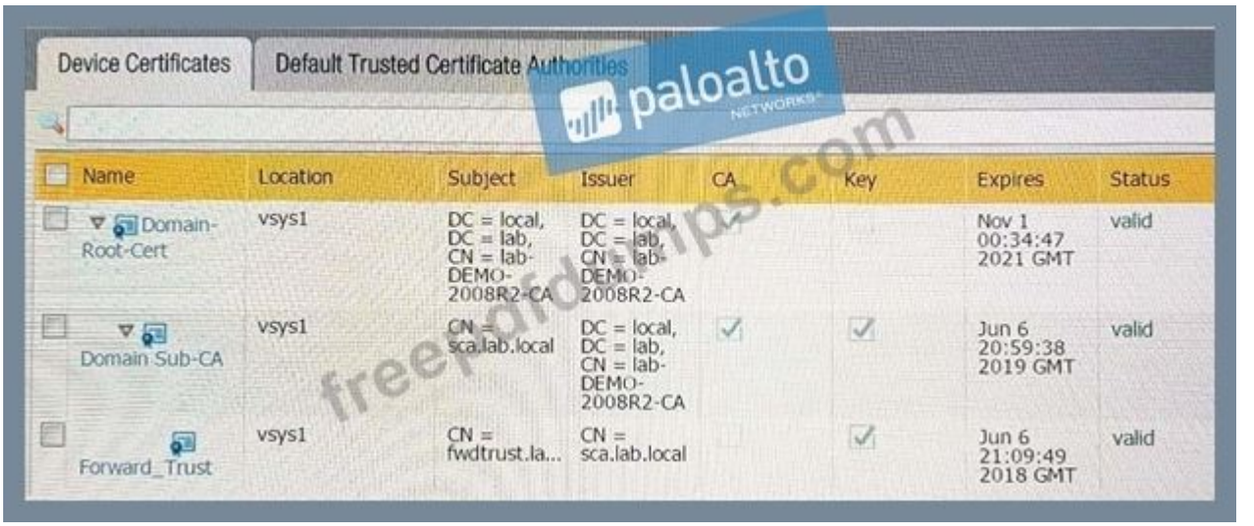
NEW QUESTION: 61
What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?
A. Panorama cannot be reverted to an earlier PAN-OS release if variables are used in templates or template stacks.
B. An administrator must use the Expedition tool to adapt the configuration to the pre-PAN-OS 8.1 state.
C. When Panorama is reverted to an earlier PAN-OS release, variables used in templates or template stacks will be removed automatically.
D. Administrators need to manually update variable characters to those used in pre-PAN-OS 8.1.
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan- os-81/upgradedowngrade-considerations

NEW QUESTION: 62
Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?
A. Session Browser
B. Application Command Center
C. TCP Dump
D. Packet Capture
Answer: (SHOW ANSWER)
Explanation/Reference: https://live.paloaltonetworks.com/t5/Management-Articles/Tips-amp-Tricks-How-to-Use-the- Application-Command-Center-ACC/ta-p/67342

NEW QUESTION: 63
Which event will happen if an administrator uses an Application Override Policy?
A. Threat-ID processing time is decreased.
B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.
C. The application name assigned to the traffic by the security rule is written to the Traffic log.
D. App-ID processing time is increased.
Answer: B (LEAVE A REPLY)
Reference:
https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Override
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/manage-custom-or-unknown-applications#

NEW QUESTION: 64
Which version of GlobalProtect supports split tunneling based on destination domain, client process, and
HTTP/HTTPS video streaming application?
A. GlobalProtect version 4.0 with PAN-OS 8.1
B. GlobalProtect version 4.1 with PAN-OS 8.1
C. GlobalProtect version 4.1 with PAN-OS 8.0
D. GlobalProtect version 4.0 with PAN-OS 8.0
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/41/globalprotect/globalprotect-app-new-features/new-features-released-in-gp-agent-4_1/split-tunnel-for-public-applications

NEW QUESTION: 65
Refer to the exhibit.

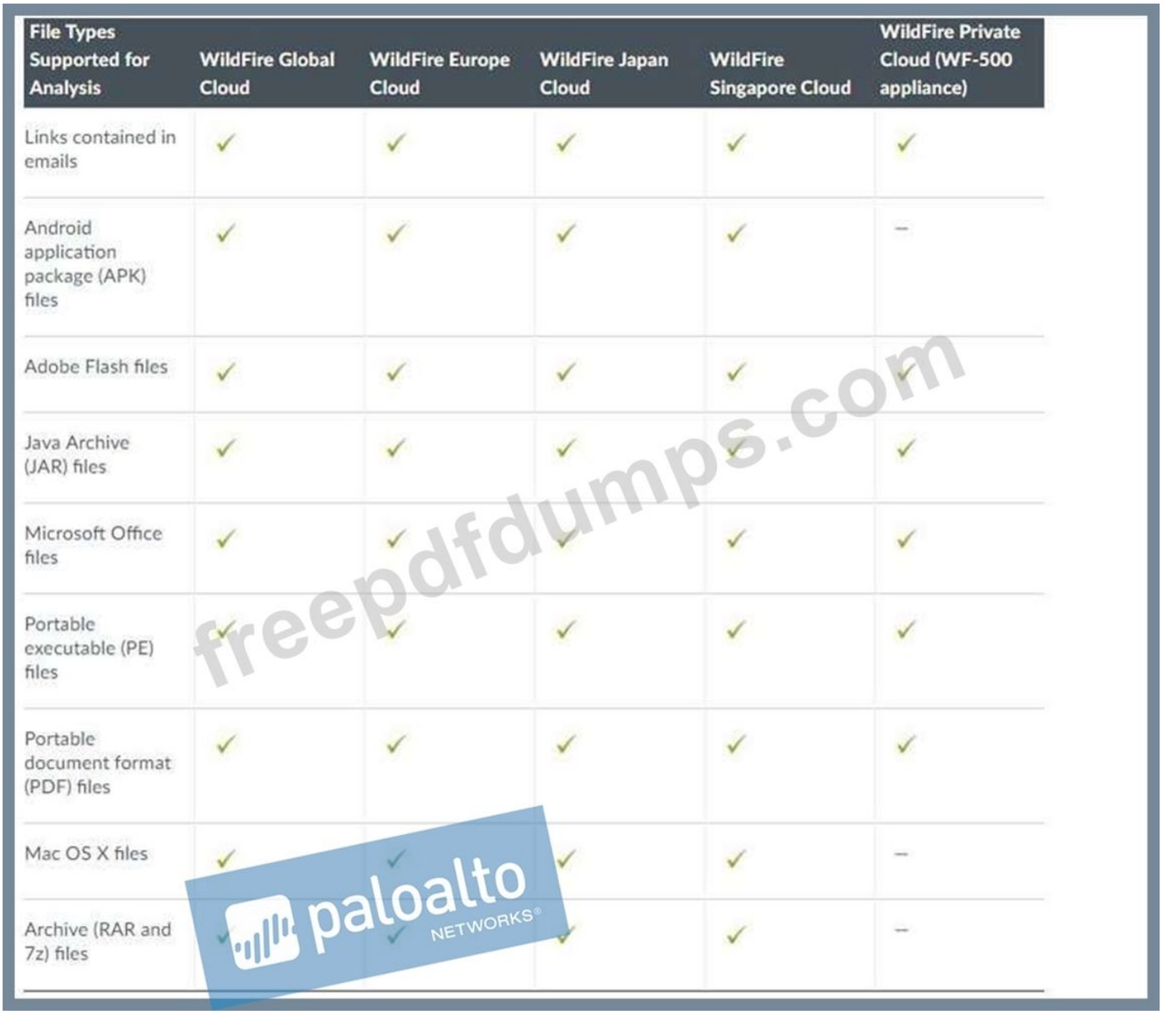


Which certificates can be used as a Forwarded Trust certificate?
A. Domain-Root-Cert
B. Domain Sub-CA
C. Certificate from Default Trust Certificate Authorities
D. Forward_Trust
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?
A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096 in the "Tag Allowed" field of the V-Wire object.
B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the Tag Allowed" field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each iinterface/sub interface to a unique zone.
C. Create Layer 3 subinterfaces that are each assigned tA. single VLAN ID and a common virtual router.
The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface tA.
unique zone. Do not assign any interface an IP address.
D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/sub interface to a unique zone.
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfa Virtual wire interfaces by default allow all untagged traffic. You can,

however, use a virtual wire to connect two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags.
VLAN tag 0 indicates untagged traffic.You can also create multiple subinterfaces, add them into different zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.

NEW QUESTION: 67
Which three options does the WF-500 appliance support for local analysis? (Choose three)
A. E-mail links
B. APK files
C. jar files
D. PNG files
E. Portable Executable (PE) files
Answer: A,C,E (LEAVE A REPLY)



File Types Supported for Analysis	WildFire Global Cloud	WildFire Europe Cloud	WildFire Japan Cloud	WildFire Singapore Cloud	WildFire Private Cloud (WF-500 appliance)
Links contained in emails	✓	✓	✓	✓	✓
Android application package (APK) files	✓	✓	✓	✓	–
Adobe Flash files	✓	✓	✓	✓	✓
Java Archive (JAR) files	✓	✓	✓	✓	✓
Microsoft Office files	✓	✓	✓	✓	✓
Portable executable (PE) files	✓	✓	✓	✓	✓
Portable document format (PDF) files	✓	✓	✓	✓	✓
Mac OS X files	✓	✓	✓	✓	–
Archive (RAR and 7z) files	✓	✓	✓	✓	–

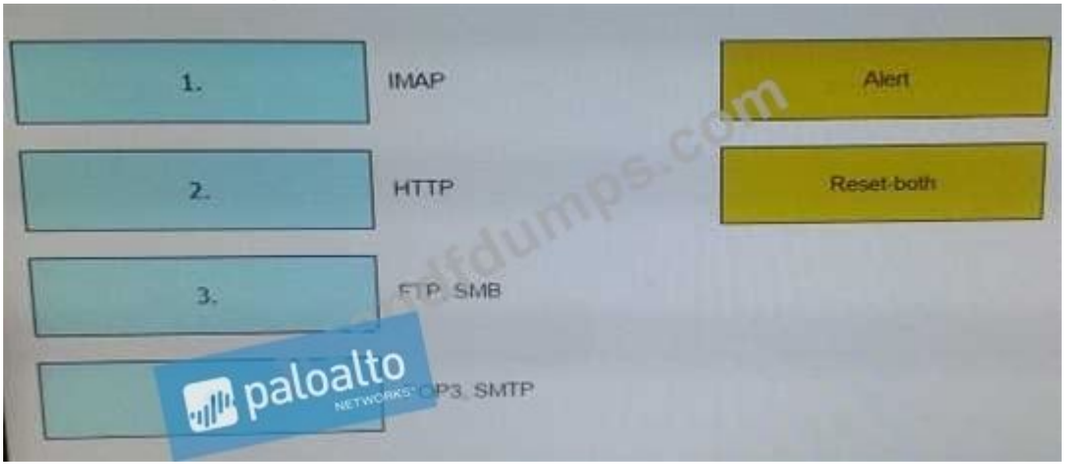
NEW QUESTION: 68

DRAG DROP

When using the predefined default profile, the policy will inspect for viruses on the decoders.

Match each decoder with its default action.

Answer options may be used more than once or not at all.



Answer:

IMAP , POP3 , SMTP -> Alert
HTTP,FTP,SMB -> Reset-both

NEW QUESTION: 69

The certificate information displayed in the following image is for which type of certificate?

Exhibit:

A. Public CA signed certificate

B. Web Server certificate

C. Self-Signed Root CA certificate

D. Forward Trust certificate
Answer: C (LEAVE A REPLY)

NEW QUESTION: 70
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?
A. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
B. Use the debug dataplane packet-diag set capture stage management file command.
C. Use the topdump command.
D. Use the debug dataplane packet-diag set capture stage firewall file command.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 71
A prospect is eager to conduct a Security Lifecycle Review (SLR) with the aid of the Palo Alto Networks NGFW.
Which interface type is best suited to provide the raw data for an SLR from the network in a way that is minimally invasive?
A. Layer 3
B. Tap
C. Layer 2
D. Virtual Wire
Answer: (SHOW ANSWER)

NEW QUESTION: 72
Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)
A. HA1 IP Address
B. Network Interface Type
C. Zone Protection Profile
D. Master Key
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 73
A organizations administrator has the funds available to purchase more firewalls to increase the organization's security posture.
The partner SE recommends placing the firewalls as close as possible to the resources that they protect Is the SE's advice correct and why or why not?
A. Yes Firewalls are session based so they do not scale to millions of CPS
B. No Placing firewalls m front of perimeter DDoS devices provides greater protection tor sensitive devices inside the network

C. Yes Zone Protection profiles can be tailored to the resources that they protect via the configuration of specific device types and operating systems
D. No Firewalls provide new defense and resilience to prevent attackers at every stage of the cyberattack lifecycle independent of placement
Answer: A (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/f

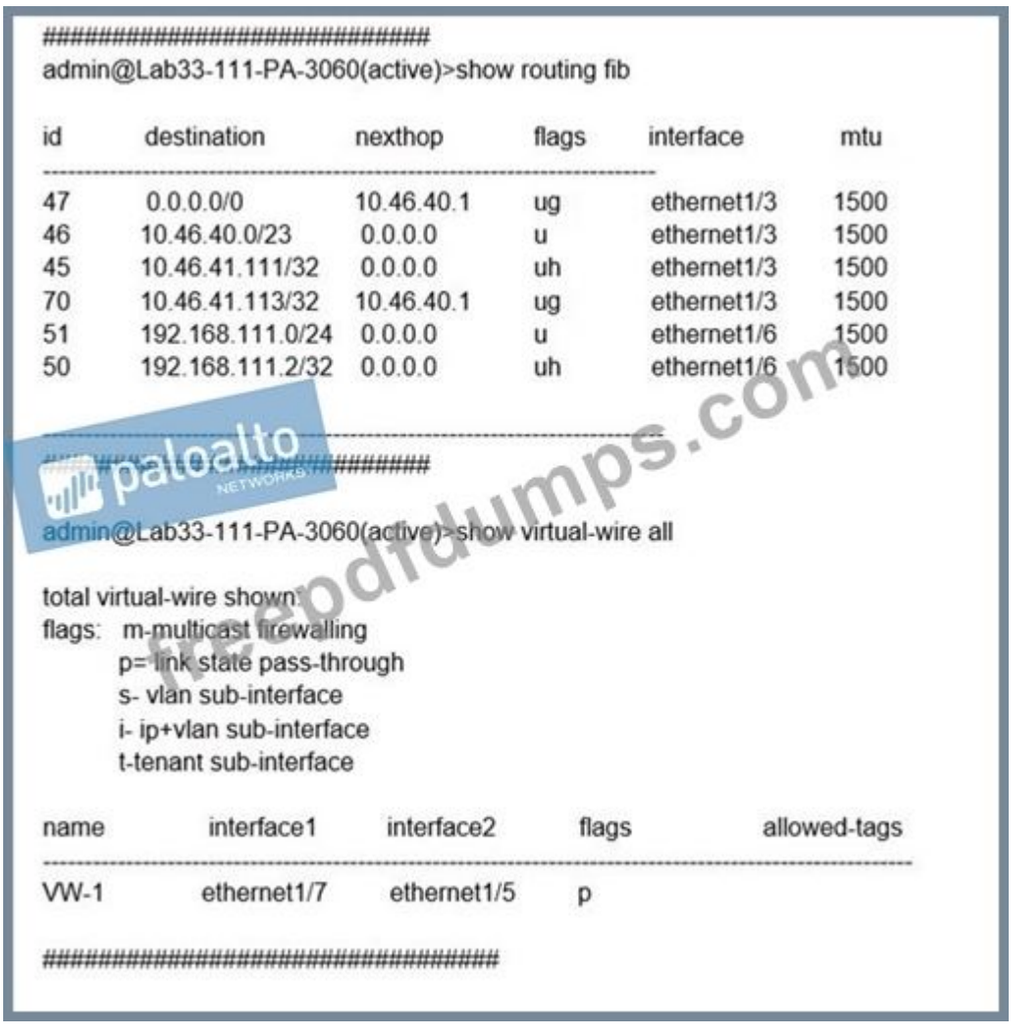
NEW QUESTION: 74
What must be used in Security Policy Rule that contain addresses where NAT policy applies?
A. Post-Nat addresses and Pre-NAT zones
B. Pre-NAT addresse and Pre-NAT zones
C. Post-NAT addresse and Post-Nat zones
D. Pre-NAT addresse and Post-Nat zones
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which Zone Pair and Rule Type will allow a successful connection for a user on the internet zone to a web server hosted in the DMZ zone? The web server is reachable using a destination Nat policy in the Palo Alto Networks firewall.
A. Zone Pair:
Source Zone: Internet
Destination Zone: DMZ
Rule Type:
"intrazone"
B. Zone Pair:
Source Zone: Internet
Destination Zone: DMZ
Rule Type:
"intrazone" or "universal"
C. Zone Pair:
Source Zone: Internet
Destination Zone: Internet
Rule Type:
"intrazone" or "universal"
D. Zone Pair:
Source Zone: Internet
Destination Zone: Internet
Rule Type:
"intrazone"

Answer: B (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zo
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

NEW QUESTION: 76
An administrator wants to upgrade an NGFW from PAN-OS 9.0 to PAN-OS 10.0. The firewall is not a part of an HA pair. What needs to be updated first?
A. XML Agent
B. Applications and Threats
C. WildFire
D. PAN-OS Upgrade Agent
Answer: B (LEAVE A REPLY)
https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-the-firewall-to-pan-os-80/upgrade-a-firewall-to-pan-os-80

NEW QUESTION: 77
Refer to the exhibit.



```
##################################
admin@Lab33-111-PA-3060(active)>show routing fib

id      destination      nexthop      flags   interface      mtu
--------------------------------------------------------------------------
47      0.0.0.0/0        10.46.40.1   ug      ethernet1/3    1500
46      10.46.40.0/23    0.0.0.0      u       ethernet1/3    1500
45      10.46.41.111/32  0.0.0.0      uh      ethernet1/3    1500
70      10.46.41.113/32  10.46.40.1   ug      ethernet1/3    1500
51      192.168.111.0/24 0.0.0.0      u       ethernet1/6    1500
50      192.168.111.2/32 0.0.0.0      uh      ethernet1/6    1500

--------------------------------------------------------------------------
##################################
admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p=link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name          interface1      interface2      flags          allowed-tags
--------------------------------------------------------------------------------
VW-1          ethernet1/7     ethernet1/5     p

##################################
```


Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

A. ethernet1/5

B. ethernet1/7

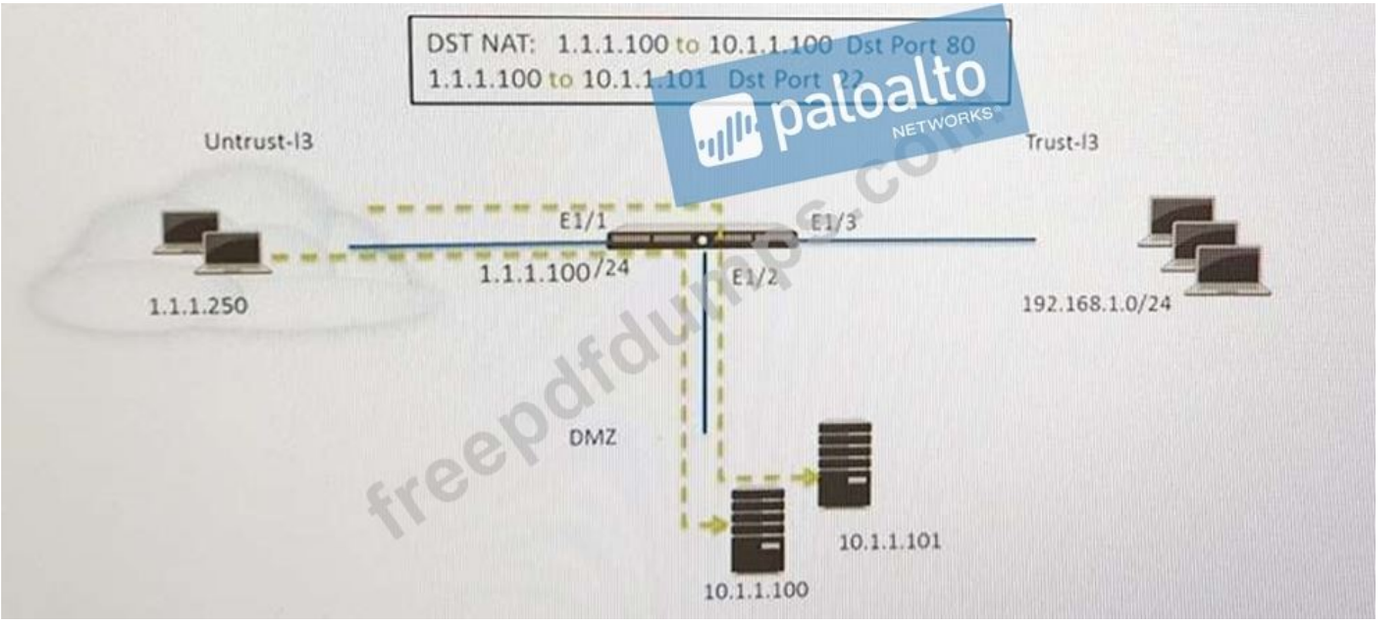
C. ethernet1/3

D. ethernet1/6

Answer: A (LEAVE A REPLY)

NEW QUESTION: 78

Refer to the exhibit.



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and HOST B (10.1.1.101) receives SSH traffic.) Which two security policy rules will accomplish this configuration? (Choose two.)

A. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow

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

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

D. Untrust (Any) to Untrust (10.1.1.1), SSH -Allow

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

Answer: (SHOW ANSWER)

https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-many-mapping#

NEW QUESTION: 79

O: 49

A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers.

Which option will protect the individual servers?

A. Enable packet buffer protection on the Zone Protection Profile.

B. Apply an Anti-Spyware Profile with DNS sinkholing.

C. Use the DNS App-ID with application-default.

D. Apply a classified DoS Protection Profile.

Answer: D (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/do To protect critical web or DNS servers on your network, protect the individual servers. To do this, set appropriate flooding and resource protection thresholds in a

DoS protection profile, and create a DoS protection policy rule that applies the profile to each server's IP address by adding the IP addresses as the rule's destination criteria.

NEW QUESTION: 80
Which three items are import considerations during SD-WAN configuration planning? (Choose three.)
A. link requirements
B. the name of the ISP
C. IP Addresses
D. branch and hub locations
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration

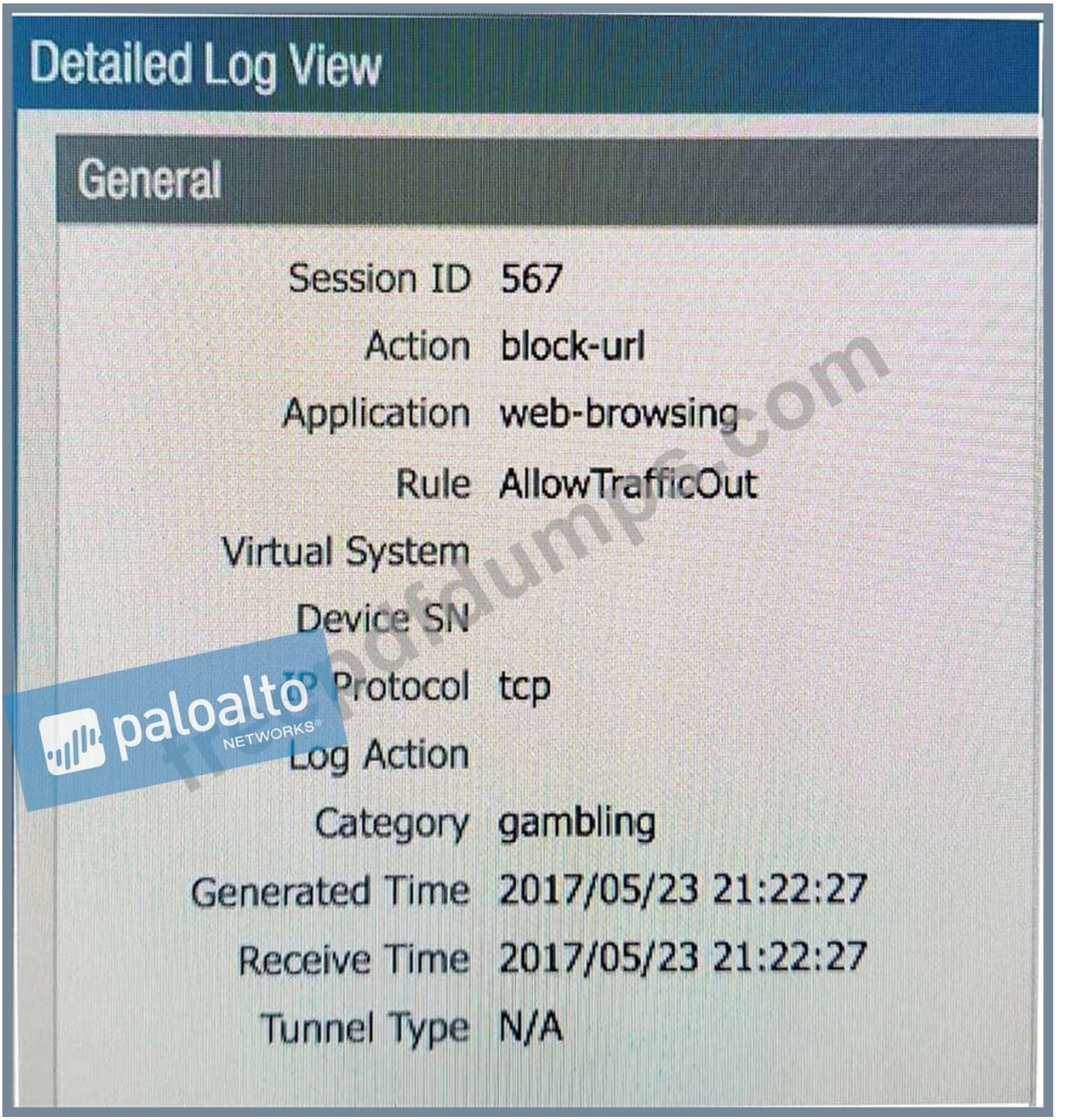
NEW QUESTION: 81
A distributed log collection deployment has dedicated log Collectors. A developer needs a device to send logs to Panorama instead of sending logs to the Collector Group.
What should be done first?
A. Revert to a previous configuration
B. Remove the cable from the management interface, reload the log Collector and then re-connect that cable
C. remove the device from the Collector Group
D. Contact Palo Alto Networks Support team to enter kernel mode commands to allow adjustments
Answer: C (LEAVE A REPLY)

NEW QUESTION: 82
Which GlobalProtect Client connect method requires the distribution and use of machine certificates?
A. User-logon (Always on)
B. At-boot
C. On-demand
D. Pre-logon
Answer: D (LEAVE A REPLY)
Client certificate refers to user cert, it can be used for 'user-logon'/'on-demand' connect methods. Used to authenticate a user. -Machine certificate refers to device cert, it can be used for 'pre-logon' connect method. This is used to authenticate a device, not a user.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFoCAK

NEW QUESTION: 83

An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image. Which configuration change should the administrator make?

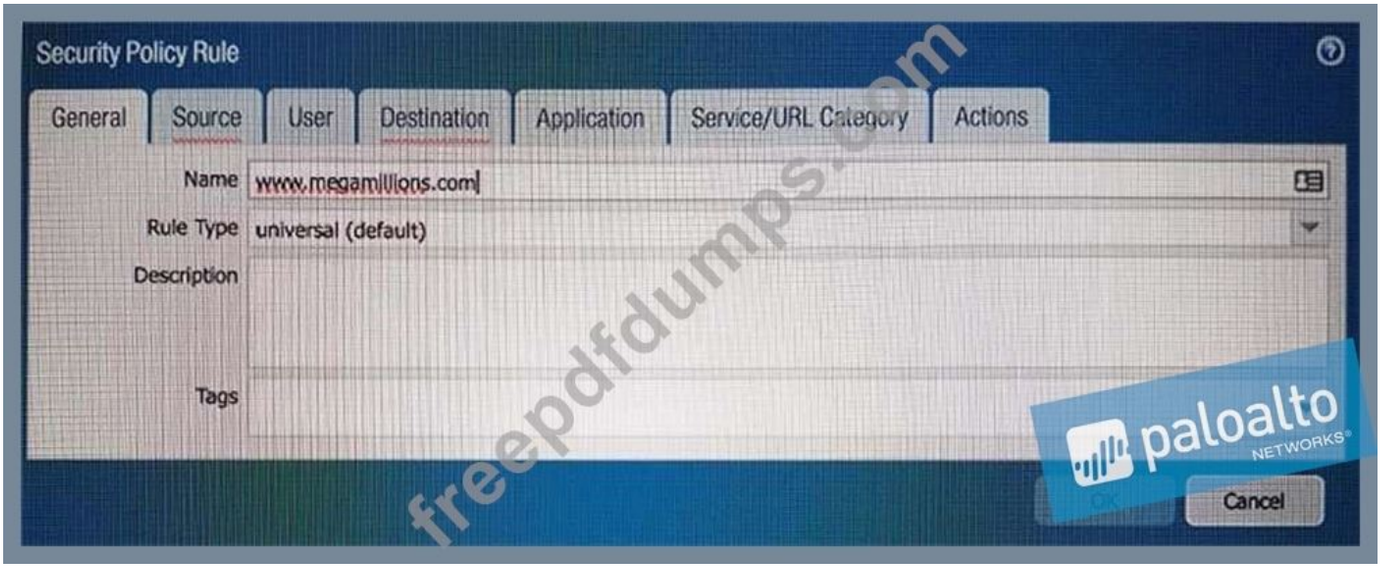
A:



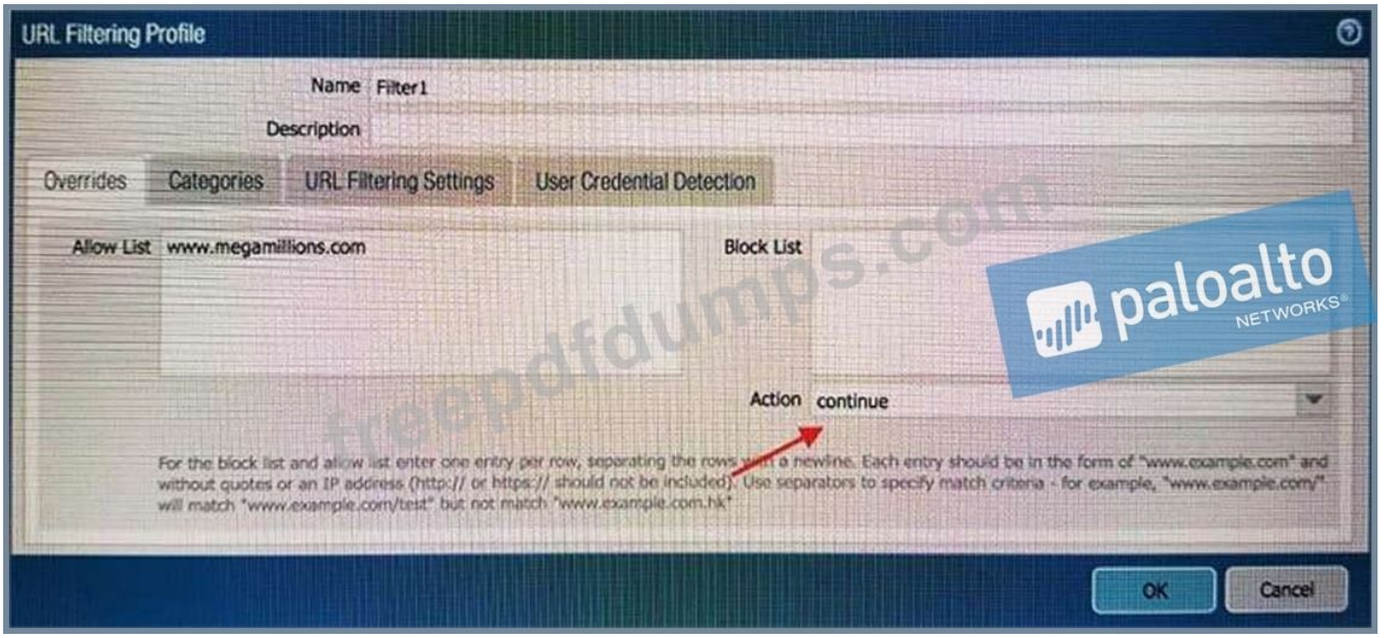
B:


URL Filtering Profile
Name Filter1
Description
Overrides
Categories
URL Filtering Settings
65 items
Category
Site Access
User Credential Submission
educational-institutions
entertainment-and-arts
extremism
financial-services
gambling
games
government
hacking
health-and-medicine
home-and-garden
hunting-and-fishing
allow
block
alert
allow
block
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category
OK
Cancel
paloalto NETWORKS
freepdfdumps.com

C:


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Name www.megamillions.com
Rule Type universal (default)
Description
Tags
Cancel
paloalto NETWORKS
freepdfdumps.com

D:



E:

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

NEW QUESTION: 84
Which User-ID method should be configured to map IP addresses to username for users connected through a terminal server?
A. port mapping
B. server monitoring
C. client probing

D. XFF headers

Answer: (SHOW ANSWER)

Explanation

https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/user-id/map-ip-addresses-to-users/configur e-user-mapping-for-terminal-server-users

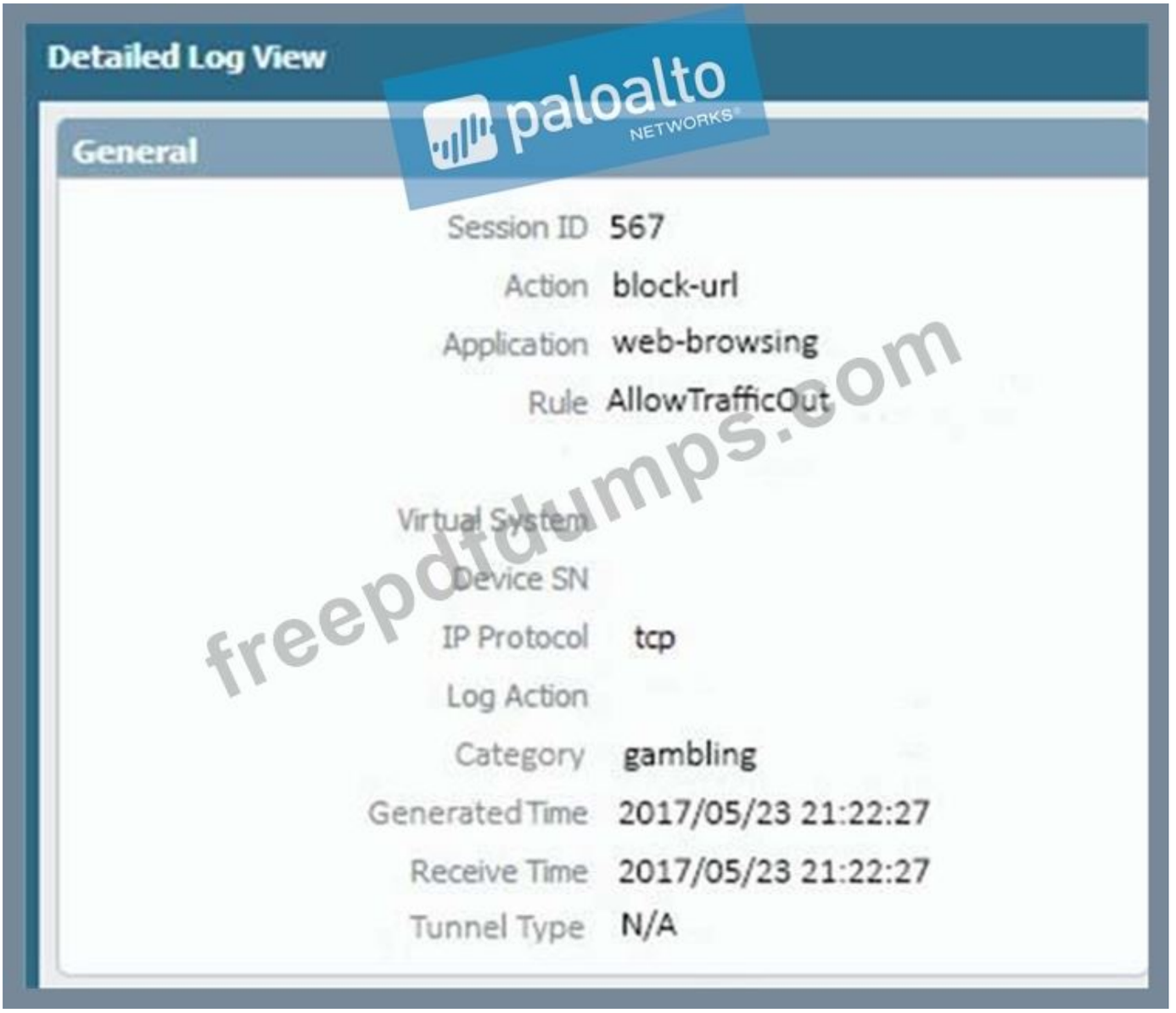
NEW QUESTION: 85

An administrator needs to determine why users on the trust zone cannot reach certain websites. The only

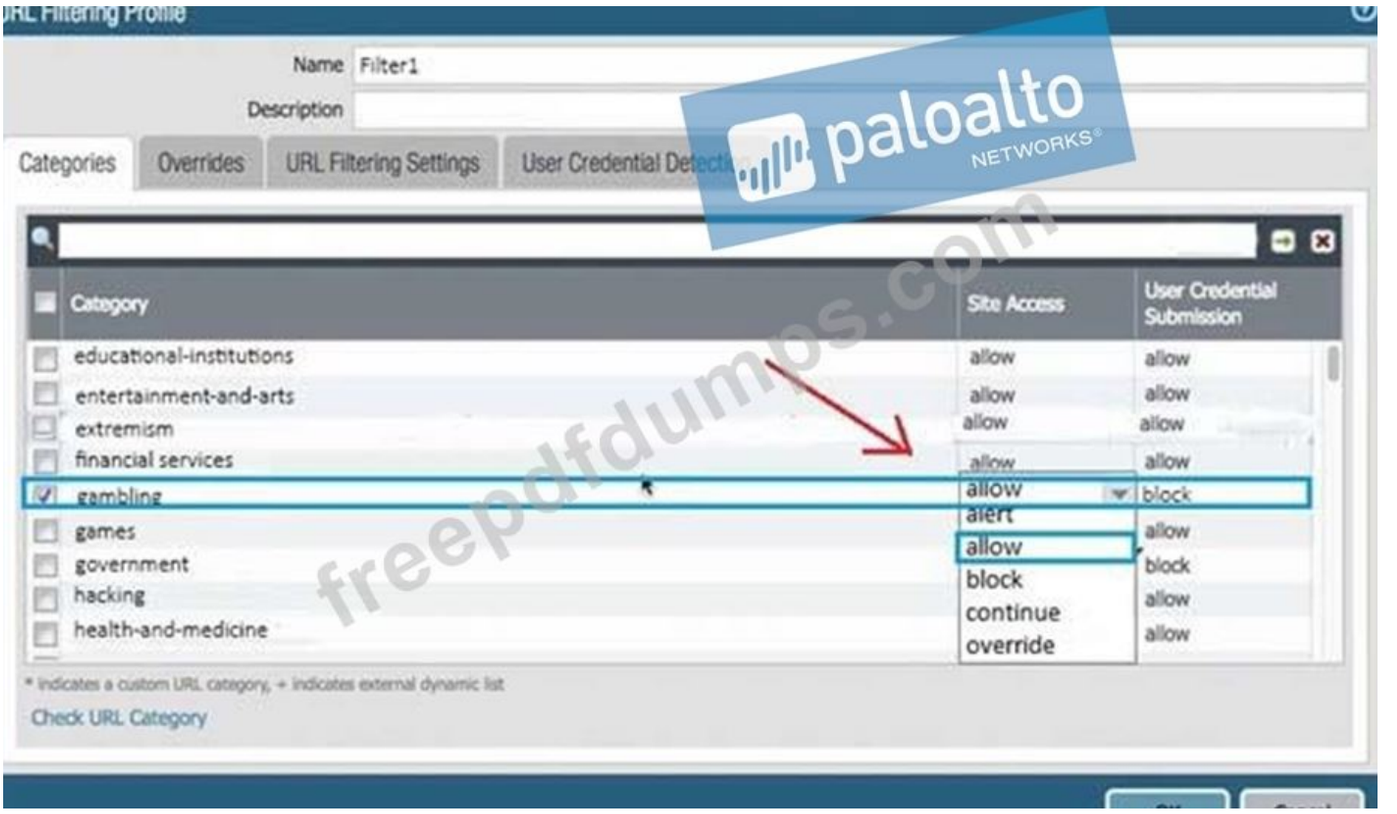
information available is shown on the following image.

