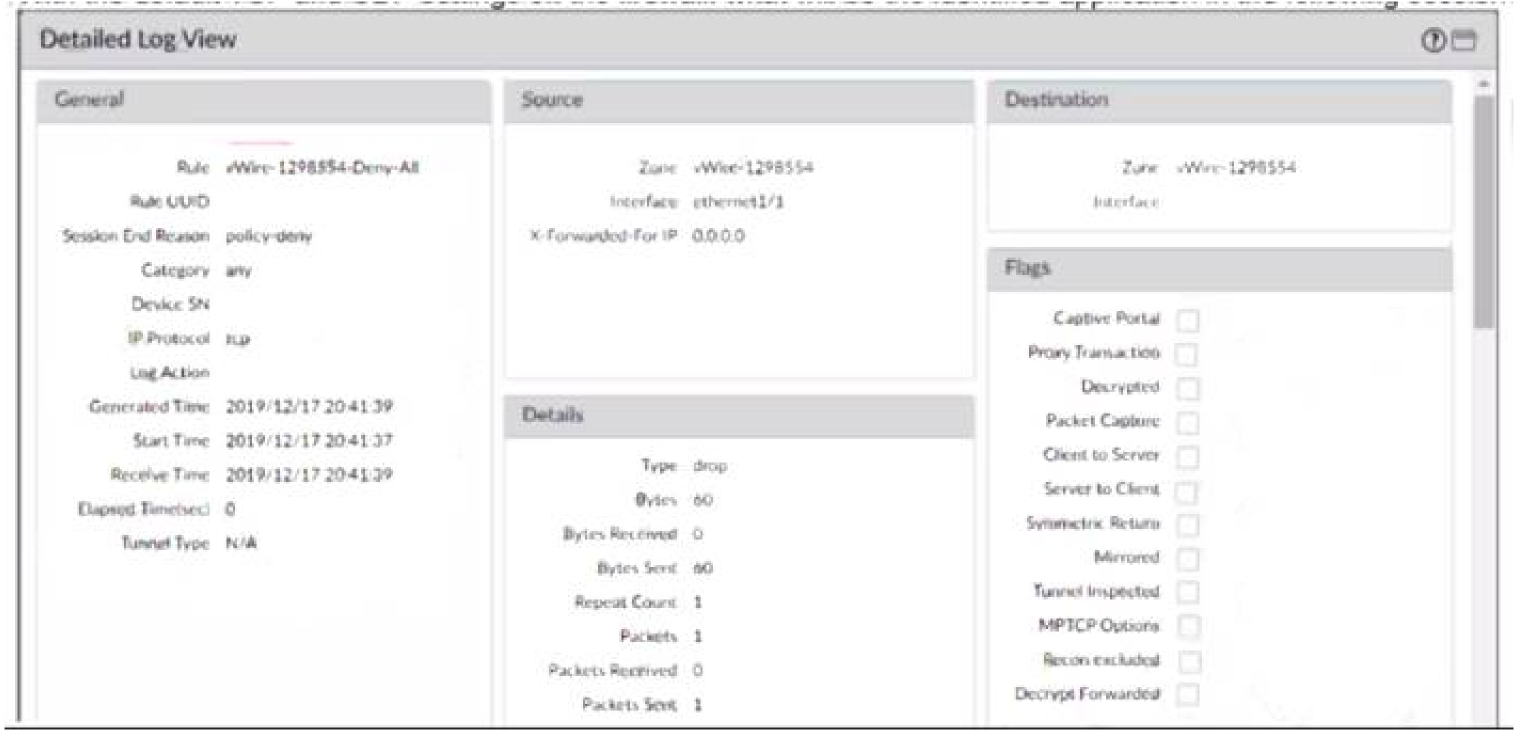
Paloalto-Networks

Exam Questions PCNSE

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

NEW QUESTION 1
With the default TCP and UDP settings on the firewall, what will be the identified application in the following session?



Detailed Log View

General

Rule vWire-1298554-Deny-All
Rule UUID
Session End Reason policy-deny
Category any
Device SN
IP Protocol tcp
Log Action
Generated Time 2019/12/17 20:41:39
Start Time 2019/12/17 20:41:37
Receive Time 2019/12/17 20:41:39
Elapsed Time(sec) 0
Tunnel Type N/A

Source

Zone vWire-1298554
Interface ethernet1/1
X-Forwarded-For IP 0.0.0.0

Details

Type drop
Bytes 60
Bytes Received 0
Bytes Sent 60
Repeat Count 1
Packets 1
Packets Received 0
Packets Sent 1

Destination

Zone vWire-1298554
Interface

Flags

Captive Portal □
Proxy Transaction □
Decrypted □
Packet Capture □
Client to Server □
Server to Client □
Symmetric Return □
Mirrored □
Tunnel Inspected □
MPTCP Options □
Recon excluded □
Decrypt Forwarded □

A. Incomplete
B. unknown-tcp
C. Insufficient-data
D. not-applicable

Answer: D

Explanation:
Traffic didnt match any other policies and so landed at the implicit "deny all" policy. If it's deny all, the traffic was dropped before the application could be determined. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

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
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 to the target device group and apply a master device to the device group.
B. Reference the targeted device's templates in the target device group.
C. Clone the security policy and add it to the other device groups.
D. Add the policy in the shared device group as a pre-rule

Answer: D

Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-device-groups/man
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-conf

NEW QUESTION 4
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 5
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 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 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 8
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 9
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 10
Which GloDalProtecl gateway setting is required to enable split-tunneting by access route, destination domain and application?

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

Answer: A

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

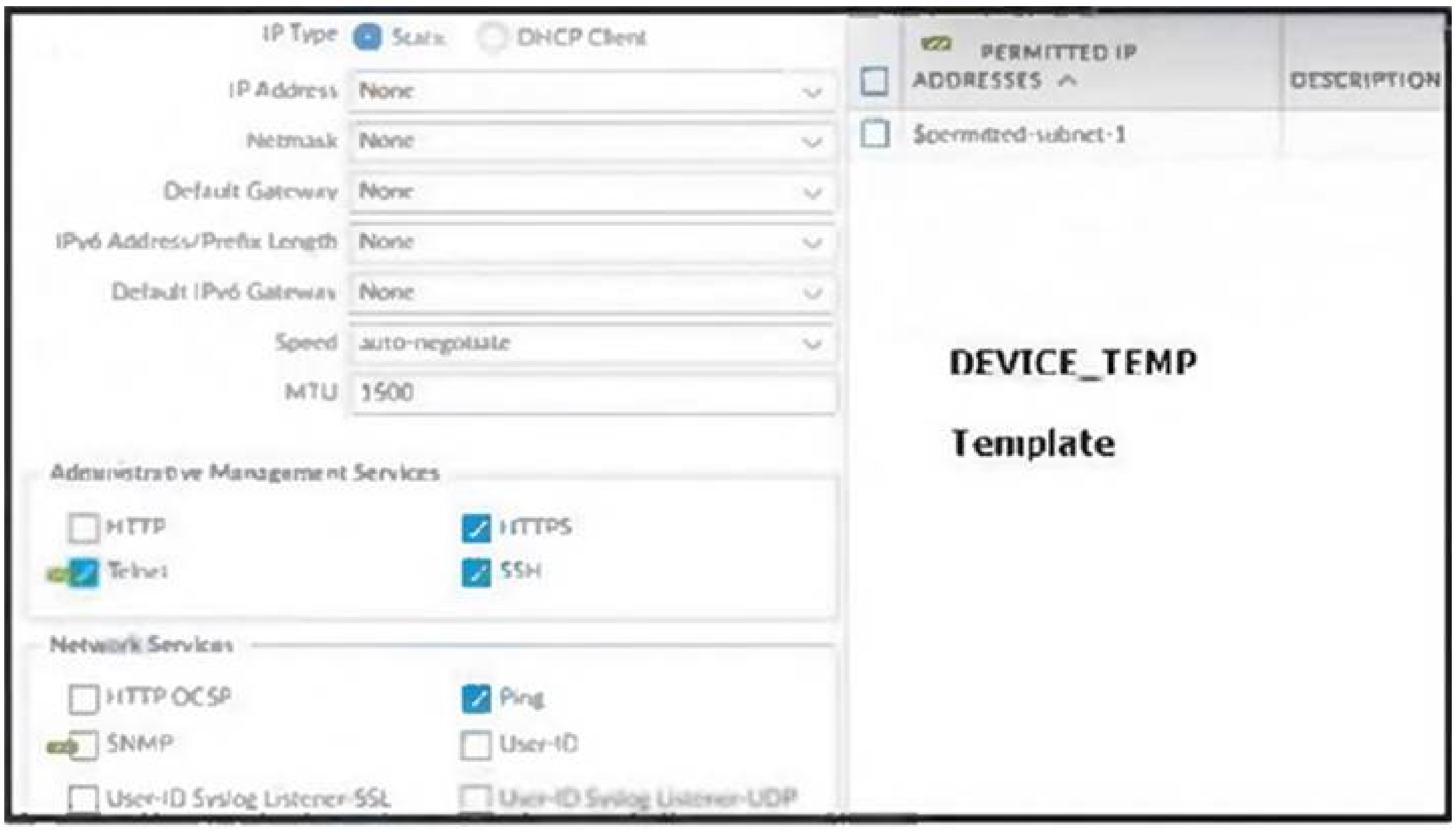
NEW QUESTION 10
An organization is interested in migrating from their existing web proxy architecture to the Web Proxy feature of their PAN-OS 11.0 firewalls. Currently. HTTP and SSL requests contain the c IP address of the web server and the client browser is redirected to the proxy
Which PAN-OS proxy method should be configured to maintain this type of traffic flow?

