Paloalto-Networks

Exam Questions PCNSE

Palo Alto Networks Certified Security Engineer (PCNSE)PAN-OS 9.0

NEW QUESTION 1
Which GlobalProtect gateway selling is required to enable split-tunneling by access route, destination domain, and application?

A. No Direct Access to local networks
B. Tunnel mode
C. iPSec mode
D. Satellite mode

Answer: B

Explanation:
https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-gateways/split-tunnel-tra

NEW QUESTION 2
A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours.
Which two steps are likely to mitigate the issue? (Choose TWO)

A. Exclude video traffic
B. Enable decryption
C. Block traffic that is not work-related
D. Create a Tunnel Inspection policy

Answer: AC

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PP3ICAW

NEW QUESTION 3
An engineer configures a specific service route in an environment with multiple virtual systems instead of using the inherited global service route configuration.
What type of service route can be used for this configuration?

A. IPv6 Source or Destination Address
B. Destination-Based Service Route
C. IPv4 Source Interface
D. Inherit Global Setting

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/virtual-systems/customize-service-routes-for-a-vir

NEW QUESTION 4
Which protocol is supported by GlobalProtect Clientless VPN?

A. FTP
B. RDP
C. SSH
D. HTTPS

Answer: D

Explanation:
Virtual Desktop Infrastructure (VDI) and Virtual Machine (VM) environments, such as Citrix XenApp and XenDesktop or VMWare Horizon and Vcenter, support access natively through HTML5. You can RDP, VNC, or SSH to these machines through Clientless VPN without requiring additional third-party middleware. In environments that do not include native support for HTML5 or other web application technologies supported by Clientless VPN, you can use third-party vendors, such as Thinfinity, to RDP through Clientless VPN. Reference:
https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-clientless-vpn/supporte
https://networkwiki.blogspot.com/2017/03/palo-alto-networks-clientless-vpn-and.html

NEW QUESTION 5
When you import the configuration of an HA pair into Panorama, how do you prevent the import from affecting ongoing traffic?

A. Set the passive link state to shutdown".
B. Disable config sync.
C. Disable the HA2 link.
D. Disable HA.

Answer: B

Explanation:
To prevent the import from affecting ongoing traffic when you import the configuration of an HA pair into Panorama, you should disable config sync on both firewalls. Config sync is a feature that enables the firewalls in an HA pair to synchronize their configurations and maintain consistency. However, when you import the configuration of an HA pair into Panorama, you want to avoid any changes to the firewall configuration until you verify and commit the imported configuration on Panorama. Therefore, you should disable config sync before importing the configuration, and re-enable it after committing the changes on Panorama12. References: Migrate a Firewall HA Pair to Panorama Management, PCNSE Study Guide (page 50)

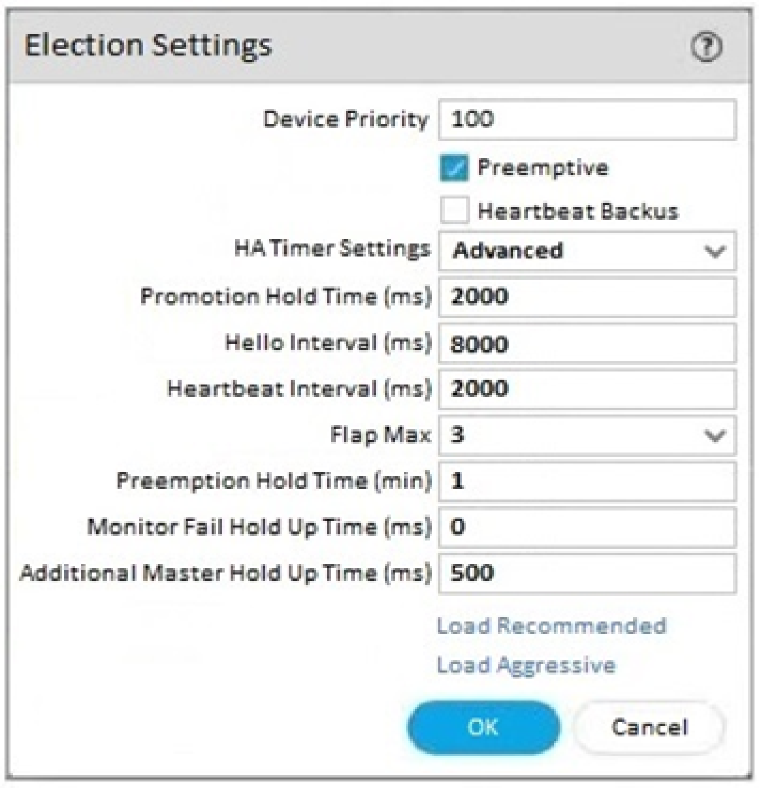
NEW QUESTION 6
A security engineer needs firewall management access on a trusted interface.
Which three settings are required on an SSL/TLS Service Profile to provide secure Web UI authentication? (Choose three.)

A. Minimum TLS version
B. Certificate
C. Encryption Algorithm
D. Maximum TLS version
E. Authentication Algorithm

Answer: ABD

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssltls-service

NEW QUESTION 7
An engineer is reviewing the following high availability (HA) settings to understand a recent HAfailover event.



Election Settings

Device Priority	100
	☑ Preemptive
	□ Heartbeat Backus
HA Timer Settings	Advanced
Promotion Hold Time (ms)	2000
Hello Interval (ms)	8000
Heartbeat Interval (ms)	2000
Flap Max	3
Preemption Hold Time (min)	1
Monitor Fail Hold Up Time (ms)	0
Additional Master Hold Up Time (ms)	500

Which timer determines the frequency between packets sent to verify that the HA functionality on the other HA firewall is operational?

A. Monitor Fail Hold Up Time
B. Promotion Hold Time
C. Heartbeat Interval
D. Hello Interval

Answer: D

Explanation:
The timer that determines the frequency between packets sent to verify that the HA functionality on the other HA firewall is operational is the Hello Interval. The Hello Interval is the interval in milliseconds between hello packets that are sent to check the HA status of the peer firewall. The default value for the Hello Interval is 8000 ms for all platforms, and the range is 8000-60000 ms. If the firewall does not receive a hello packet from its peer within the specified interval, it will declare the peer as failed and initiate a failover12. References: H Timers, Layer 3 High Availability with Optimal Failover Times Best Practices
How to Configure Ping Interval/Timeout Settings ... - Palo Alto Networks

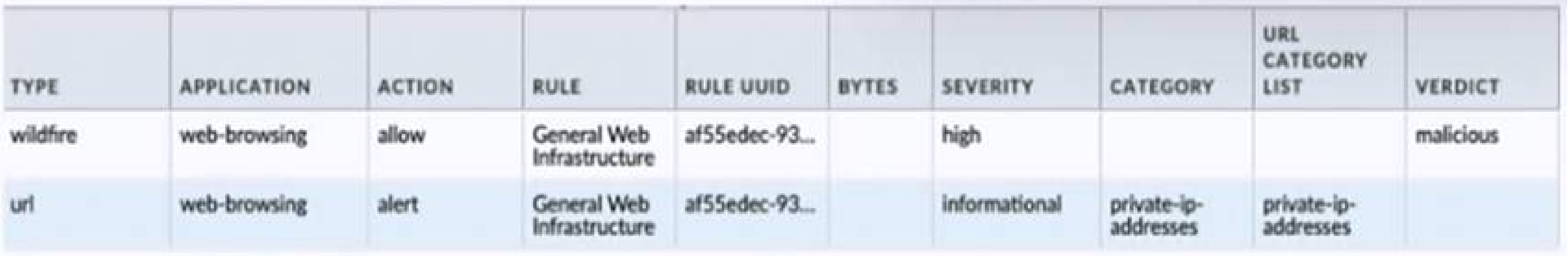
NEW QUESTION 8
In a security-first network, what is the recommended threshold value for apps and threats to be dynamically updated?

A. 1 to 4 hours
B. 6 to 12 hours
C. 24 hours
D. 36 hours

Answer: B

Explanation:
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-thr
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/software-and-content-updates/best-practices-for

NEW QUESTION 9
Given the following snippet of a WildFire submission log did the end-user get access to the requested information and why or why not?



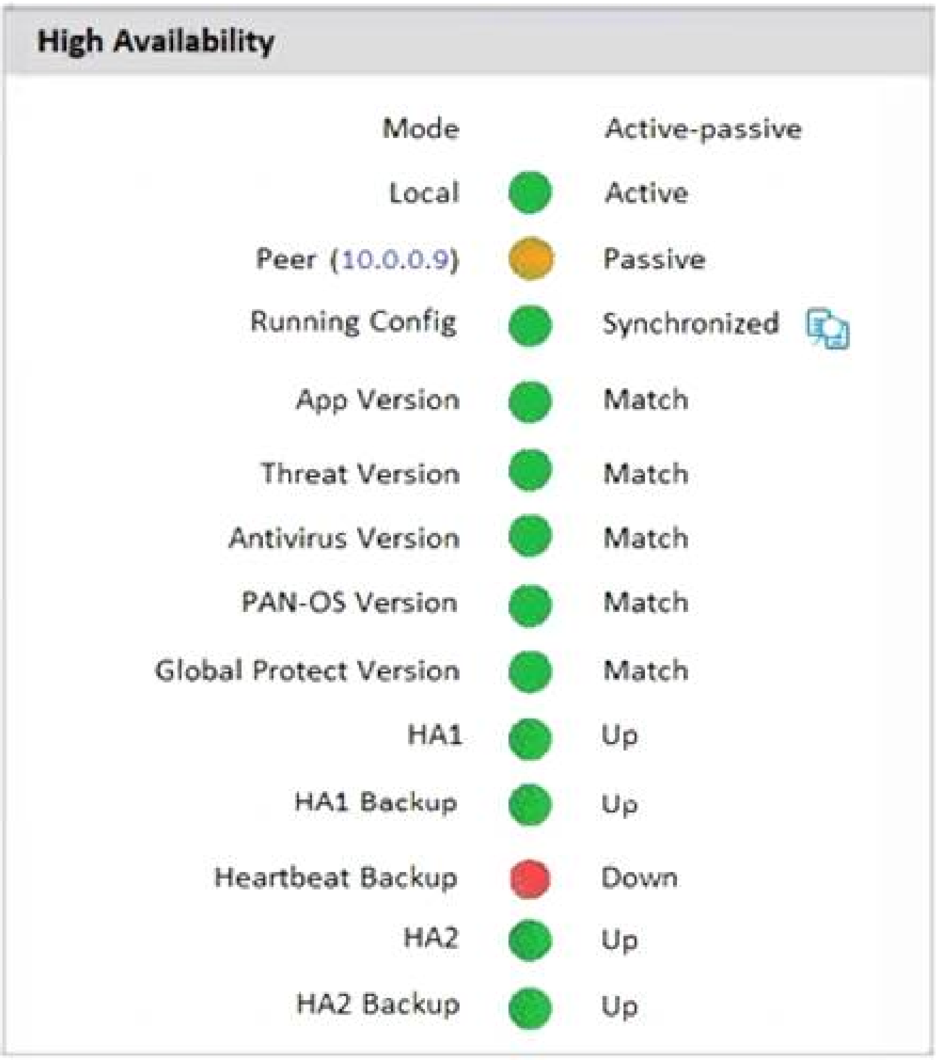
TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	web-browsing	allow	General Web Infrastructure	af55edec-93...		high			malicious
url	web-browsing	alert	General Web Infrastructure	af55edec-93...		informational	private-ip-addresses	private-ip-addresses	

A. Yes, because the action is set to alert
B. No, because this is an example from a defeated phishing attack
C. No, because the severity is high and the verdict is malicious.
D. Yes, because the action is set to allow.

Answer: D

Explanation:
https://live.paloaltonetworks.com/t5/general-topics/wildfire-submission-entries-with-severity-high-showing-acti

NEW QUESTION 10
An administrator Just enabled HA Heartbeat Backup on two devices However, the status on tie firewall's dashboard is showing as down High Availability.



High Availability

Mode		Active-passive
Local	🟢	Active
Peer (10.0.0.9)	🟠	Passive
Running Config	🟢	Synchronized
App Version	🟢	Match
Threat Version	🟢	Match
Antivirus Version	🟢	Match
PAN-OS Version	🟢	Match
Global Protect Version	🟢	Match
HA1	🟢	Up
HA1 Backup	🟢	Up
Heartbeat Backup	🔴	Down
HA2	🟢	Up
HA2 Backup	🟢	Up

What could an administrator do to troubleshoot the issue?

A. Go to Device > High Availability> General > HA Pair Settings > Setup and configuring the peer IP for heartbeat backup
B. Check peer IP address In the permit list In Device > Setup > Management > Interfaces > Management Interface Settings
C. Go to Device > High Availability > HA Communications> General> and check the Heartbeat Backup under Election Settings
D. Check peer IP address for heartbeat backup to Device > High Availability > HA Communications > Packet Forwarding settings.

Answer: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClF4CAK

NEW QUESTION 10
An administrator is using Panorama to manage multiple firewalls. After upgrading all devices to the latest PAN-OS software, the administrator enables log forwarding from the firewalls to Panorama.
However, pre-existing logs from the firewalls are not appearing in Panorama.
Which action should be taken to enable the firewalls to send their pre-existing logs to Panorama?

A. Export the log database.
B. Use the import option to pull logs.
C. Use the scp logdb export command.
D. Use the ACC to consolidate the logs.

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/use-the-cli/use-secure-copy-to-import-and

NEW QUESTION 12
Which two policy components are required to block traffic in real time using a dynamic user group (DUG)? (Choose two.)

A. A Deny policy for the tagged traffic
B. An Allow policy for the initial traffic
C. A Decryption policy to decrypt the traffic and see the tag
D. A Deny policy with the "tag" App-ID to block the tagged traffic

Answer: AB

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups Use the dynamic user group in a policy to regulate traffic for the members of the group. You will need to
configure at least two rules: one to allow initial traffic to populate the dynamic user group and one to deny traffic for the activity you want to prevent (in this case, questionable-activity). To tag users, the rule to allow traffic must have a higher rule number in your rulebase than the rule that denies traffic.
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-dynamic-user-groups-in-policy

NEW QUESTION 17
Why would a traffic log list an application as "not-applicable”?

A. The firewall denied the traffic before the application match could be performed.
B. The TCP connection terminated without identifying any application data
C. There was not enough application data after the TCP connection was established
D. The application is not a known Palo Alto Networks App-ID.