Which configuration change should the administrator make?

A:



B:

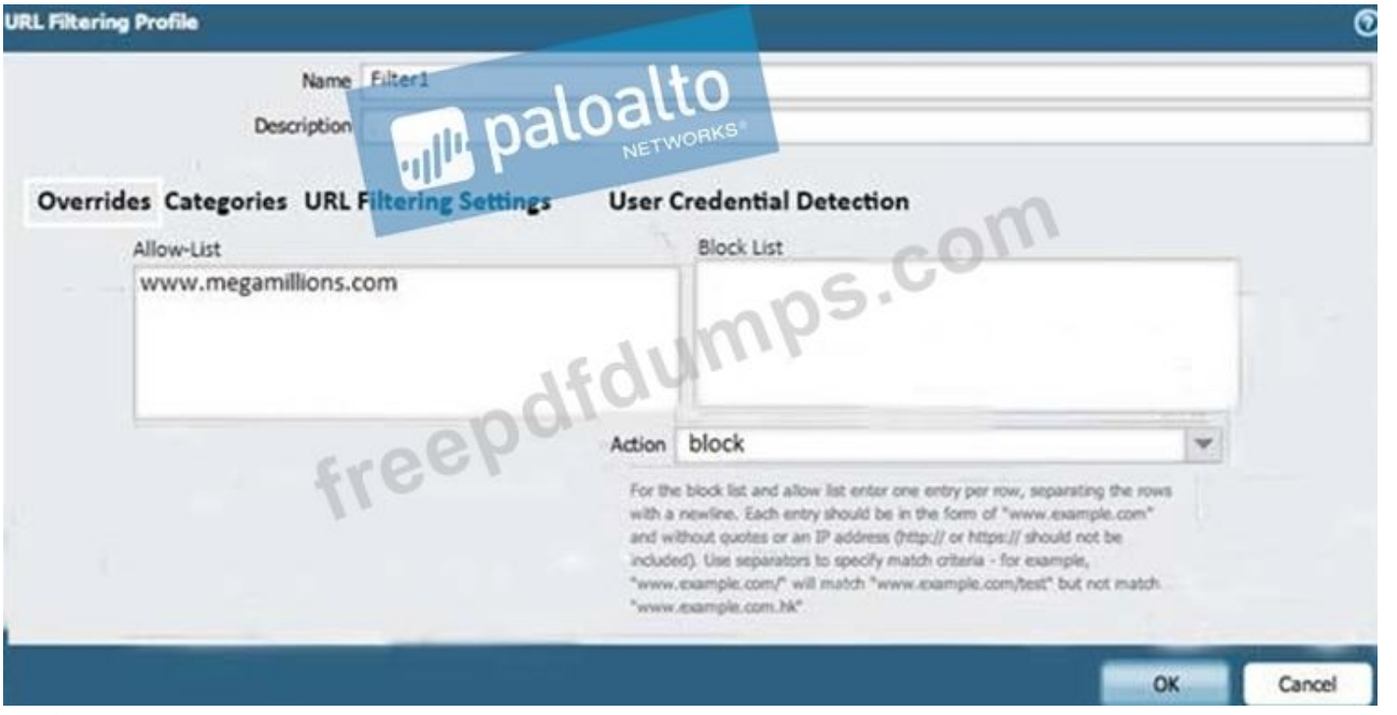

URL Filtering Profile
Name Filter1
Description
Categories
Overrides
URL Filtering Settings
User Credential Detection
Category
Site Access
User Credential Submission
educational-institutions
entertainment-and-arts
extremism
financial services
gambling
games
government
hacking
health-and-medicine
allow
block
alert
allow
block
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category
paloalto NETWORKS
freepdfdumps.com

C:


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Target
Name www.megamillions.com
Rule Type universal (default)
Description
Tags
OK
Cancel
paloalto NETWORKS
freepdfdumps.com

D:

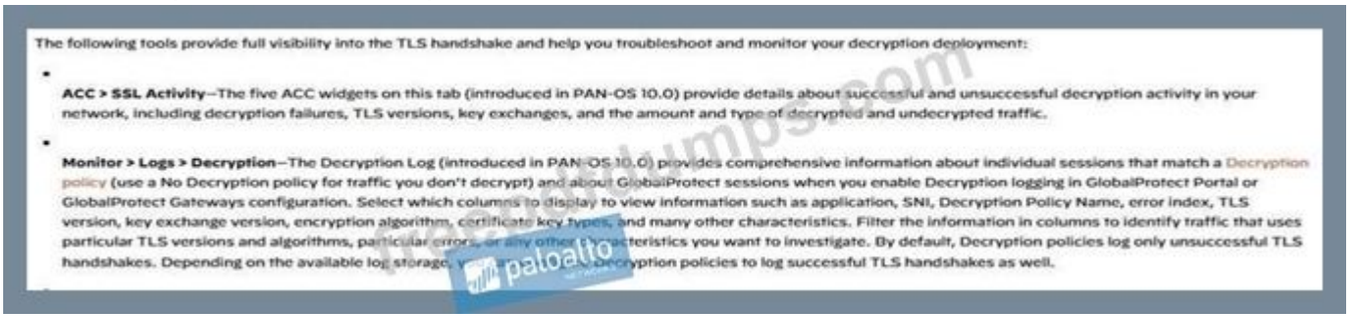
E:



A. Option E
B. Option D
C. Option A
D. Option B
E. Option C
Answer: (SHOW ANSWER)

NEW QUESTION: 86
Which CLI command displays the physical media that are connected to ethernetl/8?
A. > show system state filter-pretty sys.si.p8.med
B. > show system state filter-pretty sys.sl.p8.phy
C. > show interface ethernetl/8
D. > show system state filter-pretty sys.si.p8.stats
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port.
Which log entry can the administrator use to verify that sessions are being decrypted?
A. In the details of the Traffic log entries
B. Decryption log
C. Data Filtering log
D. In the details of the Threat log entries
Answer: B (LEAVE A REPLY)



https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/troubleshoot-and-monitor-decryption.html#ida09e44a8-fd80-41e8-8572-33e9b122ad22

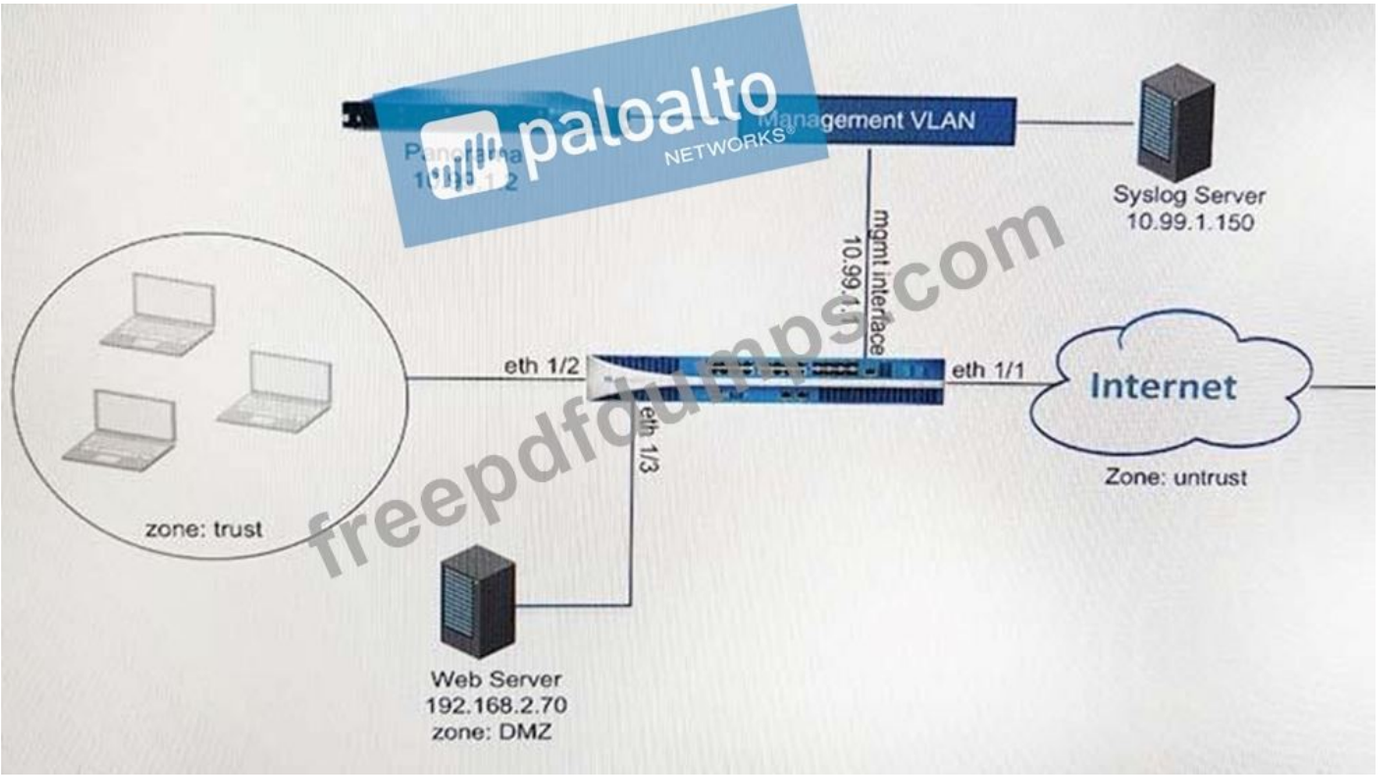
NEW QUESTION: 88
What are three valid actions in a File Blocking Profile? (Choose three)
A. Forward
B. Block
C. Alret
D. Upload
E. Reset-both
F. Continue
Answer: A,B,C (LEAVE A REPLY)
https://live.paloaltonetworksHYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623".com/t5/Configuration-ArticHYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623"les/File-Blocking-RulebHYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623"ase-and-Action-Precedence/ta-p/53623

NEW QUESTION: 89
To protect your firewall and network from single source denial of service (DoS) attacks that can overwhelm its packet buffer and cause legitimate traffic to drop, you can configure.
A. BGP (Border Gateway Protocol)
B. PGP (Packet Gateway Protocol)

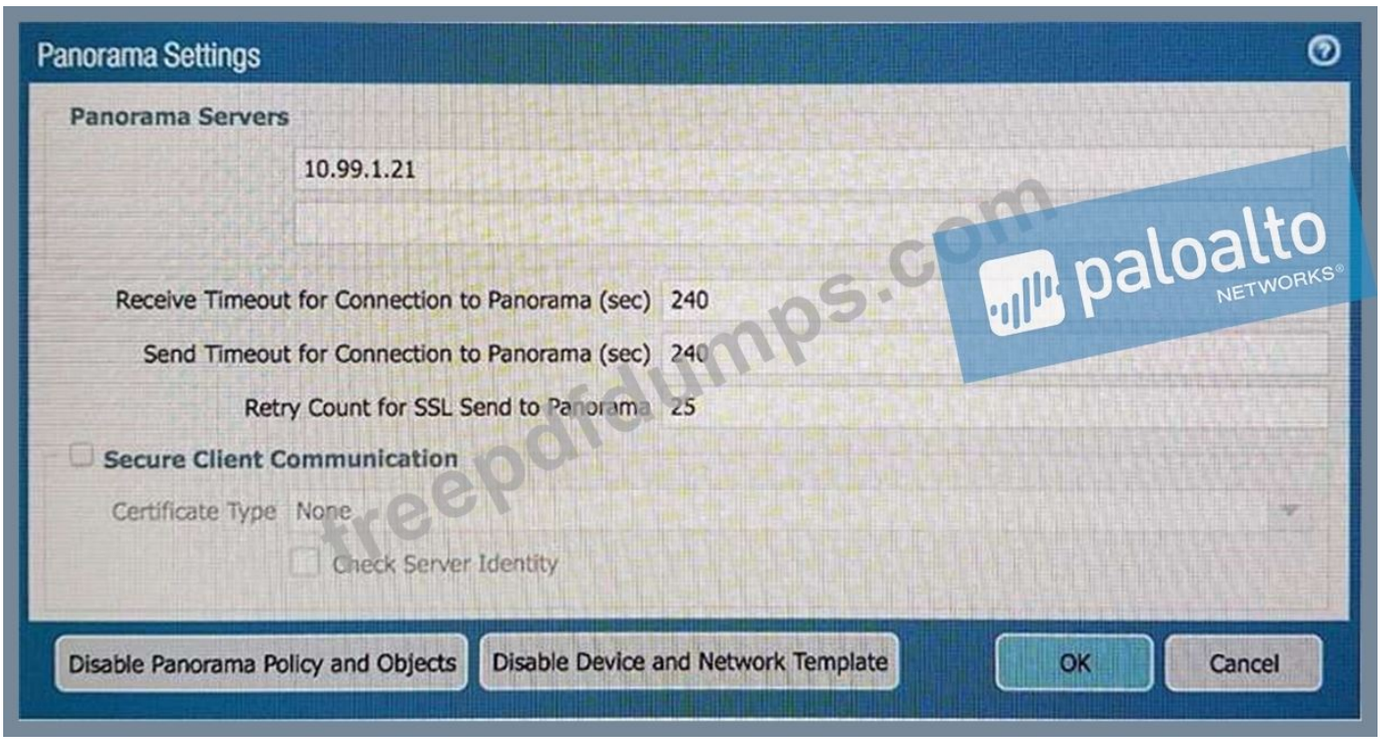
C. PBP (Protocol Based Protection)
D. PBP (Packet Buffer Protection)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
ESTION NO: 86
Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)
A. The firewall is in multi-vsys mode.
B. The traffic is offloaded.
C. The traffic does not match the packet capture filter.
D. The firewall's DP CPU is higher than 50%.
Answer: (SHOW ANSWER)
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-ha offload

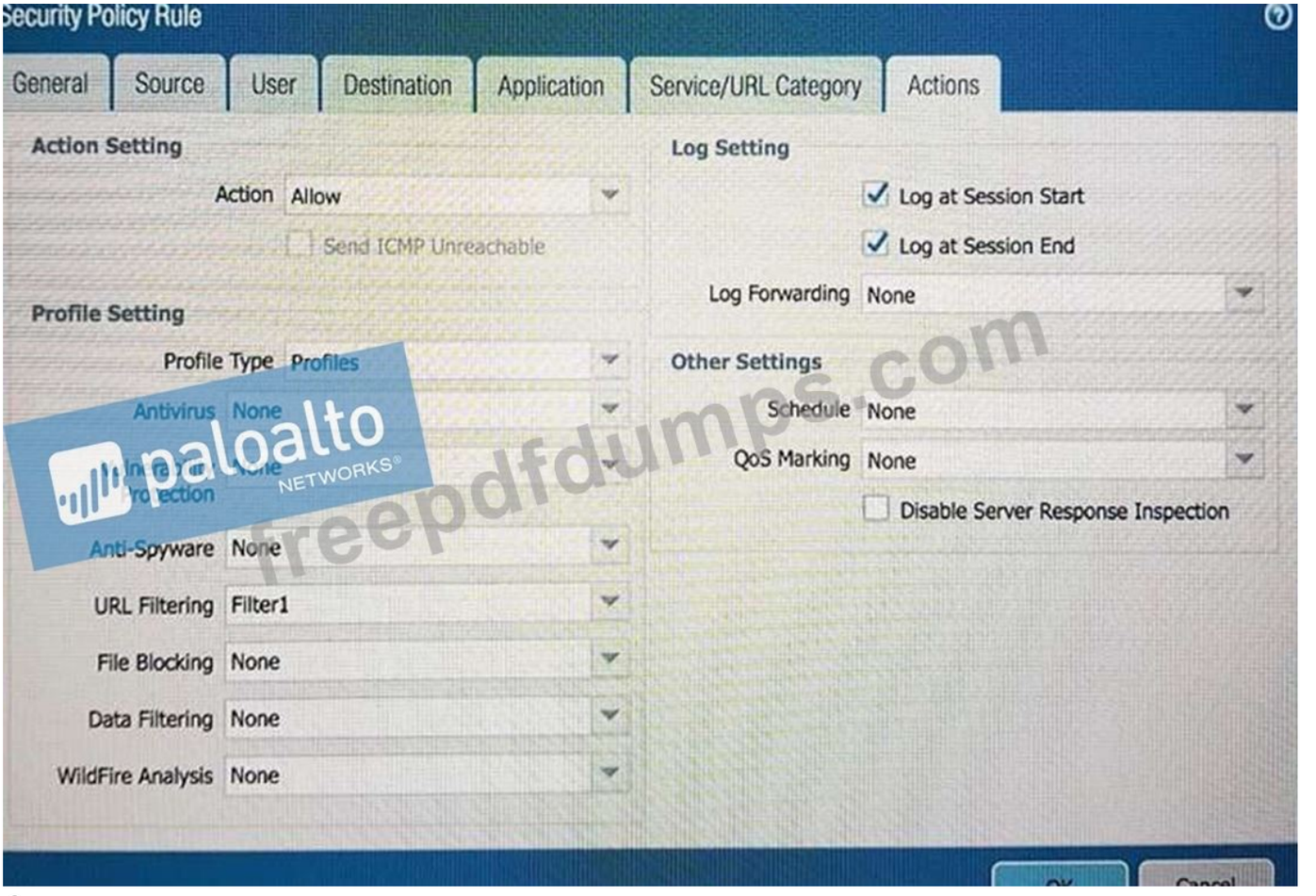
NEW QUESTION: 91
Refer to the exhibit.



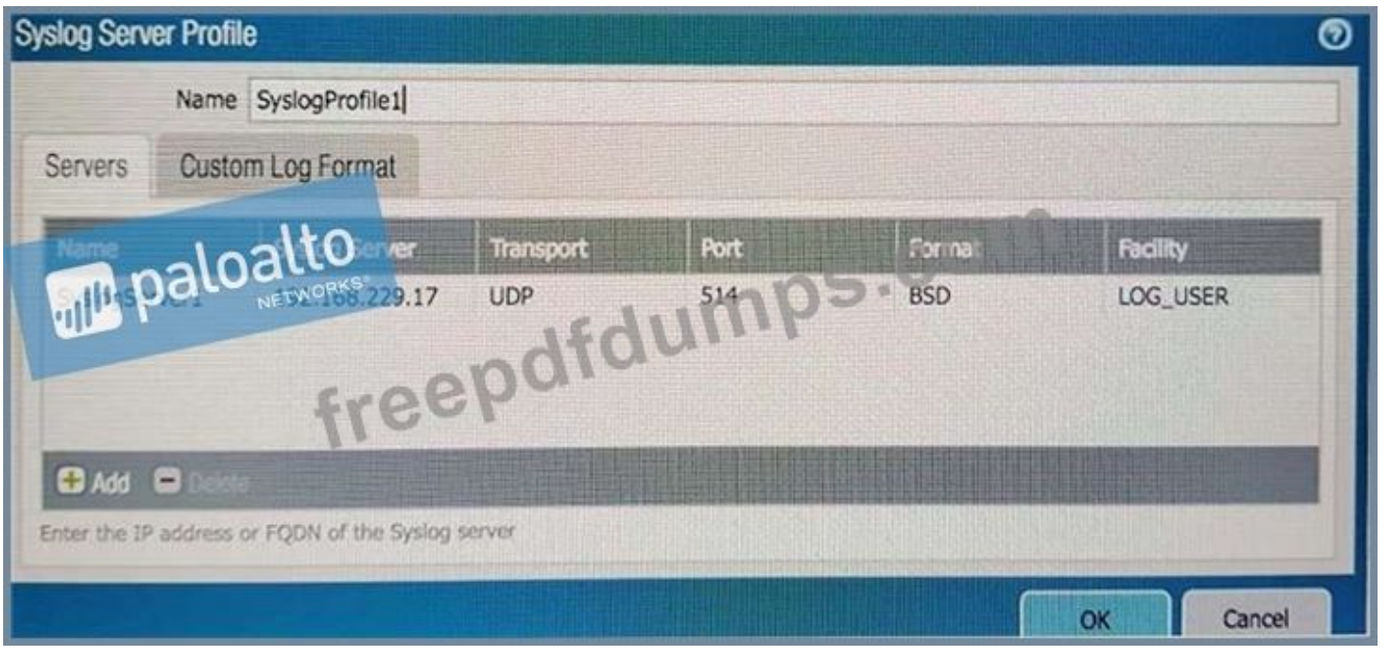
An administrator cannot see any if the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side. Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?
A:


Panorama Settings
Panorama Servers
10.99.1.21
Receive Timeout for Connection to Panorama (sec) 240
Send Timeout for Connection to Panorama (sec) 240
Retry Count for SSL Send to Panorama 25
Secure Client Communication
Certificate Type None
Check Server Identity
Disable Panorama Policy and Objects
Disable Device and Network Template
OK
Cancel

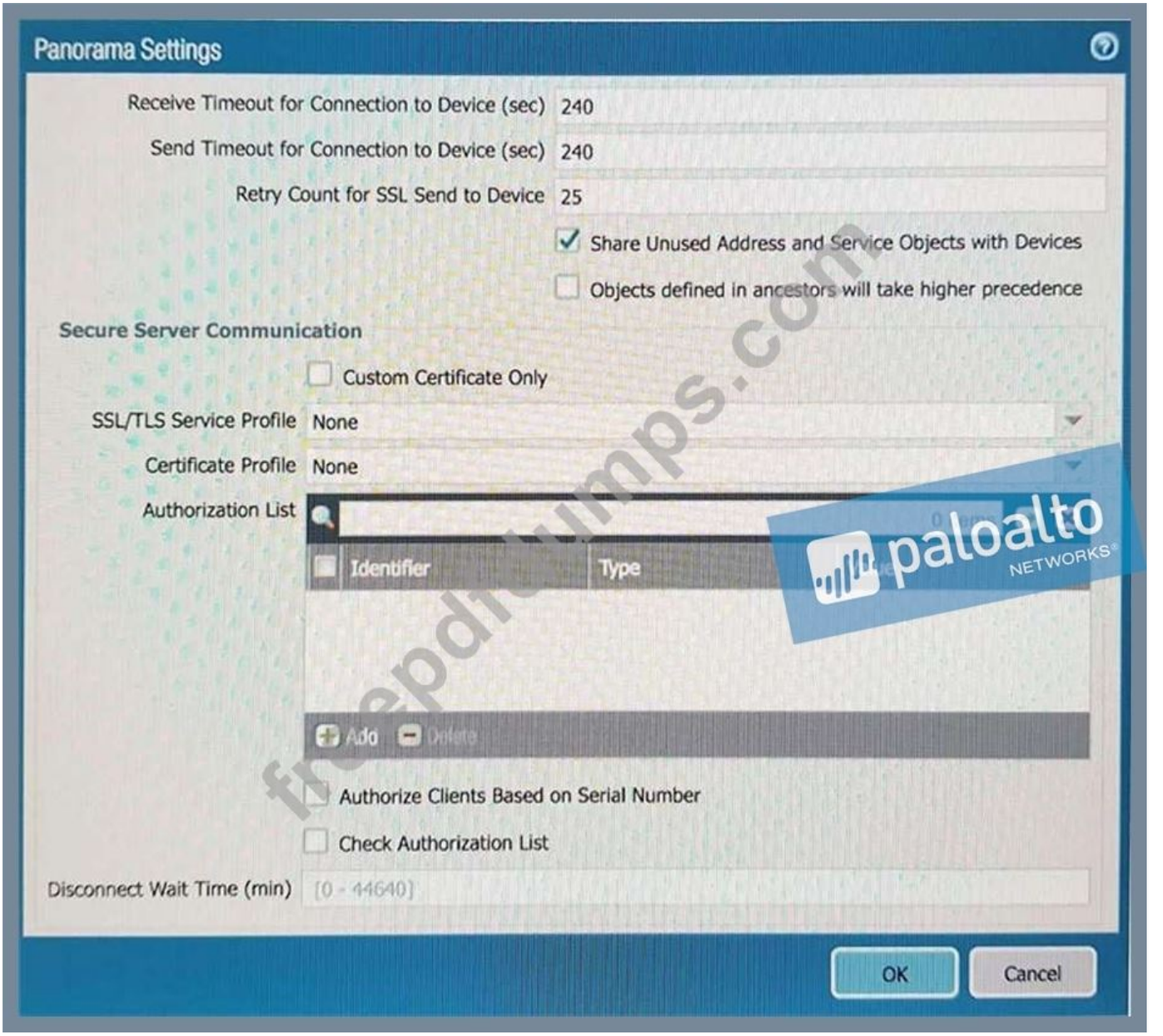
B:


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Action Setting
Action Allow
Send ICMP Unreachable
Profile Setting
Profile Type Profiles
Antivirus None
Anti-Spyware None
URL Filtering Filter1
File Blocking None
Data Filtering None
WildFire Analysis None
Log Setting
Log at Session Start
Log at Session End
Log Forwarding None
Other Settings
Schedule None
QoS Marking None
Disable Server Response Inspection

C:


Syslog Server Profile
Name SyslogProfile1
Servers
Custom Log Format
Name
Server
Transport
Port
Format
Facility
UDP
514
BSD
LOG_USER
Add
Delete
Enter the IP address or FQDN of the Syslog server
OK
Cancel

D:

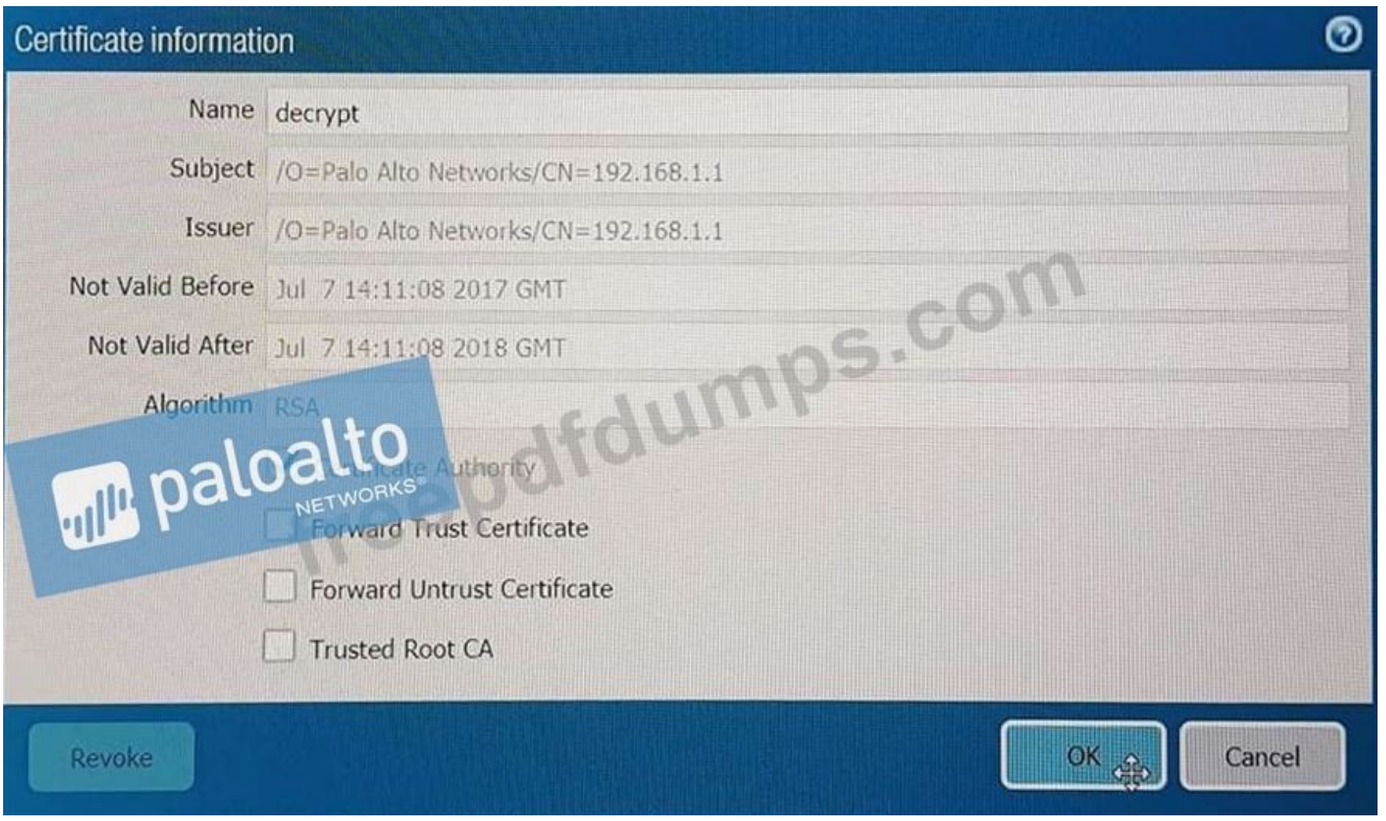

Panorama Settings
Receive Timeout for Connection to Device (sec) 240
Send Timeout for Connection to Device (sec) 240
Retry Count for SSL Send to Device 25
Share Unused Address and Service Objects with Devices
Objects defined in ancestors will take higher precedence
Secure Server Communication
Custom Certificate Only
SSL/TLS Service Profile None
Certificate Profile None
Authorization List
Identifier
Type
Add
Delete
Authorize Clients Based on Serial Number
Check Authorization List
Disconnect Wait Time (min) [0 - 44640]
OK
Cancel

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

NEW QUESTION: 92
View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?
A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.
Answer: (SHOW ANSWER)
Reference:
https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-por the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations

NEW QUESTION: 93
The certificate information displayed in the following image is for which type of certificate?
Exhibit:



A. Forward Trust certificate
B. Public CA signed certificate
C. Self-Signed Root CA certificate
D. Web Server certificate
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
Which three authentication services can administrator use to authenticate admins into the Palo Alto Networks NGFW without defining a corresponding admin account on the local firewall? (Choose three.)
A. Kerberos
B. PAP
C. SAML
D. TACACS+
E. RADIUS
F. LDAP
Answer: A,C,F (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication
The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall. For details, see:

Configure SAML Authentication Configure TACACS+ Authentication Configure RADIUS Authentication

NEW QUESTION: 95
As a best practice, which URL category should you target first for SSL decryption?
A. Online Storage and Backup
B. High Risk
C. Health and Medicine
D. Financial Services
Answer: B (LEAVE A REPLY)
https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment.html Phase in decryption. Plan to decrypt the riskiest traffic first (URL Categories most likely to harbor malicious traffic, such as gaming or high-risk)

NEW QUESTION: 96
Which Panorama administrator types require the configuration of at least one access domain? (Choose two.)
A. Dynamic
B. Template Admin
C. Device Group
D. Custom Panorama Admin
E. Role Based
Answer: (SHOW ANSWER)

NEW QUESTION: 97
Based on the following image,

what is the correct path of root, intermediate, and end-user certificate?

A. VeriSign > Symantec > Palo Alto Networks

B. Symantec > VeriSign > Palo Alto Networks

C. VeriSign > Palo Alto Networks > Symantec

D. Palo Alto Networks > Symantec > VeriSign

Answer: B (LEAVE A REPLY)

NEW QUESTION: 98

Which CLI command displays the current management plane memory utilization?

A. > show system info

B. > show system resources

C. > show running resource-monitor

D. > debug management-server show

Answer: B (LEAVE A REPLY)

When running show system resources from the PAN-OS CLI, the top process in the output shows 9999% CPU utilization.