A. DNS proxy
B. Explicit proxy
C. SSL forward proxy
D. Transparent proxy

Answer: D

Explanation:
For the transparent proxy method, the request contains the destination IP address of the web server and the proxy transparently intercepts the client request (either by being in-line or by traffic steering). There is no client configuration and Panorama is optional. Transparent proxy requires a loopback interface, User-ID configuration in the proxy zone, and specific Destination NAT (DNAT) rules. Transparent proxy does not support X-Authenticated Users (XAU) or Web Cache Communications Protocol (WCCP). https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy

NEW QUESTION 14
Based on the screenshots above, and with no configuration inside the Template Stack itself, what access will the device permit on its Management port?



IP Type ● Static ○ DHCP Client

IP Address: None

Netmask: None

Default Gateway: None

IPv6 Address/Prefix Length: None

Default IPv6 Gateway: None

Speed: auto-negotiate

MTU: 1500

Administrative Management Services

□ HTTP ☑ HTTPS

☑ Telnet ☑ SSH

Network Services

□ HTTP OCSP ☑ Ping

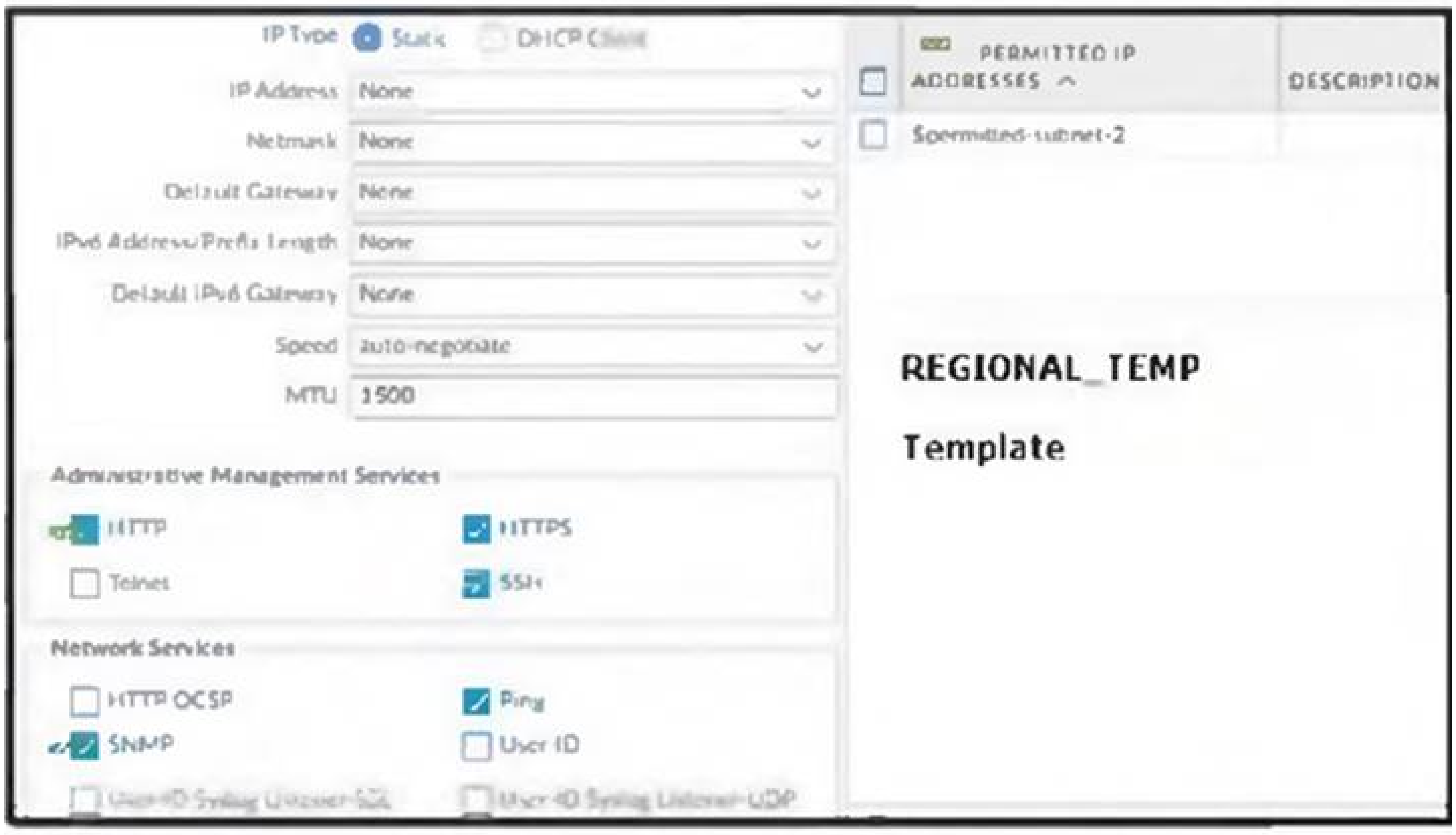
□ SNMP □ User-ID

□ User-ID Syslog Listener-SSL □ User-ID Syslog Listener-UDP

□	PERMITTED IP ADDRESSES	DESCRIPTION
□	$permitted-subnet-1	

DEVICE_TEMP

Template



IP Type ● Static ○ DHCP Client

IP Address: None

Netmask: None

Default Gateway: None

IPv6 Address/Prefix Length: None

Default IPv6 Gateway: None

Speed: auto-negotiate

MTU: 1500

Administrative Management Services

☑ HTTP ☑ HTTPS

□ Telnet ☑ SSH

Network Services

□ HTTP OCSP ☑ Ping

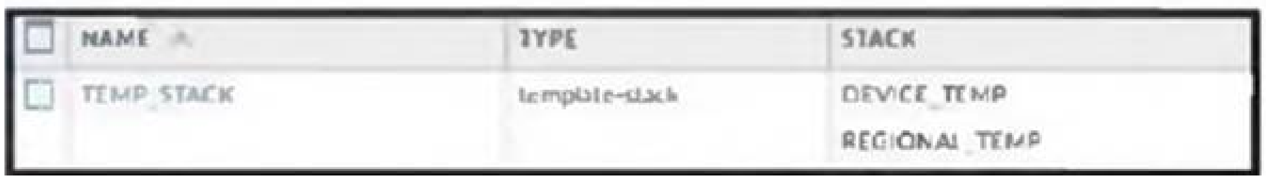
☑ SNMP □ User ID

□ User-ID Syslog Listener-SSL □ User-ID Syslog Listener-UDP

□	PERMITTED IP ADDRESSES	DESCRIPTION
□	$permitted-subnet-2	

REGIONAL_TEMP

Template



□	NAME	TYPE	STACK
□	TEMP_STACK	template-stack	DEVICE_TEMP REGIONAL_TEMP

A. The firewall will allow HTTP Telnet, HTTPS, SSH, and Ping from IP addresses defined as$permitted-subnet-1.
B. The firewall will allow HTTP Telnet, HTTPS, SSH, and Ping from IP addresses defined as$permitted-subnet-2.
C. The firewall will allow HTTP, Telnet, SNMP, HTTPS, SSH and Ping from IP addresses defined as$permitted-subnet-1 and $permitted-subnet-2.
D. The firewall will allow HTTP, Telnet, HTTPS, SSH, and Ping from IP addresses defined as$permitted-subnet-1 and $permitted-subnet-2.

Answer: A

Explanation:
https://live.paloaltonetworks.com/t5/panorama-discussions/panorama-force-template-value-option/td-p/496620 "- Force Template Value will as the name suggest remove any local configuratio and apply the value define the panorama template. But this is valid only for overlapping configuration" "You need to be careful, what is actually defined in the template. For example - if you decide to enable HA in the template, but after that you decide to not push it with template and just disable it again (remove the check from the "Enable HA" checkbox). This still will be part of the template, because now your template is explicitely defining HA disabled. If you made a change in the template, and later decide that you don't want to control this setting with template, you need to revert the config by clicking the green bar next to the changed value"

NEW QUESTION 16
A network administrator wants to deploy SSL Forward Proxy decryption. What two attributes should a forward trust certificate have? (Choose two.)

A. A subject alternative name
B. A private key
C. A server certificate
D. A certificate authority (CA) certificate

Answer: BD

Explanation:
The two attributes that a forward trust certificate should have for SSL Forward Proxy decryption are:

- B: A private key. This is the key that the firewall uses to sign the certificates that it generates for the decrypted sessions. The private key must be securely stored on the firewall and not shared with anyone1.
- D: A certificate authority (CA) certificate. This is the certificate that the firewall uses to issue the certificates for the decrypted sessions. The CA certificate must be trusted by the client browsers and devices that receive the certificates from the firewall1.