Answer: A

Explanation:
traffic log would list an application as “not-applicable” if the firewall denied the traffic before the application match could be performed. This can happen if the traffic matches a security rule that is set to deny based on any parameter other than the application, such as source, destination, port, service, etc1. In this case, the firewall does not inspect the application data and discards the traffic, resulting in a “not-applicable” entry in the application field of the traffic log1.

NEW QUESTION 22
An engineer is configuring a firewall with three interfaces:
• MGT connects to a switch with internet access.
• Ethernet1/1 connects to an edge router.
• Ethernet1/2 connects to a visualization network.
The engineer needs to configure dynamic updates to use a dataplane interface for internet traffic. What should be configured in Setup > Services > Service Route Configuration to allow this traffic?

A. Set DNS and Palo Alto Networks Services to use the ethernet1/1 source interface.
B. Set DNS and Palo Alto Networks Services to use the ethernet1/2 source interface.
C. Set DNS and Palo Alto Networks Services to use the MGT source interface.
D. Set DDNS and Palo Alto Networks Services to use the MGT source interface.

Answer: A

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGJCA0

NEW QUESTION 24
An engineer troubleshoots a Panorama-managed firewall that is unable to reach the DNS servers configured via a global template. As a troubleshooting step, the engineer needs to configure a local DNS server in place of the template value.
Which two actions can be taken to ensure that only the specific firewall is affected during this process? (Choose two)

A. Configure the DNS server locally on the firewall.
B. Change the DNS server on the global template.
C. Override the DNS server on the template stack.
D. Configure a service route for DNS on a different interface.

Answer: AC

Explanation:
To override a device and network setting applied by a template, you can either configure the setting locally on the firewall or override the setting on the template stack. Configuring the setting locally on the firewall will
copy the setting to the local configuration of the device and will no longer be controlled by the template. Overriding the setting on the template stack will apply the setting to all the firewalls that are assigned to the template stack, unless the setting is also overridden locally on a firewall. Changing the setting on the global template will affect all the firewalls that inherit the setting from the template, which is not desirable in this scenario. Configuring a service route for DNS on a different interface will not change the DNS server address, but only the interface that the firewall uses to reach the DNS server. References:
➢ Override a Template Setting
➢ Overriding Panorama Template settings

NEW QUESTION 27
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)

A. upload-onlys
B. install and reboot
C. upload and install

D. upload and install and reboot
E. verify and install

Answer: ACD

Explanation:
ttps://www.kareemccie.com/2021/05/palo-alto-firewall-packet-flow.html

NEW QUESTION 30
Which three multi-factor authentication methods can be used to authenticate access to the firewall? (Choose three.)

A. Voice
B. Fingerprint
C. SMS
D. User certificate
E. One-time password

Answer: CDE

Explanation:
The firewall can use three multi-factor authentication methods to authenticate access to the firewall: SMS, user certificate, and one-time password. These methods can be used in combination with other authentication factors, such as username and password, to provide stronger security for accessing the firewall web interface or CLI. The firewall can integrate with various MFA vendors that support these methods through RADIUS or SAML protocols5. Voice and fingerprint are not supported by the firewall as MFA methods. References: MF Vendor Support, PCNSE Study Guide (page 48)

NEW QUESTION 33
What is the best definition of the Heartbeat Interval?

A. The interval in milliseconds between hello packets
B. The frequency at which the HA peers check link or path availability
C. The frequency at which the HA peers exchange ping
D. The interval during which the firewall will remain active following a link monitor failure

Answer: C

Explanation:
The firewalls exchange hello messages and heartbeats at configurable intervals to verify that the peer firewall is responsive and operational. Hello messages are sent from one peer to the other to verify the state of the firewall. The heartbeat is an ICMP ping to the HA peer. A response from the peer indicates that the firewalls are connected and responsive.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClUcCAK
"A "heartbeat-interval" CLI command was added to the election settings for HA, this interval has a 1000ms minimum for all Palo Alto Networks platforms and is an ICMP ping to the other device through the HA control link." https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClMaCAK

NEW QUESTION 34
A network security administrator has been tasked with deploying User-ID in their organization. What are three valid methods of collecting User-ID information in a network? (Choose three.)

A. Windows User-ID agent
B. GlobalProtect
C. XMLAPI
D. External dynamic list
E. Dynamic user groups

Answer: ABC

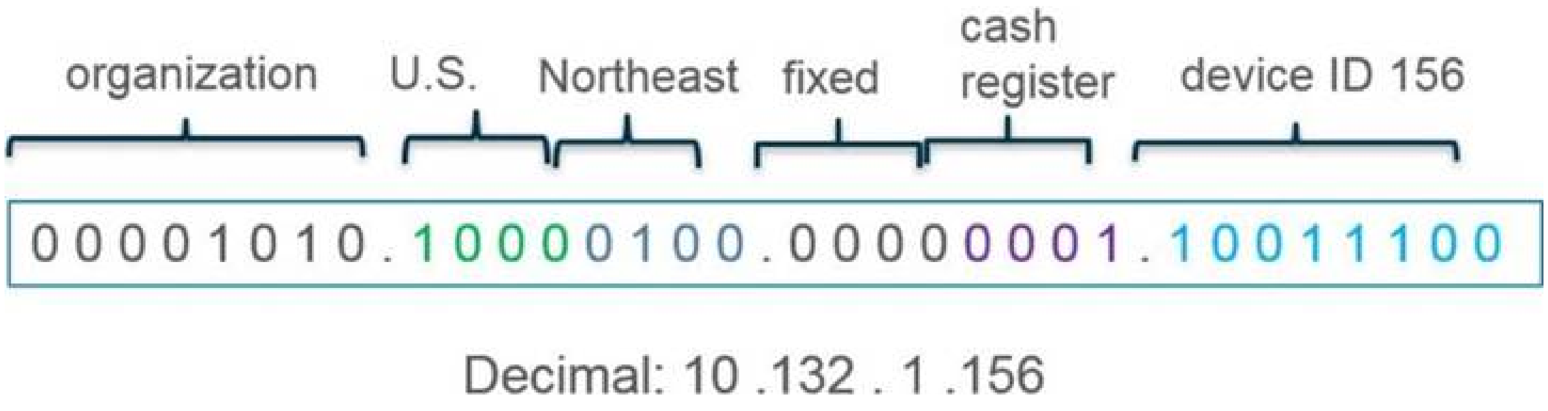
Explanation:
User-ID is a feature that allows the firewall to identify and classify users and groups on the network based on their usernames, IP addresses, and other attributes1. User-ID information can be collected from various sources, such as:

> A: Windows User-ID agent: A software agent that runs on a Windows server and collects user information from Active Directory domain controllers, Exchange servers, or eDirectory servers2. The agent then sends the user information to the firewall or Panorama for user mapping2.

> B: GlobalProtect: A software agent that runs on the endpoints and provides secure VPN access to the network3. GlobalProtect also collects user information from the endpoints and sends it to the firewall or Panorama for user mapping4.

> C: XMLAPI: An application programming interface that allows external systems or scripts to send user information to the firewall or Panorama in XML format. The XMLAPI can be used to integrate with third-party systems, such as identity providers, captive portals, or custom applications.

NEW QUESTION 36
What type of address object would be useful for internal devices where the addressing structure assigns meaning to certain bits in the address, as illustrated in the diagram?



A. IP Netmask
B. IP Wildcard Mask
C. IP Address
D. IP Range

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-address-object-to-represent-ip-addresse

NEW QUESTION 37
An administrator configures a site-to-site IPsec VPN tunnel between a PA-850 and an external customer on their policy-based VPN devices.
What should an administrator configure to route interesting traffic through the VPN tunnel?

A. Proxy IDs
B. GRE Encapsulation
C. Tunnel Monitor
D. ToS Header

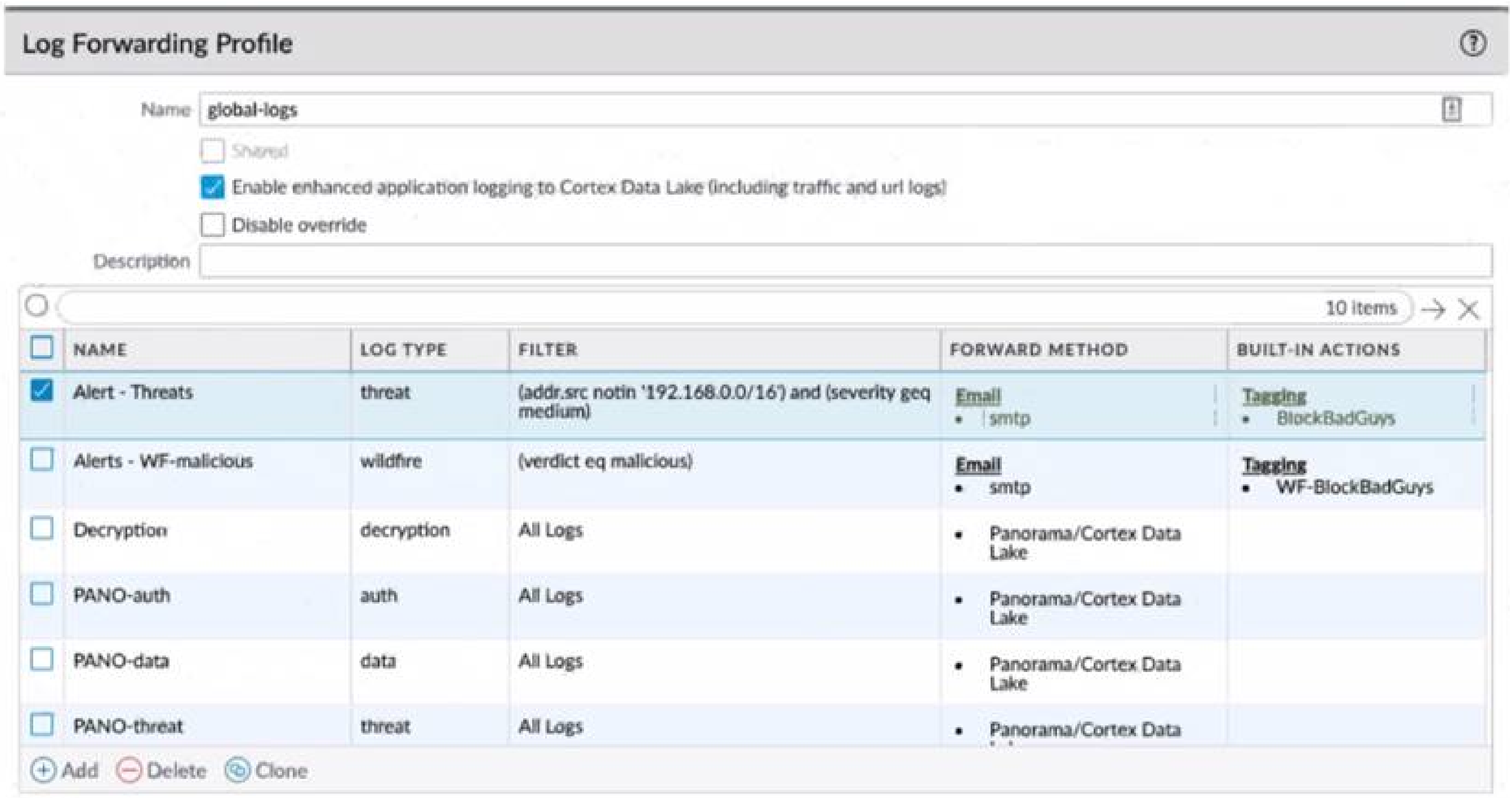
Answer: A

Explanation:
An administrator should configure proxy IDs to route interesting traffic through the VPN tunnel when the peer device is a policy-based VPN device. Proxy IDs are used to identify the traffic that belongs to a particular IPSec VPN and to direct it to the appropriate tunnel. Proxy IDs consist of a local IP address, a remote IP address, and an application (protocol and port numbers). Each proxy ID is considered to be a VPN tunnel and is counted towards the IPSec VPN tunnel capacity of the firewall. Proxy IDs are required for IKEv1 VPNs and optional for IKEv2 VPNs. If the proxy ID is not configured, the firewall uses the default values of source IP: 0.0.0.0/0, destination IP: 0.0.0.0/0, and application: any, which may not match the peer's policy and result in a failure to establish the VPN connection.
References:

> Proxy ID for IPSec VPN

> Set Up an IPSec Tunnel

NEW QUESTION 38
Review the images.



Log Forwarding Profile

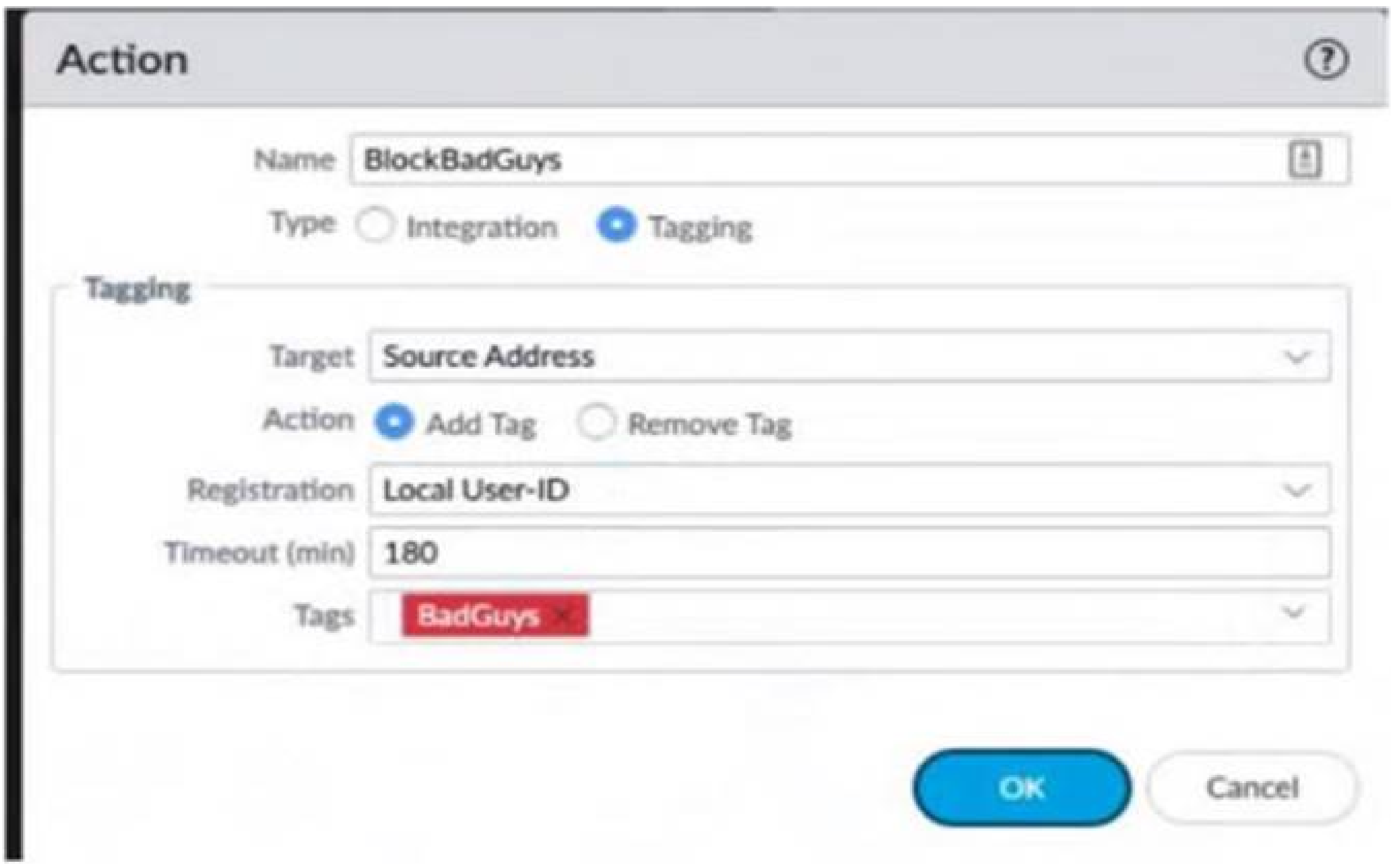
Name: global-logs

□ Shared
☑ Enable enhanced application logging to Cortex Data Lake (including traffic and url logs)
□ Disable override