The following is an example output:

> show system resources

```
top - 09:41:01 up 11 days, 14:40,  2 users, load average: 0.00, 0.00, 0.00
Tasks: 138 total,   3 running, 134 sleeping,   0 stopped,   1 zombie
Cpu(s):  0.2%us,  0.1%sy, 0.0%ni, 99.7%id,  0.0%wa,  0.0%hi, 0.0%si,  0.0%st
Mem:   4055392k total,  3643912k used,   411480k free,   366956k buffers
Swap:  2007992k total,        0k used,  2007992k free,  2840368k cached
  PID USER      PR NI  VIRT  RES SHR S %CPU %MEM    TIME+  COMMAND
2359 root      20  0  430m 251m 6068 S 9999 25.9   4:57.37 mgmtsrvr
    1 root      20  0  1772  560 492 S    0  0.0   47:29.14 init
    2 root      20  0     0    0   0 S    0  0.0   0:00.00 kthreadd
    3 root      RT  0     0    0   0 S    0  0.0   0:06.82 migration/0
    4 root      20  0     0    0   0 S    0  0.0   0:00.00 ksoftirqd/0
    5 root      RT  0     0    0   0 S    0  0.0   0:06.78 migration/1
    6 root      20  0     0    0   0 S    0  0.0   0:00.00 ksoftirqd/1
```

https://live.paloaltonetworks.com/t5/Management-Articles/Show-System-Resource-CommandDisplays-CPU-Utilization-of-9999/ta-p/58149

NEW QUESTION: 99

Which processing order will be enabled when a Panorama administrator selects the setting "Objects defined in ancestors will take higher precedence?"

A. Descendant objects will take precedence over other descendant objects.

B. Descendant objects will take precedence over ancestor objects.

C. Ancestor objects will have precedence over descendant objects.

D. Ancestor objects will have precedence over other ancestor objects.

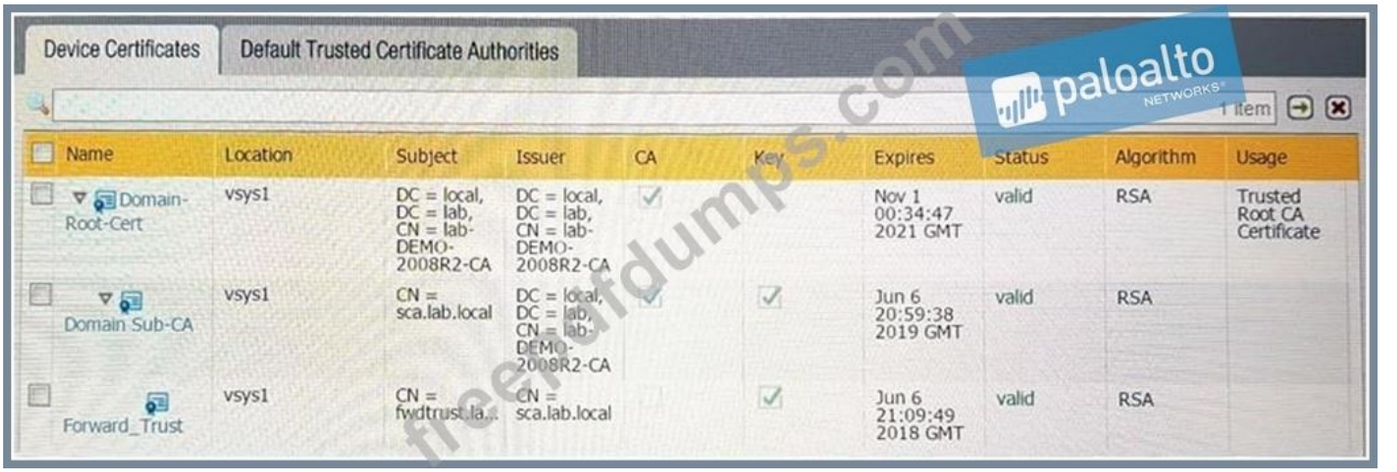
Answer: (SHOW ANSWER)

Explanation/Reference:

Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device- setup-management

NEW QUESTION: 100

Refer to the exhibit.



Which certificates can be used as a Forwarded Trust certificate?

A. Domain-Root-Cert

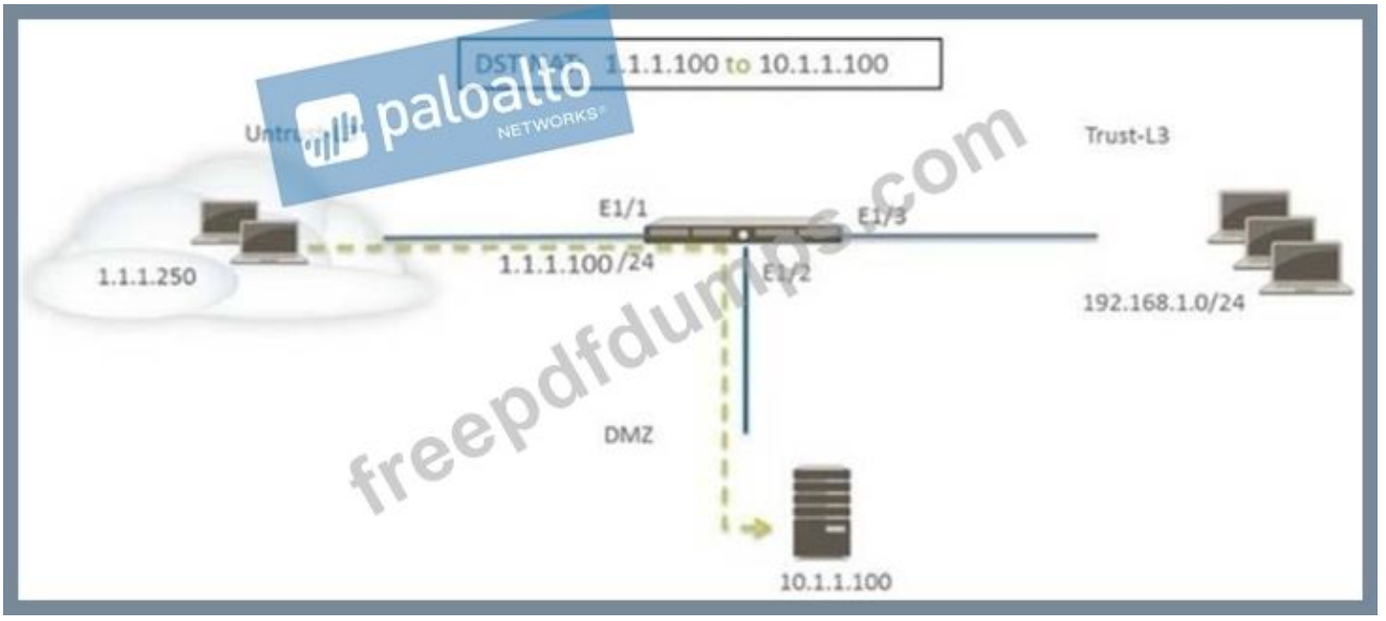
B. Domain Sub-CA
C. Forward_Trust
D. Certificate from Default Trust Certificate Authorities
Answer: (SHOW ANSWER)

NEW QUESTION: 101
After Migrating from an ASA firewall to a Palo Alto Networks Firewall, the VPN connection between a remote network and the Palo Alto Networks Firewall is not establishing correctly. The following entry is appearing in the logs:
Pfs group mismatched: my:0 peer:2
Which setting should be changed on the Palo Alto Networks Firewall to resolve this error message?
A. Update the IKE Crypto profile for the Vendor IKE gateway from no pfs to group2.
B. Update the IPSec Crypto profile for the Vendor IPSec Tunnel from no-pfs to group2.
C. Update- the IPSec Crypto profile for the Vendor IPSec Tunnel from group2 to no-pfs.
D. Update the IKE Crypto profile for the Vendor IKE gateway from group2 to no pfs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 102
On the NGFW, how can you generate and block a private key from export and thus harden your security posture and prevent rogue administrators or other bad actors from misusing keys?
A. 1. Select Device > Certificate Management > Certificates > Device > Certificates
2. Import the certificate
3. Select Import Private key
4. Click Generate to generate the new certificate
B. 1. Select Device > Certificates
2. Select Certificate Profile
3. Generate the certificate
4. Select Block Private Key Export
C. 1. Select Device > Certificate Management > Certificates > Device > Certificates
2. Generate the certificate
3. Select Block Private Key Export
4. Click Generate to generate the new certificate
D. 1. Select Device > Certificates
2. Select Certificate Profile
3. Generate the certificate
4. Select Block Private Key Export
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/decryption-features/block- export-of-private-keys.html

NEW QUESTION: 103
Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?
A. Configure a Decryption Profile and select SSL/TLS services.
B. Set up SSL/TLS under Policies > Service/URL Category > Service.
C. Set up Security policy rule to allow SSL communication.
D. Configure an SSL/TLS Profile.
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device- certificate-management-ssltls-service-profile

NEW QUESTION: 104
Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.



Which Security policy rule will allow traffic to flow to the web server?
A. Untrust (any) to Untrust (10. 1.1. 100), web browsing - Allow
B. Untrust (any) to Untrust (1. 1. 1. 100), web browsing - Allow
C. Untrust (any) to DMZ (1. 1. 1. 100), web browsing - Allow
D. Untrust (any) to DMZ (10. 1. 1. 100), web browsing - Allow
Answer: (SHOW ANSWER)

NEW QUESTION: 105
What are three reasons why an installed session can be identified with the "application incomplete" tag? (Choose three.)
A. There was no application data after the TCP connection was established.
B. The client sent a TCP segment with the PUSH flag set.
C. The TCP connection was terminated without identifying any application data.
D. There is not enough application data after the TCP connection was established.
E. The TCP connection did not fully establish.

Answer: A,D,E (LEAVE A REPLY)
Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

NEW QUESTION: 106
A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects. How would an administrator configure the interface to 1Gbps?
A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
B. set deviceconfig system speed-duplex 1Gbps-duplex
C. set deviceconfig system speed-duplex 1Gbps-full-duplex
D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex
Answer: (SHOW ANSWER)
Reference:
user@PA# set deviceconfig system speed-duplex 100Mbps-full-duplex 100Mbps-full-duplex 100Mbps-half-duplex 100Mbps-half-duplex 10Mbps-full-duplex 10Mbps-full-duplex 10Mbps-half-duplex 10Mbps-half-duplex 1Gbps-full-duplex 1Gbps-full-duplex 1Gbps-half-duplex 1Gbps-half-duplex auto-negotiate auto-negotiate

NEW QUESTION: 107
An engineer is creating a security policy based on Dynamic User Groups (DUG) What benefit does this provide?
A. Automatically include users as members without having to manually create and commit policy or group changes
B. DUGs are used to only allow administrators access to the management interface on the Palo Alto Networks firewall
C. It enables the functionality to decrypt traffic and scan for malicious behaviour for User-ID based policies
D. Schedule commits at a regular intervals to update the DUG with new users matching the tags specified
Answer: A (LEAVE A REPLY)
Dynamic user groups help you to create policy that provides auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility. Previously, quarantining users in

response to suspicious activity meant time- and resource-consuming updates for all members of the group or updating the IP address-to-username mapping to a label to enforce policy at the cost of user visibility, as well as having to wait until the firewall checked the traffic. Now, you can configure a dynamic user group to automatically include users as members without having to manually create and commit policy or group changes and still maintain user-to-data correlation at the device level before the firewall even scans the traffic.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups.html

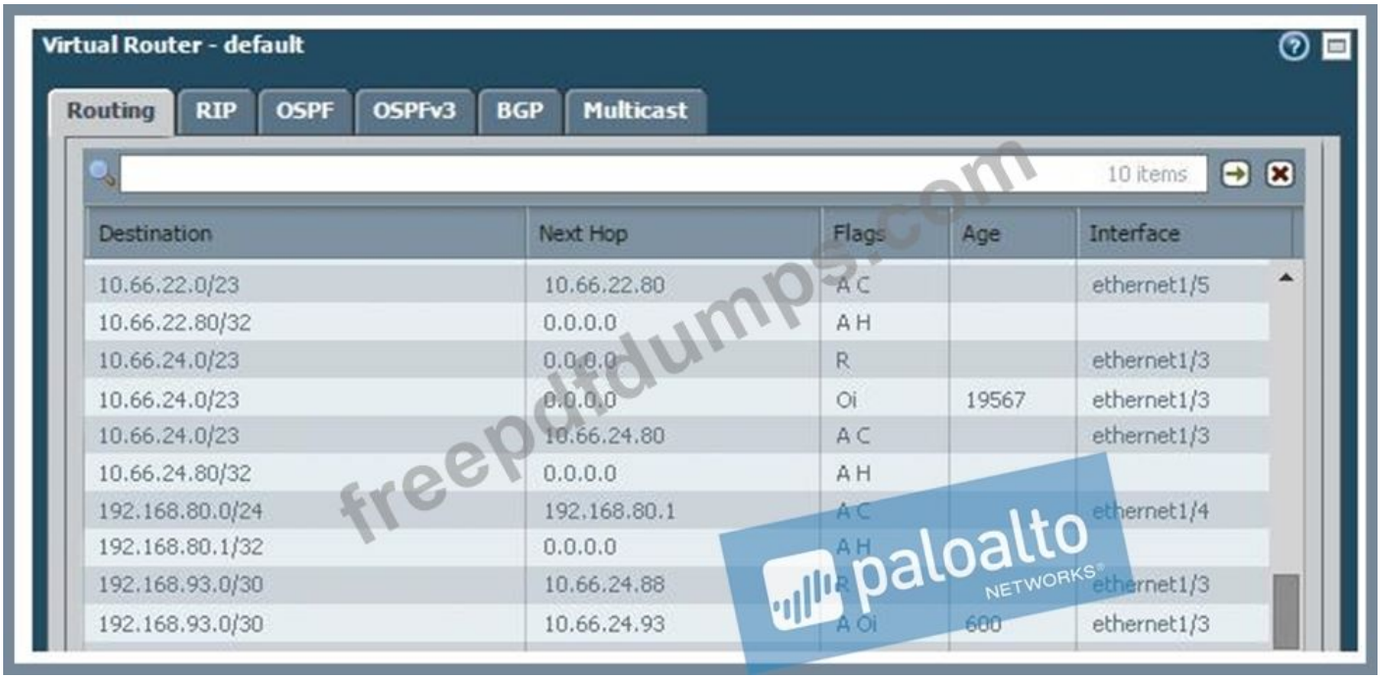
NEW QUESTION: 108
What happens when an A P firewall cluster synchronies IPsec tunnel security associations (SAs)?
A. Phase 2 SAs are synchronized over HA2 finks
B. Phase 1 and Phase 2 SAs are synchronized over HA2 links
C. Phase 1 SAs are synchronized over HA1 links
D. Phase 1 and Phase 2 SAs are synchronized over HA3 links
Answer: (SHOW ANSWER)
From the Palo Alto documentation below, "when a VPN is terminated on a Palo Alto firewall HA pair, not all IPSEC related information is synchronized between the firewalls... This is an expected behavior. IKE phase 1 SA information is NOT synchronized between the HA firewalls." And from the second link, "Data link (HA2) is used to sync sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in the HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive). It flows from the active firewall to the passive firewall."
https://know
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW
ledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&
&lang=en_US%E2%80%A9
lang=en_US%E2%80%A9&
&refURL=http%3A%2F%2Fknowledgebase.palo
refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail
altonetworks.com%2FKCSArticleDetail
https://help.aryaka.com/display/public/KNOW/Palo+Alto+Networks+NFV+Technical+Brief

NEW QUESTION: 109
View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?
A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.
Answer: C (LEAVE A REPLY)
Reference:
"Select this option to allow the GlobalProtect agent to determine if it is inside the enterprise network. This option applies only to endpoints that are configured to communicate with internal gateways. When the user attempts to log in, the agent does a reverse DNS lookup of an internal host using the specified Hostname to the specified IP Address. The host serves as a reference point that is reachable if the endpoint is inside the enterprise network. If the agent finds the host, the endpoint is inside the network and the agent connects to an internal gateway; if the agent fails to find the internal host, the endpoint is outside the network and the agent establishes a tunnel to one of the external gateways"

NEW QUESTION: 110
When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?
A. Save candidate config
B. Load named configuration snapshot
C. Export device state
D. Load configuration version
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Given the following table.



Which configuration change on the firewall would cause it to use 10.66.24.88 as the next hop for the 192.168.93.0/30 network?

A. Configuring the administrative Distance for RIP to be lower than that of OSPF Int.

B. Configuring the metric for RIP to be higher than that of OSPF Int.

C. Configuring the administrative Distance for RIP to be higher than that of OSPF Ext.

D. Configuring the metric for RIP to be lower than that OSPF Ext.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 112

The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router.

Which two options would help the administrator troubleshoot this issue? (Choose two.)

A. Perform a traffic pcap on the NGFW to see any BGP problems.

B. View the System logs and look for the error messages about BGP.

C. View the Runtime Stats and look for problems with BGP configuration.

D. View the ACC tab to isolate routing issues.

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 113

Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS software?

A. Okta

B. DUO

C. RADIUS

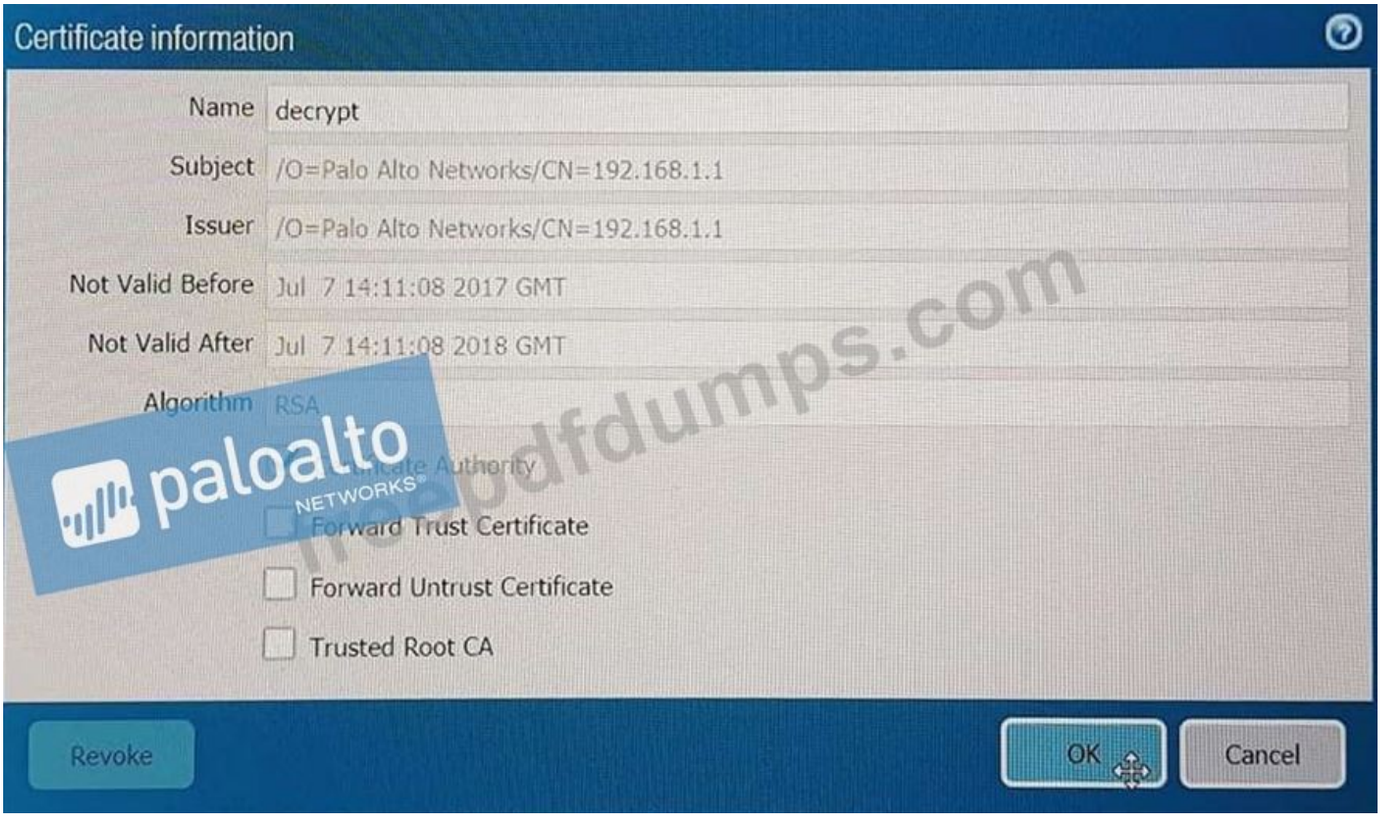
D. PingID

Answer: C (LEAVE A REPLY)

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-authentication

NEW QUESTION: 114
Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)
A. From the Panorama tab of the Panorama GUI select Log Collector mode and then commit changes
B. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.
C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.
D. Enter the command logger-mode enable the enter Y to confirm the change to Log Collector mode.
E. Log in the Panorama CLI of the dedicated Log Collector
Answer: B,E (LEAVE A REPLY)
Explanation
(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up

NEW QUESTION: 115
The certificate information displayed in the following image is for which type of certificate?
Exhibit:



A. Self-Signed Root CA certificate

B. Web Server certificate
C. Public CA signed certificate
D. Forward Trust certificate
Answer: (SHOW ANSWER)

NEW QUESTION: 116
VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?
A. Zone Protection
B. Replay
C. Web Application
D. DoS Protection
Answer: B (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/vpns/set-up-site-to-site-vpn/set-up-an-ipsec-tunnel#

NEW QUESTION: 117
Which DoS protection mechanism detects and prevents session exhaustion attacks?
A. Packet Based Attack Protection
B. Flood Protection
C. Resource Protection
D. TCP Port Scan Protection
Answer: C (LEAVE A REPLY)


DoS protection profiles provide detailed control for Denial of Service (DoS) protection policies. DoS policies allow you to control the number of sessions between interfaces, zones, addresses, and countries based on aggregate sessions or source and/or destination IP addresses. There are two DoS protection mechanisms that the Palo Alto Networks firewalls support.

- **Flood Protection**–Detects and prevents attacks where the network is flooded with packets resulting in too many half-open sessions and/or services being unable to respond to each request. In this case the source address of the attack is usually spoofed. See DoS Protection Against Flooding of New Sessions.
- **Resource Protection**– Detects and prevents session exhaustion attacks. In this type of attack, a large number of hosts (bots) are used to establish as many fully established sessions as possible to consume all of a system's resources.

You can enable both types of protection mechanisms in a single DoS protection profile.

The DoS profile is used to specify the type of action to take and details on matching criteria for the DoS policy. The DoS profile defines settings for SYN, UDP, and ICMP floods, can enable resource protect and defines the maximum number of concurrent connections. After you configure the DoS protection profile, you then attach it to a DoS policy.

When configuring DoS protection, it is important to analyze your environment in order to set the correct thresholds and due to some of the complexities of defining DoS protection policies, this guide will not go into detailed examples. For more information, refer to the Threat Prevention Tech Note.

NEW QUESTION: 118
Which CLI command enables an administrator to check the CPU utilization of the dataplane?
A. show running resource-monitor
B. debug data-plane dp-cpu
C. show system resources
D. debug running resources
Answer: A (LEAVE A REPLY)

Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXwCAK
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CluDCAS

NEW QUESTION: 119
An administrator has been asked to create 100 virtual firewalls in a local, on-premise lab environment (not in "the cloud"). Bootstrapping is the most expedient way to perform this task.
Which option describes deployment of a bootstrap package in an on-premise virtual environment?
A. Create and attach a virtual hard disk (VHD).
B. Use an S3 bucket with an ISO.
C. Use a virtual CD-ROM with an ISO.
D. Use config-drive on a USB stick.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 120
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of reconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.
Which VPN configuration would adapt to changes when deployed to the future site?
A. Preconfigured GlobalProtect satellite
B. Preconfigured GlobalProtect client
C. Preconfigured IPsec tunnels
D. Preconfigured PPTP Tunnels
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/large-scale-vpn-lsvpn/configure-the-globalprotect-portal-for-lsvpn/define-the-satellite-configurations.html

NEW QUESTION: 121
Exhibit:

What will be the source address in the ICMP packet?

A. 10.46.64.94

B. 10.46.72.93

C. 10.30.0.93

D. 192.168.93.1

Answer: A (LEAVE A REPLY)

NEW QUESTION: 122

An administrator needs to upgrade an NGFW to the most current version of PAN-OS software. The following is occurring:

*Firewall has Internet connectivity through e1/1.

*Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
*Service route is configured, sourcing update traffic from e1/1.
*A communication error appears in the System logs when updates are performed.
*Download does not complete.
What must be configured to enable the firewall to download the current version of PAN-OS software?
A. scheduler for timed downloads of PAN-OS software
B. DNS settings for the firewall to use for resolution
C. static route pointing application PaloAlto-updates to the update servers
D. Security policy rule allowing PaloAlto-updates as the application
Answer: D (LEAVE A REPLY)

NEW QUESTION: 123
Refer to Exhibit:

A firewall has three PDF rules and a default route with a next hop of 172.29.19.1 that is configured in the default VR. A user named XX-bes a PC with a 192.168.101.10 IP address. He makes an HTTPS connection to 172.16.10.29.
What is the next hop IP address for the HTTPS traffic from Wills PC.

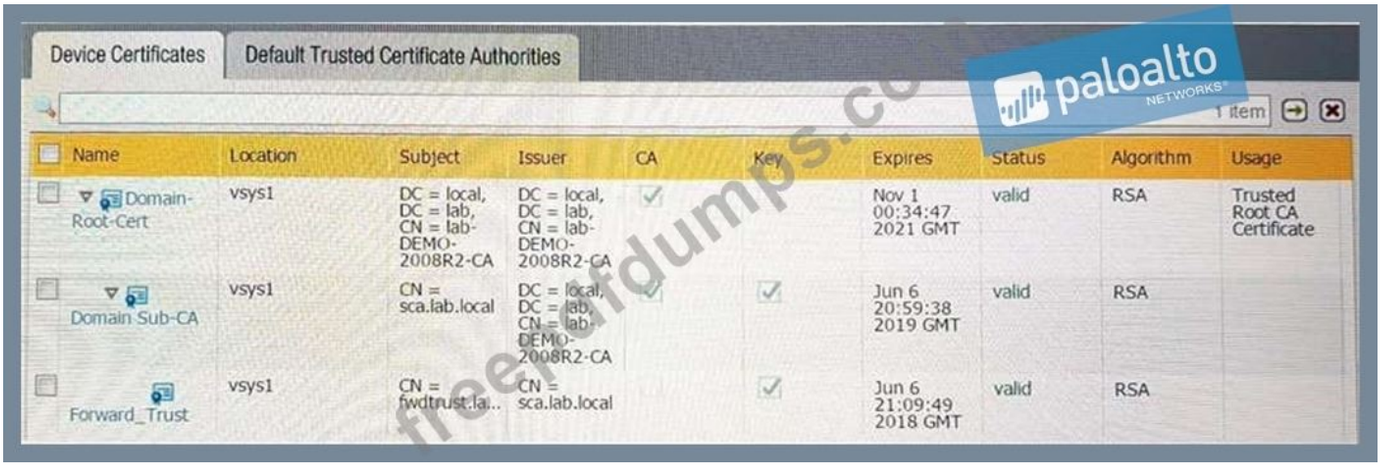
A. 172.20.40.1
B. 172.20.20.1
C. 172.20.10.1
D. 172.20.30.1
Answer: B (LEAVE A REPLY)

NEW QUESTION: 124
What happens to traffic traversing SD-WAN fabric that doesn't match any SD-WAN policies?

A. Traffic is dropped because there is no matching SD-WAN policy to direct traffic.
B. Traffic matches a catch-all policy that is created through the SD-WAN plugin.
C. Traffic matches implied policy rules and is redistributed round robin across SD-WAN links.
D. Traffic is forwarded to the first physical interface participating in SD-WAN based on lowest interface number (i.e., Eth1/1 over Eth1/3).
Answer: C (LEAVE A REPLY)
If there is no match to any SD-WAN policy rule in the list, the session matches an implied SD-WAN policy rule at the end of the list that uses the round-robin method to distribute unmatched sessions among all links in one SD-WAN interface, which is based on the route lookup.

NEW QUESTION: 125

Refer to the exhibit.



Which certificates can be used as a Forwarded Trust certificate?

A. Domain Sub-CA

B. Forward_Trust

C. Certificate from Default Trust Certificate Authorities

D. Domain-Root-Cert

Answer: (SHOW ANSWER)

NEW QUESTION: 126

A client has a sensitive application server in their data center and is particularly concerned about resource exhaustion because of distributed denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server.

B. Add a Vulnerability Protection Profile to block the attack.

C. Add QoS Profiles to throttle incoming requests.

D. Add a DoS Protection Profile with defined session count.

Answer: D (LEAVE A REPLY)

Reference:

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles

NEW QUESTION: 127

An administrator has left a firewall to use the default port for all management services.

Which three functions are performed by the dataplane? (Choose three.)

A. NAT

B. File blocking

C. WildFire updates

D. NTP

E. antivirus

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

NEW QUESTION: 128
Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS version, and serial number?
A. debug system details
B. show session info
C. show system info
D. show system details
Answer: C (LEAVE A REPLY)
Reference: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/pan-os-60/PAN-OS-6.0- CLI-ref.pdf

NEW QUESTION: 129
An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are form external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this traffic as their accounting application and to scan this traffic for threats.
Which option would achieve this result?
A. Create an Application Override policy.
B. Create an Application Override policy and custom threat signature for the application.
C. Create a custom App-ID and use the "ordered conditions" check box.
D. Create a custom App-ID and enable scanning on the advanced tab.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130
Drag and Drop Question
Match each type of DoS attack to an example of that type of attack.

Answer:

Explanation:
Plan to defend your network against different types of DoS attacks:
Application-Based Attacks
- Target weaknesses in a particular application and try to exhaust its resources so legitimate users can't use it. An example of this is the Slowloris attack.
Protocol-Based Attacks
- Also known as state-exhaustion attacks, these attacks target protocol weaknesses. A common example is a SYN flood attack.
Volumetric Attacks
- High-volume attacks that attempt to overwhelm the available network resources, especially bandwidth, and bring down the target to prevent legitimate users from accessing those resources. An example of this is a UDP flood attack.

NEW QUESTION: 131
Support for which authentication method was added in PAN-OS 8.0?
A. RADIUS
B. LDAP
C. Diameter
D. TACACS+
Answer: D (LEAVE A REPLY)
https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1

NEW QUESTION: 132
Click the Exhibit button

An administrator has noticed a large increase in bittorrent activity. The administrator wants to determine where the traffic is going on the company.
What would be the administrator's next step?
A. Create a global filter for bittorrent traffic and then view Traffic logs.
B. Right-Click on the bittorrent link and select Value from the context menu
C. Click on the bittorrent application link to view network activity
D. Create local filter for bittorrent traffic and then view Traffic logs.
Answer: (SHOW ANSWER)

NEW QUESTION: 133
What are two benefits of nested device groups in Panorama? (Choose two.)
A. All device groups inherit settings form the Shared group
B. Overwrites local firewall configuration
C. Reuse of the existing Security policy rules and objects
D. Requires configuring both function and location for every device
Answer: (SHOW ANSWER)

NEW QUESTION: 134
A customer wants to set up a site-to-site VPN using tunnel interfaces?
Which two formats are correct for naming tunnel interfaces? (Choose two.)
A. tunnel.1
B. vpn-tunnel.1
C. tunnel.1025
D. vpn-tunnel.1024
Answer: (SHOW ANSWER)

NEW QUESTION: 135
A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation.
Which two formats are correct for naming aggregate interfaces? (Choose two.)
A. aggregate.8
B. aggregate.1
C. ae.1
D. ae.8
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 136
An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router. Which two options enable the administrator to troubleshoot this issue? (Choose two.)
A. View Runtime Stats in the virtual router.
B. View System logs.
C. Add a redistribution profile to forward as BGP updates.
D. Perform a traffic pcap at the routing stage.
Answer: (SHOW ANSWER)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldcCAC

NEW QUESTION: 137
A customer wants to set up a site-to-site VPN using tunnel interfaces.

Which two formats are correct for naming tunnel interfaces? (Choose two.)

A. tunnel.1

B. vpn-tunnel.1

C. tunnel.1025

D. vpn-tunnel.1024

Answer: (SHOW ANSWER)

Explanation/Reference:

NEW QUESTION: 138

After pushing a security policy from Panorama to a PA-3020 firewall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

A. A Server Profile has not been configured for logging to this Panorama device.

B. Panorama is not licensed to receive logs from this particular firewall.

C. The firewall is not licensed for logging to this Panorama device.

D. None of the firewall's policies have been assigned a Log Forwarding profile

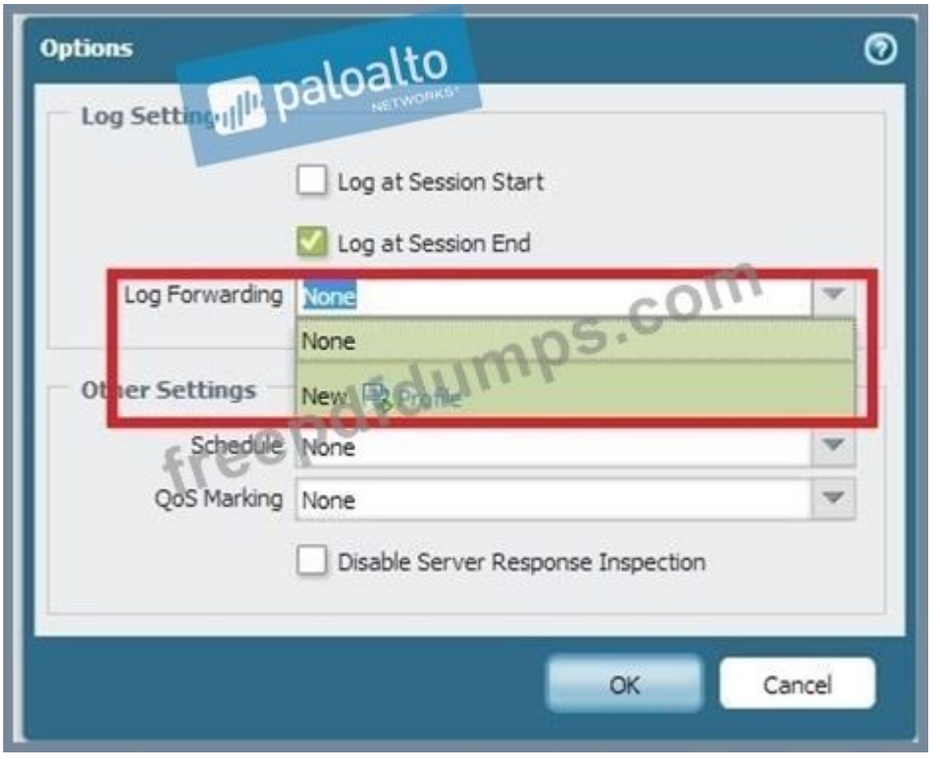
Answer: D (LEAVE A REPLY)

In order to see entries in the Panorama Monitor > Traffic or Monitor > Log screens, a profile must be created on the Palo Alto Networks device (or pushed from Panorama) to forward log traffic to Panorama.

Steps:

1. Go to Policies > Security and open the Options for a rule.

2. Under Log Setting, select New for Log Forwarding to create a new forwarding profile:



Etc.

https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Create-a-Profile-to-Forward-Logs-to-Panorama/ta-p/54038

NEW QUESTION: 139
What is the name of the debug save file for IPSec VPN tunnels?
A. Ikemgr.pcap
B. test vpn ike-sa
C. set vpn all up
D. request vpn IPsec-sa test
Answer: A (LEAVE A REPLY)

NEW QUESTION: 140
An administrator needs to implement an NGFW between their DMZ and Core network. EIGRP Routing between the two environments is required. Which interface type would support this business requirement?
A. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ
B. Layer 3 or Aggregate Ethernet interfaces, but configuring EIGRP on subinterfaces only
C. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel (with the GlobalProtect License to support LSVPN and EIGRPprotocols)
D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router
Answer: A (LEAVE A REPLY)
EIGRP is a Cisco proprietary protocol. The dynamic routing protocols supported on the PAN are RIPv2, OSPF and BGP.