NEW QUESTION 21
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

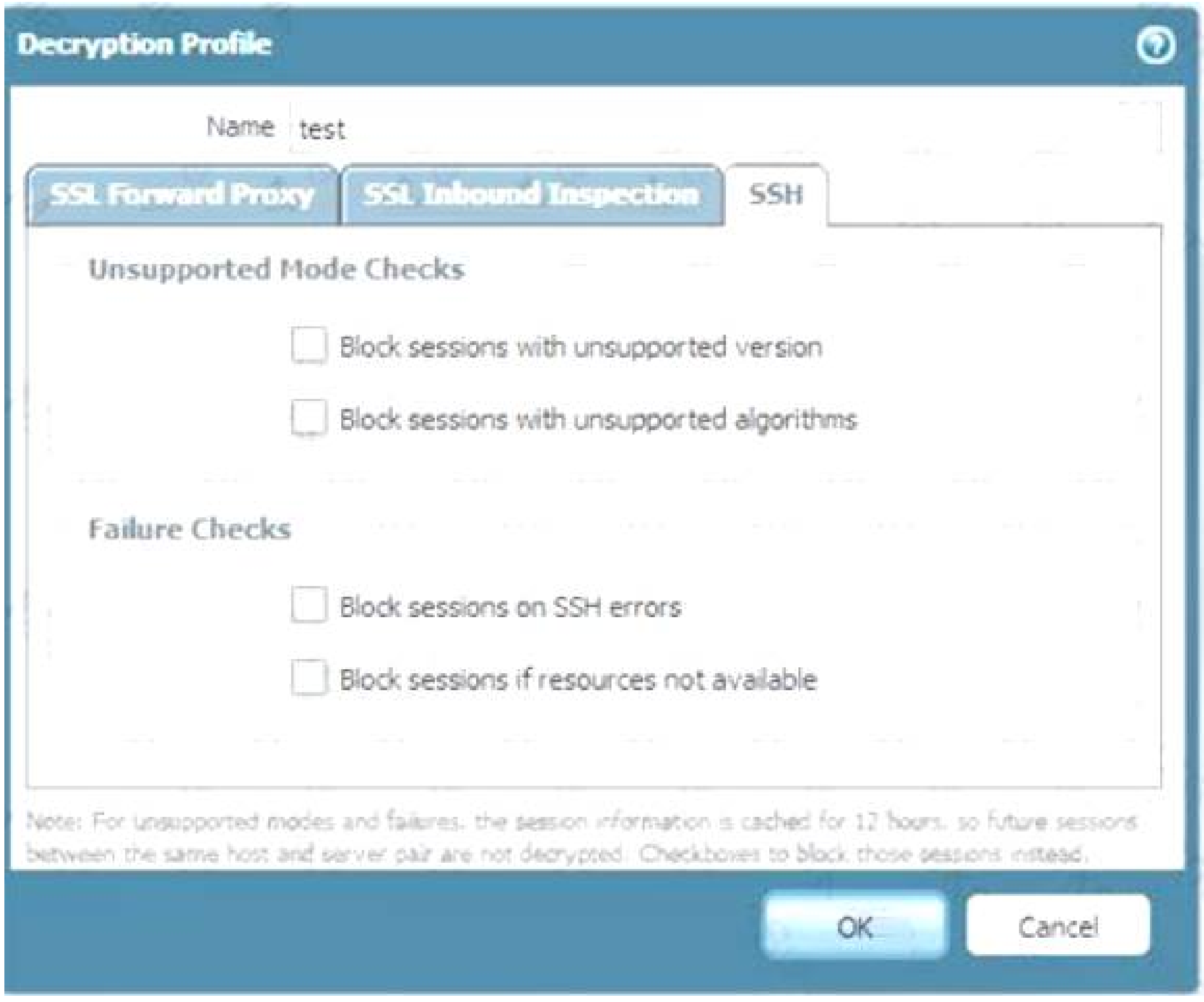
Explanation:
The firewalls exchange hello messages and heartbeats at configurable intervals to verify that the peer firewall is responsive and operational. Hello messages are sent from one peer to the other to verify the state of the firewall. The heartbeat is an ICMP ping to the HA peer. A response 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 23
An organization wants to begin decrypting guest and BYOD traffic.
Which NGFW feature can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted?

A. Authentication Portal
B. SSL Decryption profile
C. SSL decryption policy
D. comfort pages

Answer: A

Explanation:
An authentication portal is a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An authentication portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The authentication portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button. The authentication portal can also be configured to use different authentication methods, such as local database, RADIUS, LDAP, Kerberos, or SAML1. By using an authentication portal, the firewall can redirect BYOD users to a web page where they can learn about the decryption policy, download and install the CA certificate, and agree to the terms of use before accessing the network or the internet2.
An SSL decryption profile is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption profile is a set of options that define how the firewall handles SSL/TLS traffic that it decrypts. An SSL decryption profile can include settings such as certificate verification, unsupported protocol handling, session caching, session resumption, algorithm selection, etc3. An SSL decryption profile does not provide any user identification or notification functions.
An SSL decryption policy is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption policy is a set of rules that determine which traffic the firewall decrypts based on various criteria, such as source and destination zones, addresses, users, applications, services, etc. An SSL decryption policy can also specify which type of decryption to apply to the traffic, such as SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy4. An SSL decryption policy does not provide any user identification or notification functions.
Comfort pages are not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. Comfort pages are web pages that the firewall displays to users when it blocks or fails to decrypt certain traffic due to security policy or technical reasons. Comfort pages can include information such as the reason for blocking or failing to decrypt the traffic, the URL of the original site, the firewall serial number, etc5. Comfort pages do not provide any user identification or notification functions before decrypting the traffic.
References: Configure an Authentication Portal, Redirect Users Through an Authentication Portal, SSL Decryption Profile, Decryption Policy, Comfort Pages How to Implement SSH Decryption on a Palo Alto Networks Device



Name test

Unsupported Mode Checks

□ Block sessions with unsupported version

□ Block sessions with unsupported algorithms

Failure Checks

□ Block sessions on SSH errors

□ Block sessions if resources not available

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Checkboxes to block those sessions instead.

NEW QUESTION 28
Which two profiles should be configured when sharing tags from threat logs with a remote User-ID agent? (Choose two.)

A. Log Ingestion
B. HTTP
C. Log Forwarding
D. LDAP

Answer: BC

Explanation:
>Threat logs, create a log forwarding profile to define how you want the firewall or Panorama to handle logs.
>Configure an HTTP server profile to forward logs to a remote User-ID agent. > Select the log forwarding profile you created then select this server profile as the HTTP server profile https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/use-auto-tagging-to-automate-security-actio

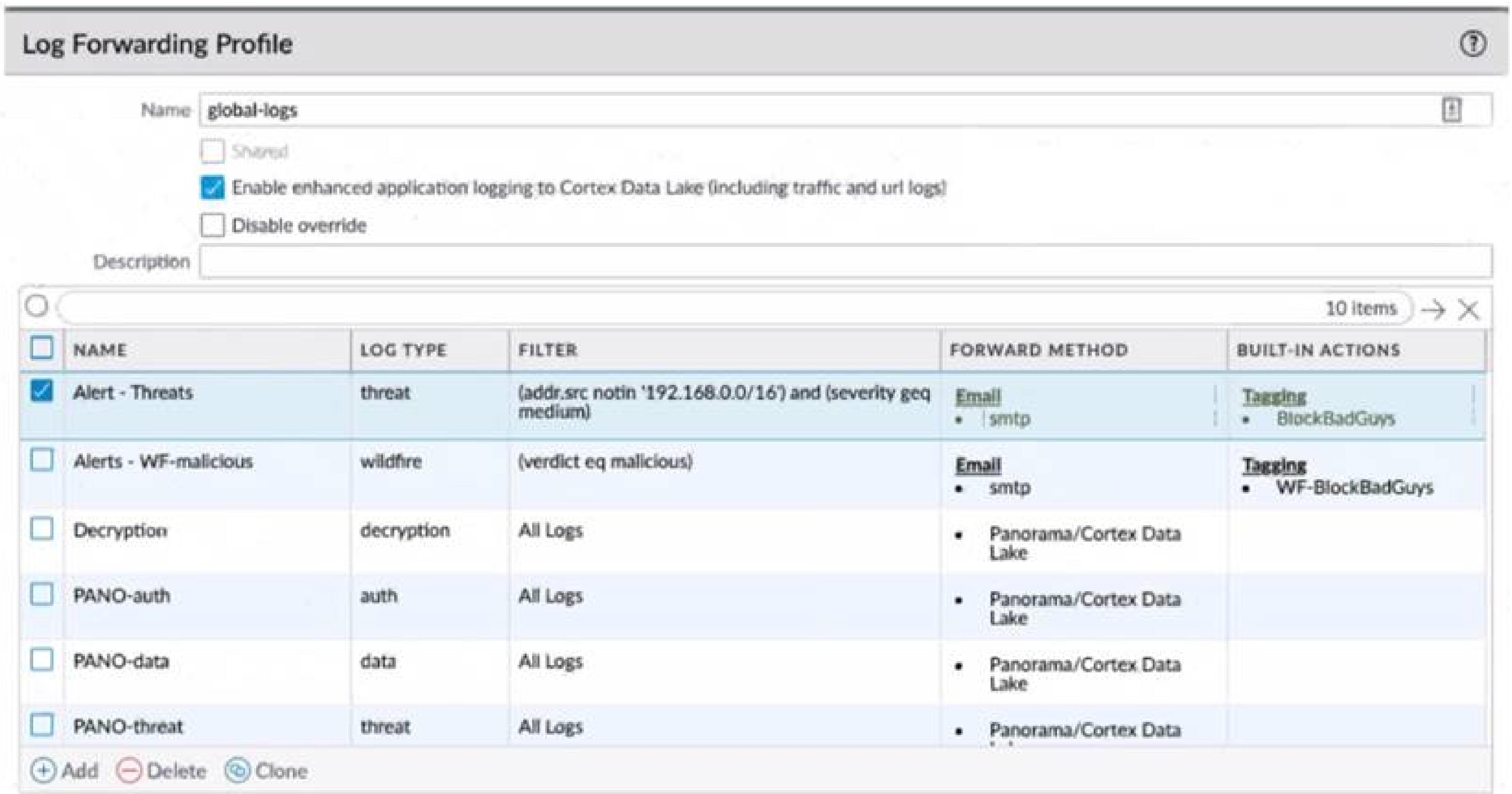
NEW QUESTION 31
An administrator configures a site-to-site IPsec VPN tunnel between a PA-850 and an external customer on their policy-based VPN devices.
What should an administrator configure to route interesting traffic through the VPN tunnel?