Description:

10 items

□	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
☑	Alert - Threats	threat	(addr.src notin '192.168.0.0/16') and (severity geq medium)	Email • smtp	Tagging • BlockBadGuys
□	Alerts - WF-malicious	wildfire	(verdict eq malicious)	Email • smtp	Tagging • WF-BlockBadGuys
□	Decryption	decryption	All Logs	• Panorama/Cortex Data Lake	
□	PANO-auth	auth	All Logs	• Panorama/Cortex Data Lake	
□	PANO-data	data	All Logs	• Panorama/Cortex Data Lake	
□	PANO-threat	threat	All Logs	• Panorama/Cortex Data	



Action

Name: BlockBadGuys

Type: ○ Integration ● Tagging

Tagging

Target: Source Address

Action: ● Add Tag ○ Remove Tag

Registration: Local User-ID

Timeout (min): 180

Tags: BadGuys

A firewall policy that permits web traffic includes the global-logs policy is depicted What is the result of traffic that matches the "Alert - Threats" Profile Match List?

A. The source address of SMTP traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.
B. The source address of traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.
C. The source address of traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.
D. The source address of SMTP traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.

Answer: C

NEW QUESTION 40
During the process of developing a decryption strategy and evaluating which websites are required for corporate users to access, several sites have been identified that cannot be decrypted due to technical reasons. In this case, the technical reason is unsupported ciphers Traffic to these sites will therefore be blocked if decrypted.
How should the engineer proceed?

A. Install the unsupported cipher into the firewall to allow the sites to be decrypted
B. Allow the firewall to block the sites to improve the security posture.
C. Add the sites to the SSL Decryption Exclusion list to exempt them from decryption.
D. Create a Security policy to allow access to those sites.

Answer: C

Explanation:
If some sites cannot be decrypted due to technical reasons, such as unsupported ciphers, and blocking them is not an option, then the engineer should add the sites to the SSL Decryption Exclusion list to exempt them from decryption. The SSL Decryption Exclusion list is a predefined list of sites that are not subject to SSL decryption by the firewall. The list includes sites that use certificate pinning, mutual authentication, or unsupported cipher suites. The engineer can also add custom sites to the list if they have a valid business reason or technical limitation for not decrypting them34. Adding the sites to the SSL Decryption Exclusion list will allow the traffic to pass through without being decrypted or blocked by the firewall. References: SSL Decryption Exclusion, Troubleshoot Unsupported Cipher Suites

NEW QUESTION 45
A company has configured a URL Filtering profile with override action on their firewall. Which two profiles are needed to complete the configuration? (Choose two)

A. SSL/TLS Service
B. HTTP Server
C. Decryption
D. Interface Management

Answer: AD

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRdCAK https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/configure-url-filtering
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/allow-password-access-to-certain-site

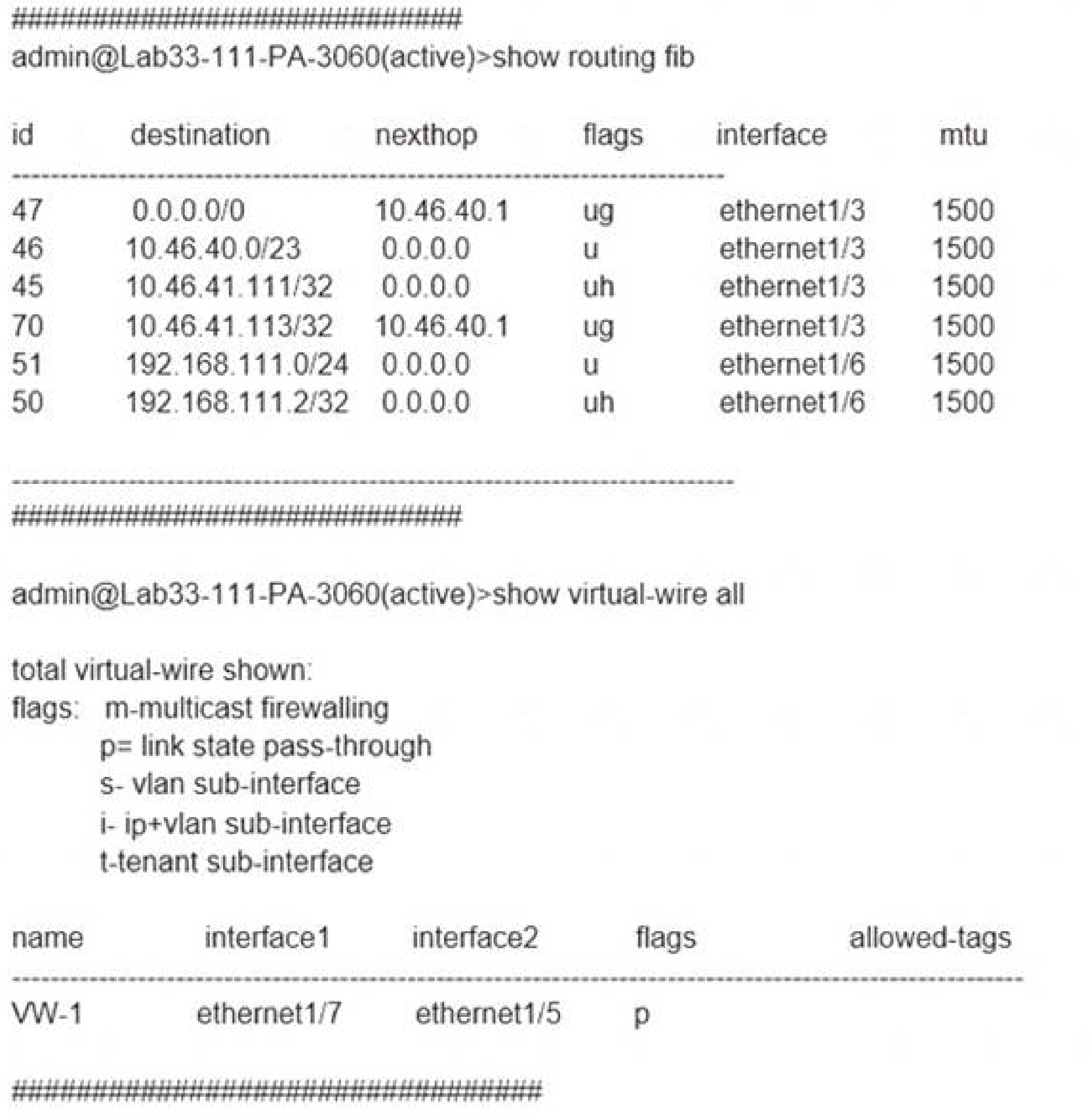
NEW QUESTION 49
If a URL is in multiple custom URL categories with different actions, which action will take priority?

A. Allow
B. Override
C. Block
D. Alert

Answer: C

Explanation:
When a URL matches multiple categories, the category chosen is the one that has the most severe action defined below (block being most severe and allow least severe).
1 block
2 override
3 continue
4 alert
5 allow https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClsmCAC

NEW QUESTION 50
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 ethernet1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

A. ethernet1/6
B. ethernet1/3
C. ethernet1/7
D. ethernet1/5

Answer: D

Explanation:
In the second image, VW ports mentioned are 1/5 and 1/7. Hence it can not be a part of any other routing. So if any traffic coming as ingress from 1/7, it has to go out via 1/5.
The egress interface for the traffic with ingress interface ethernet1/7, source 192.168.111.3, and destination 10.46.41.113 will be ethernet1/5. This is because the traffic will match the virtual wire with interfaces ethernet1/5 and ethernet1/7, which is configured to allow VLAN-tagged traffic with tags 10 and 201. The traffic will also match the security policy rule that allows traffic from zone Trust to zone Untrust, which are assigned to ethernet1/7 and ethernet1/5 respectively2. Therefore, the traffic will be forwarded to the same interface from which it was received, which is ethernet1/53.

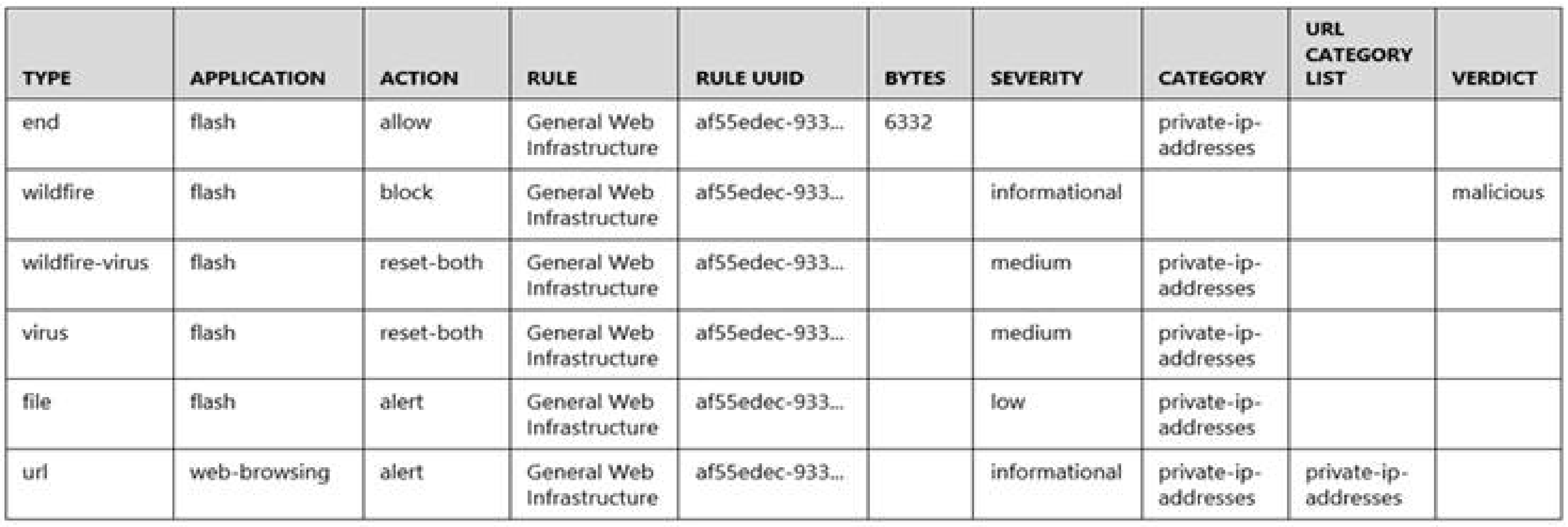
NEW QUESTION 51
An organization conducts research on the benefits of leveraging the Web Proxy feature of PAN-OS 11.0. What are two benefits of using an explicit proxy method versus a transparent proxy method? (Choose two.)

A. No client configuration is required for explicit proxy, which simplifies the deployment complexity.
B. Explicit proxy supports interception of traffic using non-standard HTTPS ports.
C. It supports the X-Authenticated-User (XAU) header, which contains the authenticated username in the outgoing request.
D. Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy.

Answer: CD

Explanation:
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-us https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy

NEW QUESTION 56
Given the following snippet of a WildFire submission log, did the end user successfully download a file?



TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
end	flash	allow	General Web Infrastructure	af55edec-933...	6332		private-ip-addresses		
wildfire	flash	block	General Web Infrastructure	af55edec-933...		informational			malicious
wildfire-virus	flash	reset-both	General Web Infrastructure	af55edec-933...		medium	private-ip-addresses		
virus	flash	reset-both	General Web Infrastructure	af55edec-933...		medium	private-ip-addresses		
file	flash	alert	General Web Infrastructure	af55edec-933...		low	private-ip-addresses		
url	web-browsing	alert	General Web Infrastructure	af55edec-933...		informational	private-ip-addresses	private-ip-addresses	

A. No, because the URL generated an alert.
B. Yes, because both the web-browsing application and the flash file have the 'alert" action.
C. Yes, because the final action is set to "allow."
D. No, because the action for the wildfire-virus is "reset-both."

Answer: C

Explanation:
Based on the snippet of the WildFire submission log provided, it appears that the end user was able to successfully download a file. The key indicator here is that the final action for the web-browsing application and the flash file is set to “allow.” This means that despite any alerts or other actions taken earlier in the process, the ultimate decision was to allow the file to be downloaded.

NEW QUESTION 61
An engineer is deploying multiple firewalls with common configuration in Panorama. What are two benefits of using nested device groups? (Choose two.)

A. Inherit settings from the Shared group
B. Inherit IPSec crypto profiles
C. Inherit all Security policy rules and objects
D. Inherit parent Security policy rules and objects

Answer: AD

Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-conf

NEW QUESTION 66
Which Panorama feature protects logs against data loss if a Panorama server fails?