NEW QUESTION: 141
What happens, by default, when the GlobalProtect app fails to establish an IPSec tunnel to the GlobalProtect gateway?
A. It keeps trying to establish an IPSec tunnel to the GlobalProtect gateway
B. It stops the tunnel-establishment processing to the GlobalProtect gateway immediately
C. It tries to establish a tunnel to the GlobalProtect gateway using SSL/TLS
D. It tries to establish a tunnel to the GlobalProtect portal using SSL/TLS
Answer: C (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/globalprotect/network-globalprotect-po

NEW QUESTION: 142
An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are form external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this traffic as their accounting application and to scan this traffic for threats.

Which option would achieve this result?

A. Create a custom App-ID and enable scanning on the advanced tab.

B. Create a custom App-ID and use the "ordered conditions" check box.

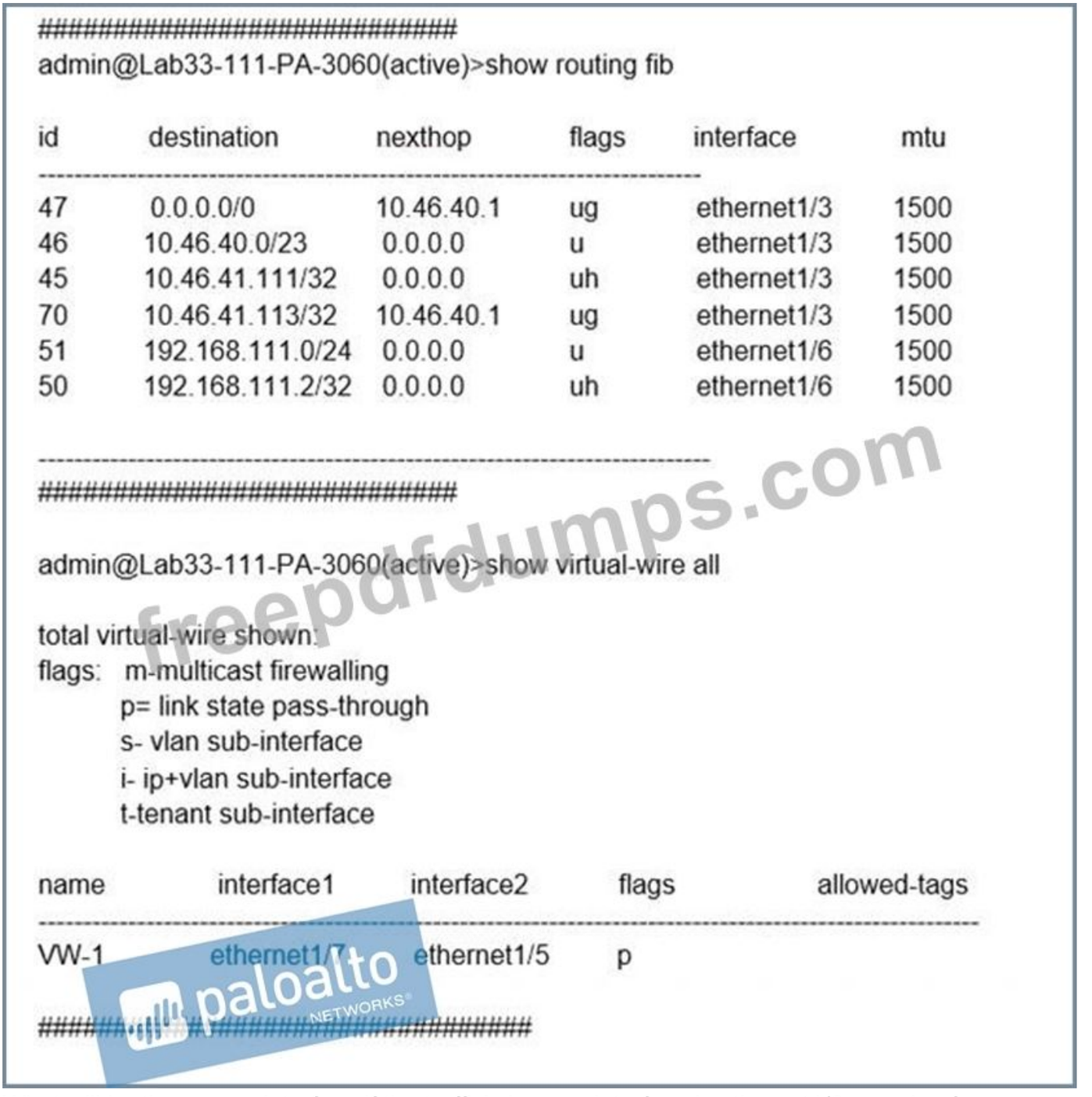
C. Create an Application Override policy.

D. Create an Application Override policy and a custom threat signature for the application.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 143

Exhibit:



```
##################################
admin@Lab33-111-PA-3060(active)>show routing fib

id        destination       nexthop       flags     interface       mtu
--------------------------------------------------------------------------
47        0.0.0.0/0         10.46.40.1    ug        ethernet1/3     1500
46        10.46.40.0/23     0.0.0.0       u         ethernet1/3     1500
45        10.46.41.111/32   0.0.0.0       uh        ethernet1/3     1500
70        10.46.41.113/32   10.46.40.1    ug        ethernet1/3     1500
51        192.168.111.0/24  0.0.0.0       u         ethernet1/6     1500
50        192.168.111.2/32  0.0.0.0       uh        ethernet1/6     1500

--------------------------------------------------------------------------
##################################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p= link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name          interface1       interface2       flags          allowed-tags
--------------------------------------------------------------------------------
VW-1          ethernet1/7      ethernet1/5      p

##################################
```


What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

A. ethernet1/6
B. ethernet1/3
C. ethernet1/7
D. ethernet1/5
Answer: B (LEAVE A REPLY)

NEW QUESTION: 144
A remote administrator needs firewall access on an untrusted interface Which two components are required on the firewall to configure certificate-based administrator authentication to the web UI? (Choose two)
A. client certificate
B. certificate profile
C. certificate authority (CA) certificate
D. server certificate
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface.html

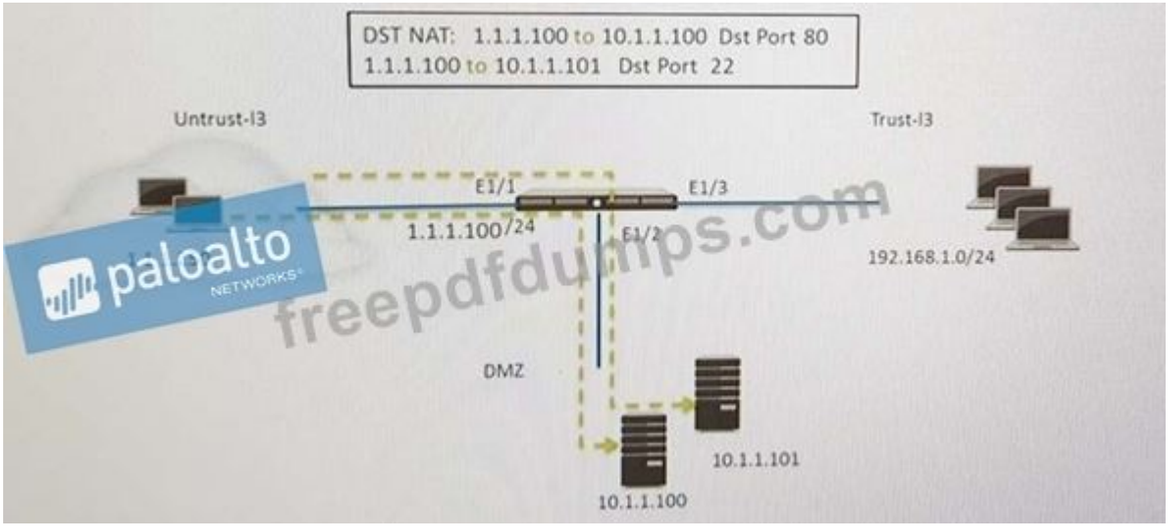
NEW QUESTION: 145
An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN-OS software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web- browsing traffic from any to any zone.
What must the administrator configure so that the PAN-OS software can be upgraded?
A. Security policy rule
B. CRL
C. Service route
D. Scheduler
Answer: C (LEAVE A REPLY)
Explanation/Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clp3CAC

NEW QUESTION: 146
Which event will happen if an administrator uses an Application Override Policy?
A. Threat-ID processing time is decreased.
B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.
C. The application name assigned to the traffic by the security rule is written to the Traffic log.
D. App-ID processing time is increased.
Answer: A (LEAVE A REPLY)
Reference:

https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Override
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/manage-custom-or-unknown-applications#

NEW QUESTION: 147
The firewall identifies a popular application as an unknown-tcp.
Which two options are available to identify the application? (Choose two.)
A. Create a custom application.
B. Create a custom object for the custom application server to identify the custom application.
C. Submit an Apple-ID request to Palo Alto Networks.
D. Create a Security policy to identify the custom application.
Answer: A,B (LEAVE A REPLY)
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/use-application-objects-in-policy/create-a- custom-application

NEW QUESTION: 148
Refer to the exhibit.



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and HOST B (10.1.1.101) receives SSH traffic.) Which two security policy rules will accomplish this configuration? (Choose two.)
A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
B. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow
C. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
D. Untrust (Any) to DMZ (10.1.1.1), ssh -Allow
E. Untrust (Any) to DMZ (10.1.1.1), web-browsing -Allow
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 149

The firewall is not downloading IP addresses from MineMeld. Based, on the image, what most likely is wrong?

A. External Dynamic Lists do not support SSL connections.

B. A Certificate Profile that contains the CA certificate needs to be selected.

C. The source address supports only files hosted with an ftp://<address/file>.

D. A Certificate Profile that contains the client certificate needs to be selected.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 150

In the following image from Panorama, why are some values shown in red?

Device Name	Logging Rate (Log/sec)	Device	Session
		Throughput (KB/sec)	Count (Sessions)
uk3	781	209	40221
sg2		953	170
us3	291	0	67455

A. sg2 has misconfigured session thresholds.

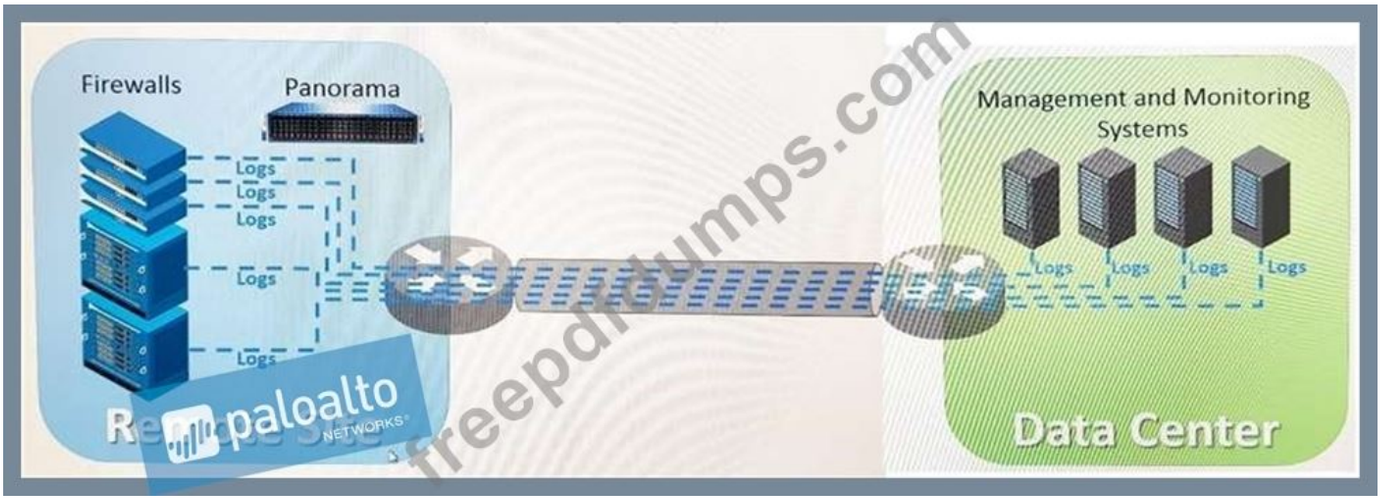
B. sg2 session count is the lowest compared to the other managed devices.

C. uk3 has a logging rate that deviates from the seven-day calculated baseline.

D. us3 has a logging rate that deviates from the administrator-configured thresholds.

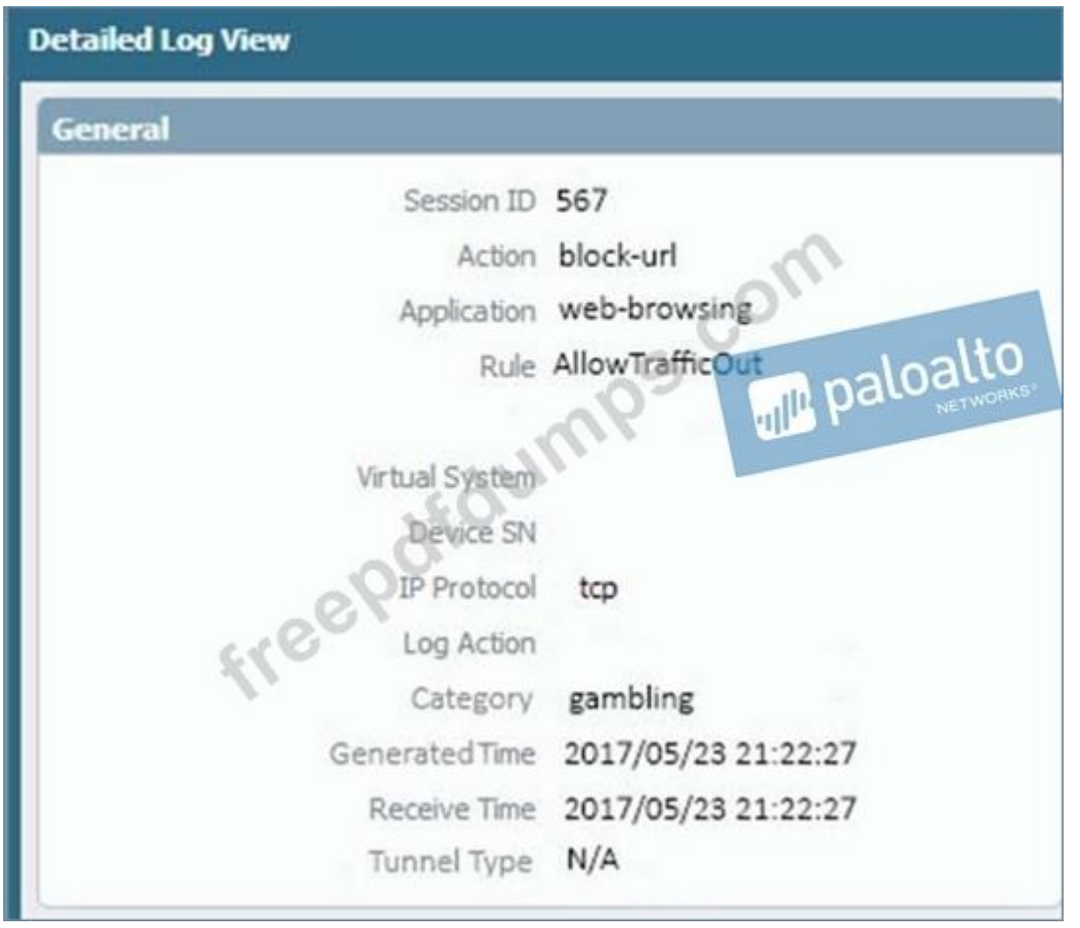
Answer: C (LEAVE A REPLY)

NEW QUESTION: 151
Refer to exhibit. An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.

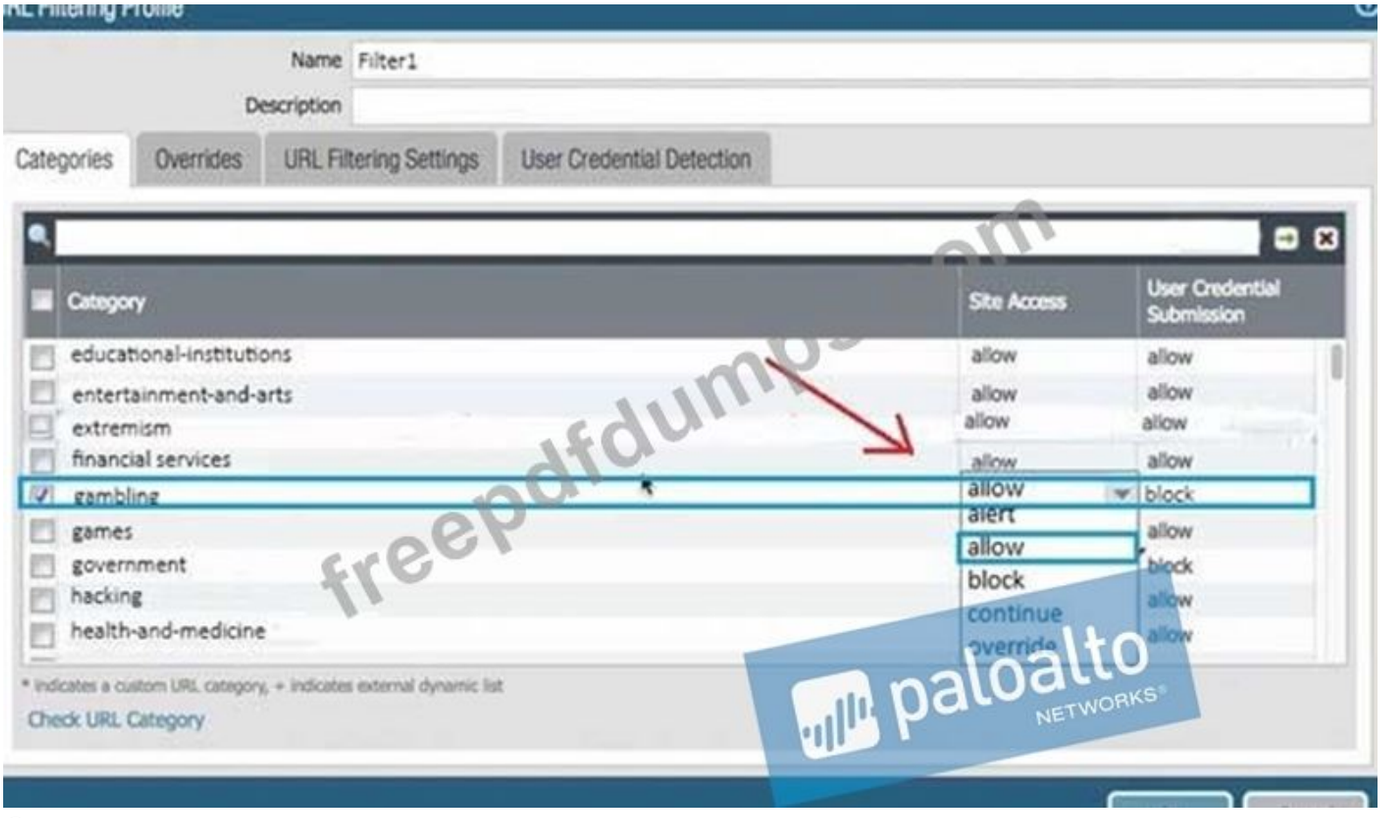


How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all existing monitoring platforms?
A. Configure log compression and optimization features on all remote firewalls.
B. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.
C. Any configuration on an M-500 would address the insufficient bandwidth concerns.
D. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.
Answer: (SHOW ANSWER)

NEW QUESTION: 152
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.
Which configuration change should the administrator make?
A:


Detailed Log View
General
Session ID 567
Action block-url
Application web-browsing
Rule AllowTrafficOut
Virtual System
Device SN
IP Protocol tcp
Log Action
Category gambling
Generated Time 2017/05/23 21:22:27
Receive Time 2017/05/23 21:22:27
Tunnel Type N/A
paloalto NETWORKS
freepdfdumps.com

B:


Name Filter1
Description
Categories
Overrides
URL Filtering Settings
User Credential Detection
Category
Site Access
User Credential Submission
educational-institutions
entertainment-and-arts
extremism
financial services
gambling
games
government
hacking
health-and-medicine
allow
block
alert
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category
paloalto NETWORKS
freepdfdumps.com

C:


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Name
www.megamillions.com
Rule Type
universal (default)
Description
Tags
Cancel
paloalto
NETWORKS
freepdfdumps.com

D:


URL Filtering Profile
Name
Filter1
Description
Overrides
Categories
URL Filtering Settings
User Credential Detection
Allow-List
www.megamillions.com
Block List
Action
continue
OK
Cancel
paloalto
NETWORKS
freepdfdumps.com

E:


URL Filtering Profile
Name
Filter1
Description
Overrides
Categories
URL Filtering Settings
User Credential Detection
Allow-List
www.megamillions.com
Block List
Action
block
OK
Cancel
paloalto
NETWORKS
freepdfdumps.com

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

NEW QUESTION: 153
Decrypted packets from the website https://www.microsoft.com will appear as which application and service within the Traffic log?
A. web-browsing and 443
B. SSL and 80
C. SSL and 443
D. web-browsing and 80
Answer: A (LEAVE A REPLY)
Explanation
We know that SSL decryption is supposed to give us visibility of traffic that would otherwise be encrypted.
Therefore, we'd expect decrypted traffic to be identified as the underlying applications, such as web-browsing, facebook-base or other, but not as SSL.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cle8CAC

NEW QUESTION: 154
Which two events trigger the operation of automatic commit recovery? (Choose two.)
A. when an aggregate Ethernet interface component fails
B. when Panorama pushes a configuration
C. when a firewall HA pair fails over
D. when a firewall performs a local commit
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html
Automatic commit recovery allows you to configure the firewall to attempt a specified number of connectivity tests after:
1- you push a configuration from Panorama or
2- commit a configuration change locally on the firewall.
Additionally, the firewall checks connectivity to Panorama every hour to ensure consistent communication in the event unrelated network configuration changes have disrupted connectivity between the firewall and Panorama or if implications to a pushed committed configuration may have affected connectivity.

NEW QUESTION: 155
Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?
A. Configure a Decryption Profile and select SSL/TLS services.
B. Set up SSL/TLS under Polices > Service/URL Category>Service.
C. Set up Security policy rule to allow SSL communication.
D. Configure an SSL/TLS Profile.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device- certificate-management-ssltls-service-profile

NEW QUESTION: 156
Which three authentication services can administrator use to authenticate admins into the Palo Alto Networks NGFW without defining a corresponding admin account on the local firewall? (Choose three.)
A. Kerberos
B. PAP
C. SAML
D. TACACS+
E. RADIUS
F. LDAP
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication

NEW QUESTION: 157
Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)
A. Red Hat Enterprise Virtualization (RHEV)
B. Kernel Virtualization Module (KVM)
C. Boot Strap Virtualization Module (BSVM)
D. Microsoft Hyper-V
Answer: (SHOW ANSWER)
Reference:
docs.paloaltonetworks.com/vm-series/8-0/vm-series-deployment/about-the-vm-series-firewall/vm-series-deployments

NEW QUESTION: 158
An administrator is configuring an IPSec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. the following is the output from the command:

What could be the cause of this problem?

A. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.

B. The shared secrets do not match between the Palo Alto Networks Firewall and the ASA.

C. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA.

D. The Proxy IDs on the Palo Alto Networks Firewall do not match the setting on the ASA.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 159

An administrator needs to troubleshoot a User-ID deployment. The administrator believes that there is an issue related to LDAP authentication. The administrator wants to create a packet capture on the management plane.

Which CLI command should the administrator use to obtain the packet capture for validating the configuration?

A. > ftp export mgmt-pcap from mgmt.pcap to <FTP host>

B. > scp export mgmt-pcap from mgmt.pcap to (username@host:path)

C. > scp export poap-mgmt from poap.mgmt to (username@host:path)

D. > scp export pcap from pcap to (usernameQhost:path)

Answer: B (LEAVE A REPLY)

Additionally, you can manually export the PCAP via SCP or TFTP, i.e.:

> scp export mgmt-pcap from mgmt.pcap to

<value> Destination (username@host:path)

Ref: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleECAS

NEW QUESTION: 160

Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?

A. Configure a Decryption Profile and select SSL/TLS services.

B. Set up SSL/TLS under Polices > Service/URL Category>Service.

C. Set up Security policy rule to allow SSL communication.

D. Configure an SSL/TLS Profile.

Answer: D (LEAVE A REPLY)

Reference:

https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-certificate-manag ssltls-service-profile

NEW QUESTION: 161
Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)
A. Create a no-decrypt Decryption Policy rule.
B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
C. Create a Dynamic Address Group for untrusted sites
D. Create a Security Policy rule with vulnerability Security Profile attached.
E. Enable the "Block sessions with untrusted issuers" setting.
Answer: A,E (LEAVE A REPLY)
Explanation
You can use the No Decryption tab to enable settings to block traffic that is matched to a decryption policy configured with the No Decrypt action (Policies > Decryption > Action). Use these options to control server certificates for the session, though the firewall does not decrypt and inspect the session traffic.
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-decryption-profile

NEW QUESTION: 162
A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?
A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096 in the "Tag Allowed" field of the V-Wire object.
B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the Tag Allowed" field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/sub interface to a unique zone.
C. Create Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router.
The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface tA.
unique zone. Do not assign any interface an IP address.
D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/sub interface to a unique zone.
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfa Virtual wire interfaces by default allow all untagged traffic. You can, however, use a virtual wire to connect two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags.

VLAN tag 0 indicates untagged traffic.You can also create multiple subinterfaces, add them into different zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.

NEW QUESTION: 163
A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server.
Which solution in PAN-OS software would help in this case?
A. application override
B. Virtual Wire mode
C. content inspection
D. redistribution of user mappings
Answer: D (LEAVE A REPLY)
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-network

NEW QUESTION: 164


What will be the source address in the ICMP packet?
A. 10.46.64.94
B. 10.30.0.93

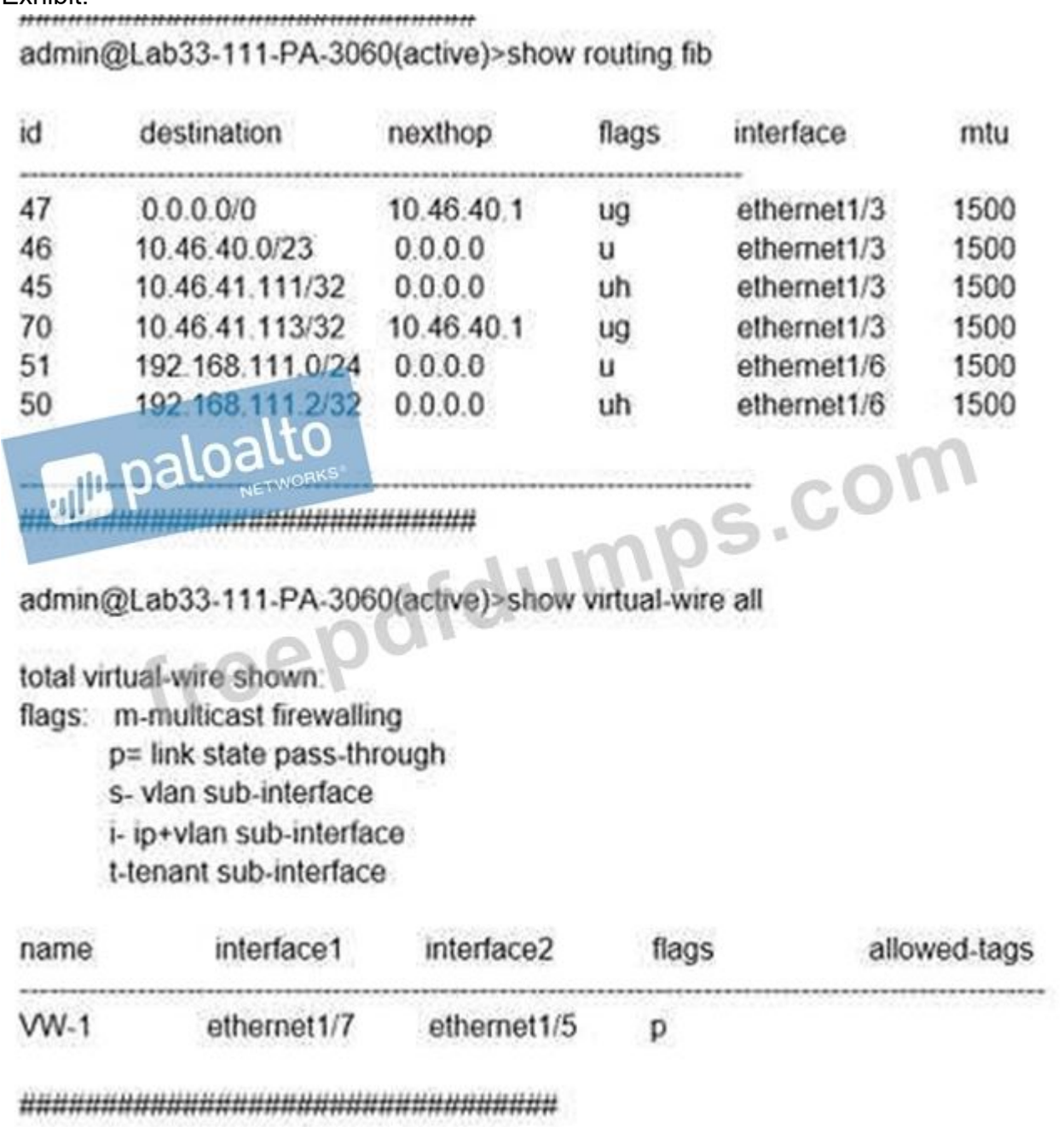
C. 192.168.93.1

D. 10.46.72.93

Answer: A (LEAVE A REPLY)

NEW QUESTION: 165

Exhibit:



```
admin@Lab33-111-PA-3060(active)>show routing fib

id      destination      nexthop      flags   interface      mtu
-------------------------------------------------------------------
47      0.0.0.0/0        10.46.40.1   ug      ethernet1/3    1500
46      10.46.40.0/23    0.0.0.0      u       ethernet1/3    1500
45      10.46.41.111/32  0.0.0.0      uh      ethernet1/3    1500
70      10.46.41.113/32  10.46.40.1   ug      ethernet1/3    1500
51      192.168.111.0/24 0.0.0.0      u       ethernet1/6    1500
50      192.168.111.2/32 0.0.0.0      uh      ethernet1/6    1500
-------------------------------------------------------------------

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p= link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name      interface1     interface2     flags     allowed-tags
-------------------------------------------------------------------
VW-1      ethernet1/7    ethernet1/5    p
```

What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

A. ethernet1/3

B. ethernet1/5

C. ethernet1/7

D. ethernet1/6

Answer: (SHOW ANSWER)

NEW QUESTION: 166
Refer to the exhibit.

Which certificates can be used as a Forward Trust certificate?
A. Forward_Trust
B. Certificate from Default Trust Certificate Authorities
C. Domain Sub-CA
D. Domain-Root-Cert
Answer: B (LEAVE A REPLY)

NEW QUESTION: 167
Which two actions are required to make Microsoft Active Directory users appear in a firewall traffic log? (Choose two.)
A. Enable User-ID on the zone object for the destination zone
B. Run the User-ID Agent using an Active Directory account that has "domain administrator" permissions
C. Configure a RADIUS server profile to point to a domain controller
D. Run the User-ID Agent using an Active Directory account that has "event log viewer" permissions
E. Enable User-ID on the zone object for the source zone
Answer: (SHOW ANSWER)

NEW QUESTION: 168
A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects. How would an administrator configure the interface to 1Gbps?
A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
B. set deviceconfig system speed-duplex 1Gbps-duplex
C. set deviceconfig system speed-duplex 1Gbps-full-duplex
D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex
Answer: B (LEAVE A REPLY)
Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Management- Port/ta-p/59034

NEW QUESTION: 169
A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects.
How would an administrator configure the interface to 1Gbps?
A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
B. set deviceconfig system speed-duplex 1Gbps-duplex
C. set deviceconfig system speed-duplex 1Gbps-full-duplex
D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex- of-the-Management-Port/ta-p/59034

NEW QUESTION: 170
Which two features does PAN-OS software use to identify applications? (Choose two)
A. port number
B. session number
C. transaction characteristics
D. application layer payload
Answer: A,D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/application-level-gateways#

NEW QUESTION: 171
A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)
A. Security zone
B. Netflow Profile
C. ARP entries
D. Virtual router
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 172
Which three options are supported in HA Lite? (Choose three.)
A. Virtual link
B. Active/passive deployment
C. Synchronization of IPsec security associations
D. Configuration synchronization
E. Session synchronization
Answer: B,C,D (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability

NEW QUESTION: 173
An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?
A. Security policy rule allowing SSL to the target server
B. Firewall connectivity to a CRL
C. Root certificate imported into the firewall with "Trust" enabled
D. Importation of a certificate from an HSM
Answer: A (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspectio

NEW QUESTION: 174
Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)
A. Red Hat Enterprise Virtualization (RHEV)
B. Kernel Virtualization Module (KVM)
C. Boot Strap Virtualization Module (BSVM)
D. Microsoft Hyper-V
Answer: (SHOW ANSWER)
Reference:
https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series docs.paloaltonetworks.com/vm-series/8-0/vm-series-deployment/about-the-vm-series-firewall/vm-series-deploym

NEW QUESTION: 175
Which log file can be used to identify SSL decryption failures?
A. Configuration

B. Threats
C. ACC
D. Traffic
Answer: D (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClboCAC

NEW QUESTION: 176
An administrator receives the following error message:
"IKE phase-2 negotiation failed when processing Proxy ID. Received local id 192. 168.33.33/24 type IPv4 address protocol 0 port 0, received remote id
172.16.33.33/24 type IPv4 address protocol 0 port 0."
How should the administrator identify the root cause of this error message?
A. Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure.
B. Check whether the VPN peer on one end is set up correctly using policy-based VPN.
C. In the IKE Gateway configuration, verify that the IP address for each VPN peer is accurate.
D. In the IPSec Crypto profile configuration, verify that PFS is either enabled on both VPN peers or disabled on both VPN peers.
Answer: B (LEAVE A REPLY)
Explanation
The VPN peer on one end is using policy-based VPN. You must configure a Proxy ID on the Palo Alto Networks firewall.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-me

NEW QUESTION: 177
What is exchanged through the HA2 link?
A. hello heartbeats
B. User-ID information
C. session synchronization
D. HA state information
Answer: C (LEAVE A REPLY)
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links

NEW QUESTION: 178
Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)
A. From the Panorama tab of the Panorama GUI select Log Collector mode and then commit changes

B. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.
C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.
D. Enter the command logger-mode enable the enter Y to confirm the change to Log Collector mode.
E. Log in the Panorama CLI of the dedicated Log Collector
Answer: B,E (LEAVE A REPLY)
(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance)

NEW QUESTION: 179
Use the image below If the firewall has the displayed link monitoring configuration what will cause a failover?

A. ethernet1/3 and ethernet1/6 going down
B. ethernet1/6 going down
C. etheme!1/3 going down
D. ethernet1/3 or ethernet1/6 going down
Answer: A (LEAVE A REPLY)

NEW QUESTION: 180
What happens when en A P firewall cluster synchronies IPsec tunnel secunty associations (SAs)?
A. Phase 2 SAs are synchronized over HA2 finks
B. Phase 1 and Phase 2 SAs are synchronized over HA2 links
C. Phase 1 SAs are synchronized over HA1 links
D. Phase 1 and Phase 2 SAs are synchronized over HA3 links
Answer: A (LEAVE A REPLY)

NEW QUESTION: 181
Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS version, and serial number?
A. debug system details
B. show session info
C. show system info
D. show system details
Answer: C (LEAVE A REPLY)
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClZuCAK
Reference:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/pan-os-60/PAN- CLI-ref.pdf

NEW QUESTION: 182
A remote administrator needs access to the firewall on an untrust interface. Which three options would you configure on an Interface Management profile to secure management access? (Choose three.)
A. Permitted IP Addresses
B. SSH
C. https
D. User-ID
E. HTTP
Answer: A,B,C (LEAVE A REPLY)
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/use-interface-management-profiles-to-restrict-access.html

NEW QUESTION: 183
View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?