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 35
Review the images.



Log Forwarding Profile

Name: global-logs

□ Shared

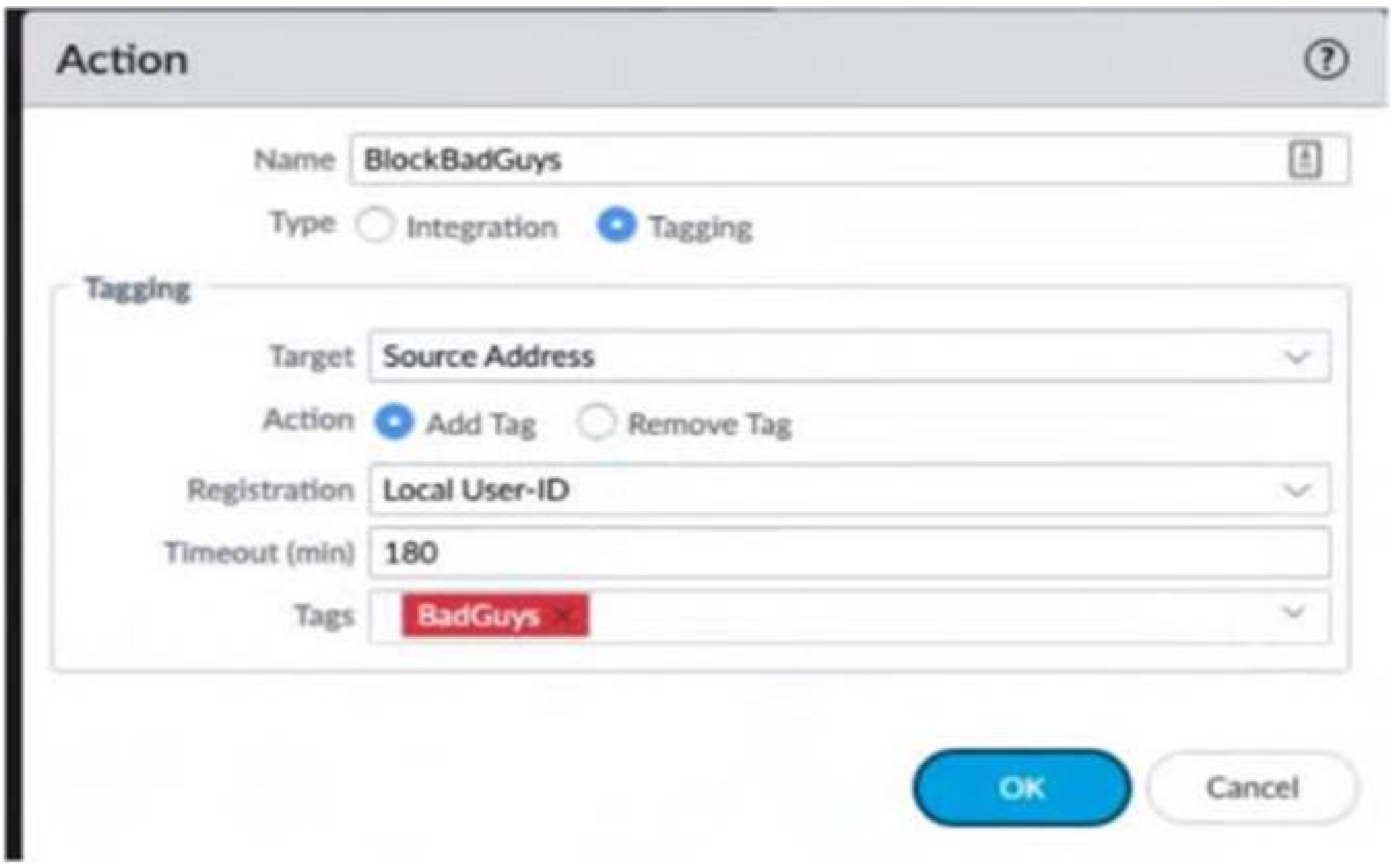
☑ Enable enhanced application logging to Cortex Data Lake (including traffic and url logs)

□ 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

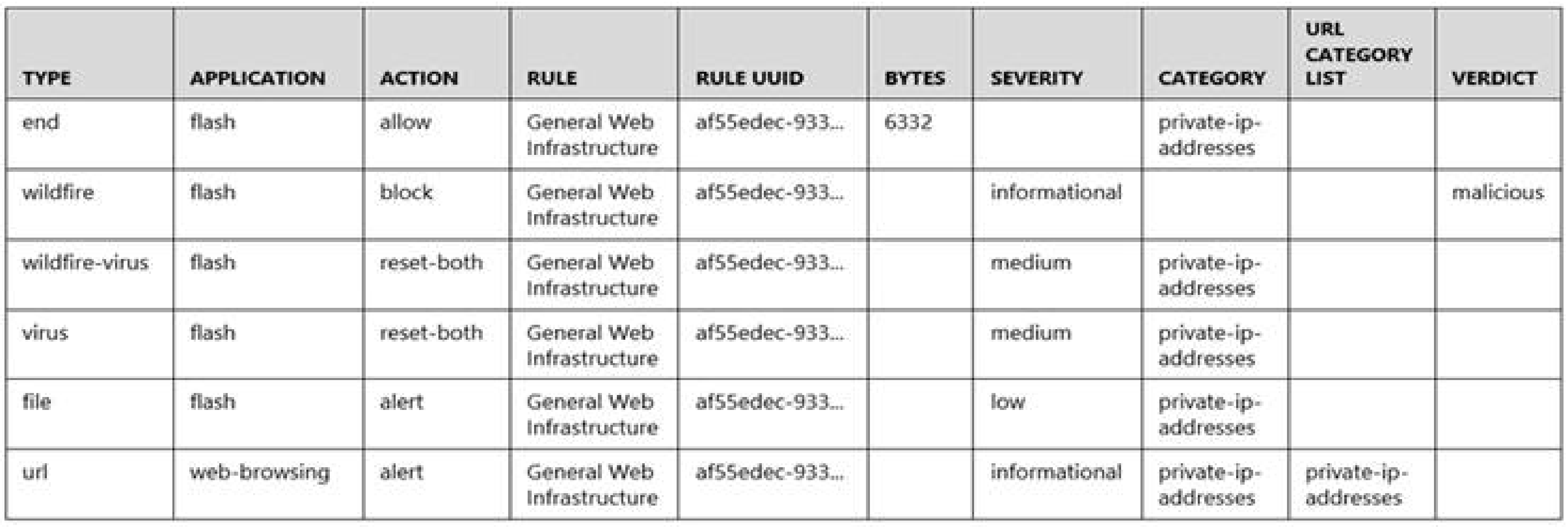
Tags: BadGuys

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 36
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 38
Which three options does Panorama offer for deploying dynamic updates to its managed devices? (Choose three.)

A. Check dependencies
B. Schedules
C. Verify
D. Revert content
E. Install

Answer: BDE

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-de https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-de

NEW QUESTION 40
A network security administrator has an environment with multiple forms of authentication. There is a network access control system in place that authenticates and restricts access for wireless users, multiple Windows domain controllers, and an MDM solution for company-provided smartphones. All of these devices have their authentication events logged.
Given the information, what is the best choice for deploying User-ID to ensure maximum coverage?