A. Panorama HA automatically ensures that no logs are lost if a server fails inside the HA Cluster.
B. Panorama Collector Group with Log Redundancy ensures that no logs are lost if a server fails inside the Collector Group.
C. Panorama HA with Log Redundancy ensures that no logs are lost if a server fails inside the HA Cluster.
D. Panorama Collector Group automatically ensures that no logs are lost if a server fails inside the Collector Group

Answer: B

Explanation:
https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/manage-log-collection/manage-collector-gr "Log redundancy is available only if each Log Collector has the same number of logging disks."
(Recommended) Enable log redundancy across collectors if you are adding multiple Log Collectors to a single Collector group. Redundancy ensures that no logs are lost if any one Log Collector becomes unavailable. Each log will have two copies and each copy will reside on a different Log Collector. For example, if you have two Log Collectors in the collector group the log is written to both Log Collectors. Enabling redundancy creates more logs and therefore requires more storage capacity, reducing storage capability in half. When a Collector Group runs out of space, it deletes older logs. Redundancy also doubles the log processing traffic in a Collector Group, which reduces its maximum logging rate by half, as each Log Collector must distribute a copy of each log it receives.

NEW QUESTION 71
An administrator is troubleshooting why video traffic is not being properly classified. If this traffic does not match any QoS classes, what default class is assigned?

A. 1
B. 2
C. 3
D. 4

Answer: D

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/quality-of-service/qos-concepts/qos-classes

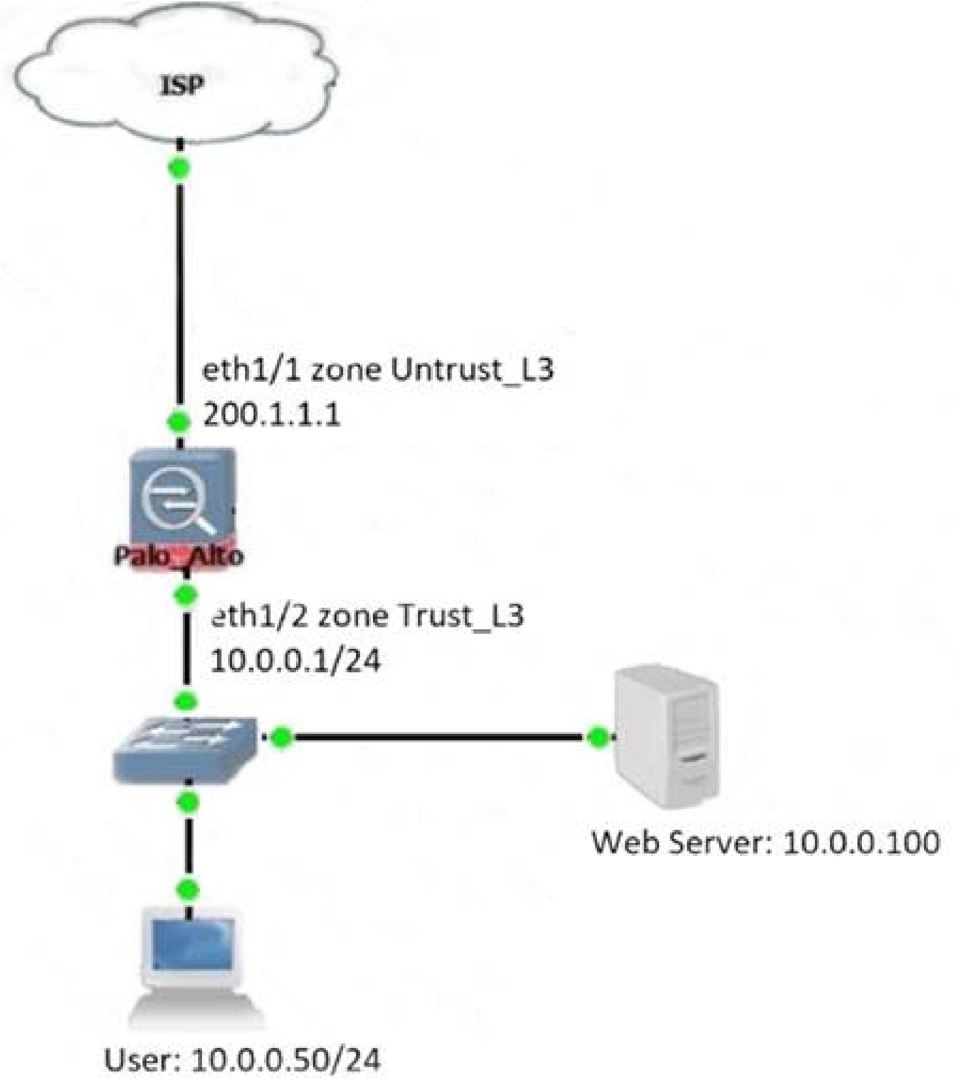
NEW QUESTION 73
An engineer decides to use Panorama to upgrade devices to PAN-OS 10.2. Which three platforms support PAN-OS 10.2? (Choose three.)

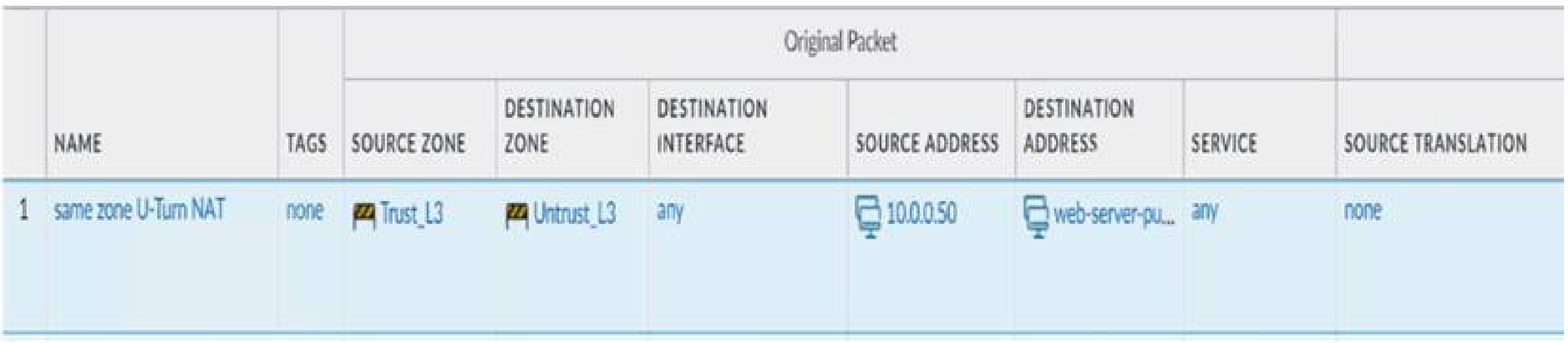
A. PA-220
B. PA-800 Series
C. PA-5000 Series
D. PA-500
E. PA-3400 Series

Answer: ABE

Explanation:
https://docs.paloaltonetworks.com/compatibility-matrix/supported-os-releases-by-model/palo-alto-networks-nex

NEW QUESTION 77
Review the information below. A firewall engineer creates a U-NAT rule to allow users in the trust zone access to a server in the same zone by using an external, public NAT IP for that server.
Given the rule below, what change should be made to make sure the NAT works as expected?





			Original Packet						
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION
1	same zone U-Turn NAT	none	Trust_L3	Untrust_L3	any	10.0.0.50	web-server-pu...	any	none

A. Change destination NAT zone to Trust_L3.
B. Change destination translation to Dynamic IP (with session distribution) using firewall ethI/2 address.
C. Change Source NAT zone to Untrust_L3.
D. Add source Translation to translate original source IP to the firewall eth1/2 interface translation.

Answer: D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEiCAK

NEW QUESTION 81
Which statement regarding HA timer settings is true?

A. Use the Recommended profile for typical failover timer settings
B. Use the Moderate profile for typical failover timer settings
C. Use the Aggressive profile for slower failover timer settings.
D. Use the Critical profile for faster failover timer settings.

Answer: A

Explanation:

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-timers

NEW QUESTION 82
An administrator is receiving complaints about application performance degradation. After checking the ACC, the administrator observes that there is an excessive amount of VoIP traffic.
Which three elements should the administrator configure to address this issue? (Choose three.)

A. An Application Override policy for the SIP traffic
B. QoS on the egress interface for the traffic flows
C. QoS on the ingress interface for the traffic flows
D. A QoS profile defining traffic classes
E. A QoS policy for each application ID

Answer: BDE

Explanation:
To address the issue of application performance degradation due to excessive VoIP traffic, the administrator should configure QoS on the egress interface for the traffic flows and a QoS profile defining traffic classes. QoS stands for Quality of Service, which is a feature that allows the firewall to manage bandwidth usage and prioritize traffic based on various criteria, such as application, user, service, etc. QoS can help improve the performance and quality of latency-sensitive applications, such as VoIP, by guaranteeing them sufficient bandwidth and priority over other traffic1.
To enable QoS on the firewall, the administrator needs to create a QoS profile and a QoS policy. A QoS profile defines the eight classes of service that traffic can receive, including priority, guaranteed bandwidth, maximum bandwidth, and weight. A QoS policy identifies the traffic that matches a specific class of service based on source and destination zones, addresses, users, applications, services, etc2. The administrator can also create a custom QoS profile or use the default one.
The administrator should apply QoS on the egress interface for the traffic flows, which is the interface where the traffic leaves the firewall. This is because QoS can only shape outbound traffic and not inbound traffic. The egress interface can be either internal or external, depending on the direction of the VoIP traffic. For example, if the VoIP traffic is from internal users to external servers, then the egress interface is the untrust interface facing the ISP. If the VoIP traffic is from external users to internal servers, then the egress interface is the trust interface facing the LAN3.
The administrator should assign a high priority and a sufficient guaranteed bandwidth to the VoIP traffic in the QoS profile. This will ensure that the VoIP packets are processed first by the firewall and are not dropped or delayed due to congestion. The administrator can also limit or block other applications that consume too much bandwidth or pose security risks in the same or different QoS classes4.
An Application Override policy for SIP traffic is not necessary to address this issue. An Application Override policy is used to change or customize the App-ID of certain traffic based on port and protocol criteria. This can be useful for optimizing performance or security for some applications that are difficult to identify or have non-standard behaviors. However, SIP is a predefined App-ID that identifies Session Initiation Protocol (SIP) traffic, which is commonly used for VoIP signaling. The firewall can recognize SIP traffic without an Application Override policy5.
QoS on the ingress interface for the traffic flows is not effective to address this issue. As mentioned earlier, QoS can only shape outbound traffic and not inbound traffic. Applying QoS on the ingress interface will not have any impact on how the firewall handles or prioritizes the incoming packets6.
A QoS policy for each application is not required to address this issue. A QoS policy can match multiple applications in a single rule by using application filters or application groups. This can simplify and consolidate the QoS policy configuration and management. The administrator does not need to create a separate QoS policy for each application unless there is a specific need to assign different classes of service or parameters to each application7.
References: QoS Overview, Configure QoS, QoS Use Cases, QoS Best Practices, Application Override FAQ, Create a QoS Policy Rule

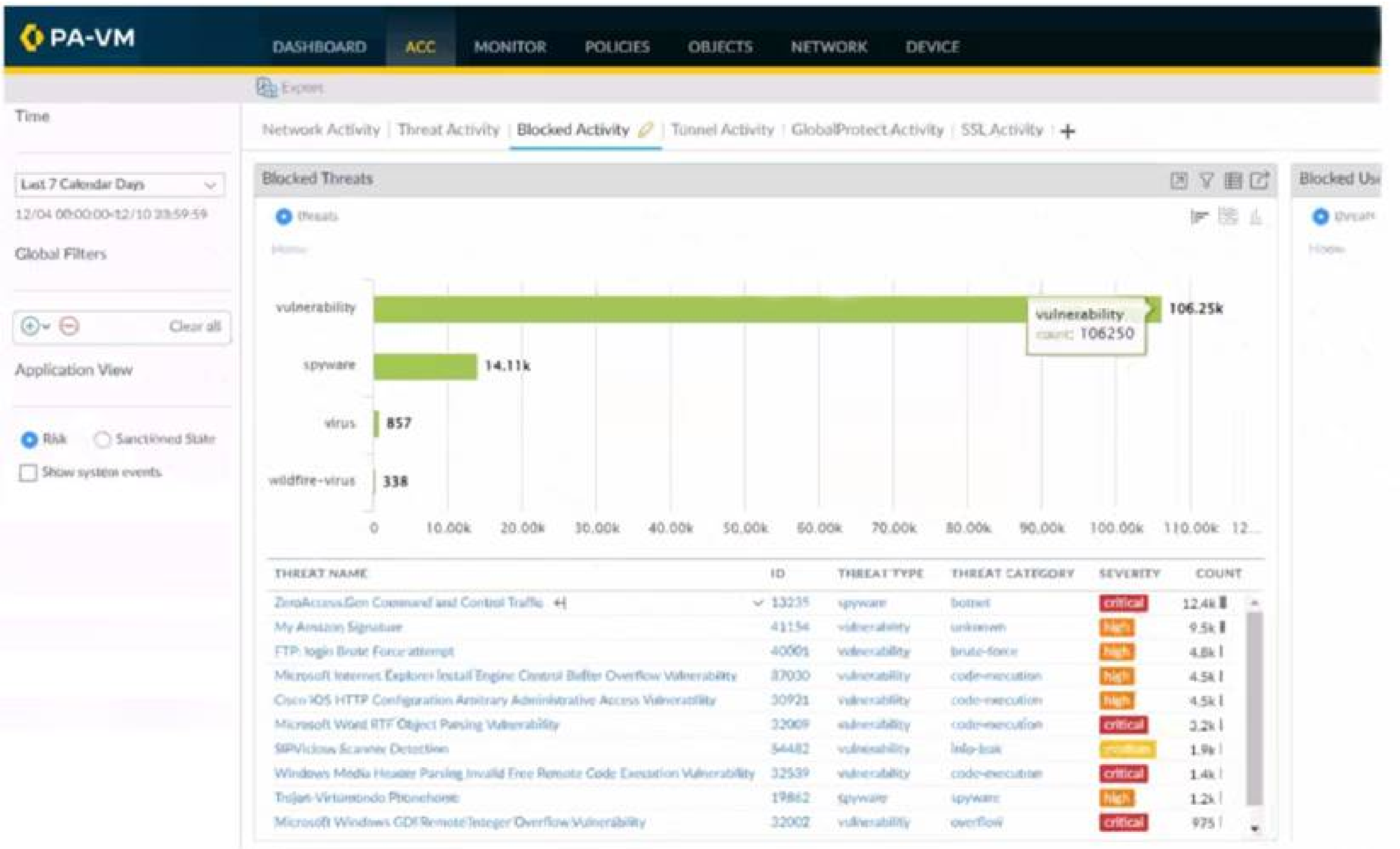
NEW QUESTION 85
Which type of policy in Palo Alto Networks firewalls can use Device-ID as a match condition?