A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.

B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.

C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.

D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.

Answer: C (LEAVE A REPLY)

Reference:

https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-por the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations

"Select this option to allow the GlobalProtect agent to determine if it is inside the enterprise network. This option applies only to endpoints that are configured to communicate with internal gateways.When the user attempts to log in, the agent does a reverse DNS lookup of an internal host using the specified Hostname to the specified IP Address. The host serves as a reference point that is reachable if the endpoint is inside the enterprise network. If the agent finds the host, the endpoint is inside the network and the agent connects to an internal gateway; if the agent fails to find the internal host, the endpoint is outside the network and the agent establishes a tunnel to one of the external gateways"

NEW QUESTION: 184

An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to

the virtual router.

Which two options enable the administrator to troubleshoot this issue? (Choose two.)

A. View System logs.

B. Perform a traffic pcap at the routing stage.

C. View Runtime Stats in the virtual router.

D. Add a redistribution profile to forward as BGP updates.

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 185

An administrator with 84 firewalls and Panorama does not see any WildFire logs in Panorama.

All 84 firewalls have an active WildFire subscription On each firewall WildFire logs are available. This issue is occurring because forwarding of which type of logs from the firewalls to Panorama is missing?

A. WridFire logs

B. System logs

C. Traffic logs

D. Threat logs

Answer: (SHOW ANSWER)

NEW QUESTION: 186

An engineer must configure a new SSL decryption deployment

Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

A. There must be a certificate with both the Forward Trust option and Forward Untrust option selected

B. A Decryption profile must be attached to the Decryption policy that the traffic matches

C. A Decryption profile must be attached to the Security policy that the traffic matches

D. There must be a certificate with only the Forward Trust option selected

Answer: B (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html

NEW QUESTION: 187

Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)

A. Red Hat Enterprise Virtualization (RHEV)

B. Kernel Virtualization Module (KVM)

C. Boot Strap Virtualization Module (BSVM)

D. Microsoft Hyper-V

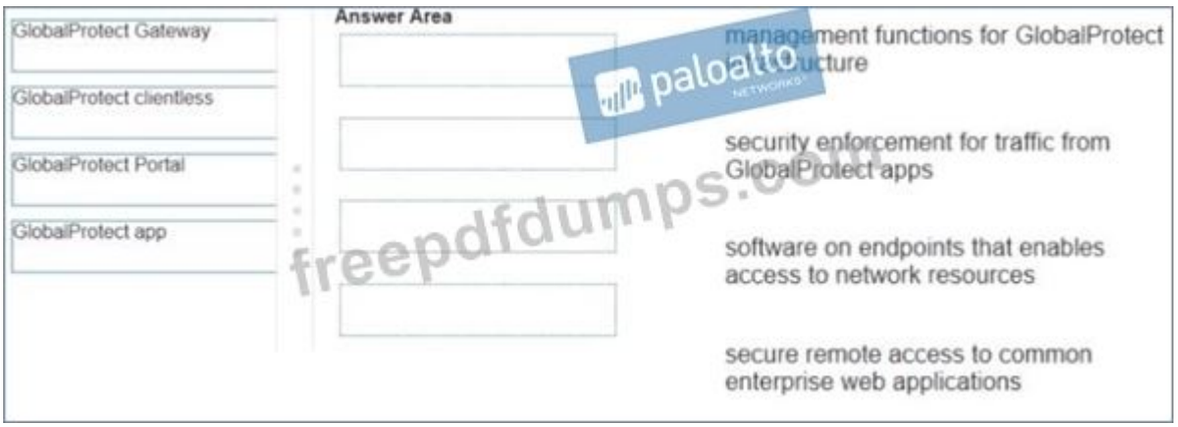
Answer: (SHOW ANSWER)

Reference:

https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series

NEW QUESTION: 188

Match each GlobalProtect component to the purpose of that component



Answer:

NEW QUESTION: 189

SAML SLO is supported for which two firewall features? (Choose two.)

A. GlobalProtect Portal

B. CaptivePortal

C. WebUI

D. CLI

Answer: A,B (LEAVE A REPLY)

Explanation/Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-saml- authentication

NEW QUESTION: 190

Which two are valid ACC GlobalProtect Activity tab widgets? (Choose two)

A. Successful GlobalProtect Connection Activity

B. Successful GlobalProtect Deployed Activity

C. GlobalProtect Quarantine Activity

D. GlobalProtect Deployment Activity

Answer: C,D (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/globalprotect-features/enhanced-logging-for- The ACC displays a graphical view of user activity in your

GlobalProtect deployment on the GlobalProtect Activity tab. The following charts are available:
*Successful GlobalProtect Connection Activity
*Unsuccessful GlobalProtect Connection Activity *GlobalProtect Deployment Activity

NEW QUESTION: 191
Exhibit:

```
##################################
admin@Lab33-111-PA-3060(active)>show routing fib

id        destination        nexthop        flags      interface        mtu
--------------------------------------------------------------------------
47        0.0.0.0/0          10.46.40.1     ug         ethernet1/3      1500
46        10.46.40.0/23      0.0.0.0        u          ethernet1/3      1500
45        10.46.41.111/32    0.0.0.0        uh         ethernet1/3      1500
70        10.46.41.113/32    10.46.40.1     ug         ethernet1/3      1500
51        192.168.111.0/24   0.0.0.0        u          ethernet1/6      1500
50        192.168.111.2/32   0.0.0.0        uh         ethernet1/6      1500

--------------------------------------------------------------------------
##################################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p= link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name          interface1       interface2       flags          allowed-tags
--------------------------------------------------------------------------------
VW-1          ethernet1/7      ethernet1/5      p

##################################
```


What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?
A. ethernet1/5
B. ethernet1/6
C. ethernet1/3

D. ethernet1/7

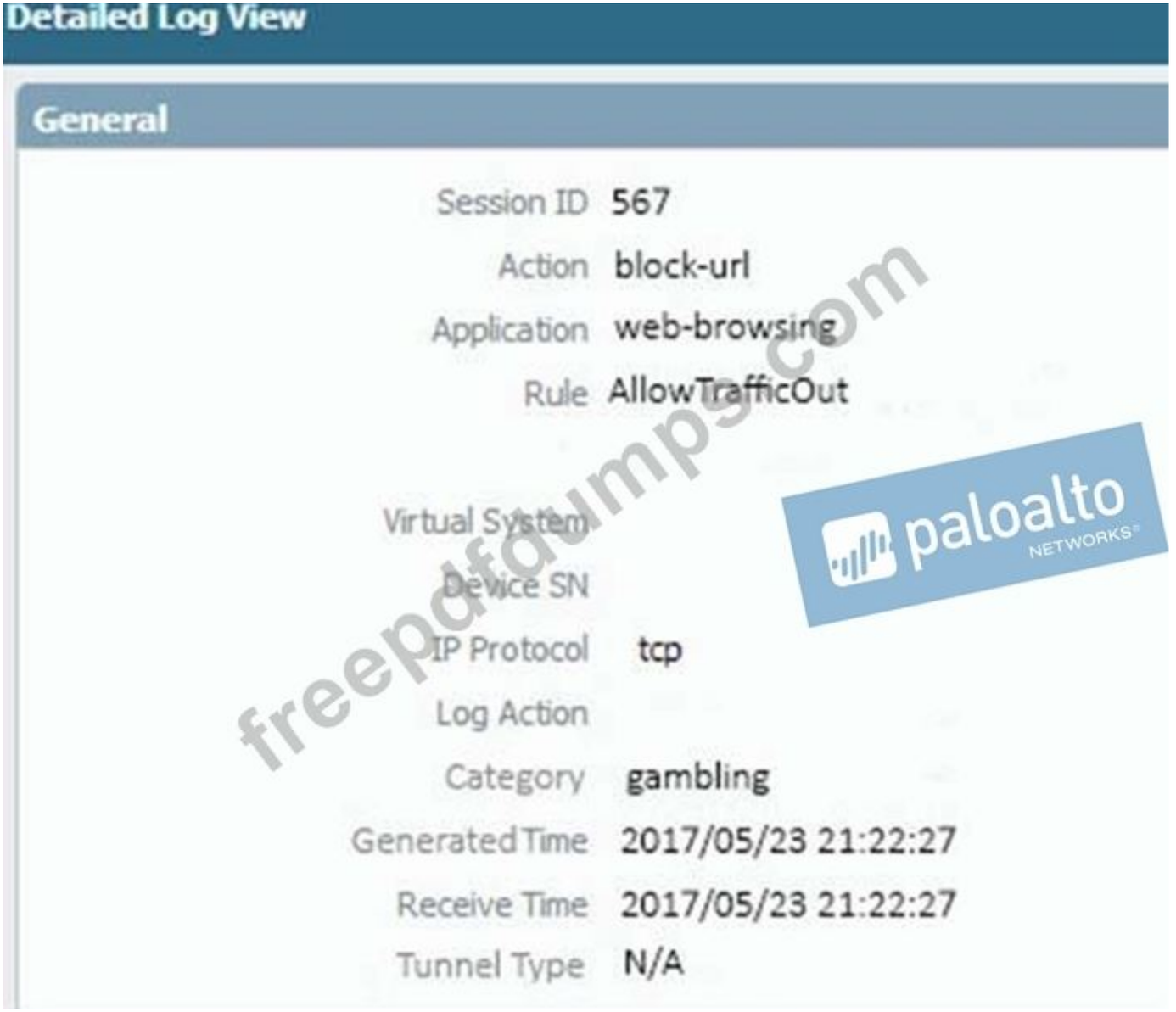
Answer: (SHOW ANSWER)

NEW QUESTION: 192

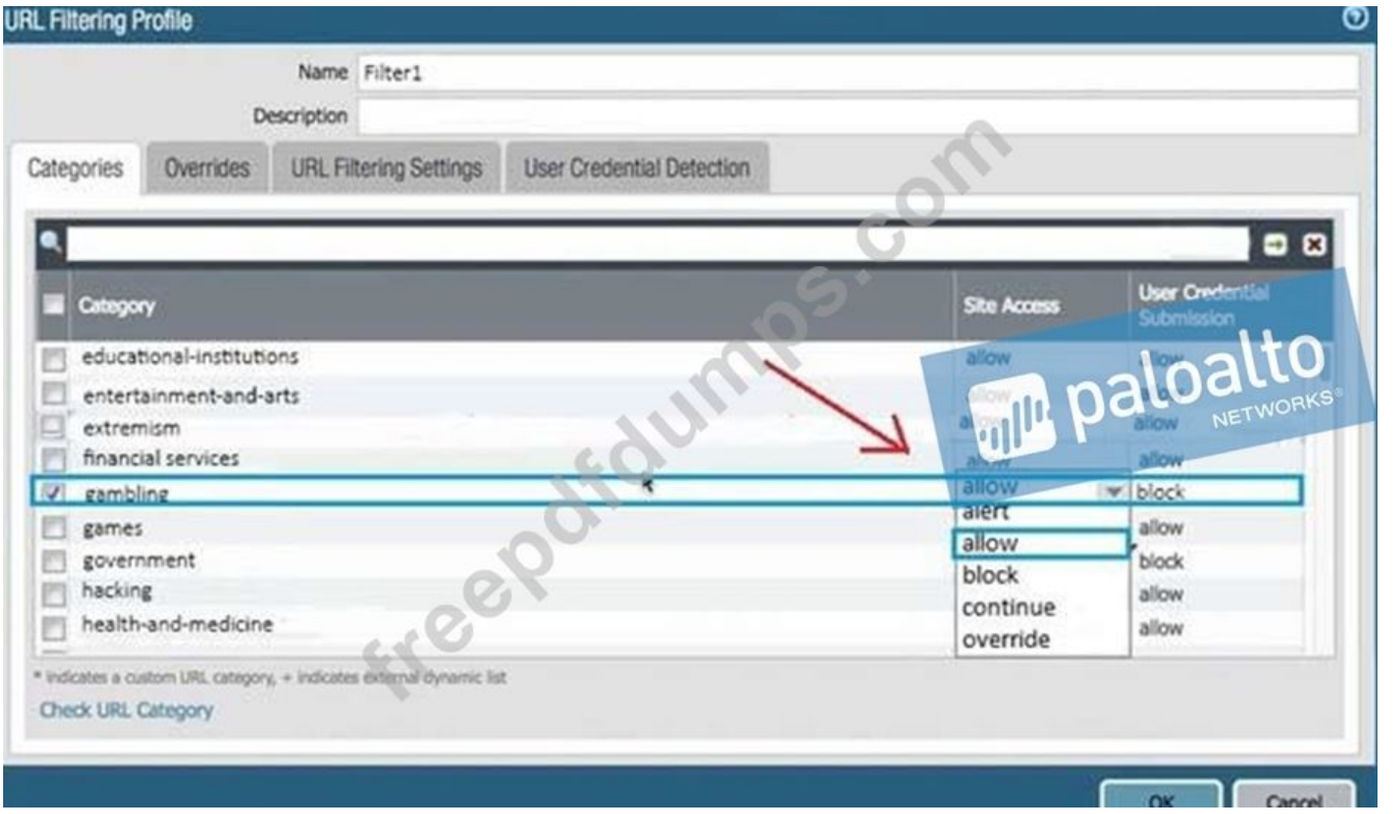
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.

Which configuration change should the administrator make?

A:



B:


URL Filtering Profile
Name Filter1
Description
Categories
Overrides
URL Filtering Settings
User Credential Detection
Category
Site Access
User Credential Submission
educational-institutions
entertainment-and-arts
extremism
financial services
gambling
games
government
hacking
health-and-medicine
allow
block
alert
allow
block
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category
OK
Cancel

C:


ecurity Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Target
Name www.megamillions.com
Rule Type universal (default)
Description
Tags
OK
Cancel

D:

E:

A. Option E

B. Option C

C. Option B

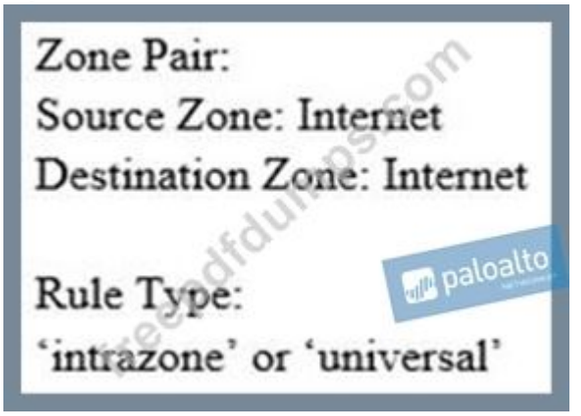
D. Option D

E. Option A

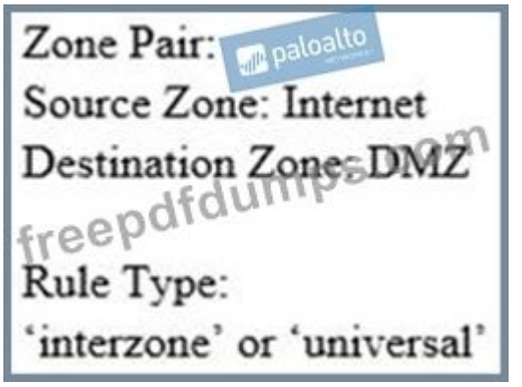
Answer: C (LEAVE A REPLY)

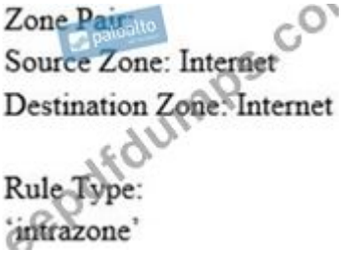
NEW QUESTION: 193

Which Zone Pair and Rule Type will allow a successful connection for a user on the Internet zone to a web server hosted on the DMZ zone? The web server is reachable using a Destination NAT policy in the Palo Alto Networks firewall.

A. 

B. 

C. 

D. 

Answer: C (LEAVE A REPLY)

NEW QUESTION: 194

Which method will dynamically register tags on the Palo Alto Networks NGFW?

A. Restful API or the VMWare API on the firewall or on the User-ID agent or the read-only domain controller (RODC)

B. Restful API or the VMware API on the firewall or on the User-ID agent

C. XML-API or the VMware API on the firewall or on the User-ID agent or the CLI

D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent

Answer: (SHOW ANSWER)

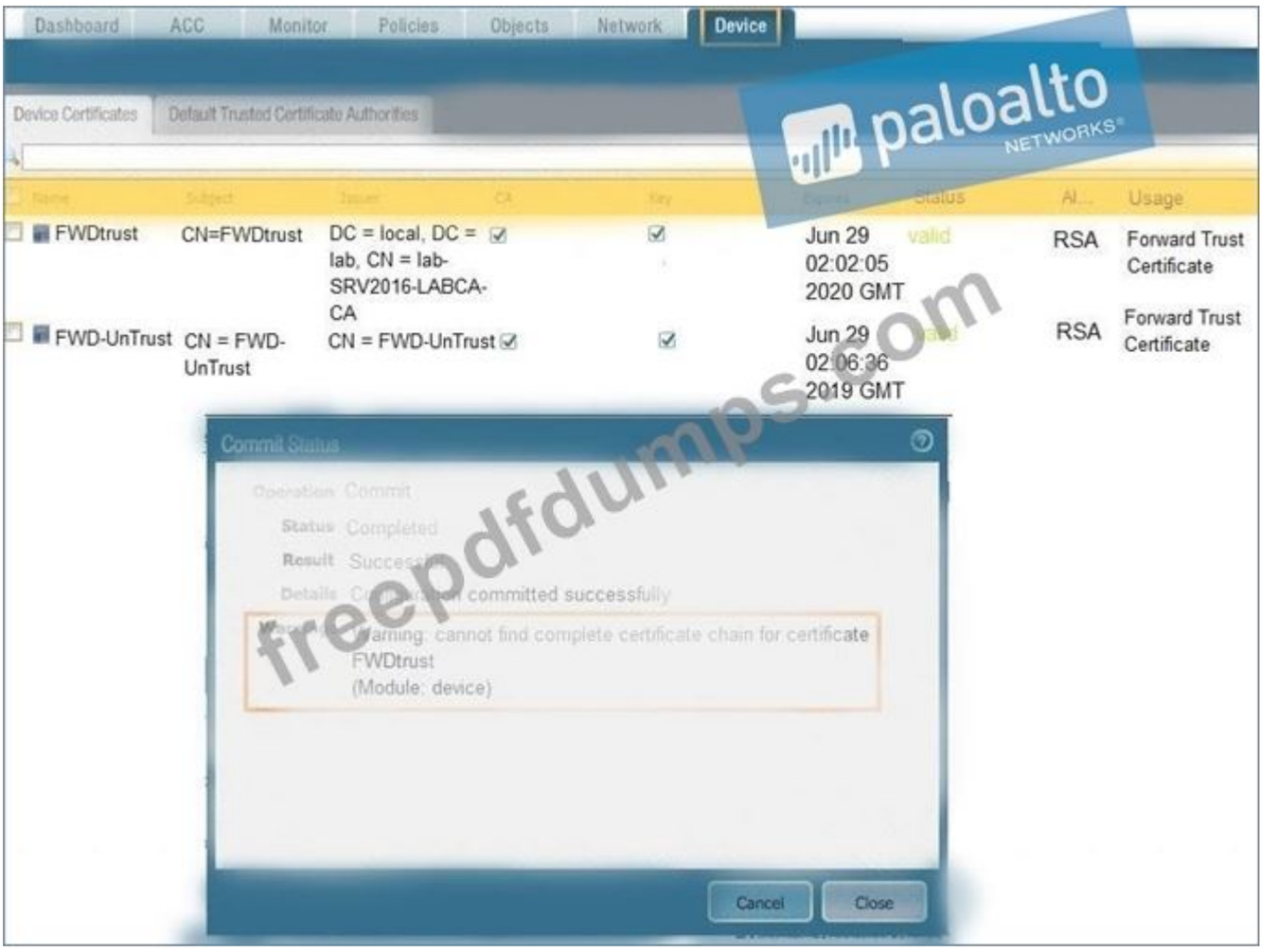
To mitigate the challenges of scale, lack of flexibility, and performance, network architectures today allow for virtual machines (VMs) and applications to be provisioned, changed, and deleted on demand. This agility, though, poses a challenge for security administrators because they have limited visibility into the IP addresses of the dynamically provisioned VMs and the plethora of applications that can be enabled on these virtual resources. Firewalls (hardware-based and VM-Series models) support the ability to register IP addresses, IP sets (IP ranges and subnets), and tags dynamically. The IP addresses and tags can be registered on the firewall directly or from Panorama. You can also automatically remove tags on the source and destination IP addresses included in a firewall log.
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/register-ip-addresses-and-tags-dynamically.html

NEW QUESTION: 195
In the following image from Panorama, why are some values shown in red?

Device Name	Logging Rate (Log/sec)	Throughput (KB/sec)	Session Count (Sessions)
uk3	781	209	40221
sg2	0	953	170
us3	291	0	67455

A. us3 has a logging rate that deviates from the administrator-configured thresholds.
B. sg2 session count is the lowest compared to the other managed devices.
C. sg2 has misconfigured session thresholds.
D. uk3 has a logging rate that deviates from the seven-day calculated baseline.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 196
Based on the image, what caused the commit warning?



A. SSL Forward Proxy requires a public certificate to be imported into the firewall.
B. The CA certificate for FWDtrust has not been imported into the firewall.
C. The FWDtrust certificate does not have a certificate chain.
D. The FWDtrust certificate has not been flagged as Trusted Root CA.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 197
An administrator has a PA-820 firewall with an active Threat Prevention subscription.
The administrator is considering adding a WildFire subscription.
How does adding the WildFire subscription improve the security posture of the organization1?
A. WildFire and Threat Prevention combine to minimize the attack surface

B. WildFire and Threat Prevention combine to provide the utmost security posture for the firewall
C. After 24 hours WildFire signatures are included in the antivirus update
D. Protection against unknown malware can be provided in near real-time
Answer: (SHOW ANSWER)

NEW QUESTION: 198
A firewall should be advertising the static route 10 2 0 0/24 into OSPF The configuration on the neighbor is correct but the route is not in the neighbor's routing table Which two configurations should you check on the firewall'? (Choose two)
A. In the OSFP configuration ensure that the correct redistribution profile is selected in the OSPF Export Rules section
B. Within the redistribution profile ensure that Redist is selected
C. In the redistribution profile check that the source type is set to "ospf"
D. Ensure that the OSPF neighbor state is "2-Way"
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 199
Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?
A. Configure an SSL/TLS Profile.
B. Set up SSL/TLS under Polices > Service/URL Category>Service.
C. Set up Security policy rule to allow SSL communication.
D. Configure a Decryption Profile and select SSL/TLS services.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 200
A organizations administrator has the funds available to purchase more firewalls to increase the organization's security posture.
The partner SE recommends placing the firewalls as close as possible to the resources that they protect
Is the SE's advice correct and why or why not?
A. Yes Firewalls are session based so they do not scale to millions of CPS
B. No Placing firewalls m front of perimeter DDoS devices provides greater protection tor sensitive devices inside the network
C. Yes Zone Protection profiles can be tailored to the resources that they protect via the configuration of specific device types and operating systems
D. No Firewalls provide new defense and resilience to prevent attackers at every stage of the cyberattack lifecycle independent of placement
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/firewall-placement-for-dos-protection

NEW QUESTION: 201
N NO: 54
Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only?
A. Add server IP Security Policy exception
B. Apply an Application Override
C. Disable HIP Profile
D. Disable Server Response Inspection
Answer: (SHOW ANSWER)

NEW QUESTION: 202
YouTube videos are consuming too much bandwidth on the network, causing delays in mission-critical traffic. The administrator wants to throttle YouTube traffic.
The following interfaces and zones are in use on the firewall:
- ethernet 1/1, Zone: Untrust (Internet-facing)
- ethernet 1/2, Zone: Trust (client-facing)
A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet 1/1 has a QoS profile called Outbound, and interface Ethernet 1/21 has a QoS profile called Inbound.
Which setting for Class 6 will throttle YouTube traffic?
A. Outbound profile with Guaranteed Ingress
B. Inbound profile with Maximum Egress
C. Inbound profile with Guaranteed Egress
D. Outbound profile with Maximum Ingress
Answer: B (LEAVE A REPLY)
Identify the egress interface for applications that you identified as needing QoS treatment.
The egress interface for traffic depends on the traffic flow. If you are shaping incoming traffic, the egress interface is the internal-facing interface. If you are shaping outgoing traffic, the egress interface is the external-facing interface.
https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/quality-of-service/configure-qos

NEW QUESTION: 203
If malware is detected on the internet perimeter, what other places in the network might be affected?
A. Data Center
B. Endpoints
C. Cloud
D. All of the above
E. Branch Offices

Answer: (SHOW ANSWER)

NEW QUESTION: 204
An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?
A. Enable and configure the Packet Buffer Protection thresholds.
Enable Packet Buffer Protection per ingress zone.
B. Enable and then configure Packet Buffer thresholds.
Enable Interface Buffer protection.
C. Create and Apply Zone Protection Profiles in all ingress zones.
Enable Packet Buffer Protection per ingress zone.
D. Configure and apply Zone Protection Profiles for all egress zones.
Enable Packet Buffer Protection per egress zone.
E. Enable per-vsys Session Threshold alerts and triggers for Packet Buffer Limits.
Enable Zone Buffer Protection per zone.
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/zone-protection-and-dos- protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection

NEW QUESTION: 205
Based on the following image,

what is the correct path of root, intermediate, and end-user certificate?

A. VeriSign > Palo Alto Networks > Symantec

B. Palo Alto Networks > Symantec > VeriSign

C. VeriSign > Symantec > Palo Alto Networks

D. Symantec > VeriSign > Palo Alto Networks

Answer: C (LEAVE A REPLY)

NEW QUESTION: 206

If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto networks NGFW to inspect when users browse to HTTP(S) websites?

A. SSL Forward Proxy

B. SSL Inbound Inspection

C. TLS Bidirectional proxy

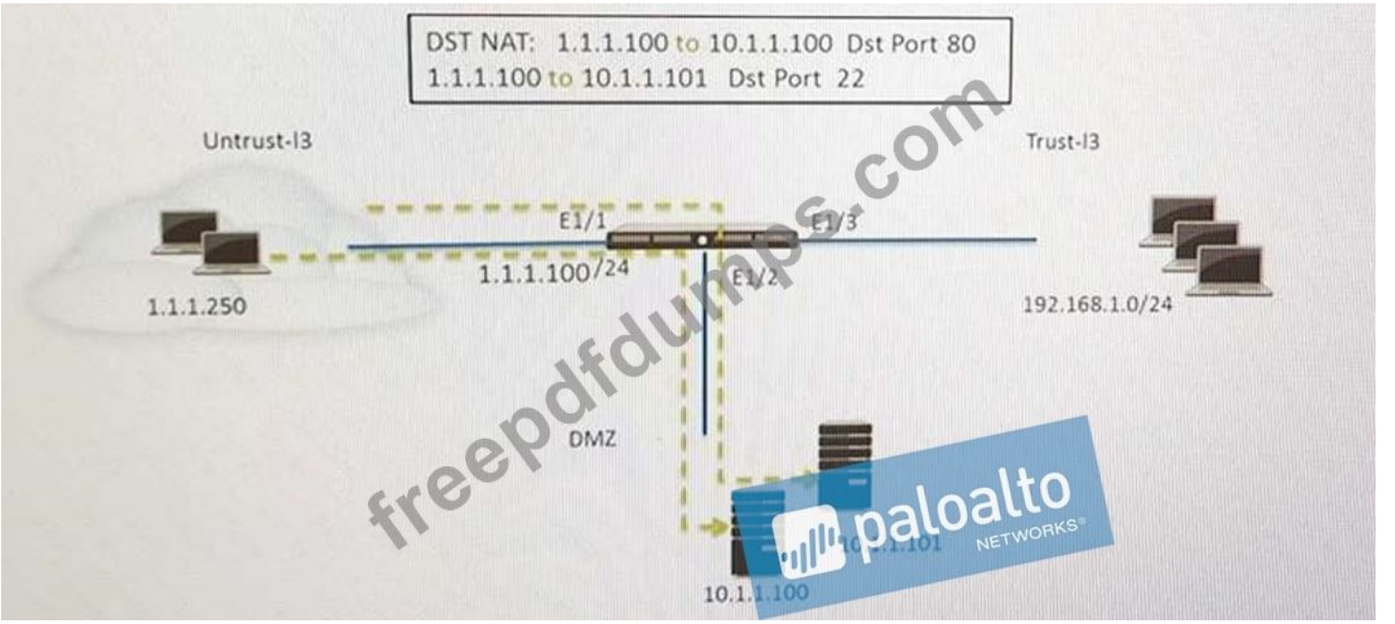
D. SSL Outbound Inspection

Answer: A (LEAVE A REPLY)

https://live.paloaltonetworks.com/t5/Learning-Articles/Difference-Between-SSL-Forward-Proxy-and-Inbound-Inspection/ta-p/55553

NEW QUESTION: 207

Refer to the exhibit.



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

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

A. Untrust (Any) to Untrust (10.1.1.1) Ssh-Allow

B. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow

C. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow

D. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow

Answer: (SHOW ANSWER)

NEW QUESTION: 208

In the screenshot above which two pieces ot information can be determined from the ACC configuration shown? (Choose two)

A. Threats with a severity of "high" are always listed at the top of the Threat Name list

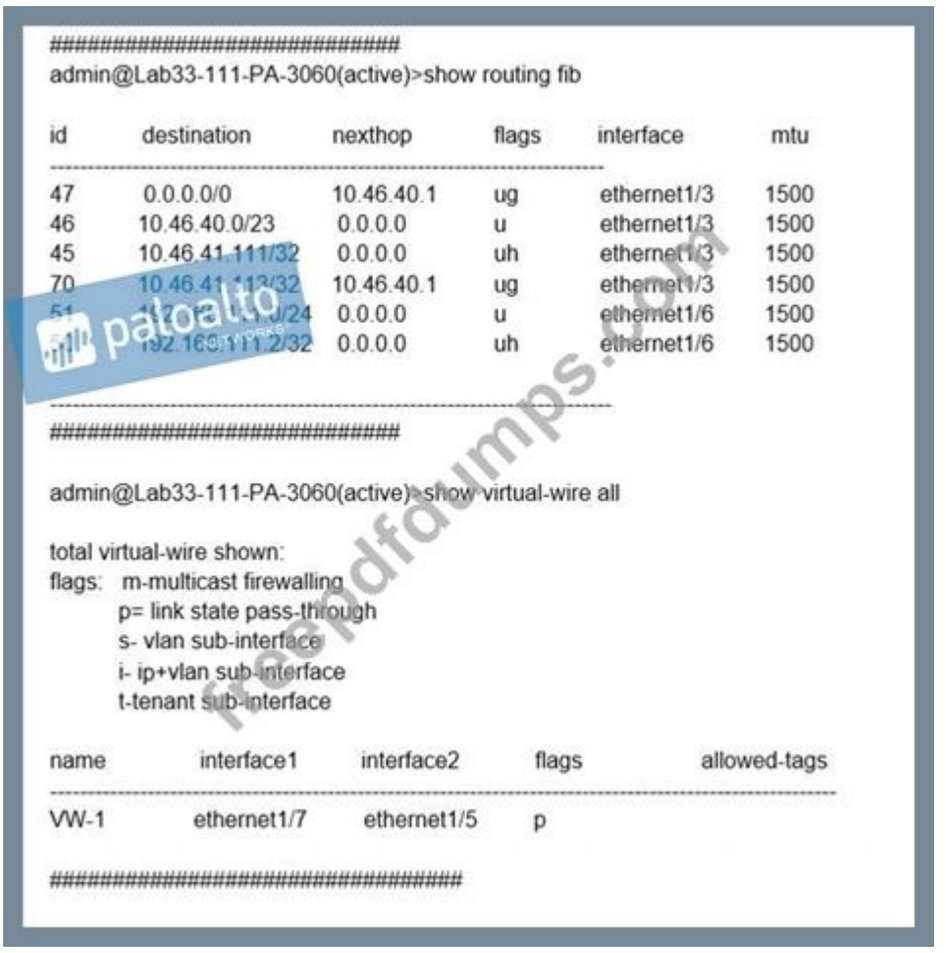
B. The ACC has been filtered to only show the FTP application

C. The Network Activity tab will display all applications, including FTP.
D. Insecure-credentials, brute-force and protocol-anomaly are all a part of the vulnerability Threat Type
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 209
A customer is replacing its legacy remote-access VPN solution. Prisma Access has been selected as the replacement. During onboarding, the following options and licenses were selected and enabled:
- Prisma Access for Remote Networks: 300Mbps
- Prisma Access for Mobile Users: 1500 Users
- Cortex Data Lake: 2TB
- Trusted Zones: trust
- Untrusted Zones: untrust
- Parent Device Group: shared
The customer wants to forward to a Splunk SIEM the logs that are generated by users that are connected to Prisma Access for Mobile Users.
Which two settings must the customer configure? (Choose two.)
A. Configure Panorama Collector group device log forwarding to send logs to the Splunk syslog server.
B. Configure Cortex Data Lake log forwarding and add the Splunk syslog server.
C. Configure a log forwarding profile and select the Panorama/Cortex Data Lake checkbox. Apply the Log Forwarding profile to all of the security policy rules in Mobile_User_Device_Group.
D. Configure a Log Forwarding profile, select the syslog checkbox, and add the Splunk syslog server. Apply the Log Forwarding profile to all of the security policy rules in the Mobile_User_Device_Group.
Answer: (SHOW ANSWER)
Reference: https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-log-forwarding-app/forward-logs-from-logging-service-to-syslog-server.html

NEW QUESTION: 210
How does Panorama prompt VMWare NSX to quarantine an infected VM?
A. Email Server Profile
B. HTTP Server Profile
C. Syslog Server Profile
D. SNMP Server Profile
Answer: B (LEAVE A REPLY)

NEW QUESTION: 211
Refer to the exhibit.



```
##################################
admin@Lab33-111-PA-3060(active)>show routing fib

id      destination      nexthop      flags   interface      mtu
--------------------------------------------------------------------
47      0.0.0.0/0        10.46.40.1   ug      ethernet1/3    1500
46      10.46.40.0/23    0.0.0.0      u       ethernet1/3    1500
45      10.46.41.111/32  0.0.0.0      uh      ethernet1/3    1500
70      10.46.41.113/32  10.46.40.1   ug      ethernet1/3    1500
51      192.168.111.0/24 0.0.0.0      u       ethernet1/6    1500
50      192.168.111.2/32 0.0.0.0      uh      ethernet1/6    1500
--------------------------------------------------------------------
##################################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p= link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name      interface1    interface2    flags    allowed-tags
--------------------------------------------------------------------
VW-1      ethernet1/7   ethernet1/5   p

##################################
```

Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

A. ethernet1/3

B. ethernet1/5

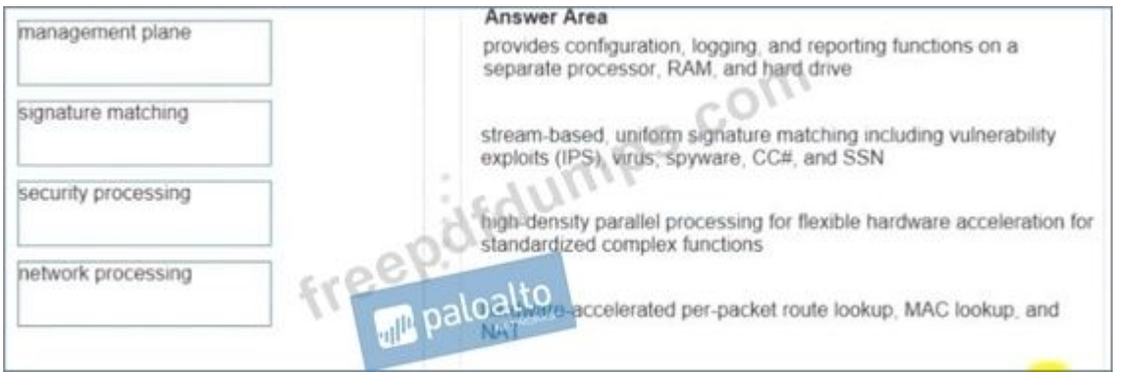
C. ethernet1/6

D. ethernet1/7

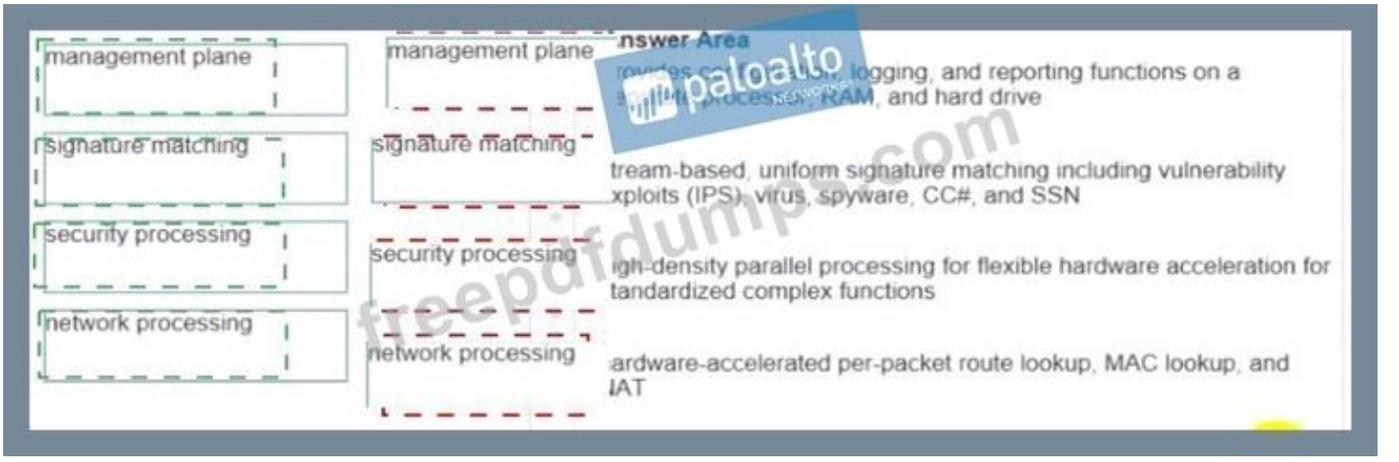
Answer: (SHOW ANSWER)

NEW QUESTION: 212

Please match the terms to their corresponding definitions.