A. Captive portal
B. Standalone User-ID agent
C. Syslog listener
D. Agentless User-ID with redistribution

Answer: C

Explanation:
A syslog listener is the best choice for deploying User-ID to ensure maximum coverage in an environment with multiple forms of authentication. A syslog listener is a feature that enables the firewall or Panorama to receive syslog messages from other systems and parse them for IP address-to-username mappings. A syslog listener can collect user mapping information from a variety of sources, such as network access control systems, domain controllers, MDM solutions, VPN gateways, wireless controllers, proxies, and more2. A syslog listener can also support multiple platforms and operating systems, such as Windows, Linux, macOS, iOS, Android, etc3. Therefore, a syslog listener can provide a comprehensive and flexible solution for User-ID deployment in a large-scale network. References: Configure a Syslog Listener for User Mapping, User-ID Agent Deployment Guide, PCNSE Study Guide (page 48)

NEW QUESTION 44
A network administrator configured a site-to-site VPN tunnel where the peer device will act as initiator None of the peer addresses are known
What can the administrator configure to establish the VPN connection?

A. Set up certificate authentication.
B. Use the Dynamic IP address type.
C. Enable Passive Mode
D. Configure the peer address as an FQDN.

Answer: B

Explanation:
When the peer device will act as the initiator and none of the peer addresses are known, the administrator can enable Passive Mode to establish the VPN connection. Passive Mode tells the firewall to wait for the peer device to initiate the VPN connection. The other options are incorrect. Option A, setting up certificate authentication, would require the administrator to know the peer device's certificate. Option C, using the Dynamic IP address type, would require the administrator to know the peer device's dynamic IP address.
Option D, configuring the peer address as an FQDN, would require the administrator to know the peer device's fully qualified domain name.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClIGCA0

NEW QUESTION 47
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 49
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

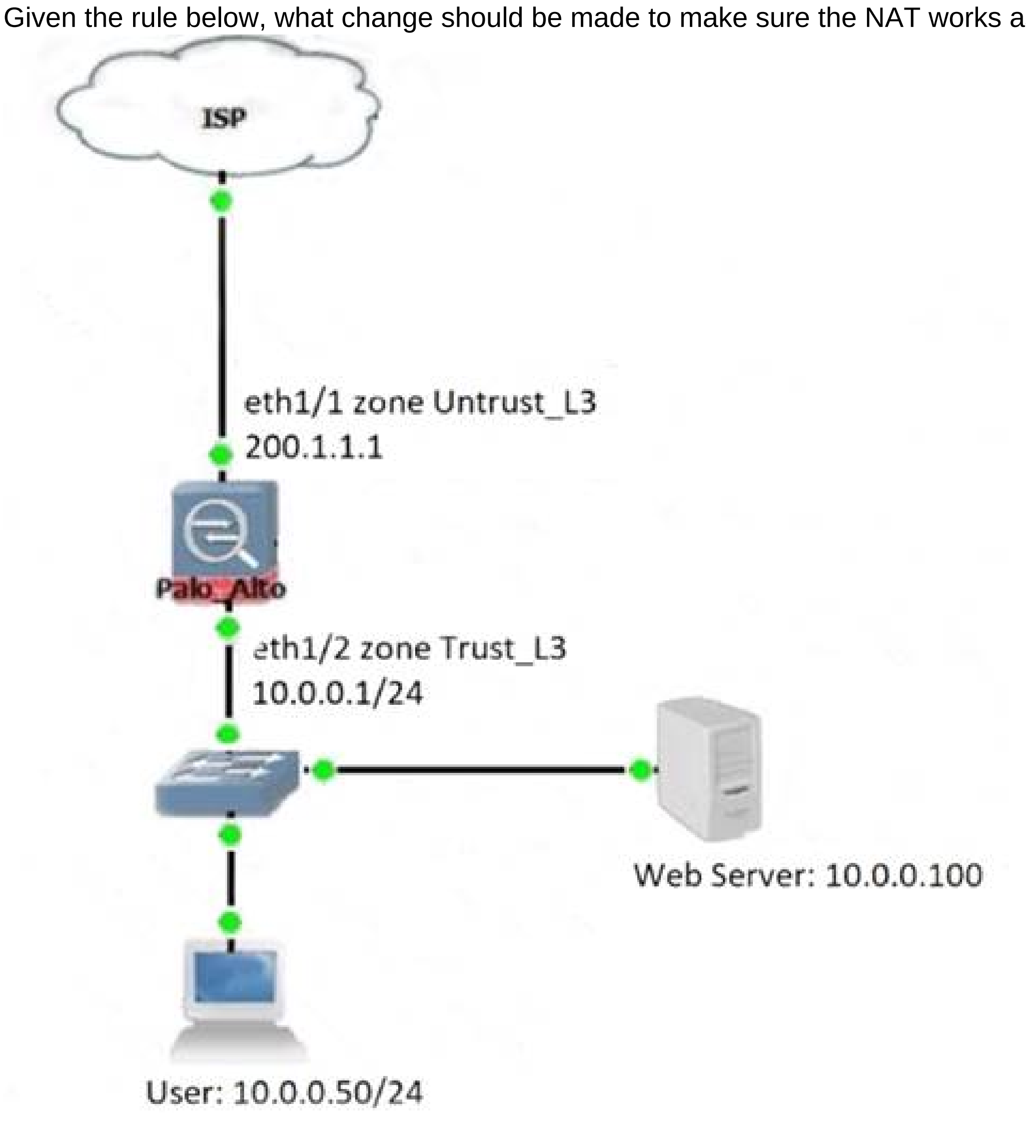
NEW QUESTION 52
An engineer is tasked with deploying SSL Forward Proxy decryption for their organization. What should they review with their leadership before implementation?

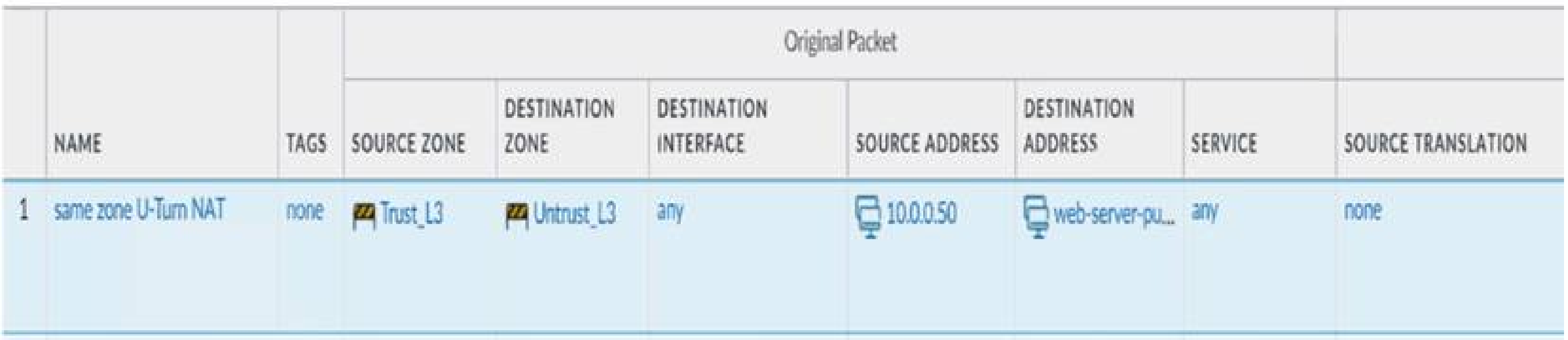
A. Browser-supported cipher documentation
B. Cipher documentation supported by the endpoint operating system
C. URL risk-based category distinctions
D. Legal compliance regulations and acceptable usage policies

Answer: D

Explanation:
The engineer should review the legal compliance regulations and acceptable usage policies with their leadership before implementing SSL Forward Proxy decryption for their organization. SSL Forward Proxy decryption allows the firewall to decrypt and inspect the traffic from internal users to external servers. This can raise privacy and legal concerns for the users and the organization. Therefore, the engineer should ensure that the leadership is aware of the implications and benefits of SSL Forward Proxy decryption and that they have a clear policy for informing and obtaining consent from the users. Option A is incorrect because browser-supported cipher documentation is not relevant for SSL Forward Proxy decryption. The firewall uses its own cipher suite to negotiate encryption with the external server, regardless of the browser settings. Option B is incorrect because cipher documentation supported by the endpoint operating system is not relevant for SSL Forward Proxy decryption. The firewall uses its own cipher suite to negotiate encryption with the external server, regardless of the endpoint operating system. Option C is incorrect because URL risk-based category distinctions are not relevant for SSL Forward Proxy decryption. The firewall can decrypt and inspect traffic based on any URL category, not just risk-based ones.
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-concepts "Understand local laws and regulations about the traffic you can legally decrypt and user notification requirements."