A. NAT
B. DOS protection
C. QoS
D. Tunnel inspection

Answer: C

Explanation:
The type of policy in Palo Alto Networks firewalls that can use Device-ID as a match condition is QoS. This is because Device-ID is a feature that allows the firewall to identify and classify devices on the network based on their characteristics, such as vendor, model, OS, and role1. QoS policies are used to allocate bandwidth and prioritize traffic based on various criteria, such as application, user, source, destination, and device2. By using Device-ID as a match condition in QoS policies, the firewall can apply different QoS actions to different types of devices, such as IoT devices, laptops, smartphones, etc3. This can help optimize the network performance and ensure the quality of service for critical applications and devices.

NEW QUESTION 89
Refer to the exhibit.



THREAT NAME	ID	THREAT TYPE	THREAT CATEGORY	SEVERITY	COUNT
ZeroAccess.Gen Command and Control Traffic	13235	spyware	botnet	critical	12.4k
My Amazon Signature	41154	vulnerability	unknown	high	9.5k
FTP: login Brute Force attempt	40001	vulnerability	brute-force	high	4.8k
Microsoft Internet Explorer Install Engine Control Buffer Overflow Vulnerability	37030	vulnerability	code-execution	high	4.5k
Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability	30921	vulnerability	code-execution	high	4.5k
Microsoft Word RTF Object Parsing Vulnerability	32009	vulnerability	code-execution	critical	3.2k
SIPVicious Scanner Detection	54482	vulnerability	info-leak	medium	1.9k
Windows Media Header Parsing Invalid Free Remote Code Execution Vulnerability	32539	vulnerability	code-execution	critical	1.4k
Trojan-Virtumondo Phonehome	19862	spyware	spyware	high	1.2k
Microsoft Windows GDI Remote Integer Overflow Vulnerability	32002	vulnerability	overflow	critical	975

Using the above screenshot of the ACC, what is the best method to set a global filter, narrow down Blocked User Activity, and locate the user(s) that could be compromised by a botnet?

A. Click the hyperlink for the Zero Access.Gen threat.
B. Click the left arrow beside the Zero Access.Gen threat.
C. Click the source user with the highest threat count.
D. Click the hyperlink for the hotport threat Category.

Answer: B

Explanation:
Hover over an attribute in the table below the chart and click the arrow icon to the right of the attribute. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-the-application-command-center/int

NEW QUESTION 91
If an administrator wants to apply QoS to traffic based on source, what must be specified in a QoS policy rule?

A. Post-NAT destination address
B. Pre-NAT destination address
C. Post-NAT source address
D. Pre-NAT source address

Answer: C

Explanation:
If an administrator wants to apply QoS to traffic based on source, they must specify the post-NAT source address in a QoS policy rule. This is because QoS is enforced on traffic as it egresses the firewall, and the firewall applies NAT rules before QoS rules. Therefore, the firewall will match the QoS policy rule based on the translated source address, not the original source address. If the administrator uses the pre-NAT source address in the QoS policy rule, the firewall will not be able to identify the traffic correctly and apply the desired QoS treatment. References:

- QoS Policy
- Configure QoS

NEW QUESTION 95
A company wants to add threat prevention to the network without redesigning the network routing. What are two best practice deployment modes for the firewall? (Choose two.)

A. VirtualWire
B. Layer3
C. TAP
D. Layer2

Answer: AD

Explanation:

- A and D are the best practice deployment modes for the firewall if the company wants to add threat prevention to the network without redesigning the network routing. This is because these modes allow the firewall to act as a transparent device that does not affect the existing network topology or routing1.
- A: VirtualWire mode allows the firewall to be inserted into any existing network segment without changing the IP addressing or routing of that segment2. The firewall inspects traffic between two interfaces that are configured as a pair, called a virtual wire. The firewall applies security policies to the traffic and forwards it to the same interface from which it was received2.

- D: Layer 2 mode allows the firewall to act as a switch that forwards traffic based on MAC addresses3.

The firewall inspects traffic between interfaces that are configured as Layer 2 interfaces and belong to the same VLAN. The firewall applies security policies to the traffic and forwards it to the appropriate interface based on the MAC address table3.

Verified References:

- 1: https://www.garlandtechnology.com/blog/whats-your-palo-alto-ngfw-deployment-plan
- 2: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/networking/configure-interfaces/virtual-wire
- 3: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/networking/configure-interfaces/layer-2.htm

NEW QUESTION 96

Which three items must be configured to implement application override? (Choose three)

A. Custom app
B. Security policy rule
C. Application override policy rule
D. Decryption policy rule
E. Application filter

Answer: ABC

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/policies/policies-application-override
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PPDrCAO

NEW QUESTION 99

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?

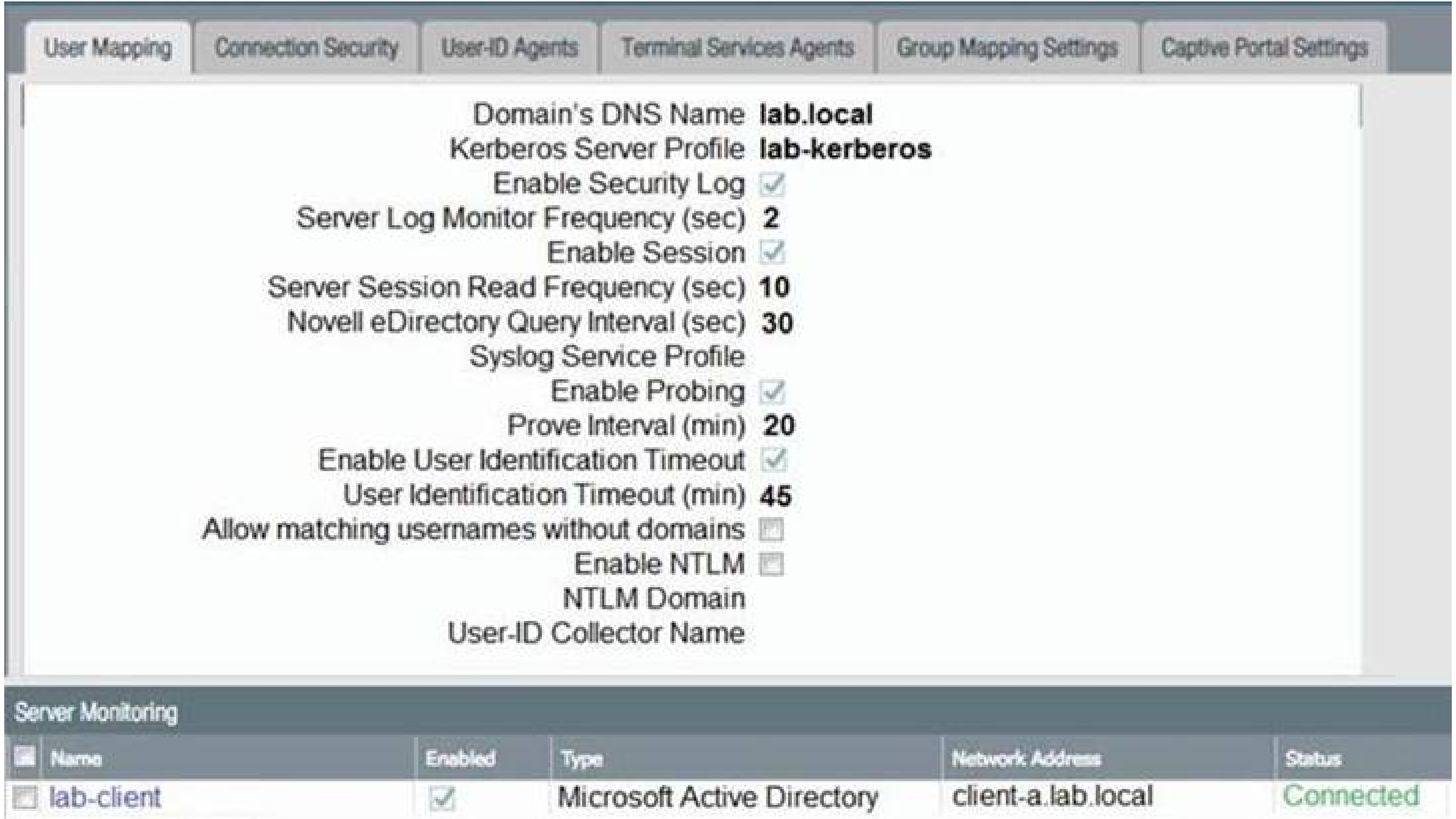
A. In the IKE Gateway configuration, verify that the IP address for each VPN peer is accurate
B. Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure
C. Check whether the VPN peer on one end is set up correctly using policy-based VPN
D. In the IPSec Crypto profile configuration, verify that PFS is either enabled on both VPN peers or disabled on both VPN peers.

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-me 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 103

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



Domain's DNS Name	lab.local
Kerberos Server Profile	lab-kerberos
Enable Security Log	☑
Server Log Monitor Frequency (sec)	2
Enable Session	☑
Server Session Read Frequency (sec)	10
Novell eDirectory Query Interval (sec)	30
Syslog Service Profile	
Enable Probing	☑
Prove Interval (min)	20
Enable User Identification Timeout	☑
User Identification Timeout (min)	45
Allow matching usernames without domains	☐
Enable NTLM	☐
NTLM Domain	
User-ID Collector Name	

Server Monitoring

☐	Name	Enabled	Type	Network Address	Status
☐	lab-client	☑	Microsoft Active Directory	client-a.lab.local	Connected

A. The User-ID agent is connected to a domain controller labeled lab-client
B. The host lab-client has been found by a domain controller
C. The host lab-client has been found by the User-ID agent.
D. The User-ID aaent is connected to the firewall labeled lab-client

Answer: A

NEW QUESTION 106
A network security administrator wants to inspect HTTPS traffic from users as it egresses through a firewall to the Internet/Untrust zone from trusted network zones.
The security admin wishes to ensure that if users are presented with invalid or untrusted security certificates, the user will see an untrusted certificate warning.
What is the best choice for an SSL Forward Untrust certificate?

A. A web server certificate signed by the organization's PKI
B. A self-signed certificate generated on the firewall
C. A subordinate Certificate Authority certificate signed by the organization's PKI
D. A web server certificate signed by an external Certificate Authority

Answer: B

Explanation:
- B is the best choice for an SSL Forward Untrust certificate because a self-signed certificate generated on the firewall is not trusted by any client browsers by default1. This means that if the firewall observes an invalid or untrusted security certificate from the server, it will present the self-signed certificate to the client, which will trigger an untrusted certificate warning2. This way, the security admin can ensure that users are aware of any potential risks when accessing HTTPS sites with untrusted certificates.
- A web server certificate signed by the organization’s PKI (A) or a subordinate Certificate Authority certificate signed by the organization’s PKI © are not good choices for an SSL Forward Untrust certificate because they are trusted by the client browsers that have the organization’s root CA installed1. This means that if the firewall observes an invalid or untrusted security certificate from the server, it will present the web server or subordinate CA certificate to the client, which will not trigger an untrusted certificate warning2. This way, the security admin cannot ensure that users are aware of any potential risks when accessing HTTPS sites with untrusted certificates.
- A web server certificate signed by an external Certificate Authority (D) is not a good choice for an SSL Forward Untrust certificate because it is trusted by most client browsers that have the external CA in
their trust store1. This means that if the firewall observes an invalid or untrusted security certificate from the server, it will present the web server certificate to the client, which will not trigger an untrusted certificate warning2. This way, the security admin cannot ensure that users are aware of any potential
risks when accessing HTTPS sites with untrusted certificates.

Verified References:
- 1: How to Configure SSL Decryption - Palo Alto Networks Knowledge Base
- 2: How to Implement and Test SSL Decryption - Palo Alto Networks Knowledge Base

NEW QUESTION 110
Phase two of a VPN will not establish a connection. The peer is using a policy-based VPN configuration. What part of the configuration should the engineer verify?

A. IKE Crypto Profile
B. Security policy
C. Proxy-IDs
D. PAN-OS versions

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClbXCAS https://live.paloaltonetworks.com/t5/general-topics/phase-2-tunnel-is-not-up/td-p/424789

NEW QUESTION 112
Which three external authentication services can the firewall use to authenticate admins into the Palo Alto Networks NGFW without creating administrator account on the firewall? (Choose three.)

A. RADIUS
B. TACACS+
C. Kerberos
D. LDAP
E. SAML

Answer: ABE

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administra

NEW QUESTION 116
Which operation will impact the performance of the management plane?

A. Decrypting SSL sessions
B. Generating a SaaS Application report
C. Enabling DoS protection
D. Enabling packet buffer protection

Answer: B

Explanation:
TIPS & TRICKS: REDUCING MANAGEMENT PLANE LOAD:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSvCAK TIPS & TRICKS: REDUCING MANAGEMENT PLANE LOAD—PART 2:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClU4CAK

NEW QUESTION 120

A company has recently migrated their branch office's PA-220S to a centralized Panorama. This Panorama manages a number of PA-7000 Series and PA-5200 Series devices All device group and template configuration is managed solely within Panorama
They notice that commit times have drastically increased for the PA-220S after the migration What can they do to reduce commit times?