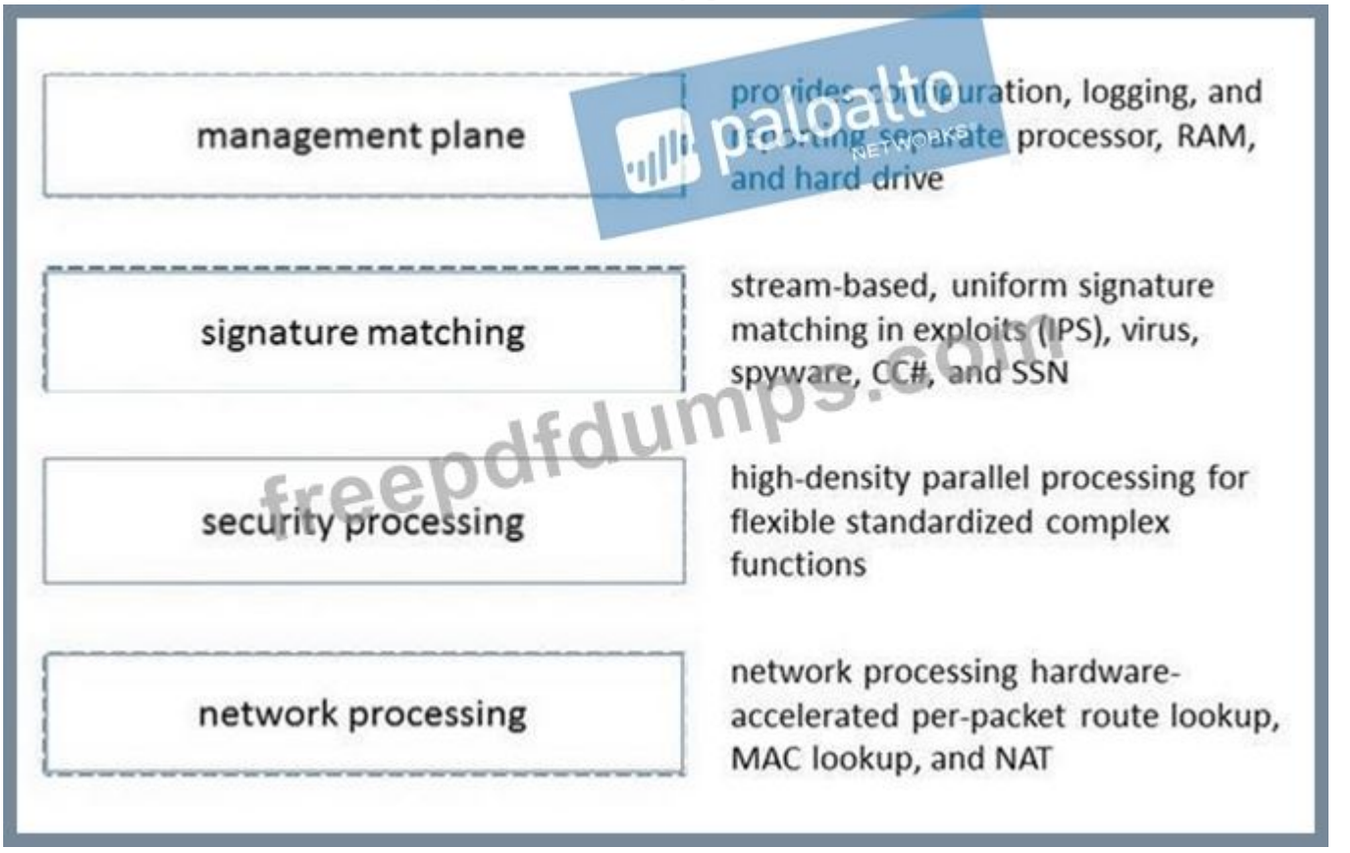


Answer:



Explanation

Graphical user interface Description automatically generated with medium confidence



NEW QUESTION: 213

A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

A. Security policy to identify the custom application.

B. Custom application.

C. Application Override policy.

D. Custom Service object.

Answer: (SHOW ANSWER)

NEW QUESTION: 214

Which three rule types are available when defining policies in Panorama? (Choose three.)

A. Pre Rules

B. Post Rules

C. Default Rules

D. Stealth Rules

E. Clean Up Rules

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

https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama-web-interface/defining-policies-on-panorama

NEW QUESTION: 215

Which three options are supported in HA Lite? (Choose three.)

A. Virtual link

B. Active/passive deployment

C. Synchronization of IPsec security associations

D. Configuration synchronization

E. Session synchronization

Answer: (SHOW ANSWER)

Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability/ha-lite

NEW QUESTION: 216

If the firewall is configured for credential phishing prevention using the "Domain Credential Filter" method, which login will be detected as credential theft?

A. Mapping to the IP address of the logged-in user.

B. First four letters of the username matching any valid corporate username.

C. Using the same user's corporate username and password.

D. Marching any valid corporate username.

Answer: A (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential- ention Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/crede phishing-prevention

NEW QUESTION: 217
Which two are valid ACC GlobalProtect Activity tab widgets? (Choose two)
A. Successful GlobalProtect Connection Activity
B. Successful GlobalProtect Deployed Activity
C. GlobalProtect Quarantine Activity
D. GlobalProtect Deployment Activity
Answer: C,D (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/globalprotect-features/enhanced-logging-for-globalprotect.html
The ACC displays a graphical view of user activity in your GlobalProtect deployment on the GlobalProtect Activity tab. The following charts are available: *Successful GlobalProtect Connection Activity *Unsuccessful GlobalProtect Connection Activity *GlobalProtect Deployment Activity

NEW QUESTION: 218
A customer is replacing their legacy remote access VPN solution.
The current solution is in place to secure internet egress and provide access to resources located in the main datacenter for the connected clients.
Prisma Access has been selected to replace the current remote access VPN solution.
During onboarding the following options and licenses were selected and enabled

What must be configured on Prisma Access to provide connectivity to the resources in the datacenter?
A. Configure a service connection to provide connectivity to the datacenter
B. Configure Dynamic Routing to provide connectivity to the datacenter
C. Configure a remote network to provide connectivity to the datacenter
D. Configure a mobile user gateway in the region closest to the datacenter to enable connectivity to the datacenter
Answer: C (LEAVE A REPLY)

NEW QUESTION: 219
An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair.
Which NGFW receives the configuration from Panorama?
A. The active firewall, which then synchronizes to the passive firewall
B. The Passive firewall, which then synchronizes to the active firewall
C. Both the active and passive firewalls independently, with no synchronization afterward
D. Both the active and passive firewalls, which then synchronize with each other
Answer: (SHOW ANSWER)

NEW QUESTION: 220
Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)
A. Create a no-decrypt Decryption Policy rule.
B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
C. Create a Dynamic Address Group for untrusted sites
D. Create a Security Policy rule with vulnerability Security Profile attached.
E. Enable the "Block sessions with untrusted issuers" setting.
Answer: (SHOW ANSWER)
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-decryption-profile

NEW QUESTION: 221
Which Panorama administrator types require the configuration of at least one access domain? (Choose two.)
A. Device Group
B. Role Based
C. Custom Panorama Admin
D. Template Admin
E. Dynamic
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 222
Use the image below. If the firewall has the displayed link monitoring configuration what will cause a failover?

A. ethernet1/3 and ethernet1/6 going down
B. etheme!1/3 going down
C. ethernet1/3 or ethernet1/6 going down
D. ethernet1/6 going down
Answer: A (LEAVE A REPLY)

NEW QUESTION: 223
In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)
A. wildcard server certificate
B. enterprise CA certificate
C. client certificate
D. server certificate
E. self-signed CA certificate
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-forward-proxy.html

NEW QUESTION: 224
A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green.
The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured.
What can be the cause of this problem?
A. Interface Ethernet 1/1 is in Virtual Wire Mode.
B. DNS has not been properly configured on the firewall.
C. No Zone has been configured on Ethernet 1/4.
D. DNS has not been properly configured on the host.
Answer: (SHOW ANSWER)

NEW QUESTION: 225
A company.com wants to enable Application Override. Given the following screenshot:

Which two statements are true if Source and Destination traffic match the Application Override policy?
(Choose two)
A. Traffic utilizing UDP Port 16384 will bypass the App-ID and Content-ID engines.
B. Traffic that matches "rtp-base" will bypass the App-ID and Content-ID engines.
C. Traffic utilizing UDP Port 16384 will now be identified as "rtp-base".
D. Traffic will be forced to operate over UDP Port 16384.
Answer: (SHOW ANSWER)

NEW QUESTION: 226
Which CLI command can be used to export the tcpdump capture?
A. scp export tcpdump from mgmt.pcap to <username@host:path>
B. scp extract mgmt-pcap from mgmt.pcap to <username@host:path>
C. scp export mgmt-pcap from mgmt.pcap to <username@host:path>
D. download mgmt.-pcap
Answer: C (LEAVE A REPLY)
Reference:
https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management-Interface/ta- p/55415

NEW QUESTION: 227
Before you upgrade a Palo Alto Networks NGFW what must you do?
A. Make sure that the PAN-OS support contract is valid for at least another year
B. Export a device state of the firewall
C. Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.
D. Make sure that the firewall is running a supported version of the app + threat update
Answer: D (LEAVE A REPLY)
Before you upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRrCAK

NEW QUESTION: 228
A firewall administrator has completed most of the steps required to provision a standalone Palo Alto Networks Next-Generation Firewall. As a final step, the administrator wants to test one of the security policies.
Which CLI command syntax will display the rule that matches the test?
A. test security -policy- match source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number
B. show security rule source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>
C. test security rule source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>
D. show security-policy-match source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>
Answer: A (LEAVE A REPLY)
test security-policy-match source
test security-policy-match source <source IP> destination <destination IP> protocol <protocol number>
https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Test-Which-Security-Policy-Applies-to-a-Traffic-Flow/ta-p/53693

NEW QUESTION: 229
Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service?
(Choose three.)
A. .dll

B. .exe
C. .src
D. .apk
E. .pdf
F. .jar
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding

NEW QUESTION: 230
Ethernet1/1 has been configured with the following subinterfaces:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	Security Zone
ethernet1/1	Layer3	pingsshhttpssnmp		none	none	Untagged	none
ethernet1/1.798	Layer3			10.10.30.1/24	VR1	798	none
ethernet1/1.799	Layer3			10.10.30.1/24	default	799	none
ethernet1/1.801	Layer3			10.10.30.1/24	VR1	801	none

The following security policy rule is applied:

	Name	Tags	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Application	Service	Action	Profile	Options
1	Allow all	798 799 801	any	any	any	any	any	any	any	any	✓	none	

The Interface Management Profile permits the following:

A customer is trying to ping 10.10.10.1 from VLAN 799 IP 10.10.10.2/24.
What will be the result of this ping?

A. The ping will not successful because the security policy permits this traffic.
B. The ping will not be successful because the virtual router is different from the other subinterfaces.
C. The ping will not be successful because the security policy does not apply to VLAN 799.
D. The ping will not be successful because there is no management profile attached to ethernet1/1.799.
E. The ping will not successful because the management profile applied to ethernet1/1 allows ping.
Answer: (SHOW ANSWER)

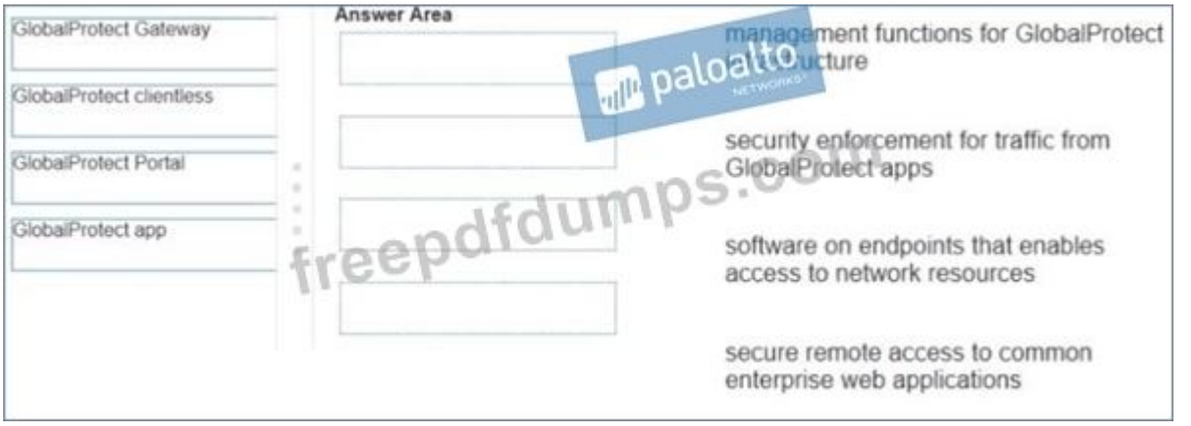
NEW QUESTION: 231
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration Once deployed each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers Which VPN preconfigured configuration would adapt to changes when deployed to the future site?
A. PPTP tunnels
B. IPsec tunnels using IKEv2
C. GlobalProtect satellite
D. GlobalProtect client
Answer: (SHOW ANSWER)

NEW QUESTION: 232
Cortex XDR notifies an administrator about grayware on the endpoints.
There are no entnes about grayware in any of the logs of the corresponding firewall.
Which setting can the administrator configure on the firewall to log grayware verdicts?
A. within the log settings option in the Device tab
B. in WildFire General Settings, select "Report Grayware Files"
C. within the log forwarding profile attached to the Security policy rule
D. in Threat General Settings^ select "Report Grayware Files"
Answer: D (LEAVE A REPLY)

NEW QUESTION: 233
During SSL decryption which three factors affect resource consumption1? (Choose three)
A. TLS protocol version
B. transaction size
C. key exchange algorithm
D. applications that use non-standard ports
E. certificate issuer
Answer: A,B,C (LEAVE A REPLY)
https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment.html

NEW QUESTION: 234

Match each GlobalProtect component to the purpose of that component



Answer:

NEW QUESTION: 235

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. Application changed from content inspection

D. Session application identified.

Answer: (SHOW ANSWER)

http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309

NEW QUESTION: 236

The certificate information displayed in the following image is for which type of certificate?

Exhibit:

A. Self-Signed Root CA certificate
B. Forward Trust certificate
C. Public CA signed certificate
D. Web Server certificate
Answer: A (LEAVE A REPLY)

NEW QUESTION: 237
What best describes the HA Promotion Hold Time?
A. the time that a passive firewall with a low device priority will wait before taking over as the active firewall if the firewall is operational again
B. the time that the passive firewall will wait before taking over as the active firewall after communications with the HA peer have been lost
C. the time that is recommended to avoid an HA failover due to the occasional flapping of neighboring devices
D. the time that is recommended to avoid a failover when both firewalls experience the same link/path monitor failure simultaneously
Answer: B (LEAVE A REPLY)

NEW QUESTION: 238
Which three user authentication services can be modified to provide the Palo Alto Networks NGFW with both usernames and role names? (Choose three.)
A. TACACS+
B. Kerberos
C. PAP

D. LDAP
E. SAML
F. RADIUS
Answer: B,D,E (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrat

NEW QUESTION: 239
How can packet buffer protection be configured?
A. at zone level to protect firewall resources and ingress zones, but not at the device level
B. at the interface level to protect firewall resources
C. at the device level (globally) to protect firewall resources and ingress zones, but not at the zone level
D. at the device level (globally) and, if enabled globally, at the zone level
Answer: D (LEAVE A REPLY)
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection

NEW QUESTION: 240
Which CLI command can be used to export the tedium capture?
A. scp export tcpdump from mgmt.pcap to <username@host:path>
B. scp extract mgmt-pcap from mgmt.pcap to <username@host:path>
C. scp export mgmt-pcap from mgmt.pcap to <username@host:path>
D. download mgmt.-pcap
Answer: C (LEAVE A REPLY)
Reference:
https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management-I p/55415

NEW QUESTION: 241
Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service?
(Choose three.)
A. .dll
B. .exe
C. .src
D. .apk
E. .pdf
F. .jar

Answer: (SHOW ANSWER)
Reference:
https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-file-type-su

NEW QUESTION: 242
Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x-enabled wireless network device that has no native integration with PAN-OS software?
A. XML API
B. Port Mapping
C. Client Probing
D. Server Monitoring
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api.html
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/server-monitoring.html

NEW QUESTION: 243
Which three user authentication services can be modified to provide the Palo Alto Networks NGFW with both usernames and role names? (Choose three.)
A. TACACS+
B. Kerberos
C. PAP
D. LDAP
E. SAML
F. RADIUS
Answer: A,E,F (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrat

NEW QUESTION: 244
Where is information about packet buffer protection logged?
A. Alert entries are in the Alarms log. Entries for dropped traffic, discarded sessions, and blocked IP address are in the Threat log
B. All entries are in the System log
C. Alert entries are in the System log. Entries for dropped traffic, discarded sessions and blocked IP addresses are in the Threat log
D. All entries are in the Alarms log
Answer: B (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNGFCA4

NEW QUESTION: 245
Which CLI command enables an administrator to view details about the firewall including uptime, PAN-
OS® version, and serial number?
A. debug system details
B. show session info
C. show system info
D. show system details
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/Quick-Reference-Guide-Helpful-Commands/ta-p/56511

NEW QUESTION: 246
An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.
Which interface type and license feature are necessary to meet the requirement?
A. Decryption Mirror interface with the Threat Analysis license
B. Virtual Wire interface with the Decryption Port Export license
C. Tap interface with the Decryption Port Mirror license
D. Decryption Mirror interface with the associated Decryption Port Mirror license
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/decryption- concepts/decryption-mirroring

NEW QUESTION: 247
An organization is building a Bootstrap Package to deploy Palo Alto Networks VM-Series firewalls into their AWS tenant Which two statements are correct regarding the bootstrap package contents? (Choose two)

A. The /config /content and /software folders are mandatory while the /license and /plugin folders are optional
B. The bootstrap package is stored on an AFS share or a discrete container file bucket
C. The directory structure must include a /config /content, /software and /license folders
D. The init-cfg txt and bootstrap.xml files are both optional configuration items for the /config folder
E. The bootstrap.xml file allows for automated deployment of VM-Senes firewalls with full network and policy configurations.
Answer: C,E (LEAVE A REPLY)
https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-aws.html

NEW QUESTION: 248
Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS® version, and serial number?
A. show session info
B. debug system details
C. show system details
D. show system info
Answer: D (LEAVE A REPLY)

NEW QUESTION: 249
Which Palo Alto Networks VM-Series firewall is supported for VMware NSX?
A. VM-200
B. VM-100
C. VM-300
D. VM-1000-HV
Answer: D (LEAVE A REPLY)

NEW QUESTION: 250
Which User-ID method should be configured to map IP addresses to usernames for users connected through a terminal server?
A. port mapping
B. server monitoring
C. client probing
D. XFF headers
Answer: A (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user-mapping-for-termina users

NEW QUESTION: 251
When planning to configure SSL Froward Proxy on a PA 5260, a user asks how SSL decryption can be implemented using phased approach in alignment with Palo Alto Networks best practices What should you recommend?
A. Enable SSL decryption for known malicious destination IP addresses
B. Enable SSL decryption for malicious source users
C. Enable SSL decryption for source users and known malicious URL categories
D. Enable SSL decryption for known malicious source IP addresses
Answer: (SHOW ANSWER)

NEW QUESTION: 252
Which GlobalProtect gateway setting is required to enable split-tunneling by access route, destination domain, and application?
A. No Direct Access to local networks
B. Satellite mode
C. Tunnel mode
D. IPSec mode
Answer: A (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-gateways/split-tunnel-tra

NEW QUESTION: 253
To ensure that a Security policy has the highest priority, how should an administrator configure a Security policy in the device group hierarchy?
A. Add the policy in the shared device group as a pre-rule
B. Reference the targeted device's templates in the target device group
C. Add the policy to the target device group and apply a master device to the device group
D. Clone the security policy and add it to the other device groups
Answer: A (LEAVE A REPLY)
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/device-groups/device-group-hierarchy.html

NEW QUESTION: 254
Which URL Filtering Security Profile action logs the URL Filtering category to the URL Filtering log?
A. Log
B. Alert
C. Allow
D. Default

Answer: (SHOW ANSWER)
Explanation
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/url-filtering/url-filtering-profile-actions

NEW QUESTION: 255
Which four NGFW multi-factor authentication factors are supported by PAN-OS? (Choose four.)
A. One-Time Password
B. Short message service
C. SSH key
D. Voice
E. Push
F. User logon
Answer: A,B,D,E (LEAVE A REPLY)

NEW QUESTION: 256
What are two best practices for incorporating new and modified App-IDs? (Choose two.)
A. Run the latest PAN-OS version in a supported release tree to have the best performance for the new App-IDs
B. Configure a security policy rule to allow new App-IDs that might have network-wide impact
C. Perform a Best Practice Assessment to evaluate the impact of the new or modified App-IDs
D. Study the release notes and install new App-IDs if they are determined to have low impact
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-r

NEW QUESTION: 257
Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x-enabled wireless network device that has no native integration with PAN-OS software?
A. XML API
B. Port Mapping

C. Client Probing
D. Server Monitoring
Answer: A (LEAVE A REPLY)
Explanation
Captive Portal and the other standard user mapping methods might not work for certain types of user access.
For example, the standard methods cannot add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and send them to the PAN-OS integrated User-ID agent Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/user-id-concepts

NEW QUESTION: 258
Which method will dynamically register tags on the Palo Alto Networks NGFW?
A. Restful API or the VMWare API on the firewall or on the User-ID agent or the read-only domain controller (RODC)
B. Restful API or the VMware API on the firewall or on the User-ID agent
C. XML-API or the VMware API on the firewall or on the User-ID agent or the CLI
D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent
Answer: D (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/register-ip-addresses-and-tags-dynam

NEW QUESTION: 259
When is the content inspection performed in the packet flow process?
A. after the application has been identified
B. before session lookup
C. before the packet forwarding process
D. after the SSL Proxy re-encrypts the packet
Answer: (SHOW ANSWER)
Explanation/Reference:
https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081

NEW QUESTION: 260
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW. The update contains an application that matches the same traffic signatures as the custom application. Which application should be used to identify traffic traversing the NGFW?
A. Custom application

B. Downloaded application
C. System logs show an application error and neither signature is used.
D. Custom and downloaded application signature files are merged and both are used
Answer: (SHOW ANSWER)

NEW QUESTION: 261
A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?
A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096 in the "Tag Allowed" field of the V-Wire object.
B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the Tag Allowed" field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each iinterface/sub interface to a unique zone.
C. Create Layer 3 subinterfaces that are each assigned tA. single VLAN ID and a common virtual router.
The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface tA.
unique zone. Do not assign any interface an IP address.
D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/sub interface to a unique zone.
Answer: B (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire- Virtual wire interfaces by default allow all untagged traffic. You can, however, use a virtual wire to connect two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags. VLAN tag 0 indicates untagged traffic.You can also create multiple subinterfaces, add them into different zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.

NEW QUESTION: 262
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of reconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.
Which VPN configuration would adapt to changes when deployed to the future site?
A. Preconfigured GlobalProtect satellite
B. Preconfigured GlobalProtect client
C. Preconfigured PIsec tunnels

D. Preconfigured PPTP Tunnels

Answer: (SHOW ANSWER)

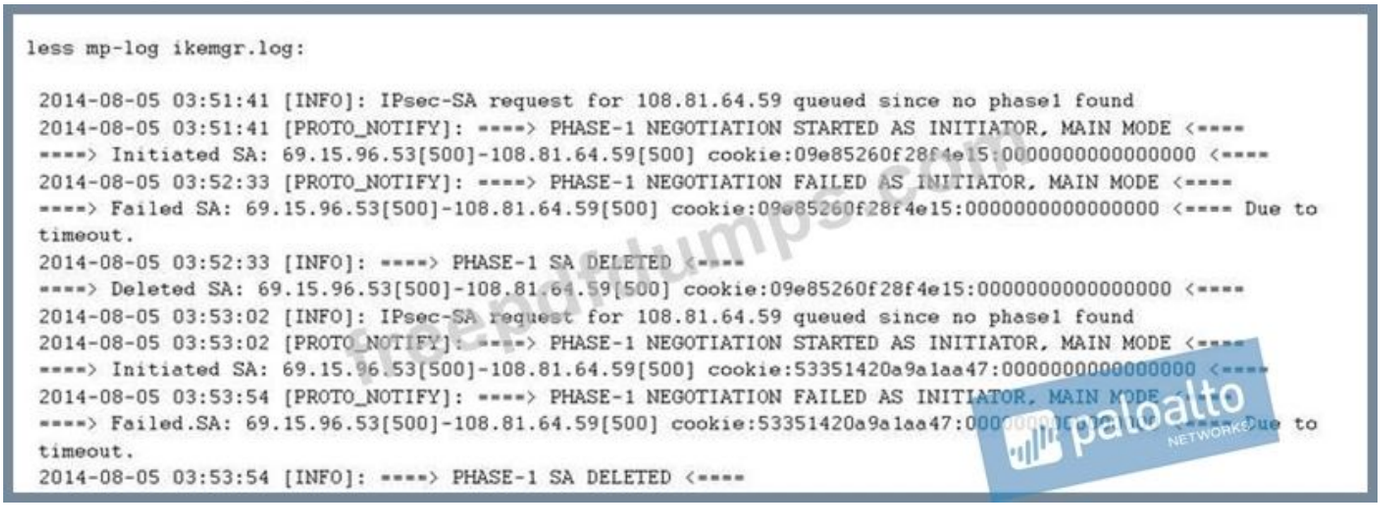
GlobalProtect Satellite

--A Palo Alto Networks firewall at a remote site that establishes IPSec tunnels with the gateway(s) at your corporate office(s) for secure access to centralized resources. Configuration on the satellite firewall is minimal, enabling you to quickly and easily scale your VPN as you add new sites.

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/large-scale-vpn-lsvpn/lsvpn-overview.html

NEW QUESTION: 263

An Administrator is configuring an IPSec VPN toa Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is th output from the command: less mp-log ikemgr.log:



What could be the cause of this problem?

A. The Proxy IDs on the Palo Alto Networks Firewall do not match the settings on the ASA.

B. The deed peer detection settings do not match between the Palo Alto Networks Firewall and the ASA

C. The public IP addresse do not match for both the Palo Alto Networks Firewall and the ASA.

D. The shared secerts do not match between the Palo Alto firewall and the ASA

Answer: (SHOW ANSWER)

NEW QUESTION: 264

What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?

A. Panorama cannot be reverted to an earlier PAN-OS release if variables are used in templates or

template stacks.

B. An administrator must use the Expedition tool to adapt the configuration to the pre-PAN-OS 8.1 state.

C. When Panorama is reverted to an earlier PAN-OS release, variables used in templates or template
stacks will be removed automatically.
D. Administrators need to manually update variable characters to those used in pre-PAN-OS 8.1.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan-os-81/upgradedowngrade-considerations

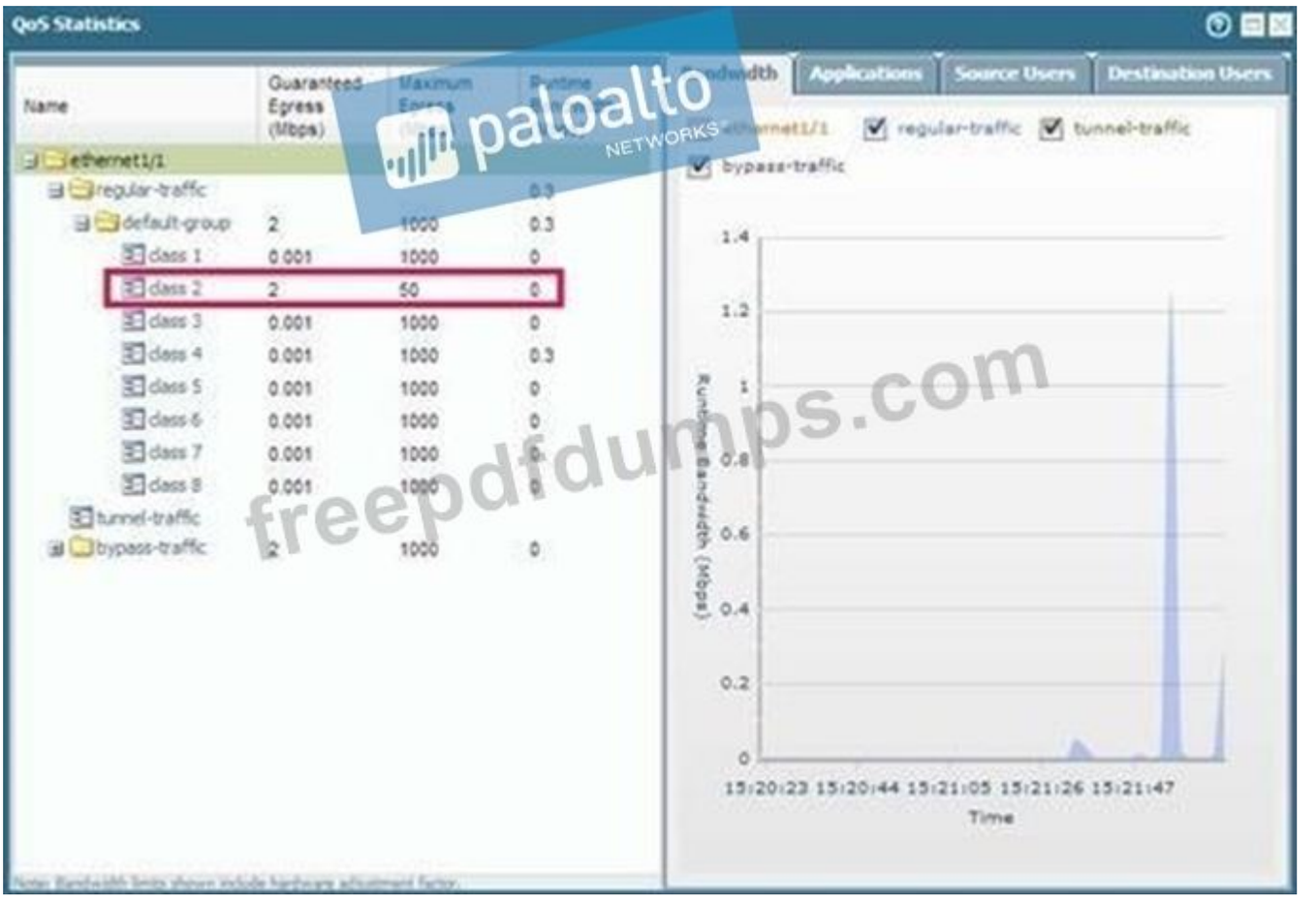
NEW QUESTION: 265
Which three authentication factors does PAN-OS® software support for MFA (Choose three.)
A. Push
B. Pull
C. Okta Adaptive
D. Voice
E. SMS
Answer: A,D,E (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication

NEW QUESTION: 266
Which is not a valid reason for receiving a decrypt-cert-validation error?
A. Unsupported HSM
B. Unknown certificate status
C. Client authentication
D. Untrusted issuer
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/networking- features/ssl-ssh-session-end-reasons

NEW QUESTION: 267
If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?
A. TLS Bidirectional Inspection
B. SSL Inbound Inspection
C. SSH Forward Proxy
D. SMTP Inbound Decryption
Answer: B (LEAVE A REPLY)
Reference:

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssl-inbound-inspectio
1. SSL Forward Proxy - Inside to Outside (To the the internet)
2. SSL Inbound Proxy - Outside to Inside (usually towards a hosted webserver in your net)
3. SSH Forward Proxy - As is states, for SSH traffic. The important one to remember for this type of decryption is that no certs are required.

NEW QUESTION: 268
The IT department has received complaints abou VoIP call jitter when the sales staff is making or receiving calls. QoS is enabled on all firewall interfaces, but there is no QoS policy written in the rulebase. The IT manager wants to find out what traffic is causing the jitter in real time when a user reports the jitter.
Which feature can be used to identify, in real time, the applications taking up the most bandwidth?
A. QoS Statistics
B. Applications Report
C. Application Command Center (ACC)
D. QoS Log
Answer: A (LEAVE A REPLY)
Select Network > QoS to view the QoS Policies page and click the Statistics link to view QoS bandwidth, active sessions of a selected QoS node or class, and active applications for the selected QoS node or class.
For example, see the statistics for ethernet 1/1 with QoS enabled:



https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/quality-of-service/configure-qos

NEW QUESTION: 269

A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment?

A. The two devices may be different models within the PA-5000 series

B. The management port may be used for a backup control connection

C. The two devices must share a routable floating IP address

D. The HA1 IP address from each peer must be on a different subnet

Answer: B (LEAVE A REPLY)

NEW QUESTION: 270

A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting. It is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem?