NEW QUESTION 56
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 ethl/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

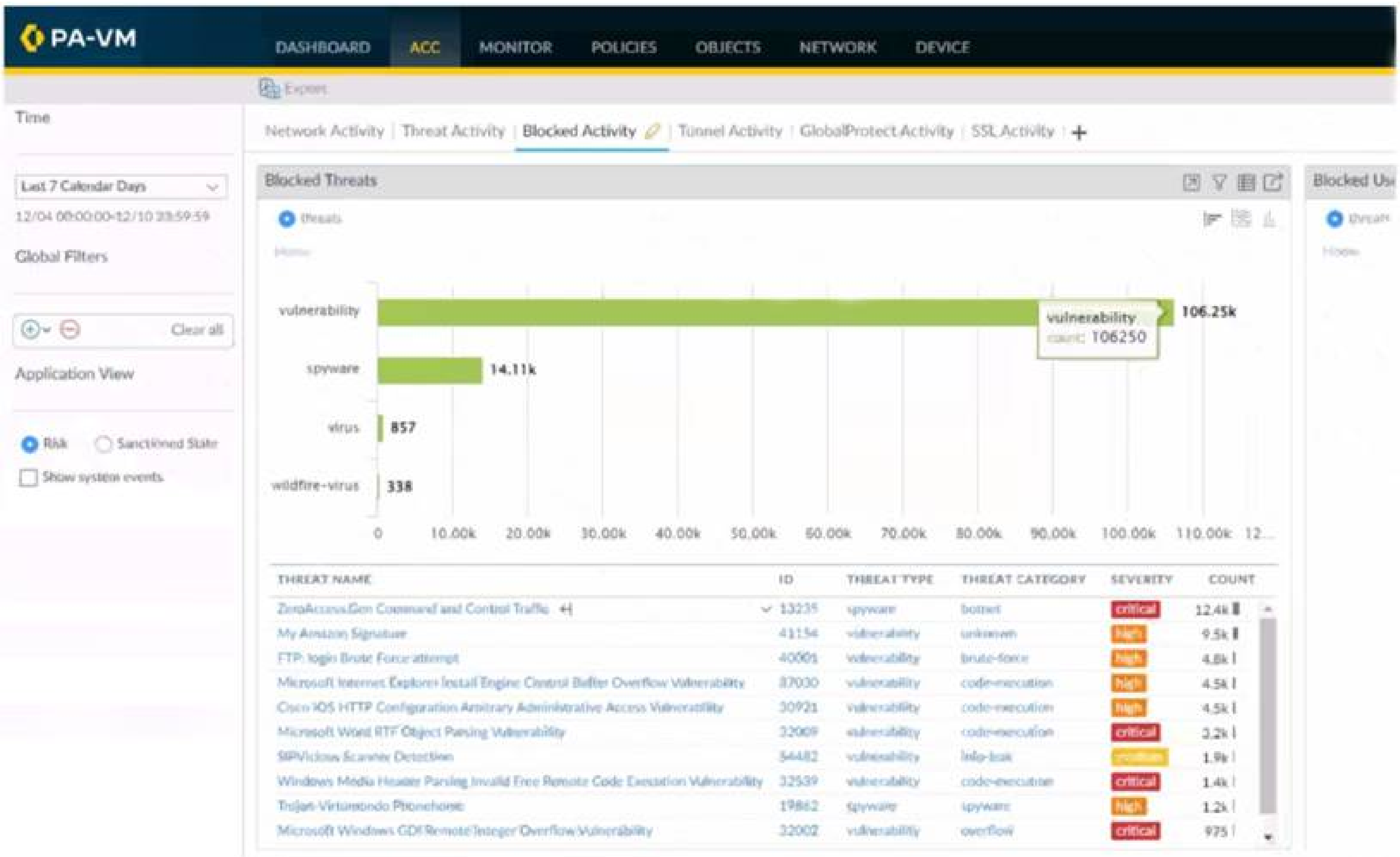
NEW QUESTION 57
Which type of policy in Palo Alto Networks firewalls can use Device-ID as a match condition?

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 60
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 64
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

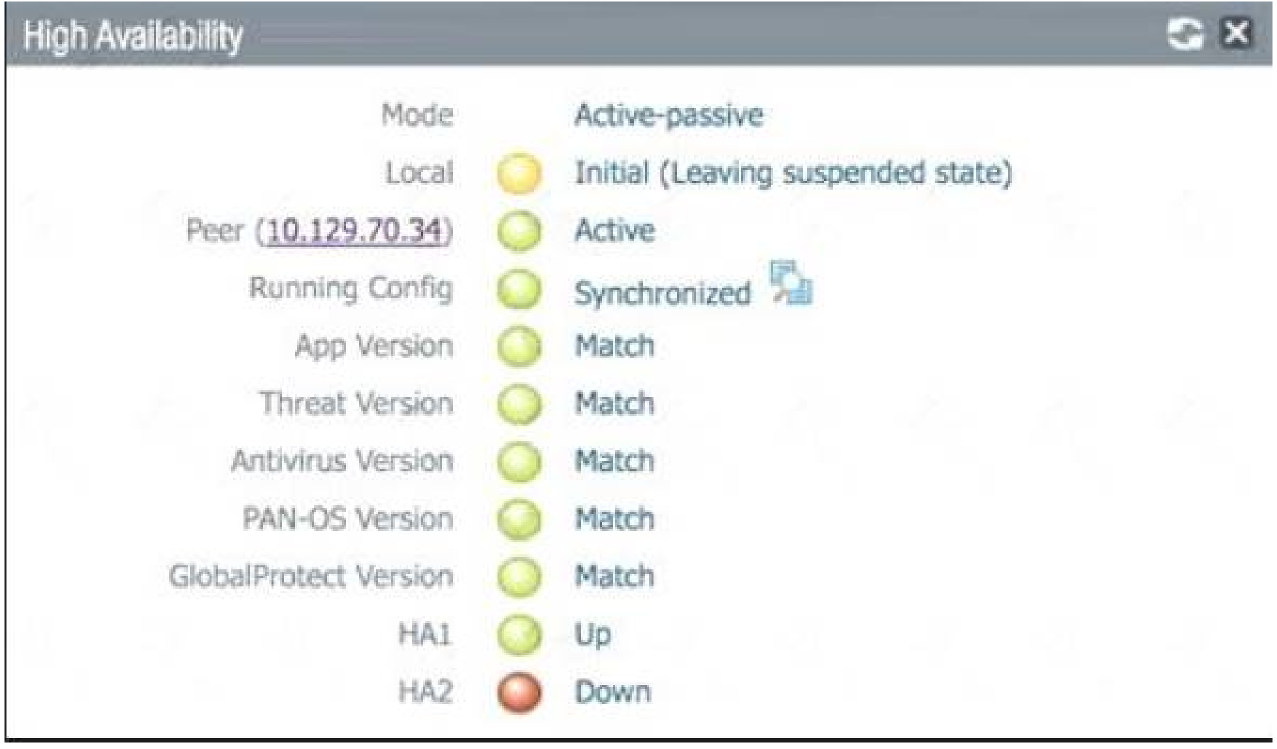
Answer: B

NEW QUESTION 68
An engineer is monitoring an active/active high availability (HA) firewall pair.
Which HA firewall state describes the firewall that is experiencing a failure of a monitored path?

A. Initial
B. Tentative
C. Passive
D. Active-secondary

Answer: B

Explanation:
In an active/active high availability (HA) firewall pair, when a firewall experiences a failure of a monitored path, it enters the “Tentative” state1. This state indicates that the firewall is synchronizing sessions and
configurations from its peer due to a failure or a change in monitored objects such as a link or path. The firewall in this state is not fully functional but is working towards resuming normal operations by syncing with its peer. Therefore, the correct answer is B. Tentative.
Firewall Stuck in Initial (Leaving Suspended State) - Palo Alto Networks



High Availability

Mode		Active-passive
Local	🟡	Initial (Leaving suspended state)
Peer (10.129.70.34)	🟢	Active
Running Config	🟢	Synchronized
App Version	🟢	Match
Threat Version	🟢	Match
Antivirus Version	🟢	Match
PAN-OS Version	🟢	Match
GlobalProtect Version	🟢	Match
HA1	🟢	Up
HA2	🔴	Down

NEW QUESTION 73
What are three tasks that cannot be configured from Panorama by using a template stack? (Choose three.)