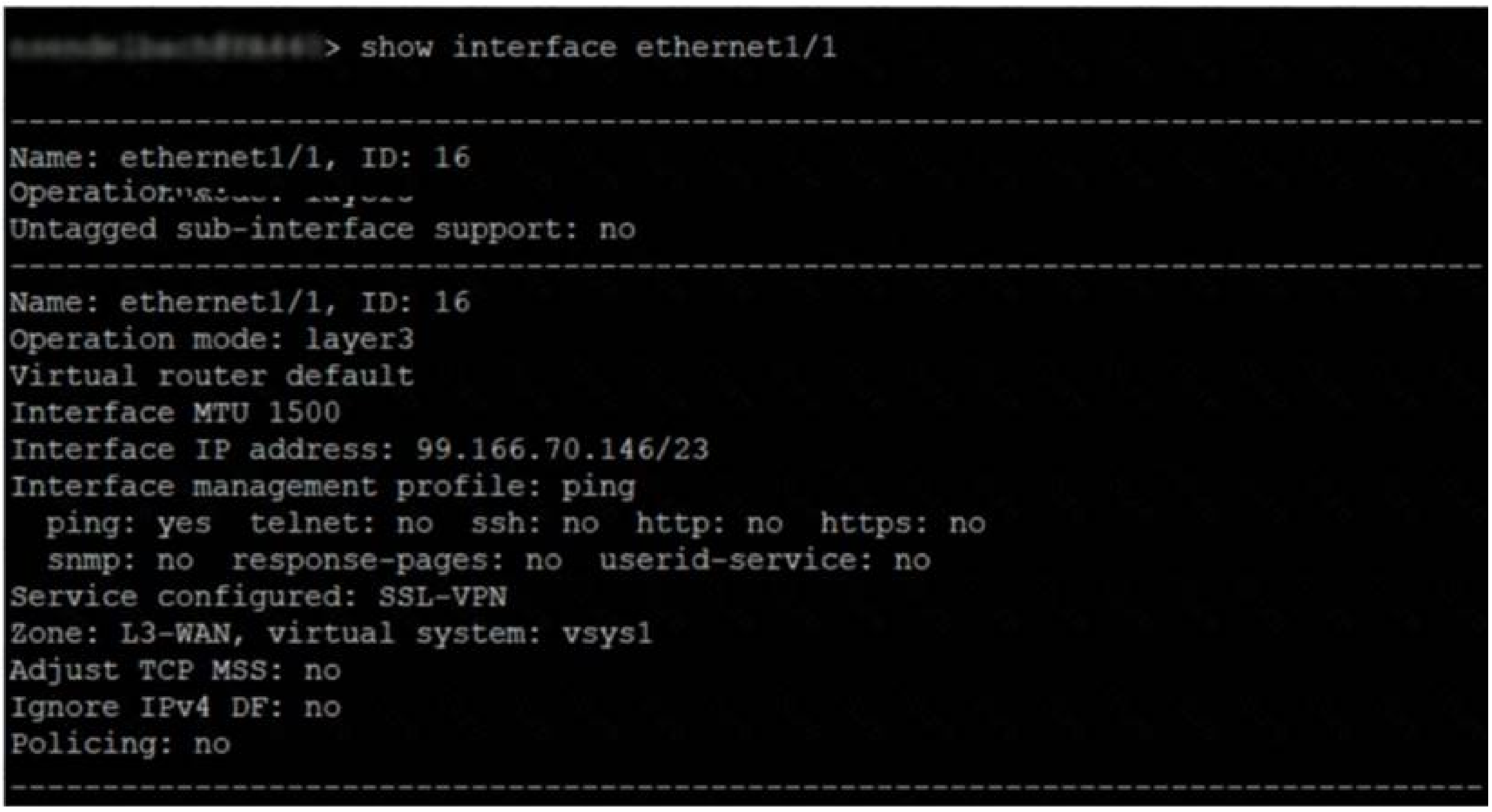
A. Disable "Share Unused Address and Service Objects with Devices" in Panorama Settings.
B. Update the apps and threat version using device-deployment
C. Perform a device group push using the "merge with device candidate config" option
D. Use "export or push device config bundle" to ensure that the firewall is integrated with the Panorama config.

Answer: A

Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-device-groups/man
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1CCAS

NEW QUESTION 125

After switching to a different WAN connection, users have reported that various websites will not load, and timeouts are occurring. The web servers work fine from other locations.
The firewall engineer discovers that some return traffic from these web servers is not reaching the users behind the firewall. The engineer later concludes that the maximum transmission unit (MTU) on an upstream router interface is set to 1400 bytes.
The engineer reviews the following CLI output for ethernet1/1.



```
[redacted] > show interface ethernet1/1

--------------------------------------------------------------------------------
Name: ethernet1/1, ID: 16
Operation mode: layer3
Untagged sub-interface support: no
--------------------------------------------------------------------------------
Name: ethernet1/1, ID: 16
Operation mode: layer3
Virtual router default
Interface MTU 1500
Interface IP address: 99.166.70.146/23
Interface management profile: ping
  ping: yes  telnet: no  ssh: no  http: no  https: no
  snmp: no  response-pages: no  userid-service: no
Service configured: SSL-VPN
Zone: L3-WAN, virtual system: vsys1
Adjust TCP MSS: no
Ignore IPv4 DF: no
Policing: no
--------------------------------------------------------------------------------
```

Which setting should be modified on ethernet1/1 to remedy this problem?

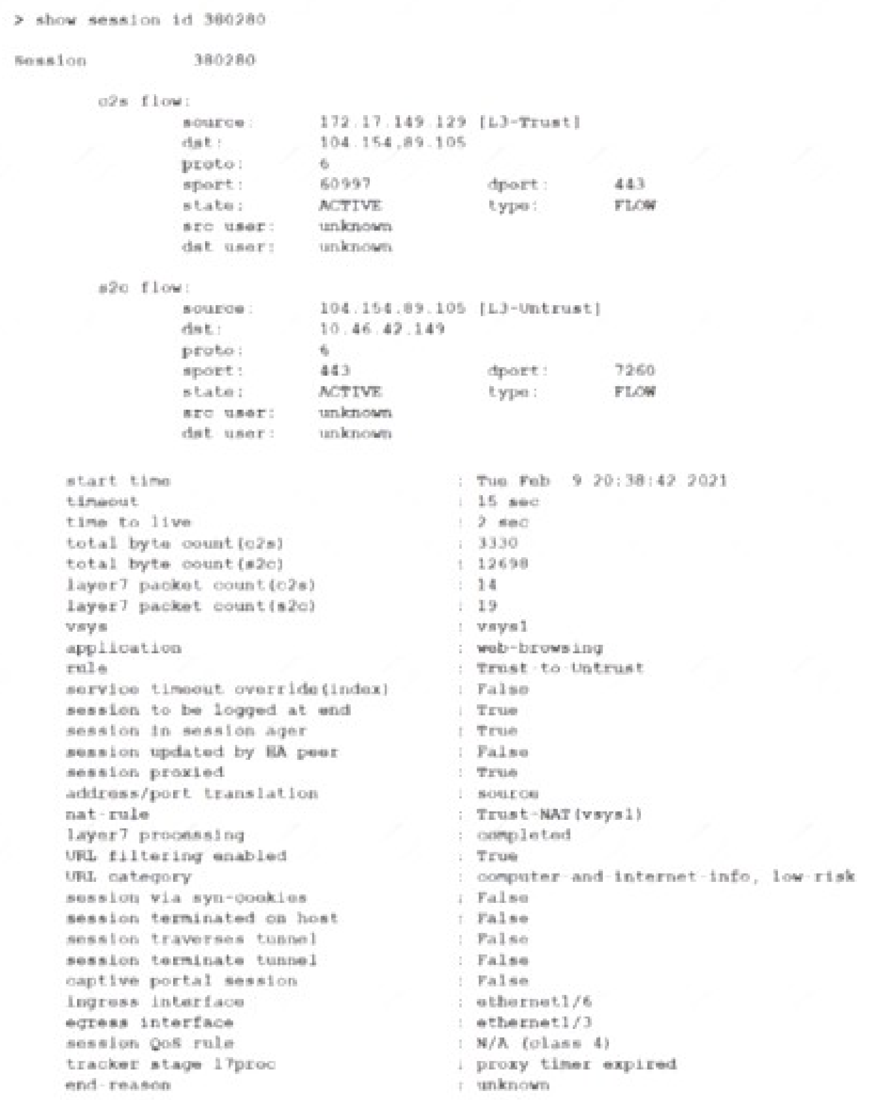
A. Lower the interface MTU value below 1500.
B. Enable the Ignore IPv4 Don't Fragment (DF) setting.
C. Change the subnet mask from /23 to /24.
D. Adjust the TCP maximum segment size (MSS) valu
E. *

Answer: D

Explanation:
The engineer should adjust the TCP maximum segment size (MSS) value on ethernet1/1 to remedy this problem. This is because the MTU on an upstream router interface is set to 1400 bytes, which is causing the return traffic from the web servers to not reach the users behind the firewall. By adjusting the TCP MSS value, the engineer can ensure that the return traffic is able to reach the users without any issues.
The TCP MSS is the maximum amount of data that can be transmitted in a single TCP segment, excluding the TCP and IP headers. The TCP MSS is usually derived from the MTU of the underlying network, which is the maximum packet size that can be transmitted without fragmentation. For example, if the MTU is 1500 bytes, which is the default value for ethernet interfaces, then the TCP MSS is 1460 bytes (1500 - 20 bytes for IP header - 20 bytes for TCP header). However, if there are intermediate devices or networks that have a lower MTU than the end-to-end path, then the TCP MSS may need to be adjusted accordingly to avoid packet loss or fragmentation1.
In this case, the firewall has an MTU of 1500 bytes on ethernet1/1, which is connected to a WAN link. However, an upstream router has an MTU of 1400 bytes on its interface, which means that any packet larger than 1400 bytes will be either dropped or fragmented by the router. This can cause problems for the return traffic from the web servers, which may have a TCP MSS of 1460 bytes or higher, depending on their MTU settings. If these packets have the Don't Fragment (DF) bit set in their IP header, which is common for TCP packets, then they will be dropped by the router and never reach the firewall or the users behind it. If they do not have the DF bit set, then they will be fragmented by the router and reassembled by the firewall, which can cause performance degradation and overhead2.
To avoid these problems, the engineer should adjust the TCP MSS value on ethernet1/1 to match or be lower than the MTU of the upstream router. This can be done by using the CLI command set network interface ethernet ethernet1/1 tcp-mss <value> , where <value> is an integer between 64 and 15003. For example, if the engineer sets the TCP MSS value to 1360 bytes (1400 - 20 - 20), then this will ensure that any TCP packet sent or received by ethernet1/1 will not exceed 1400 bytes in total size, and thus will not be dropped or fragmented by the router. This will allow the return traffic from the web servers to reach the users behind the firewall without any issues4.
References: TCP Maximum Segment Size (MSS), Configure Session Settings, TCP MSS Adjustments, PCNSE Study Guide (page 59)

NEW QUESTION 129

Which two statements correctly describe Session 380280? (Choose two.)



```
> show session id 380280

Session          380280

        c2s flow:
                source:      172.17.149.129 [L3-Trust]
                dst:         104.154.89.105
                proto:       6
                sport:       60997              dport:      443
                state:       ACTIVE             type:       FLOW
                src user:    unknown
                dst user:    unknown

        s2c flow:
                source:      104.154.89.105 [L3-Untrust]
                dst:         10.46.42.149
                proto:       6
                sport:       443                dport:      7260
                state:       ACTIVE             type:       FLOW
                src user:    unknown
                dst user:    unknown

     start time                            : Tue Feb  9 20:38:42 2021
     timeout                               : 15 sec
     time to live                          : 2 sec
     total byte count(c2s)                 : 3330
     total byte count(s2c)                 : 12698
     layer7 packet count(c2s)              : 14
     layer7 packet count(s2c)              : 19
     vsys                                  : vsys1
     application                           : web-browsing
     rule                                  : Trust-to-Untrust
     service timeout override(index)       : False
     session to be logged at end           : True
     session in session ager               : True
     session updated by HA peer            : False
     session proxied                       : True
     address/port translation              : source
     nat-rule                              : Trust-NAT(vsys1)
     layer7 processing                     : completed
     URL filtering enabled                 : True
     URL category                          : computer-and-internet-info, low-risk
     session via syn-cookies               : False
     session terminated on host            : False
     session traverses tunnel              : False
     session terminate tunnel              : False
     captive portal session                : False
     ingress interface                     : ethernet1/6
     egress interface                      : ethernet1/3
     session QoS rule                      : N/A (class 4)
     tracker stage l7proc                  : proxy timer expired
     end-reason                            : unknown
```

A. The session went through SSL decryption processing.
B. The session has ended with the end-reason unknown.
C. The application has been identified as web-browsing.
D. The session did not go through SSL decryption processing.

Answer: AC

NEW QUESTION 130

An administrator needs to identify which NAT policy is being used for internet traffic.
From the Monitor tab of the firewall GUI, how can the administrator identify which NAT policy is in use for a traffic flow?

A. Click Session Browser and review the session details.
B. Click Traffic view and review the information in the detailed log view.
C. Click Traffic view; ensure that the Source or Destination NAT columns are included and review the information in the detailed log view.
D. Click App Scope > Network Monitor and filter the report for NAT rules.

Answer: C

Explanation:

Traffic view in the Monitor tab of the firewall GUI can display the information about the NAT policy that is in use for a traffic flow, if the Source or Destination NAT columns are included and reviewed in the detailed log view1. The Source NAT column shows the translated source IP address and port, and the Destination NAT column shows the translated destination IP address and port2. These columns can help the administrator identify which NAT policy is applied to the traffic flow based on the pre-NAT and post-NAT addresses and ports.

NEW QUESTION 133

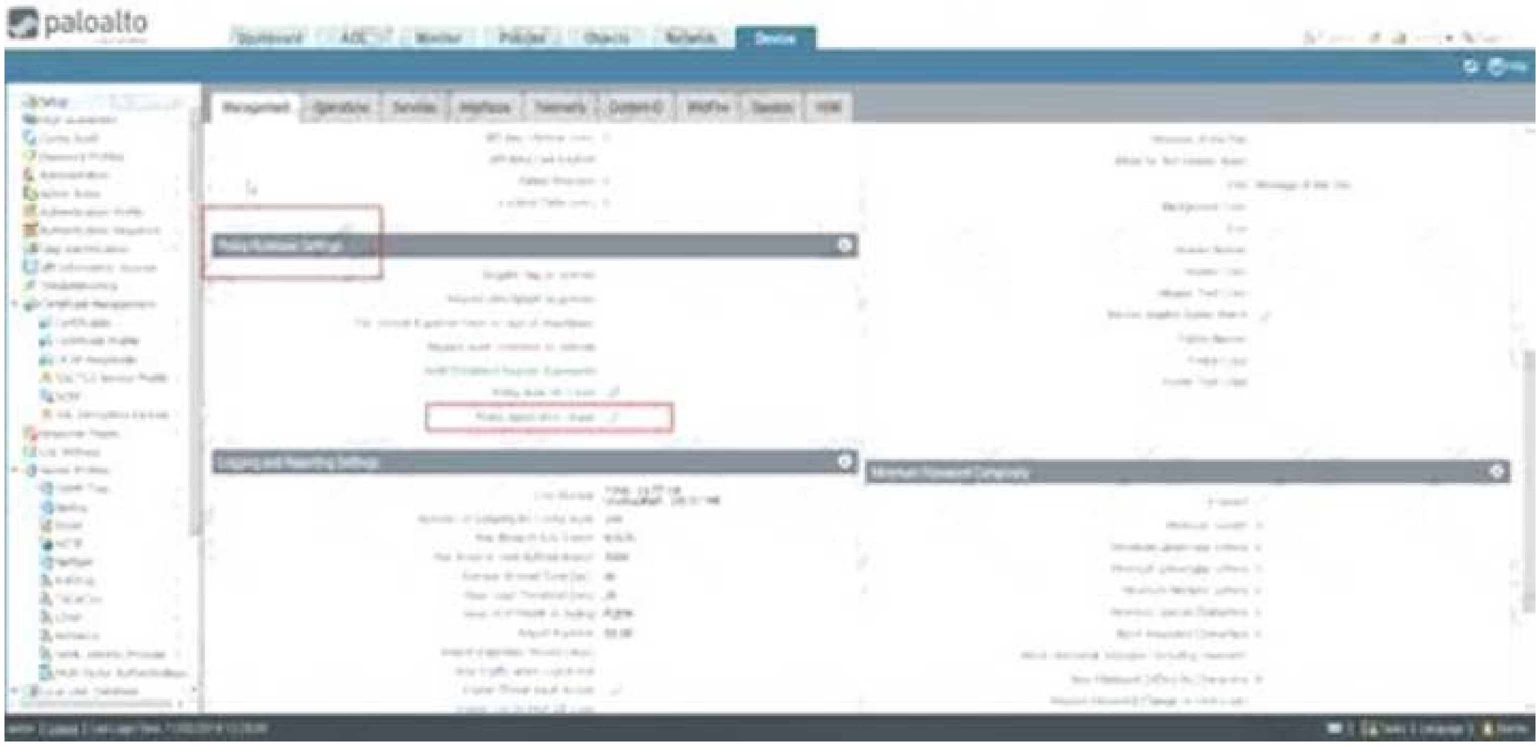
In the New App Viewer under Policy Optimizer, what does the compare option for a specific rule allow an administrator to compare?