A. DHCP has been set to Auto.

B. Interface ethernet1/3 is in Layer 2 mode and interface ethernet1/4 is in Layer 3 mode.

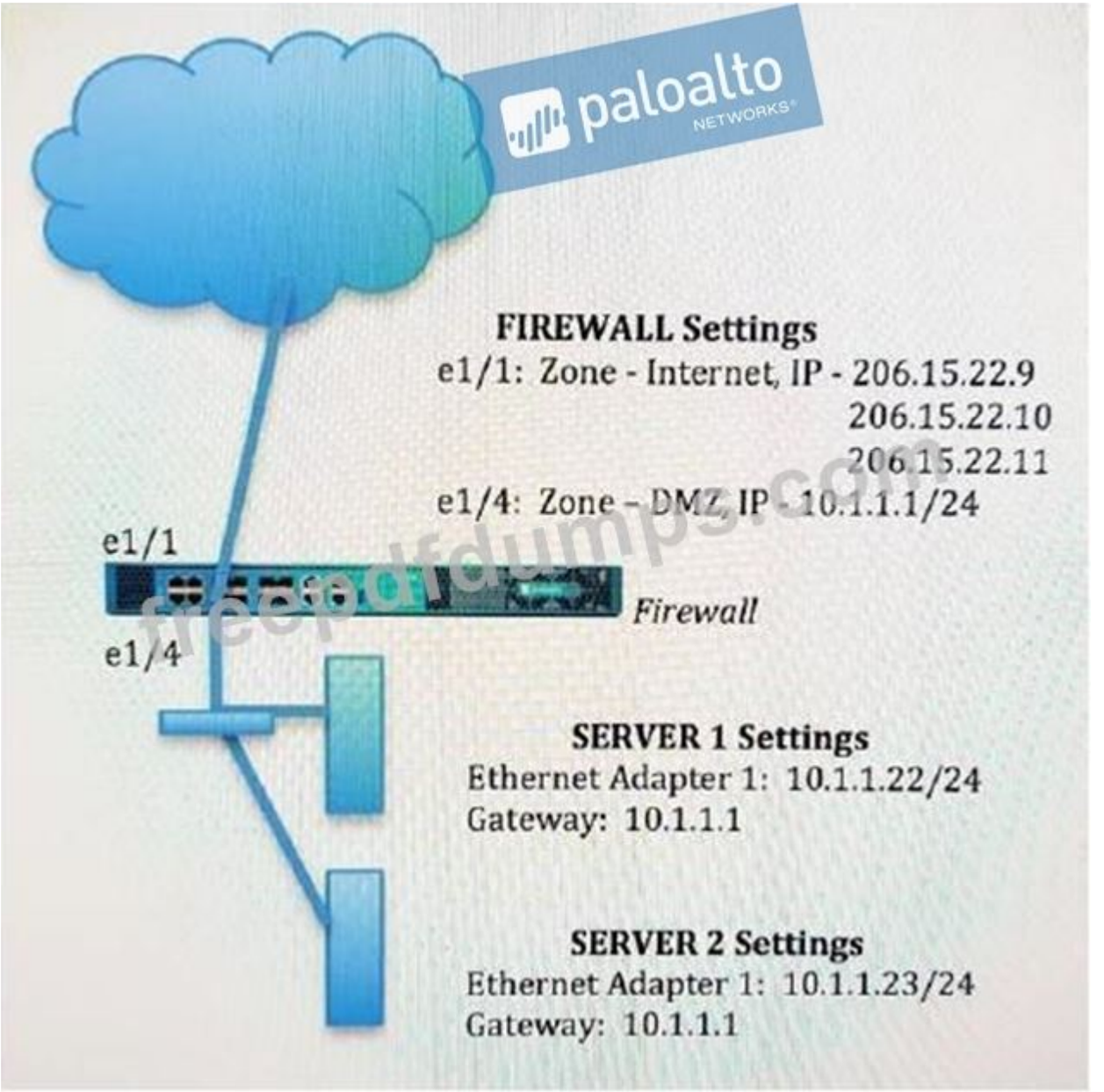
C. Interface ethernet1/3 and ethernet1/4 are in Virtual Wire Mode.

D. DNS has not been properly configured on the firewall

Answer: B (LEAVE A REPLY)

In a Layer 2 deployment, the firewall provides switching between two or more interfaces. Each group of interfaces must be assigned to a VLAN object in order for the firewall to switch between them.
In a Layer 3 deployment, the firewall routes traffic between ports. An IP address must be assigned to each interface and a virtual router must be defined to route the traffic. Choose this option when routing is required.
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/getting-started/basic-interface-deployments

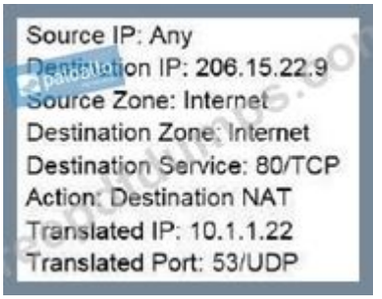
NEW QUESTION: 271
An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet.
Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22



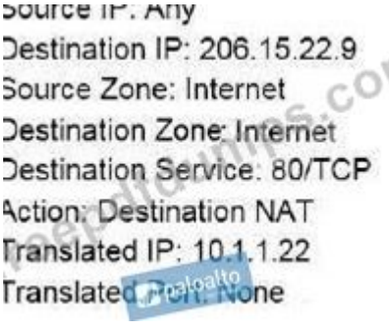
Based on the information shown in the image, which NAT rule will forward web-browsing traffic correctly?

A)

B)



C)



D)

A. Option A

B. Option B

C. Option C

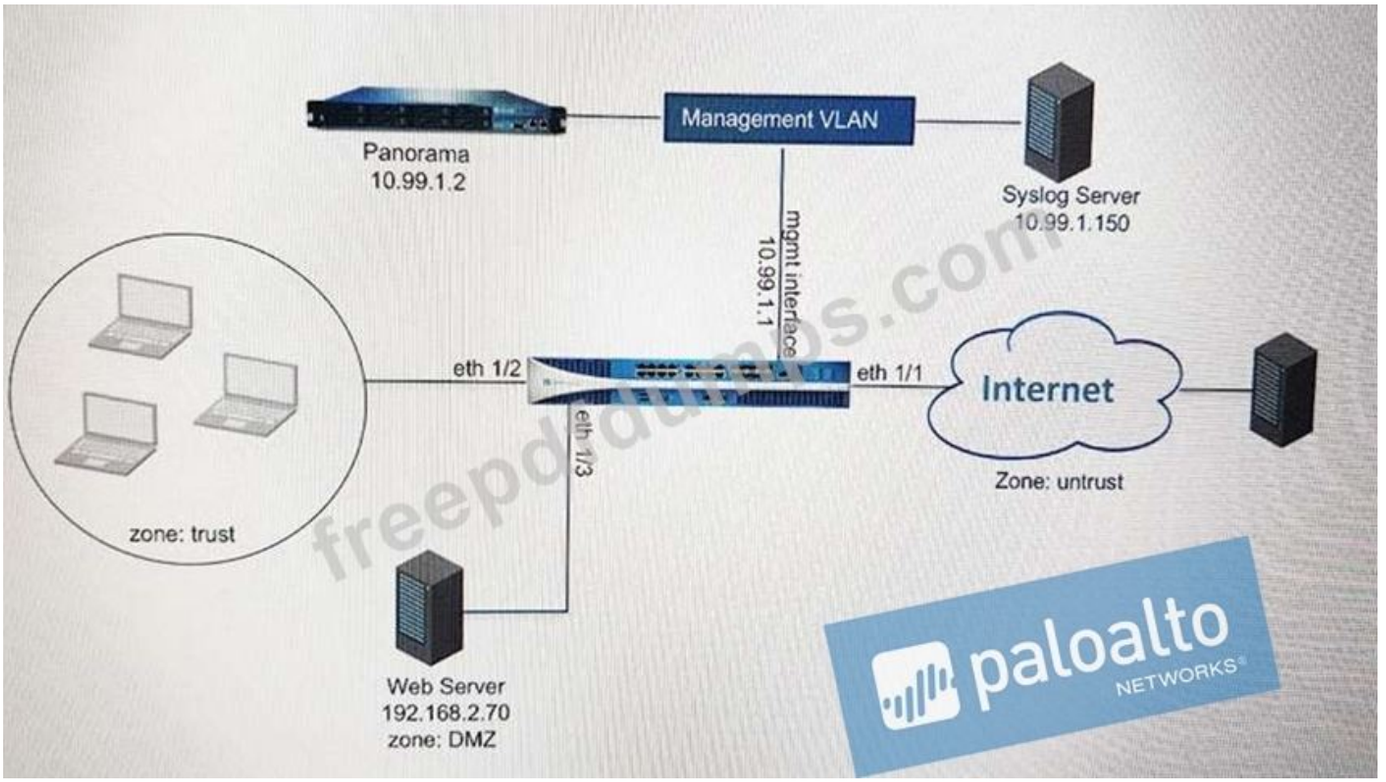
D. Option D

Answer: C (LEAVE A REPLY)

Explanation

NAT zones are just whatever interface traffic is going to. The source (the big cloud internet) is obviously internet, and the destination zone is the internet facing interface of the firewall, so the destination is also internet. It then is translated into an IP that the internal network can read.

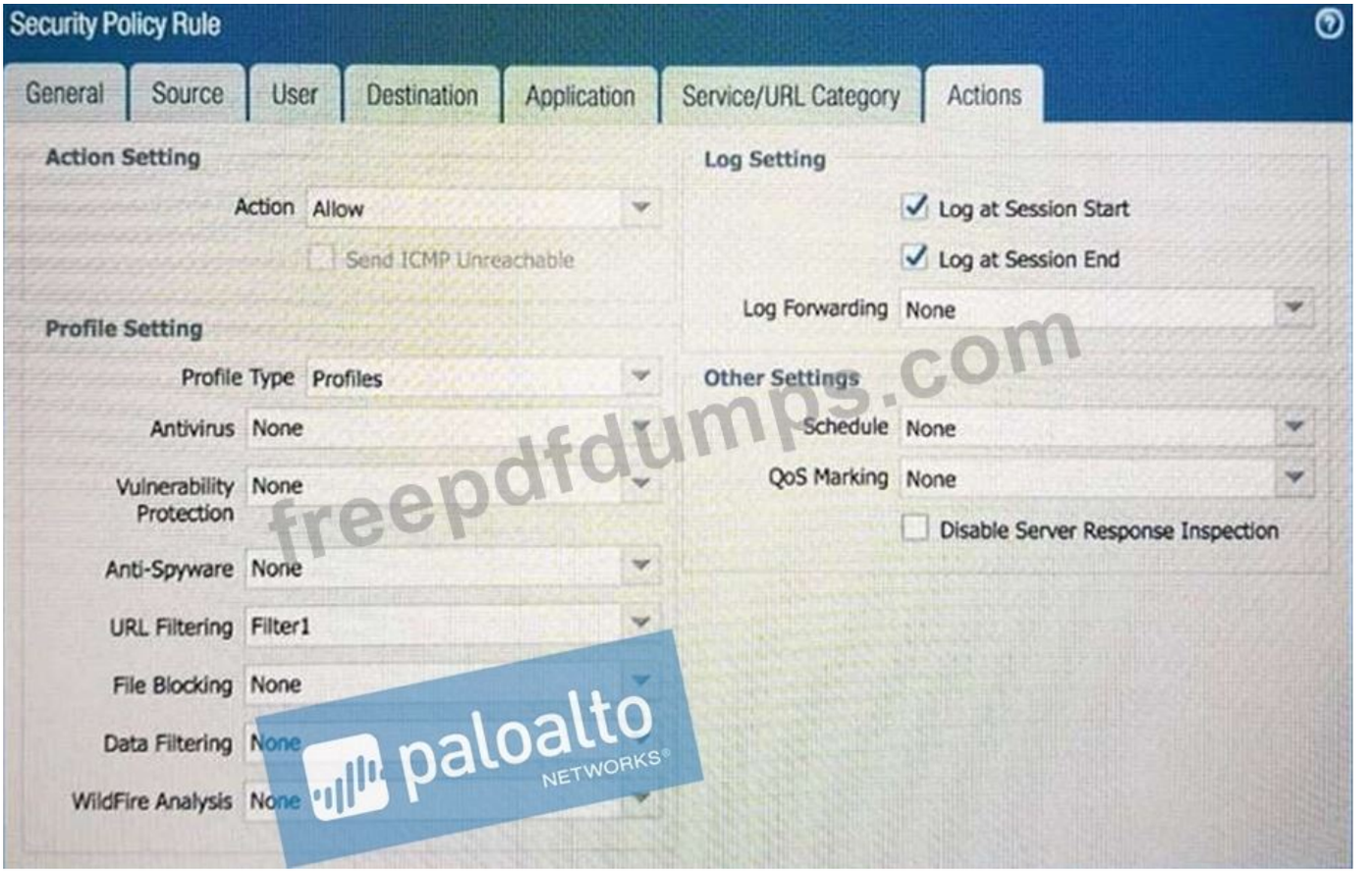
NEW QUESTION: 272
Refer to the exhibit.



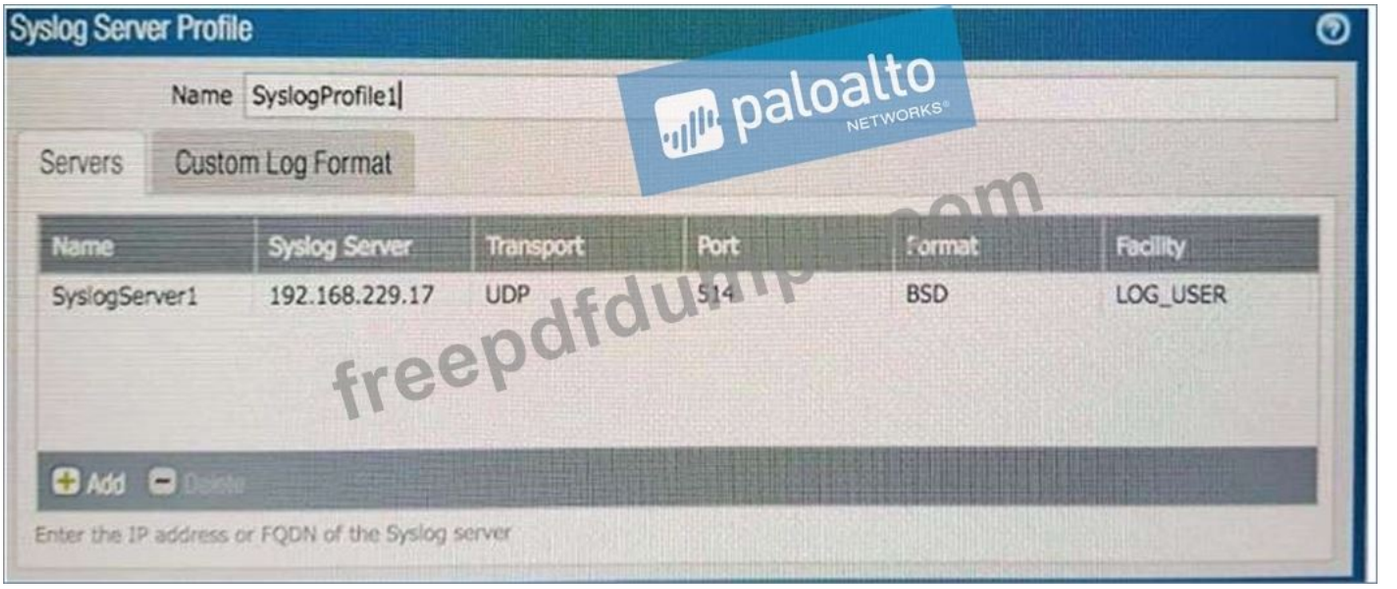
An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panoram
a. The configuration problem seems to be on the firewall side. Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?
A)


Panorama Settings
Panorama Servers
10.99.1.21
Receive Timeout for Connection to Panorama (sec) 240
Send Timeout for Connection to Panorama (sec) 240
Retry Count for SSL Send to Panorama 25
Secure Client Communication
Certificate Type None
Check Server Identity
Disable Panorama Policy and Objects
Disable Device and Network Template
OK
Cancel

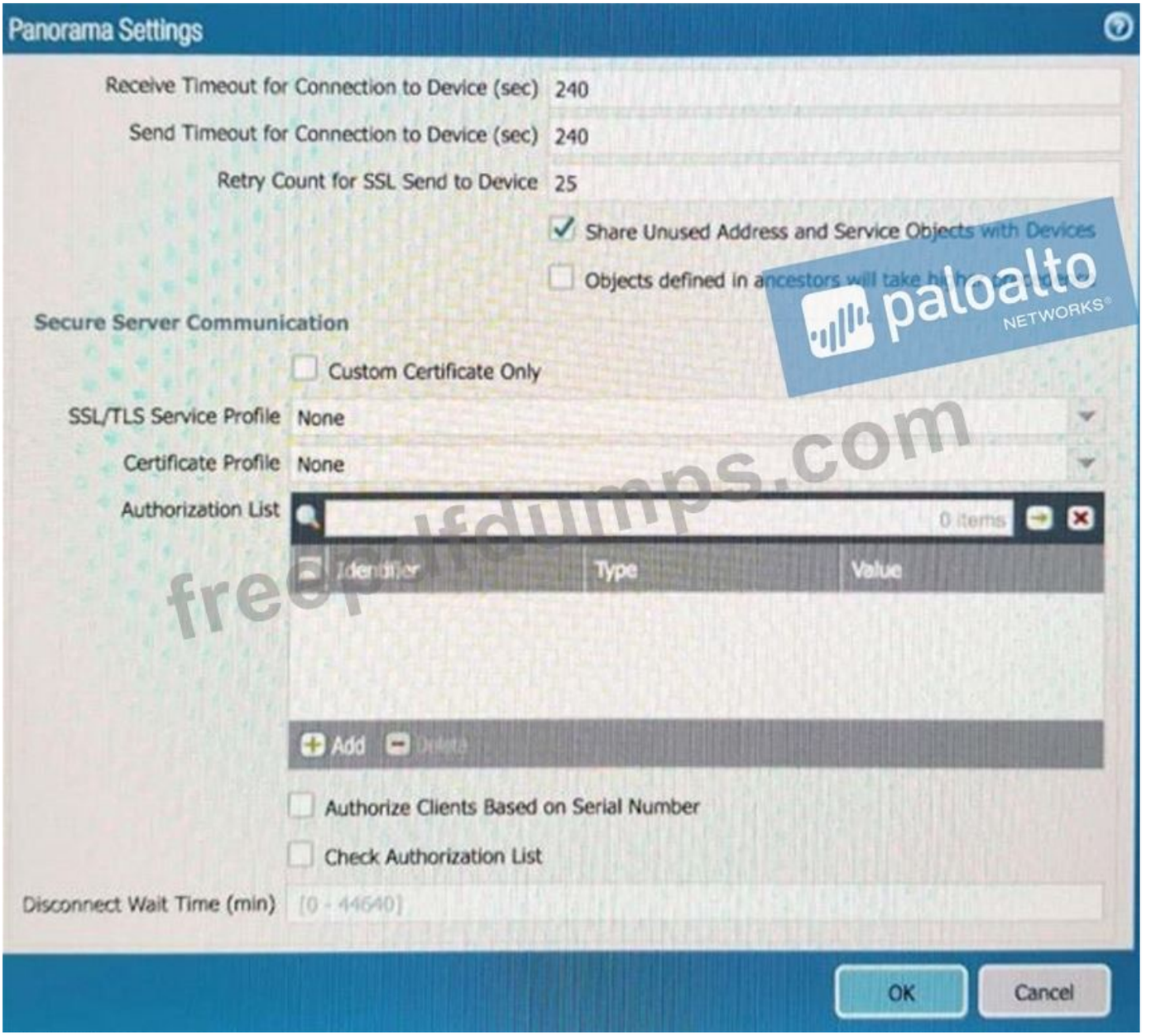
B)


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Action Setting
Action Allow
Send ICMP Unreachable
Profile Setting
Profile Type Profiles
Antivirus None
Vulnerability Protection None
Anti-Spyware None
URL Filtering Filter1
File Blocking None
Data Filtering None
WildFire Analysis None
Log Setting
Log at Session Start
Log at Session End
Log Forwarding None
Other Settings
Schedule None
QoS Marking None
Disable Server Response Inspection

C)


Syslog Server Profile
Name SyslogProfile1
Servers
Custom Log Format
Name
Syslog Server
Transport
Port
Format
Facility
SyslogServer1
192.168.229.17
UDP
514
BSD
LOG_USER
Add
Enter the IP address or FQDN of the Syslog server

D)


Panorama Settings
Receive Timeout for Connection to Device (sec) 240
Send Timeout for Connection to Device (sec) 240
Retry Count for SSL Send to Device 25
Share Unused Address and Service Objects with Devices
Secure Server Communication
Custom Certificate Only
SSL/TLS Service Profile None
Certificate Profile None
Authorization List
0 items
Type
Value
Add
Authorize Clients Based on Serial Number
Check Authorization List
Disconnect Wait Time (min)
OK
Cancel

A. Option A

B. Option B
C. Option C
D. Option D
Answer: A (LEAVE A REPLY)
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html
First of all you need to connect the Firewall to Panorama. Once that is done you configure your templates and device groups via Panorama and push that to the firewall. That includes policy and log forwarding. If you had misconfiguration on the firewall regarding logs that would be mitigated via Panorama push.

NEW QUESTION: 273
Decrypted packets from the website https://www.microsoft.com will appear as which application and service within the Traffic log?
A. web-browsing and 443
B. SSL and 80
C. SSL and 443
D. web-browsing and 80
Answer: A (LEAVE A REPLY)
We know that SSL decryption is supposed to give us visibility of traffic that would otherwise be encrypted. Therefore, we'd expect decrypted traffic to be identified as the underlying applications, such as web-browsing, facebook-base or other, but not as SSL.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cle8CAC

NEW QUESTION: 274
Based on the following image,

what is the correct path of root, intermediate, and end-user certificate?

A. VeriSign > Palo Alto Networks > Symantec

B. Palo Alto Networks > Symantec > VeriSign

C. Symantec > VeriSign > Palo Alto Networks

D. VeriSign > Symantec > Palo Alto Networks

Answer: D (LEAVE A REPLY)

NEW QUESTION: 275

A Network Administrator wants to deploy a Large Scale VPN solution. The Network Administrator has chosen a GlobalProtect Satellite solution. This configuration needs to be deployed to multiple remote offices and the Network Administrator decides to use Panorama to deploy the configurations.

How should this be accomplished?

A. Create a Template with the appropriate IKE Gateway settings.

B. Create a Device Group with the appropriate IPSec tunnel settings.

C. Create a Device Group with the appropriate IKE Gateway settings.

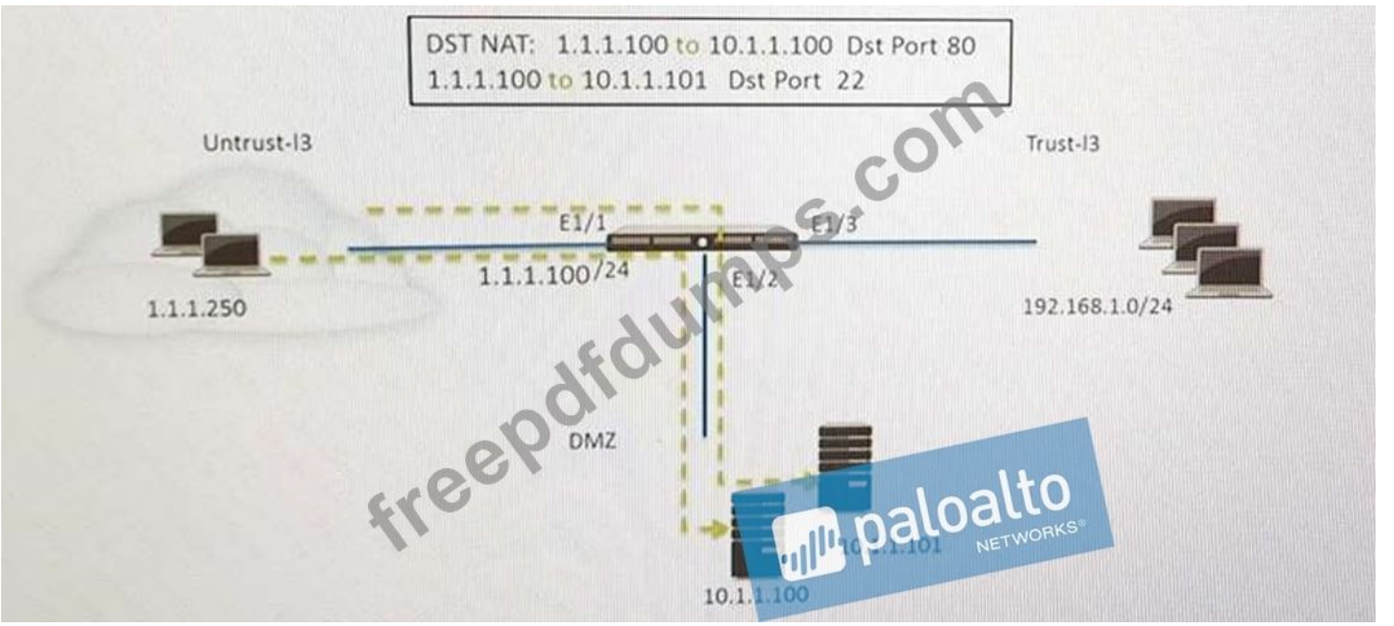
D. Create a Template with the appropriate IPSec tunnel settings.

Answer: D (LEAVE A REPLY)

Note: The administrator of the satellite must enter the credentials when the satellite connects to the portal.

This is done on the satellite by navigating to Network > IPSec Tunnels and choosing "gateway info" and then clicking on "Enter Credentials".

NEW QUESTION: 276
Refer to the exhibit.



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) received HTTP traffic and host B(10.1.1.101) receives SSH traffic.
Which two security policy rules will accomplish this configuration? (Choose two)
A. Untrust (Any) to Untrust (10.1.1.1) Ssh-Allow
B. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
C. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow
D. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 277
Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats
detected in the last 30 days?
A. Session Browser
B. Application Command Center
C. TCP Dump
D. Packet Capture
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Management-Articles/Tips-amp-Tricks-How-to-Use-the-
Application-Command-Center-ACC/ta-p/67342

NEW QUESTION: 278

A users traffic traversing a Palo Alto networks NGFW sometimes can reach http //www company com At other times the session times out. At other times the session times out The NGFW has been configured with a PBF rule that the user traffic matches when it goes to http://www.company.com
goes to http://www company com
How can the firewall be configured to automatically disable the PBF rule if the next hop goes down?
A. Enable and configure a link monitoring profile for the external interface of the firewall
B. Create and add a monitor profile with an action of fail over in the PBF rule in question
C. Create and add a monitor profile with an action of wait recover in the PBF rule in question
D. Configure path monitoring for the next hop gateway on the default route in the virtual router
Answer: B (LEAVE A REPLY)

NEW QUESTION: 279
A file sharing application is being permitted and no one knows what this application is used for. How should this application be blocked?
A. Create a File blocking profile that blocks Layer 4 and Layer 7 attacks
B. Block all known internal custom applications
C. Block all unauthorized applications using a security policy
D. Create a WildFire Analysis Profile that blocks Layer 4 and Layer 7 attacks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 280
Which Palo Alto Networks VM-Series firewall is valid?
A. VM-25
B. VM-800
C. VM-50
D. VM-400
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation- firewall/vm-series

NEW QUESTION: 281
A network security engineer needs to configure a virtual router using IPv6 addresses.
Which two routing options support these addresses? (Choose two)
A. BGP not sure
B. OSPFv3
C. RIP
D. Static Route
Answer: B,D (LEAVE A REPLY)
Explanation

https://live.paloaltonetworks.com/t5/Management-Articles/Does-PAN-OS-Support-Dynamic-Routing-Protocols-

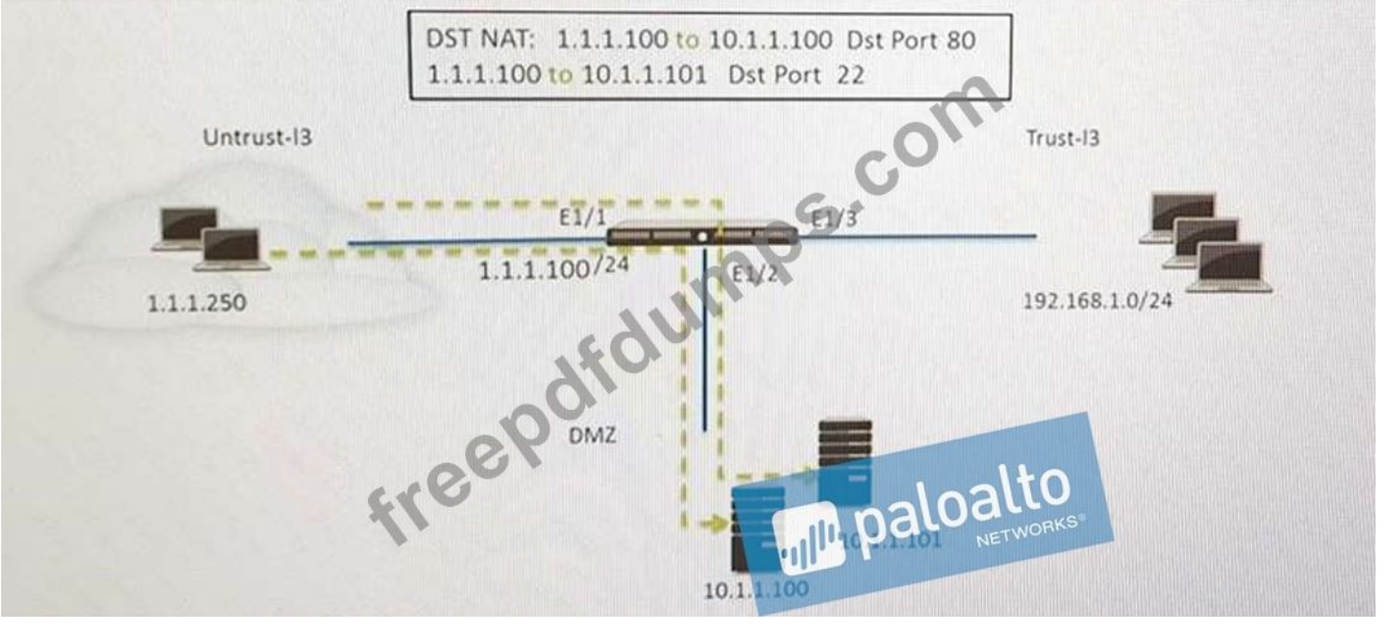
NEW QUESTION: 282
Which feature can provide NGFWs with User-ID mapping information?
A. Web Captcha
B. Native 802.1q authentication
C. GlobalProtect
D. Native 802.1x authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 283
A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.
Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web-browsing traffic to this server on tcp/443.
A. Rule #1: application: web-browsing; service: application-default; action: allow Rule #2: application: ssl; service: application-default; action: allow
B. Rule #1: application: web-browsing; service: service-https; action: allow Rule #2: application: ssl; service: application-default; action: allow
C. Rule # 1: application: ssl; service: application-default; action: allow Rule #2: application: web-browsing; service: application-default; action: allow
D. Rule #1: application: web-browsing; service: service-http; action: allow Rule #2: application: ssl; service: application-default; action: allow
Answer: A (LEAVE A REPLY)
If decrypted traffic matches the web-browsing application. Then the firewall will log it as web-browsing over ssl (443) and will never match if it is set to "application-default".
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEyCAK

NEW QUESTION: 284
A security engineer needs firewall management access on a Inside interface When three settings are required on an SSI/TVS Service Profile to provide secure Wet) Ui authentication? (Choose three.)
A. Certificate
B. Authentication Algorithm
C. Encryption Algorithm
D. Minimum TLV version
E. Maximum TLS version
Answer: (SHOW ANSWER)

NEW QUESTION: 285
Which User-ID method maps IP address to usernames for users connecting through a web proxy that has already authenticated the user?
A. Client Probing
B. Port mapping
C. Server monitoring
D. Syslog listening
Answer: D (LEAVE A REPLY)
Explanation
To obtain user mappings from existing network services that authenticate users-such as wireless controllers,
802.1x devices, Apple Open Directory servers, proxy servers, or other Network Access Control (NAC) mechanisms-Configure User-ID to Monitor Syslog Senders for User Mapping.While you can configure either the Windows agent or the PAN-OS integrated User-ID agent on the firewall to listen for authentication syslog messages from the network services, because only the PAN-OS integrated agent supports syslog listening over TLS, it is the preferred configuration.

NEW QUESTION: 286
Refer to the exhibit.



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and HOST B (10.1.1.101) receives SSH traffic.) Which two security policy rules will accomplish this configuration? (Choose two.)
A. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow
B. Untrust (Any) to DMZ (1.1.1.100), web-browsing -Allow
C. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
D. Untrust (Any) to Untrust (10.1.1.1), SSH -Allow

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

Answer: B,E (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

NEW QUESTION: 287

What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

```
admin@Lab33-111-PA-3060(active)> show clock

Thu Jun  8 12:49:55 PDT 2017
######################
admin@Lab33-111-PA-3060(active)# show vsys vsys1 rulebase pbf rules test-pbf
test-pbf {
  action {
    forward {
      egress-interface ethernet1/5;
    }
  }
  from {
    zone L3-Trust;
  }
  enforce-symmetric-return {
    enabled no;
  }
  source 192.168.111.3;
  destination 10.46.41.113;
  source-user any;
  application any;
  service any;
  schedule schedule-pbf;
}
######################
admin@Lab33-111-PA-3060(active)# show vsys vsys1 schedule schedule-pbf
schedule-pbf {
  schedule-type {
    recurring {
      daily 16:00-21:00;
    }
  }
}
######################
admin@Lab33-111-PA-3060(active)> show routing fib
id      destination           nexthop            flags  interface          mtu
-------------------------------------------------------------------------------
47      0.0.0.0/0             10.46.40.1         ug     ethernet1/3        1500
67      10.10.20.0/24         0.0.0.0            u      ethernet1/7        1500
66      10.10.20.111/32       0.0.0.0            uh     ethernet1/7        1500
46      10.46.40.0/23         0.0.0.0            u      ethernet1/3        1500
49      10.46.44.0/23         0.0.0.0            u      ethernet1/5        1500
45      10.46.41.111/32       0.0.0.0            uh     ethernet1/3        1500
70      10.46.41.113/32       10.46.40.1         ug     ethernet1/3        1500
48      10.46.45.111/32       0.0.0.0            uh     ethernet1/5        1500
51      192.168.111.0/24      0.0.0.0            u      ethernet1/6        1500
50      192.168.111.2/32      0.0.0.0            uh     ethernet1/6        1500
-------------------------------------------------------------------------------
```


A. ethernet1/7

B. ethernet1/5

C. ethernet1/3

D. ethernet1/6

Answer: C (LEAVE A REPLY)

NEW QUESTION: 288

The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

A. 6-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Protocol, and Source Security Zone

B. 5-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Protocol

C. 7-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Source User, URL Category, and Source Security Zone

D. 9-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Source User, Source Security Zone,

Answer: A (LEAVE A REPLY)

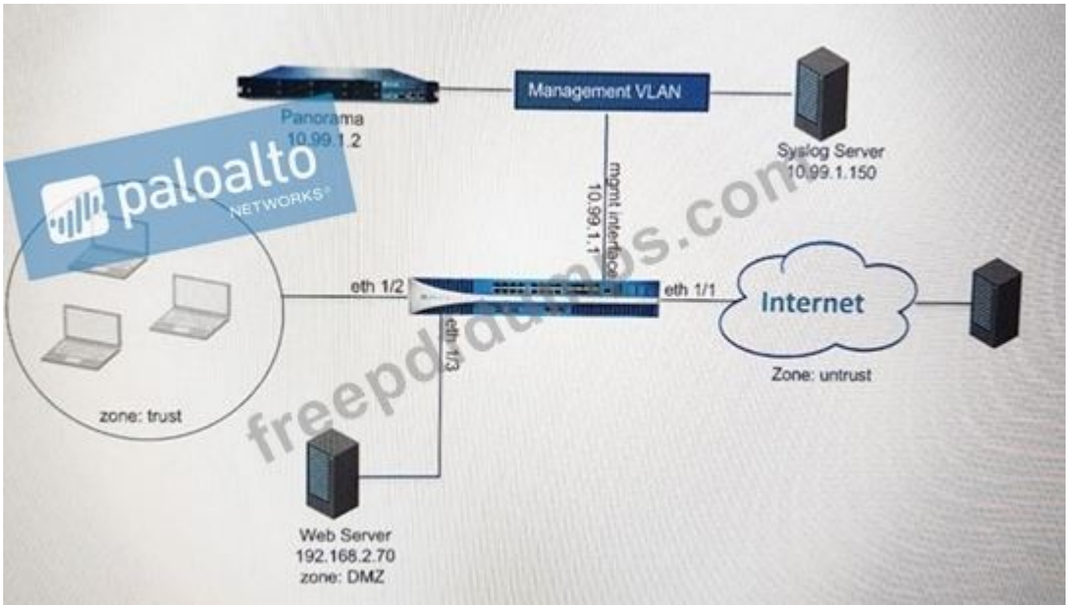
Destination Security Zone, Application, and URL Category

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVECA0

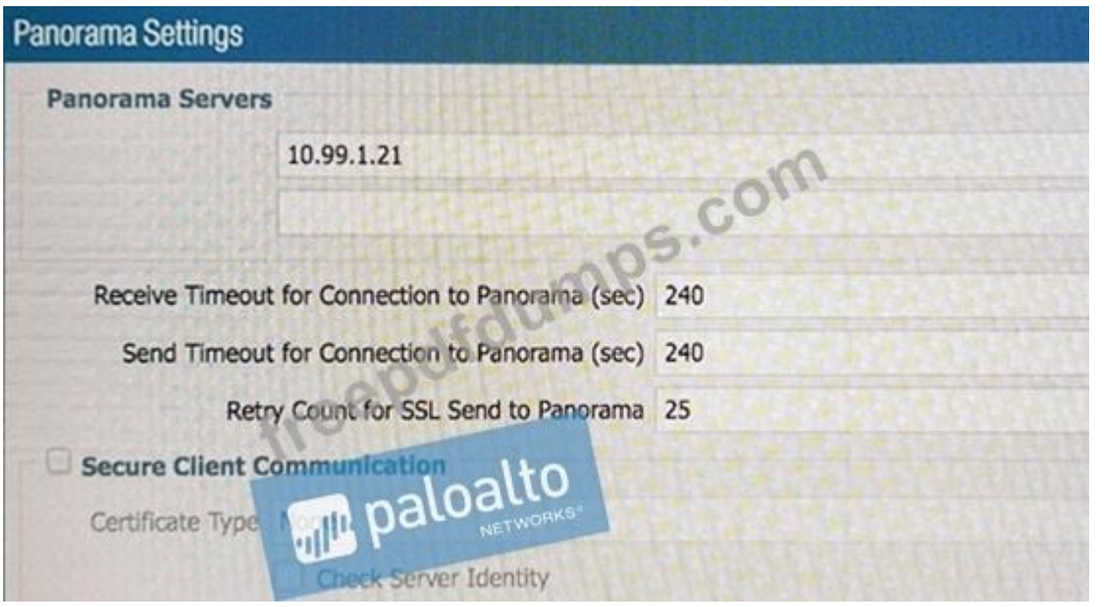
NEW QUESTION: 289

Refer to the exhibit.