A. Change the firewall management IP address
B. Configure a device block list
C. Add administrator accounts
D. Rename a vsys on a multi-vsys firewall
E. Enable operational modes such as normal mode, multi-vsys mode, or FIPS-CC mode

Answer: ACE

NEW QUESTION 74
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 79
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

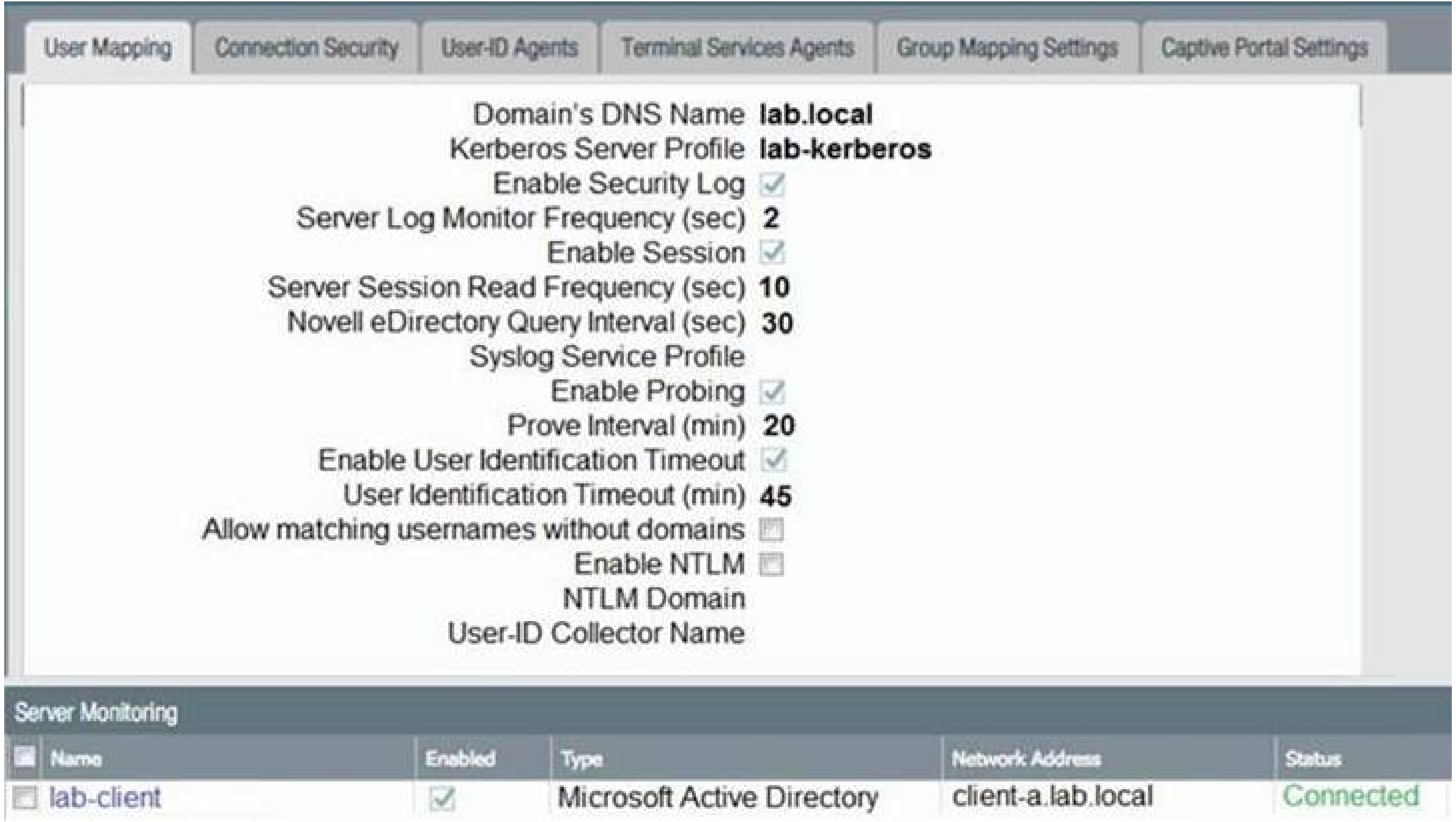
NEW QUESTION 84
An administrator receives the following error message:
"IKE phase-2 negotiation failed when processing Proxy ID. Received local id 192.168 33 33/24 type IPv4 address protocol 0 port 0, received remote id 172.16 33.33/24 type IPv4 address protocol 0 port 0."
How should the administrator 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 87
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 91
An engineer creates a set of rules in a Device Group (Panorama) to permit traffic to various services for a specific LDAP user group.
What needs to be configured to ensure Panorama can retrieve user and group information for use in these rules?

A. A service route to the LDAP server
B. A Master Device
C. Authentication Portal
D. A User-ID agent on the LDAP server

Answer: B

Explanation:
https://live.paloaltonetworks.com/t5/general-topics/what-is-a-master-device-in-device-groups/td-p/15032
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMtpCAG

NEW QUESTION 96
Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

A. PAN-OS integrated User-ID agent
B. GlobalProtect
C. Windows-based User-ID agent
D. LDAP Server Profile configuration

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user-mapping/globalprote GlobalProtect is a VPN solution that provides secure remote access to corporate networks. When a user connects to GlobalProtect, their identity is verified against an LDAP server. This ensures that all IP address-to-user mappings are explicitly known.

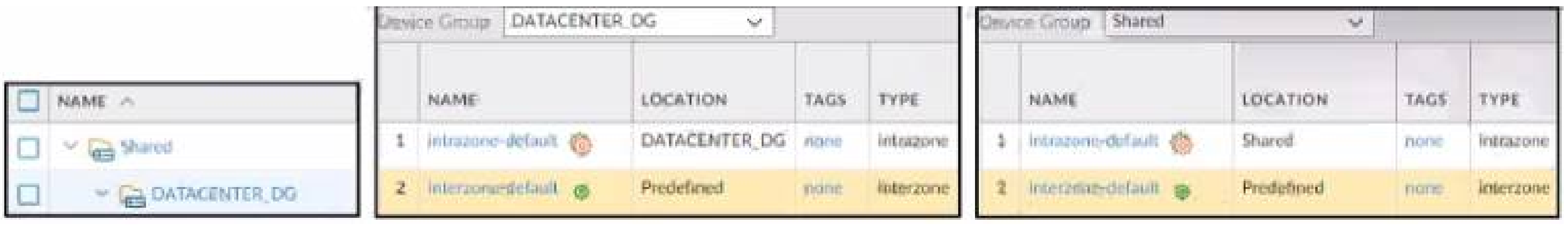
NEW QUESTION 101
Which operation will impact the performance of the management plane?

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 102
Refer to the exhibit.



□	NAME ^
□	⌄ Shared
□	⌄ DATACENTER_DG

Device Group DATACENTER_DG

	NAME	LOCATION	TAGS	TYPE
1	intrazone-default	DATACENTER_DG	none	intrazone
2	interzone-default	Predefined	none	interzone

Device Group Shared

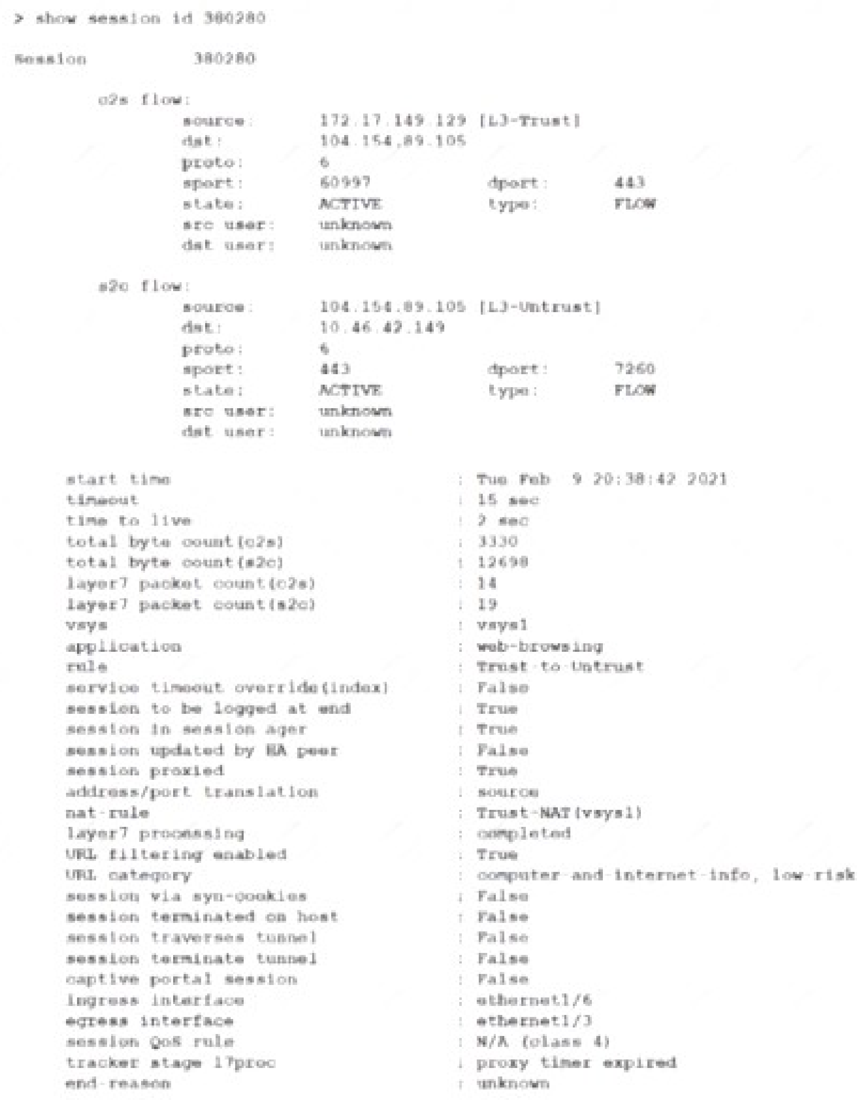
	NAME	LOCATION	TAGS	TYPE
1	intrazone-default	Shared	none	intrazone
2	interzone-default	Predefined	none	interzone

Based on the screenshots above what is the correct order in which the various rules are deployed to firewalls inside the DATACENTER_DG device group?