A. The running configuration with the candidate configuration of the firewall
B. Applications configured in the rule with applications seen from traffic matching the same rule
C. Applications configured in the rule with their dependencies
D. The security rule with any other security rule selected

Answer: B

Explanation:

The compare option for a specific rule in the New App Viewer under Policy Optimizer allows an administrator to compare the applications configured in the rule with the applications seen from traffic matching the same rule. This helps the administrator to identify any new applications that are not explicitly defined in the rule, but are implicitly allowed by the firewall based on the dependencies of the configured applications. The compare option also shows the usage statistics and risk levels of the applications, and provides suggestions for optimizing the rule by adding, removing, or replacing applications12. References: New App Viewer (Policy Optimizer), PCNSE Study Guide (page 47)
Why use Security Policy Optimizer and what are the benefits?



NEW QUESTION 138
An administrator has been tasked with configuring decryption policies, Which decryption best practice should they consider?

A. Consider the local, legal, and regulatory implications and how they affect which traffic can be decrypted.
B. Decrypt all traffic that traverses the firewall so that it can be scanned for threats.
C. Place firewalls where administrators can opt to bypass the firewall when needed.
D. Create forward proxy decryption rules without Decryption profiles for unsanctioned applications.

Answer: A

Explanation:
The best decryption best practice that the administrator should consider is A: Consider the local, legal, and regulatory implications and how they affect which traffic can be decrypted. This is because decryption involves intercepting and inspecting encrypted traffic, which may raise privacy and compliance issues depending on the jurisdiction and the type of traffic1. Therefore, the administrator should be aware of the local, legal, and regulatory implications and how they affect which traffic can be decrypted, and follow the appropriate guidelines and policies to ensure that decryption is done in a lawful and ethical manner1.

NEW QUESTION 141
During the implementation of SSL Forward Proxy decryption, an administrator imports the company's Enterprise Root CA and Intermediate CA certificates onto the firewall. The company's Root and Intermediate CA certificates are also distributed to trusted devices using Group Policy and GlobalProtect. Additional device certificates and/or Subordinate certificates requiring an Enterprise CA chain of trust are signed by the company's Intermediate CA.
Which method should the administrator use when creating Forward Trust and Forward Untrust certificates on the firewall for use with decryption?

A. Generate a single subordinate CA certificate for both Forward Trust and Forward Untrust.
B. Generate a CA certificate for Forward Trust and a self-signed CA for Forward Untrust.
C. Generate a single self-signed CA certificate for Forward Trust and another for Forward Untrust
D. Generate two subordinate CA certificates, one for Forward Trust and one for Forward Untrust.

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy

NEW QUESTION 145
A firewall engineer reviews the PAN-OS GlobalProtect application and sees that it implicitly uses web-browsing and depends on SSL.
When creating a new rule, what is needed to allow the application to resolve dependencies?

A. Add SSL and web-browsing applications to the same rule.
B. Add web-browsing application to the same rule.
C. Add SSL application to the same rule.
D. SSL and web-browsing must both be explicitly allowed.

Answer: C

Explanation:
'Implicitly Uses' has web-browsing listed. This means that if you allow facebook-posting, that it will also be allowing the web-browsing application implicitly.. In our case, we dont know which APP the question referes too but 'Implicitly means already uses HTTP.

NEW QUESTION 149
An administrator is required to create an application-based Security policy rule to allow Evernote. The Evernote application implicitly uses SSL and web browsing. What is the minimum the administrator needs to configure in the Security rule to allow only Evernote?

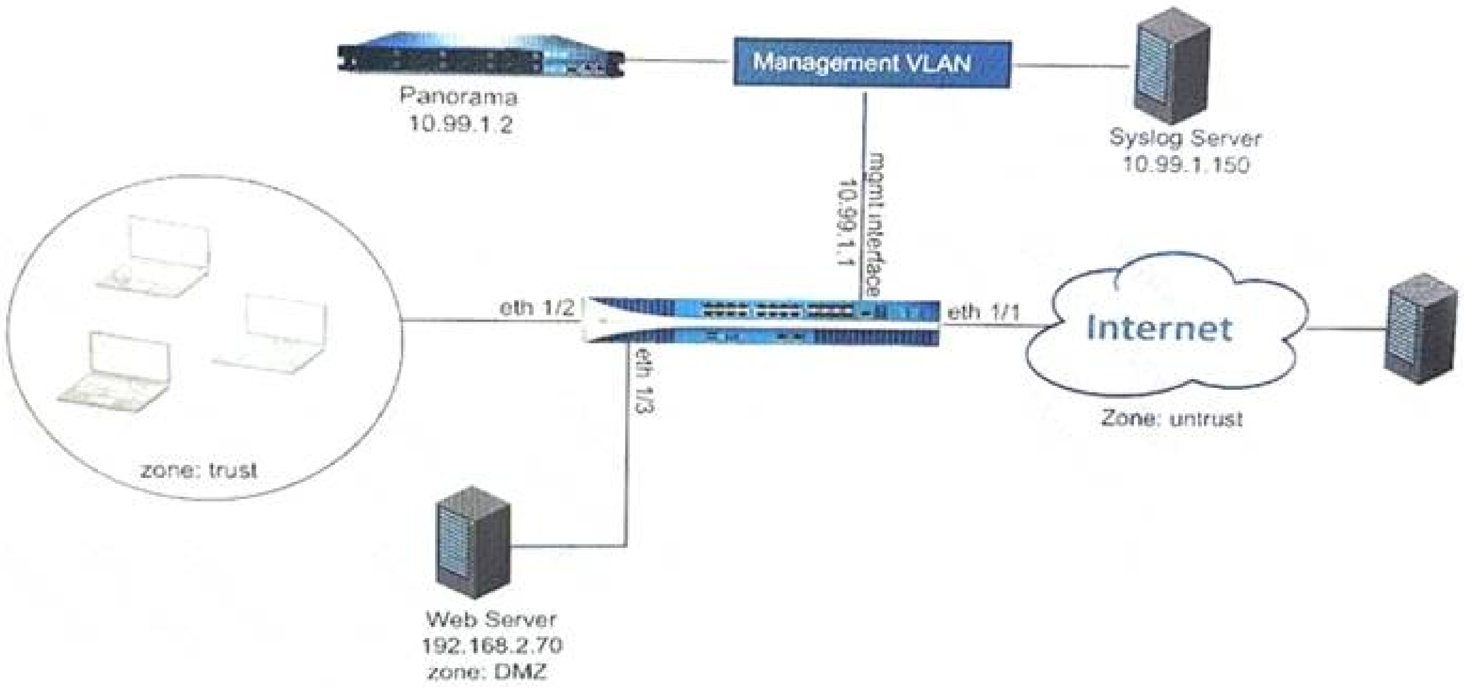
A. Add the Evernote application to the Security policy rule, then add a second Security policy rule containing both HTTP and SSL.
B. Create an Application Override using TCP ports 443 and 80.
C. Add the HTT
D. SS

E. and Evernote applications to the same Security policy.
F. Add only the Evernote application to the Security policy rule.

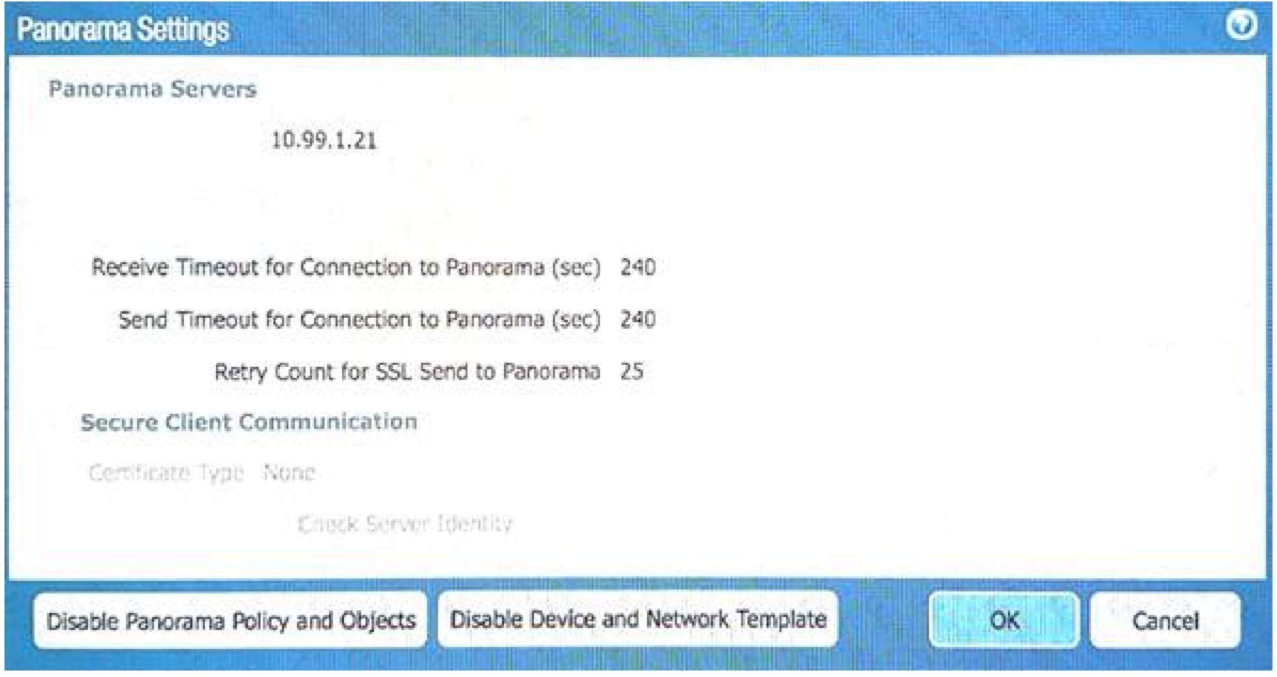
Answer: D

Explanation:
https://live.paloaltonetworks.com/t5/blogs/what-is-application-dependency/ba-p/344330
To create an application-based Security policy rule to allow Evernote, the administrator only needs to add the Evernote application to the Security policy rule. The Evernote application is a predefined App-ID that identifies the traffic generated by the Evernote client or web interface. The Evernote application implicitly uses SSL and web browsing as dependencies, which means that the firewall automatically allows these applications when the Evernote application is allowed. Therefore, there is no need to add HTTP, SSL, or web browsing applications to the same Security policy rule. Adding these applications would broaden the scope of the rule and potentially allow unwanted traffic12. References: App-ID Overview, Create a Security Policy Rule

NEW QUESTION 153
Refer to Exhibit:



An administrator can not see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall. Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?
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

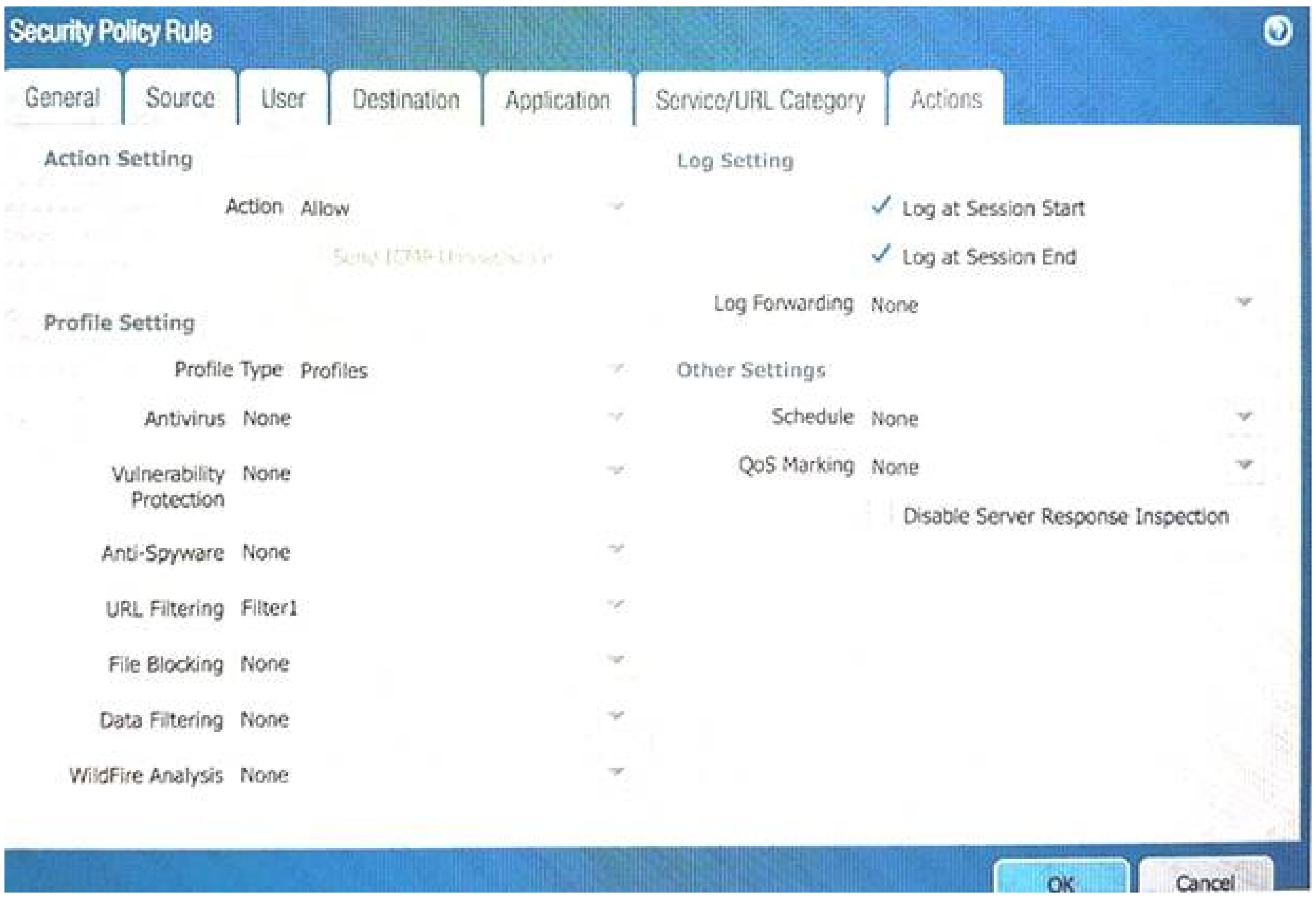
Secure Client Communication

Certificate Type None

Check Server Identity

Disable Panorama Policy and Objects
Disable Device and Network Template
OK
Cancel