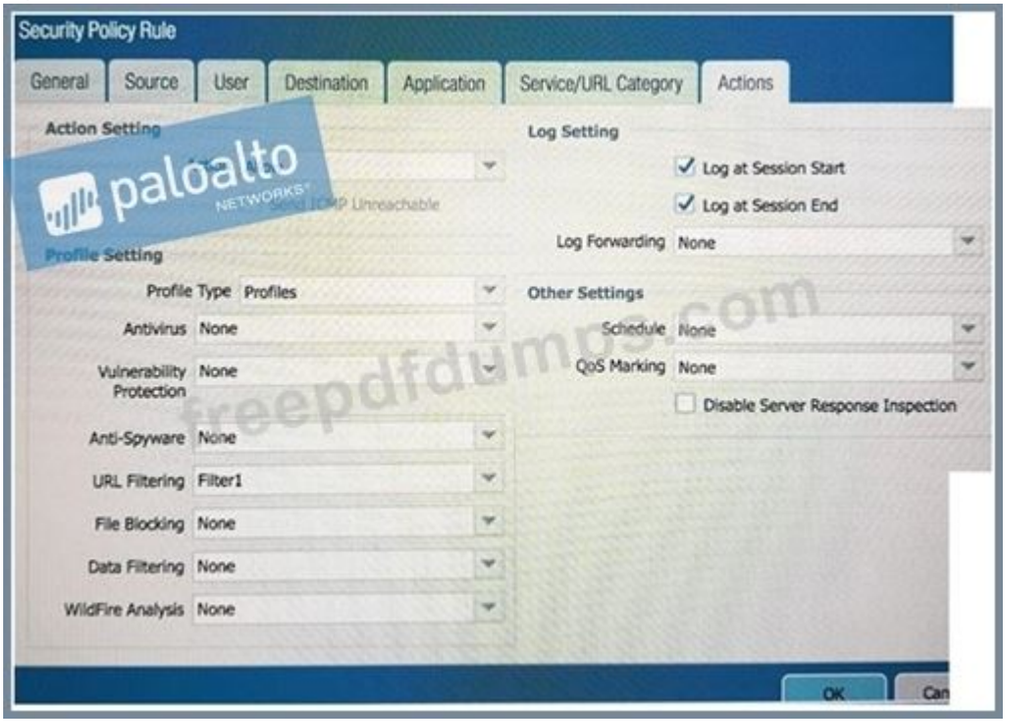


An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side. Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?

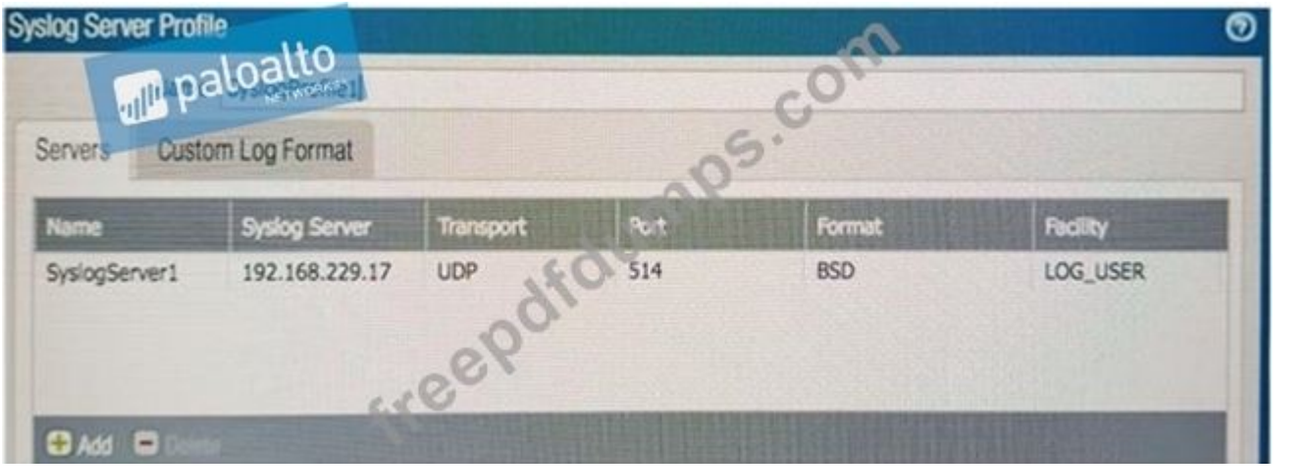
A)


Panorama Settings
Panorama Servers
10.99.1.21
Receive Timeout for Connection to Panorama (sec) 240
Send Timeout for Connection to Panorama (sec) 240
Retry Count for SSL Send to Panorama 25
Secure Client Communication
Certificate Type
Check Server Identity

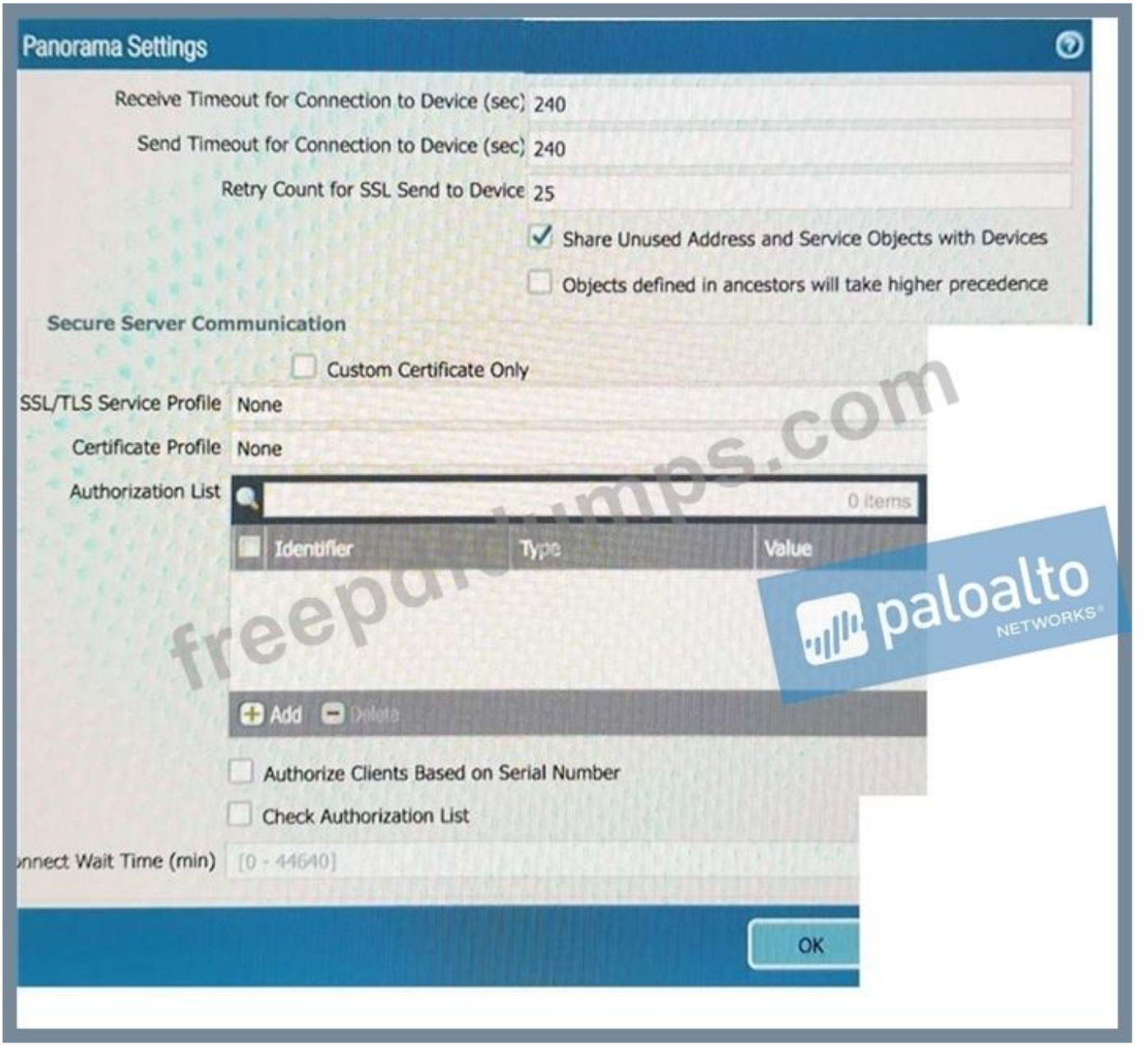
B)


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Action Setting
Log Setting
Log at Session Start
Log at Session End
Log Forwarding None
Profile Setting
Profile Type Profiles
Other Settings
Antivirus None
Schedule None
Vulnerability Protection None
QoS Marking None
Disable Server Response Inspection
Anti-Spyware None
URL Filtering Filter1
File Blocking None
Data Filtering None
WildFire Analysis None
OK

C)


Syslog Server Profile
Servers
Custom Log Format
Name
Syslog Server
Transport
Port
Format
Facility
SyslogServer1
192.168.229.17
UDP
514
BSD
LOG_USER
Add

D)



A. Option A
B. Option B
C. Option C
D. Option D
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html#

NEW QUESTION: 290
Which CLI command enables an administrator to check the CPU utilization of the dataplane?
A. show running resource-monitor
B. debug data-plane dp-cpu
C. show system resources
D. debug running resources

Answer: A (LEAVE A REPLY)

Explanation

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXwCAK

NEW QUESTION: 291

Which two benefits come from assigning a Decryption Profile to a Decryption policy rule with a "No Decrypt" action? (Choose two.)

A. Block sessions with expired certificates

B. Block sessions with client authentication

C. Block sessions with unsupported cipher suites

D. Block sessions with untrusted issuers

E. Block credential phishing

Answer: A,D (LEAVE A REPLY)

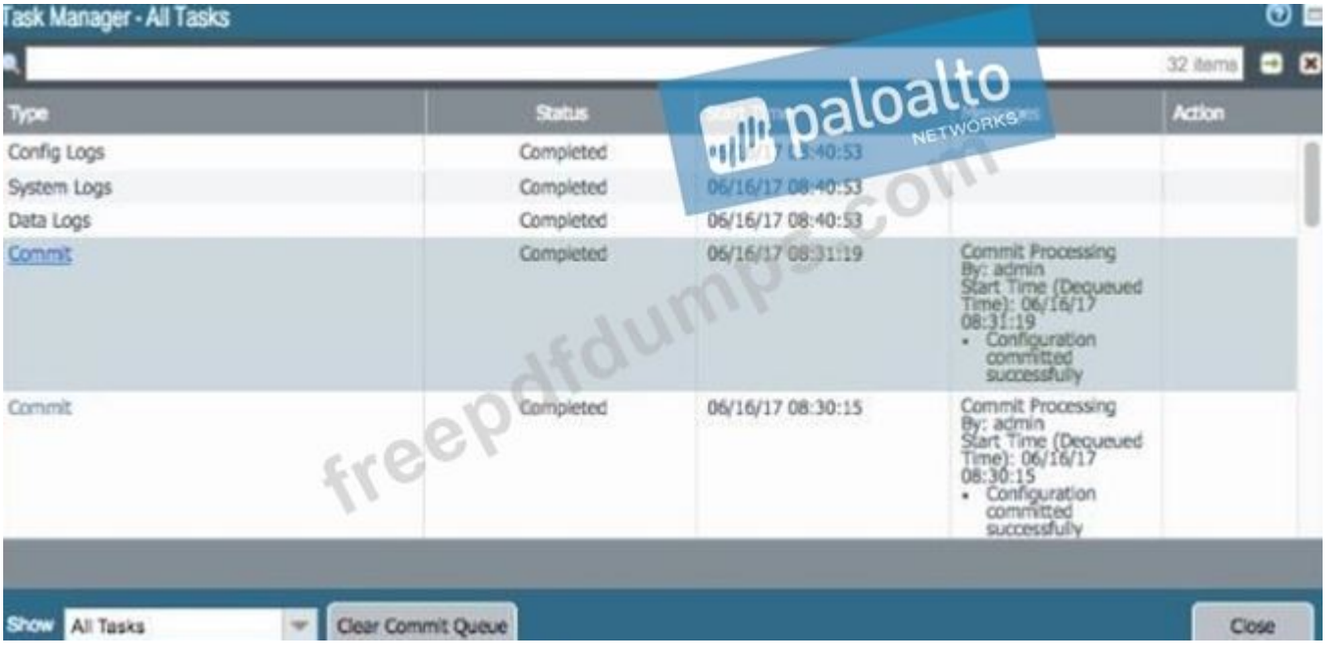
Explanation

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-decryption-exceptions

NEW QUESTION: 292

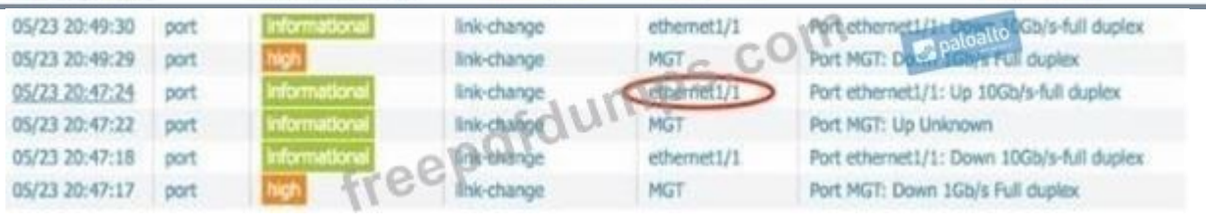
An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A.

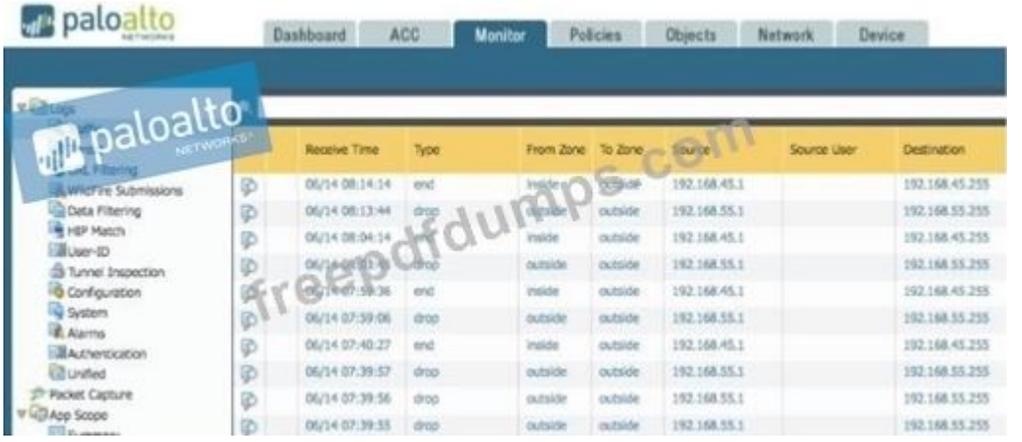


B.

C.



D.



Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 293

A firewall administrator has completed most of the steps required to provision a standalone Palo Alto Networks Next-Generation Firewall. As a final step, the administrator wants to test one of the security policies.

Which CLI command syntax will display the rule that matches the test?

A. test security -policy- match source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number

B. show security rule source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>

C. test security rule source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>

D. show security-policy-match source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number> test security-policy-match source

Answer: A (LEAVE A REPLY)

test security-policy-match source <source IP> destination <destination IP> protocol <protocol number>

https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Test-Which-Security-Policy-Applies-to-a-Traffic-Flow/ta-p/53693

NEW QUESTION: 294

Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

A. Security policy

B. Decryption policy

C. Authentication policy

D. Application Override policy

Answer: (SHOW ANSWER)

Authentication policy enables you to authenticate end users before they can access services and applications. Whenever a user requests a service or application (such as by visiting a web page), the firewall evaluates Authentication policy. Based on the matching Authentication policy rule, the firewall then prompts the user to authenticate using one or more methods (factors), such as login and password, Voice, SMS, Push, or One-time Password (OTP) authentication

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-policy

NEW QUESTION: 295

Which four NGFW multi-factor authentication factors are supported by PAN-OS@? (Choose four.)

A. Short message service

B. Push

C. User logon

D. Voice

E. SSH key

F. One-Time Password

Answer: A,B,D,F (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/authentication/authentication-types/multi-factor-auth

NEW QUESTION: 296

When configuring the firewall for packet capture, what are the valid stage types?

A. Receive, management , transmit , and drop

B. Receive , firewall, send , and non-syn

C. Receive management , transmit, and non-syn
D. Receive , firewall, transmit, and drop
Answer: D (LEAVE A REPLY)
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTJCA0
docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/monitor/monitor-packet-capture/packet-captur

NEW QUESTION: 297
Which two actions would be part of an automatic solution that would block sites with untrusted certificates
without enabling SSL Forward Proxy? (Choose two.)
A. Create a no-decrypt Decryption Policy rule.
B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
C. Create a Dynamic Address Group for untrusted sites
D. Create a Security Policy rule with vulnerability Security Profile attached.
E. Enable the "Block sessions with untrusted issuers" setting.
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/
objects-decryption-profile

NEW QUESTION: 298
A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and post.
Which option when enabled with the correction threshold would mitigate this attack without dropping legitirnate traffic to other hosts insides the network?
A. Zone Protection Policy with UDP Flood Protection
B. QoS Policy to throttle traffic below maximum limit
C. Security Policy rule to deny trafic to the IP address and port that is under attack
D. Classified DoS Protection Policy using destination IP only with a Protect action
Answer: (SHOW ANSWER)
Step 1: Configure a DoS Protection profile for flood protection.
1. Select Objects > Security Profiles > DoS Protection and Add a profile Name.
2. Select Classified as the Type.
3. For Flood Protection, select the check boxes for all of the following types of flood protection:
* SYN Flood
* UDP Flood
* ICMP Flood

* ICMPv6 Flood
* Other IP Flood

Step 2: Configure a DoS Protection policy rule that specifies the criteria for matching the incoming traffic.

This step include: (Optional) For Destination Address, select Any or enter the IP address of the device you want to protect.

https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/policy/configure-dos-protection-against-flooding-of-new-sessions

NEW QUESTION: 299

Refer to the exhibit.

```
####################################
admin@Lab33-111-PA-3060(active)>show routing fib

id        destination        nexthop        flags      interface        mtu
--------------------------------------------------------------------------
47        0.0.0.0/0          10.46.40.1     ug         ethernet1/3      1500
46        10.46.40.0/23      0.0.0.0        u          ethernet1/3      1500
45        10.46.41.111/32    0.0.0.0        uh         ethernet1/3      1500
70        10.46.41.113/32    10.46.40.1     ug         ethernet1/3      1500
51        192.168.111.0/24   0.0.0.0        u          ethernet1/6      1500
50        192.168.111.2/32   0.0.0.0        uh         ethernet1/6      1500

--------------------------------------------------------------------------
####################################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p= link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name          interface1       interface2       flags              allowed-tags
--------------------------------------------------------------------------------
VW-1          ethernet1/7      ethernet1/5      p

####################################
```

Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

A. ethernet1/6

B. ethernet1/7

C. ethernet1/3

D. ethernet1/5

Answer: (SHOW ANSWER)

NEW QUESTION: 300

Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

A. The firewall is in multi-vsys mode.

B. The traffic is offloaded.

C. The traffic does not match the packet capture filter.

D. The firewall's DP CPU is higher than 50%.

Answer: B,C (LEAVE A REPLY)

Explanation/Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet- captures/disable-hardware-offload

NEW QUESTION: 301

When setting up a security profile which three items can you use? (Choose three)

A. Wildfire analysis

B. anti-ransom ware

C. antivirus

D. URL filtering

E. decryption profile

Answer: A,C,D (LEAVE A REPLY)

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

NEW QUESTION: 302

An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs. The administrator assigns priority 100 to the active firewall.

Which priority is correct for the passive firewall?

A. 99
B. 255
C. 1
D. 0
Answer: B (LEAVE A REPLY)

NEW QUESTION: 303
Which option describes the operation of the automatic commit recovery feature?
A. It enables a firewall to revert to the previous configuration if rule shadowing is detected.
B. It enables a firewall to revert to the previous configuration if application dependency errors are found.
C. It enables a firewall to revert to the previous configuration if a commit causes HA partner connectivity failure.
D. It enables a firewall to revert to the previous configuration if a commit causes Panorama connectivity failure.
Answer: D (LEAVE A REPLY)
To ensure that broken configurations caused by configuration changes pushed from the PanoramaTM management server to managed firewalls, or committed locally on the firewall, enable Automated Commit Recovery to enable managed firewalls to test configuration changes for each commit and to verify that the changes did not break the connection between Panorama and the managed firewall.
https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/administer-panorama/enable-automated-commit-recovery

NEW QUESTION: 304
An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the Internet.
Which configuration will enable the firewall to download and install application updates automatically?
A. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from the management interfaced destined for the update servers goes out of the interface acting as your Internet connection.
B. Download and install application updates cannot be done automatically if the MGT port cannot reach the Internet.
C. Configure a service route for Palo Alto Networks Services that uses a dataplane interface that can route traffic to the Internet, and create a Security policy rule to allow the traffic from that interface to the update servers if necessary.
D. Configure a Security policy rule to allow all traffic to and from the update servers.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 305
Which three firewall states are valid? (Choose three)
A. Active
B. Functional
C. Pending
D. Passive
E. Suspended
Answer: A,D,E (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-firewall-states

NEW QUESTION: 306
Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls?
(Choose two.)
A. Red Hat Enterprise Virtualization (RHEV)
B. Kernel Virtualization Module (KVM)
C. Boot Strap Virtualization Module (BSVM)
D. Microsoft Hyper-V
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/ vm-series

NEW QUESTION: 307
Which PAN-OS policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?
A. Security policy
B. Application Override policy
C. Authentication policy
D. Decryption policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 308
An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the
Policies tab.
Which profile is the cause of the missing Policies tab?
A. Authentication
B. WebUI
C. Authorization

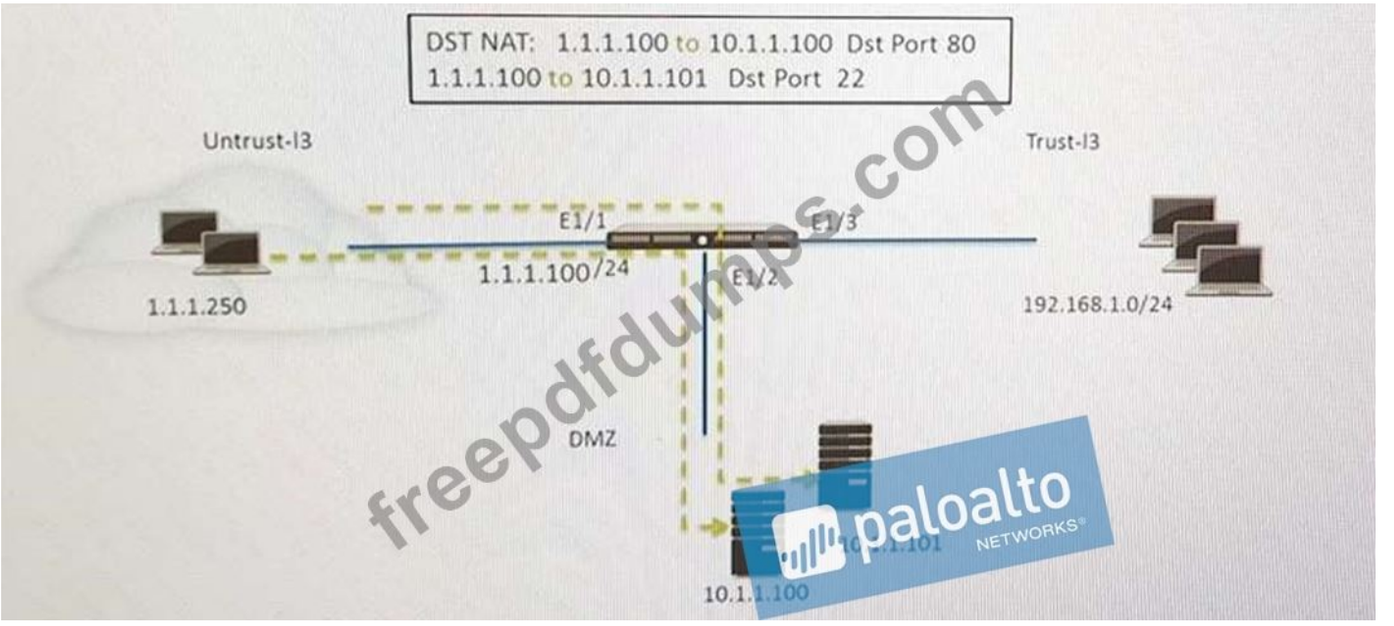
D. Admin Role
Answer: (SHOW ANSWER)

NEW QUESTION: 309
An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs.
The administrator assigns priority 100 to the active firewall.
Which priority is correct for the passive firewall?
A. 0
B. 99
C. 1
D. 255
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5.pdf (page 9)

NEW QUESTION: 310
The firewall identifies a popular application as an unknown-tcp.
Which two options are available to identify the application? (Choose two.)
A. Create a custom application.
B. Create a custom object for the custom application server to identify the custom application.
C. Submit an App-ID request to Palo Alto Networks.
D. Create a Security policy to identify the custom application.
Answer: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/use-application-objects-in-policy/create-a-custom-application
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/manage-custom-or-unknown-applications.html

NEW QUESTION: 311
If the firewall is configured for credential phishing prevention using the "Domain Credential Filter" method, which login will be detected as credential theft?
A. Mapping to the IP address of the logged-in user.
B. First four letters of the username matching any valid corporate username.
C. Using the same user's corporate username and password.
D. Matching any valid corporate username.
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection- features/credential-phishing-prevention

NEW QUESTION: 312
Refer to the exhibit.



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) received HTTP traffic and host B(10.1.1.101) receives SSH traffic.
Which two security policy rules will accomplish this configuration? (Choose two)
A. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow
B. Untrust (Any) to Untrust (10.1.1.1) Ssh-Allow
C. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
D. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
Answer: A,D (LEAVE A REPLY)

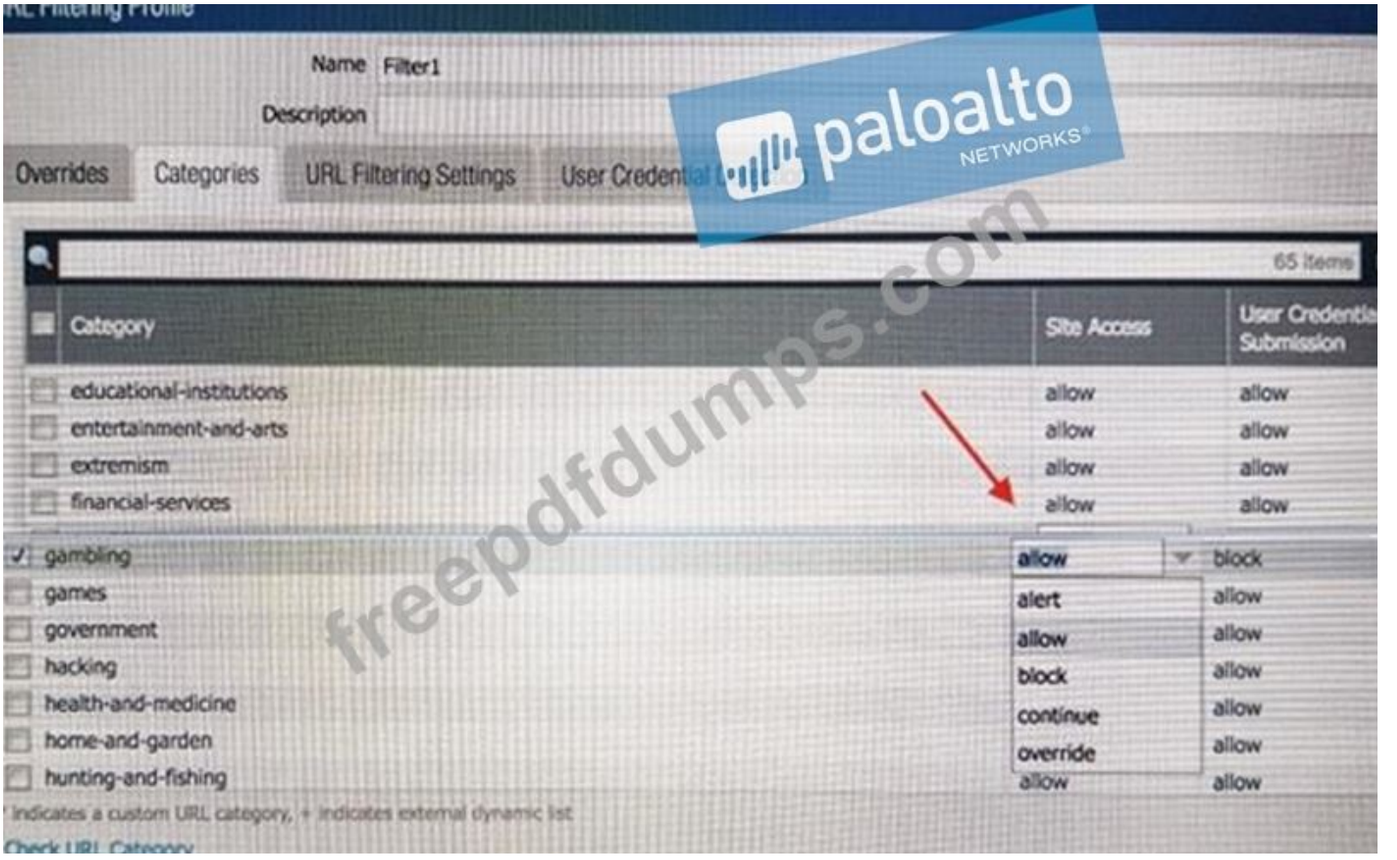
NEW QUESTION: 313
Which User-ID method maps IP address to usernames for users connecting through a web proxy that has already authenticated the user?
A. Port mapping
B. Server monitoring
C. Client Probing
D. Syslog listening
Answer: D (LEAVE A REPLY)

NEW QUESTION: 314
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image. Which configuration change should the administrator make?
A. Option

B. Option

C. Option

D. Option



E. Option

Answer: E (LEAVE A REPLY)

NEW QUESTION: 315

A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg txt. The firewall is currently running PAN-OS 10.0 and using a lab config The contents of init-cfg txi in the USB flash drive are as follows:

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsys,jumbo-frame
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command:> request resort system Upon restart, the firewall fails to begin the bootstrapping process. The failure is caused because

A. Firewall must be in factory default state or have all private data deleted for bootstrapping

B. The hostname is a required parameter, but it is missing in imt-cfg txt

C. The USB must be formatted using the ext3 file system, FAT32 is not supported
D. PANOS version must be 91.x at a minimum but the firewall is running 10.0.x
E. The bootstrap.xml file is a required file but it is missing
Answer: A (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive.html#id8378007f-d6e5-4f2d-84a4-5d50b0b3ad7d

NEW QUESTION: 316
An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN-OS software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web-browsing traffic from any to any zone. What must the administrator configure so that the PAN-OS software can be upgraded?
A. Security policy rule
B. Service route
C. CRL
D. Scheduler
Answer: (SHOW ANSWER)

NEW QUESTION: 317
How is the Forward Untrust Certificate used?
A. It issues certificates encountered on the Untrust security zone when clients attempt to connect to a site that has be decrypted/
B. It is used when web servers request a client certificate.
C. It is presented to clients when the server they are connecting to is signed by a certificate authority that is not trusted by firewall.
D. It is used for Captive Portal to identify unknown users.
Answer: C (LEAVE A REPLY)
Though a single certificate can be used for both Forward Trust and Forward Untrust, creating a separate certificate specifically for Untrust (which must be generated as a CA) allows for easy

differentiation of a valid certificate/trust error as the Palo Alto Networks device proxies the secure session.
Verify the CA to be blocked, keeping in mind that doing so blocks access to all sites issued by this CA.
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Prevent-Access-to-Encrypted-Websites-Based-on-Certificate/ta-p/57585

NEW QUESTION: 318
An administrator has left a firewall to use the default port for all management services.
Which three functions are performed by the dataplane? (Choose three.)
A. File blocking
B. NAT
C. antivirus
D. WildFire updates
E. NTP
Answer: B,D,E (LEAVE A REPLY)

NEW QUESTION: 319
Which method will dynamically register tags on the Palo Alto Networks NGFW?
A. Restful API or the VMWare API on the firewall or on the User-ID agent or the read-only domain controller (RODC)
B. Restful API or the VMware API on the firewall or on the User-ID agent
C. XML-API or the VMware API on the firewall or on the User-ID agent or the CLI
D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent
Answer: D (LEAVE A REPLY)
Reference:
dynamically register tags, you can use the XML API or the VM Monitoring agent on the firewall or on the User-ID agent. Each tag is a metadata element or attribute-value pair that is registered on the firewall or Panorama. For example, IP1 {tag1, tag2,.....tag32}, w"

NEW QUESTION: 320
Which DoS protection mechanism detects and prevents session exhaustion attacks?
A. Packet Based Attack Protection
B. Flood Protection
C. Resource Protection
D. TCP Port Scan Protection
Answer: C (LEAVE A REPLY)
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles In addition to setting IP flood thresholds, you can also use DoS Protection profiles to detect and prevent session exhaustion attacks in which a large number of hosts (bots) establish as many sessions as possible to consume a target's resources. On the profile's

Resources Protection tab, you can set the maximum number of concurrent sessions that the device(s) defined in the DoS Protection policy rule to which you apply the profile can receive. When the number of concurrent sessions reaches its maximum limit, new sessions are dropped. https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/d

NEW QUESTION: 321
An administrator needs firewall access on a trusted interface. Which two components are required to configure certificate based, secure authentication to the web UI? (Choose two)
A. certificate profile
B. server certificate
C. SSL/TLS Service Profile
D. SSH Service Profile
Answer: (SHOW ANSWER)

NEW QUESTION: 322
A customer wants to spin their session load equally across two SD-WAN-enabled interfaces. Where would you configure this setting?
A. Traffic Dtstnbution profile
B. ECMP setting on virtual router
C. Path Quality profile
D. SD-WAN Interface profile
Answer: (SHOW ANSWER)