A. shared pre-rules DATACENTER DG pre rulesrules configured locally on the firewall shared post-rules DATACENTER_DG post-rules DATACENTER.DG default rules
B. shared pre-rules DATACENTER_DG pre-rulesrules configured locally on the firewall shared post-rulesDATACENTER.DG post-rules shared default rules
C. shared pre-rules DATACENTER_DG pre-rulesrules configured locally on the firewall DATACENTER_DG post-rules shared post-rulesshared default rules
D. shared pre-rules DATACENTER_DG pre-rulesrules configured locally on the firewall DATACENTER_DG post-rules shared post-rules DATACENTER_DG default rules

Answer: A

NEW QUESTION 106
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 110
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

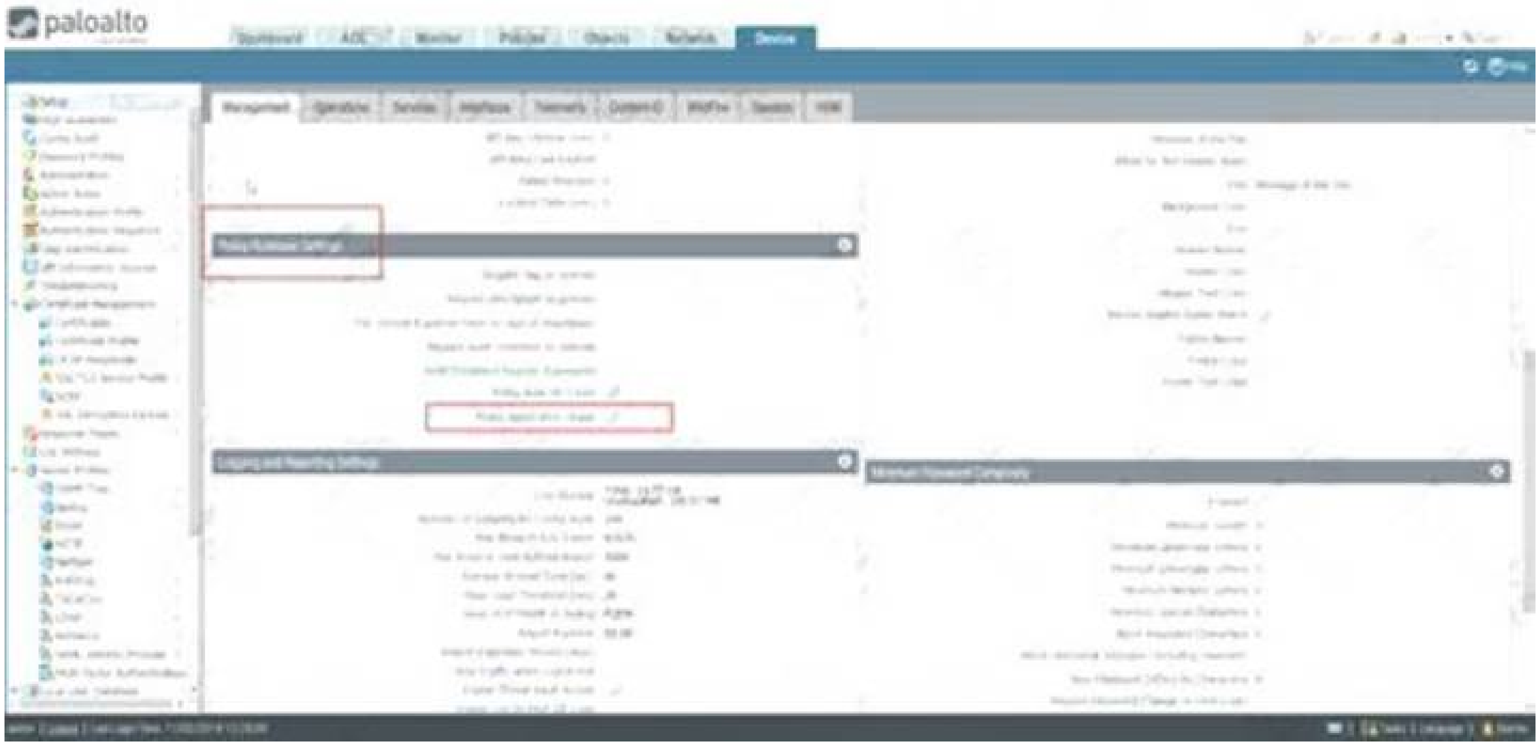
Explanation:
Traffic view in the Monitor tab of the firewall GUI can display the information about the NAT policy that is in use for a traffic flow, if the Source or Destination NAT columns are included and reviewed in the detailed log view1. The Source NAT column shows the translated source IP address 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 114
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 117
Which three authentication types can be used to authenticate users? (Choose three.)

A. Local database authentication
B. PingID
C. Kerberos single sign-on
D. GlobalProtect client
E. Cloud authentication service

Answer: ACE

Explanation:
The three authentication types that can be used to authenticate users are:

- A: Local database authentication. This is the authentication type that uses the local user database on the firewall or Panorama to store and verify user credentials1.
- C: Cloud authentication service. This is the authentication type that uses a cloud-based identity provider such as Okta, PingOne, or PingFederate, to authenticate users and provide SAML assertions to the firewall or Panorama2.
- E: Kerberos single sign-on. This is the authentication type that uses the Kerberos protocol to authenticate users who are logged in to a Windows domain and provide them with seamless access to resources on the firewall or Panorama3.

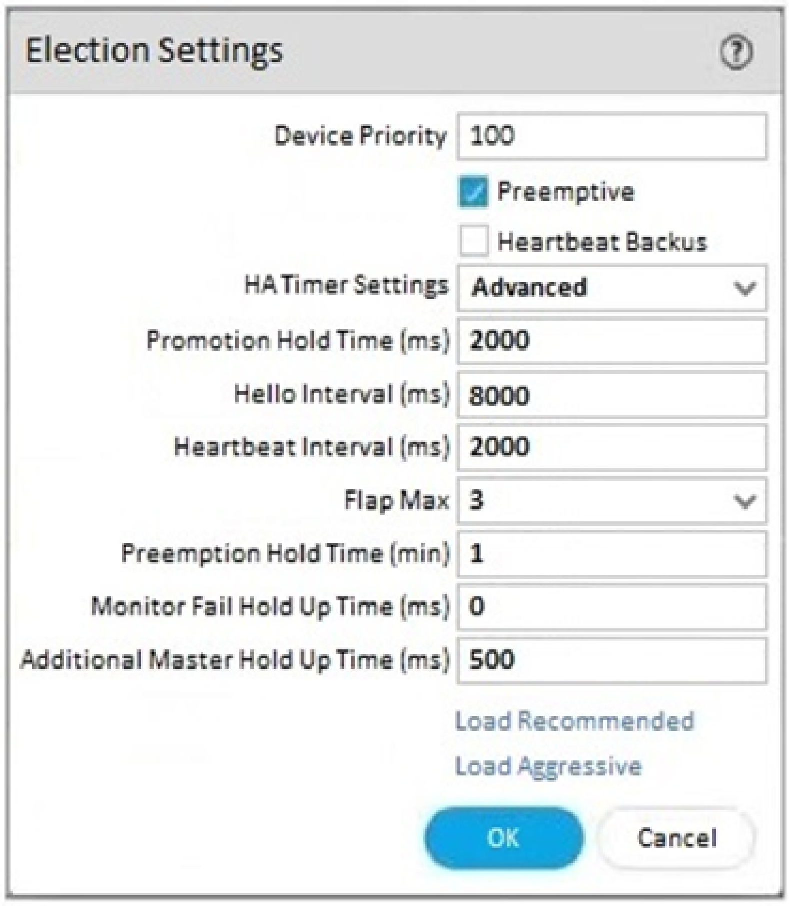
NEW QUESTION 122
An administrator troubleshoots an issue that causes packet drops.
Which log type will help the engineer verify whether packet buffer protection was activated?

A. Data Filtering
B. Configuration
C. Threat
D. Traffic

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNGFCA4

NEW QUESTION 127
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 128
An administrator has purchased WildFire subscriptions for 90 firewalls globally. What should the administrator consider with regards to the WildFire infra-structure?

A. To comply with data privacy regulations, WildFire signatures and ver-dicts are not shared globally.
B. Palo Alto Networks owns and maintains one global cloud and four WildFire regional clouds.
C. Each WildFire cloud analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds.
D. The WildFire Global Cloud only provides bare metal analysis.

Answer: C

Explanation:
https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts Each WildFire cloud—global (U.S.), regional, and private—analyzes samples and generates WildFire verdicts independently of the other WildFire clouds. With the exception of WildFire private cloud verdicts, WildFire verdicts are shared globally, enabling WildFire users to access a worldwide database of threat data.
https://docs.paloaltonetworks.com/wildfire/10-1/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts.ht

NEW QUESTION 132
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 136

......