B)



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

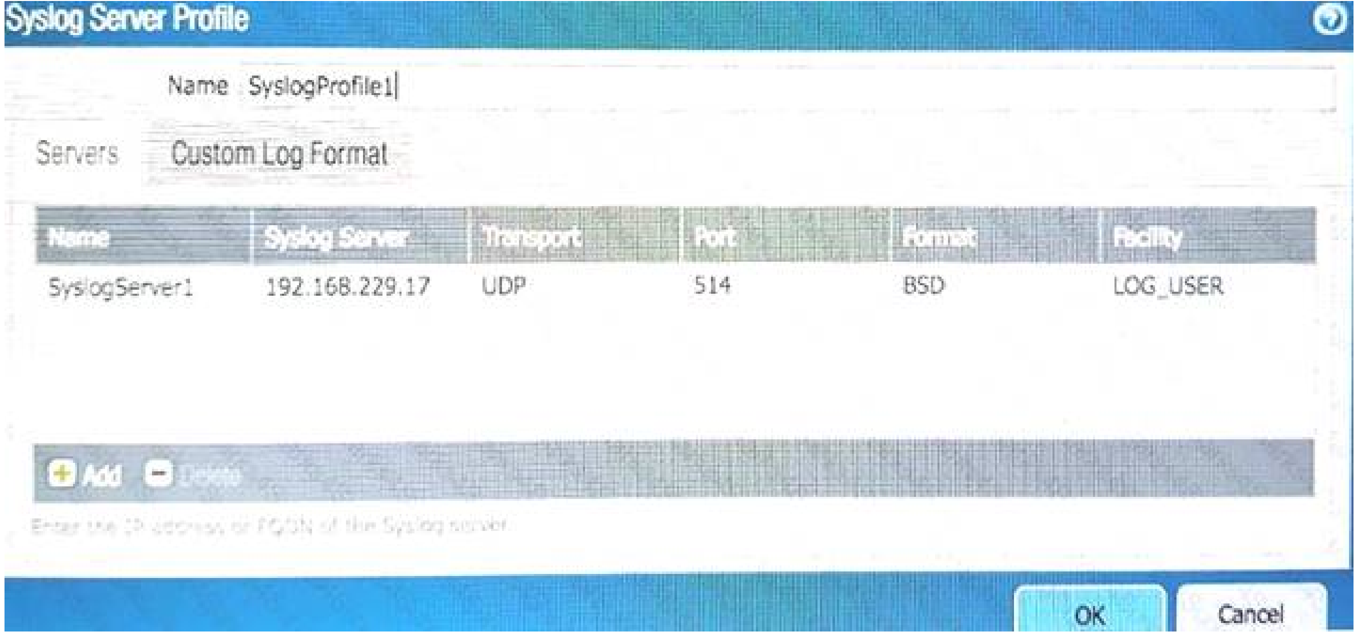
Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

C)

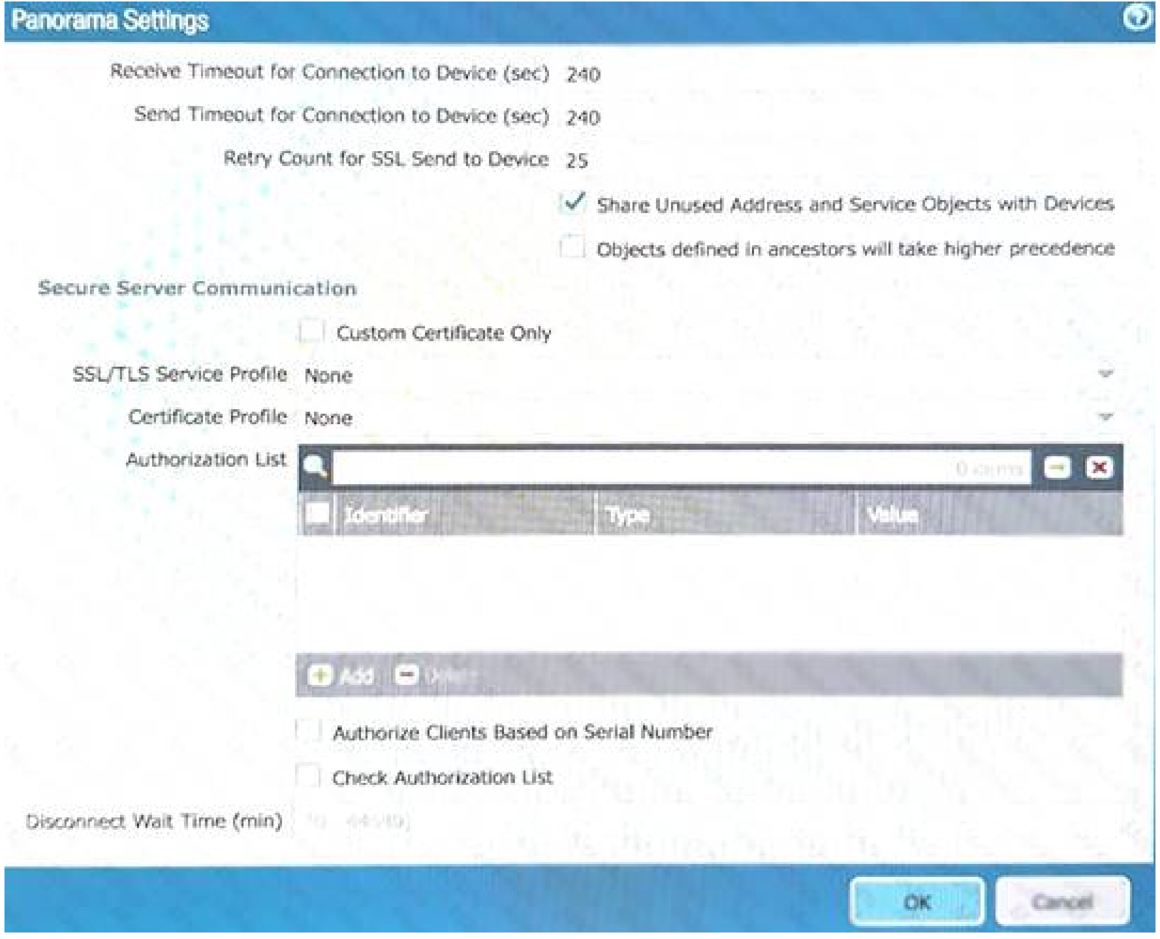


Name: SyslogProfile1

Name	Syslog Server	Transport	Port	Format	Facility
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server

D)



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

□ Authorize Clients Based on Serial Number

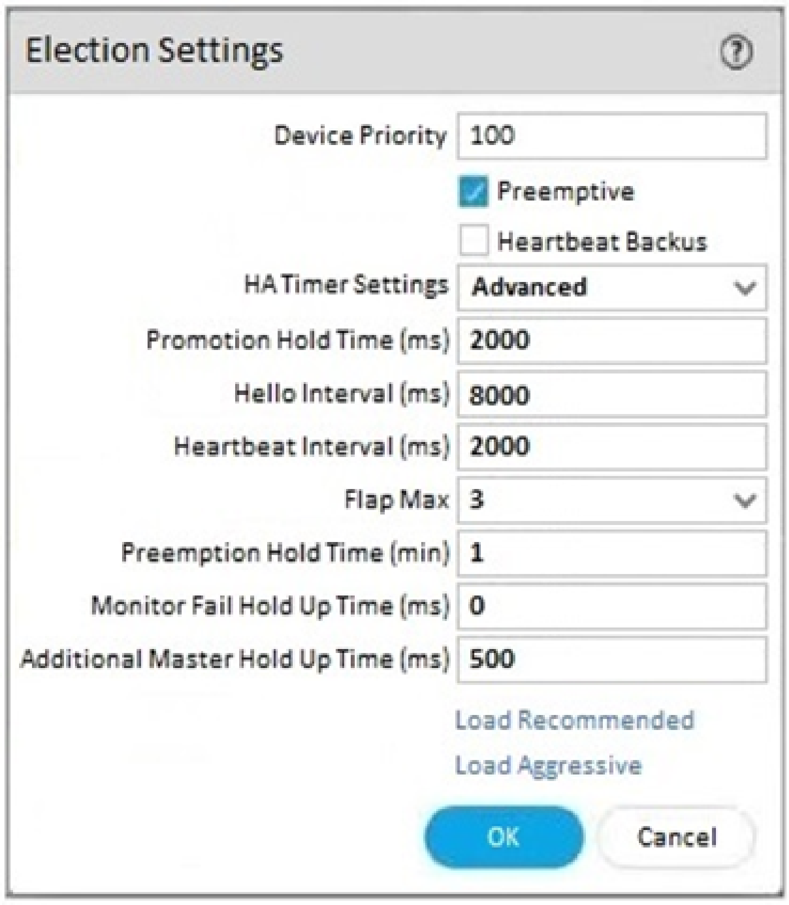
□ Check Authorization List

Disconnect Wait Time (min): [0 - 44640]

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

Answer: C

NEW QUESTION 156
An engineer reviews high availability (HA) settings to understand a recent HA failover event. Review the screenshot below.



Election Settings

Device Priority: 100
☑ Preemptive
□ Heartbeat Backus
HA Timer Settings: Advanced
Promotion Hold Time (ms): 2000
Hello Interval (ms): 8000
Heartbeat Interval (ms): 2000
Flap Max: 3
Preemption Hold Time (min): 1
Monitor Fail Hold Up Time (ms): 0
Additional Master Hold Up Time (ms): 500

Which timer determines the frequency at which the HA peers exchange messages in the form of an ICMP (ping)

A. Hello Interval
B. Promotion Hold Time
C. Heartbeat Interval
D. Monitor Fail Hold Up Time

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/ha-timers

NEW QUESTION 161
Which new PAN-OS 11.0 feature supports IPv6 traffic?

A. DHCPv6 Client with Prefix Delegation
B. OSPF
C. DHCP Server
D. IKEv1

Answer: A

Explanation:
https://docs.paloaltonetworks.com/compatibility-matrix/ipv6-support-by-feature/ipv6-support-by-feature-table

NEW QUESTION 164
Which statement is correct given the following message from the PanGPA log on the GlobalProtect app? Failed to connect to server at port:47 67

A. The PanGPS process failed to connect to the PanGPA process on port 4767
B. The GlobalProtect app failed to connect to the GlobalProtect Portal on port 4767
C. The PanGPA process failed to connect to the PanGPS process on port 4767
D. The GlobalProtect app failed to connect to the GlobalProtect Gateway on port 4767

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/kCSArticleDetail?id=kA10g000000PMiD

NEW QUESTION 169
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. A Decryption profile must be attached to the Decryption policy that the traffic matches.
B. A Decryption profile must be attached to the Security policy that the traffic matches.
C. There must be a certificate with only the Forward Trust option selected.
D. There must be a certificate with both the Forward Trust option and Forward Untrust option selected.

Answer: A

Explanation:
To use PAN-OS multi-factor authentication (MFA) to secure access to critical assets, the enterprise should configure a Captive Portal authentication policy that

uses an authentication sequence. An authentication sequence is a feature that allows the firewall to enforce multiple authentication methods (factors) for users who access sensitive services or applications. An authentication sequence can include up to four factors, such as login and password, Voice, SMS, Push, or One-time Password (OTP) authentication. The firewall can integrate with MFA vendors through RADIUS or vendor APIs to provide the additional factors12.
To configure an authentication sequence, the enterprise needs to create an authentication profile for each factor and then add them to the sequence in the desired order. The enterprise also needs to create a Captive Portal authentication policy that matches the traffic that requires MFA and applies the authentication sequence to it. The Captive Portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The Captive Portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button34.
When a user tries to access a service or application that matches the Captive Portal authentication policy, the firewall redirects the user to the Captive Portal web form for the first factor. After the user successfully authenticates for the first factor, the firewall prompts the user for the second factor through RADIUS or vendor API integration. The firewall repeats this process until all factors in the sequence are completed or until one factor fails. If all factors are completed successfully, the firewall allows the user to access the service or application. If one factor fails, the firewall denies access and logs an event56.
Configuring a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile is not sufficient to use PAN-OS MFA. This option only provides one factor of authentication through RADIUS integration with an MFA vendor. To use multiple factors of authentication, an authentication sequence is required.
Creating an authentication profile and assigning another authentication factor to be used by a Captive Portal authentication policy is not correct to use PAN-OS MFA. This option does not specify how to create or apply an authentication sequence, which is necessary for enforcing multiple factors of authentication.
Using a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns is not relevant to use PAN-OS MFA. This option is a feature of Palo Alto Networks Cortex XDR™ that helps
protect endpoints from credential theft by malicious actors. It does not provide any MFA functionality for accessing critical assets7.
References: Authentication Sequence, Configure Multi-Factor Authentication, Configure an Authenticatio Portal, Create an Authentication Profile, Create an Authentication Sequence, Create a Captive Portal Authentication Policy, Credential Phishing Agent

NEW QUESTION 173
......