Paloalto-Networks

Exam Questions PCNSE

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

NEW QUESTION 1
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 2
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 3
An engineer troubleshoots a high availability (HA) link that is unreliable. Where can the engineer view what time the interface went down?

A. Monitor > Logs > System
B. Device > High Availability > Active/Passive Settings
C. Monitor > Logs > Traffic
D. Dashboard > Widgets > High Availability

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oNlUCAU&lang=en_US

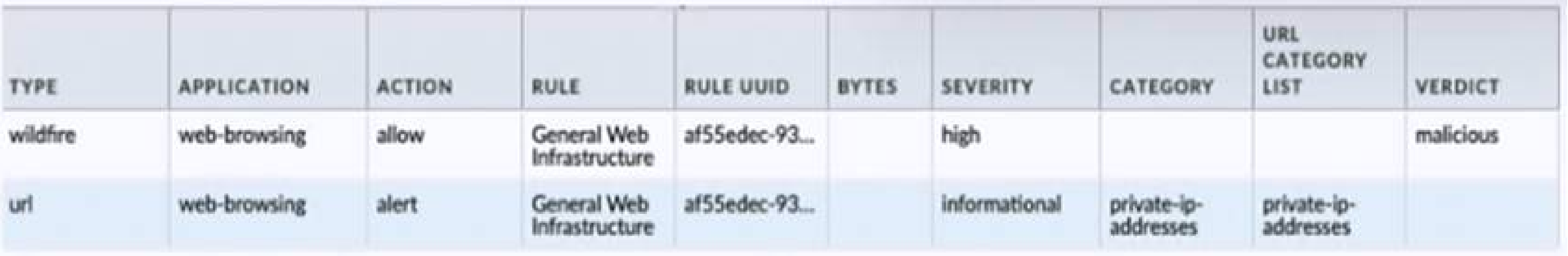
NEW QUESTION 4
An engineer needs to configure a standardized template for all Panorama-managed firewalls. These settings will be configured on a template named "Global" and will be included in all template stacks.
Which three settings can be configured in this template? (Choose three.)

A. Log Forwarding profile
B. SSL decryption exclusion
C. Email scheduler
D. Login banner
E. Dynamic updates

Answer: BDE

Explanation:
A template is a set of configuration options that can be applied to one or more firewalls or virtual systems managed by Panorama. A template can include settings from the Device and Network tabs on the firewall web interface, such as login banner, SSL decryption exclusion, and dynamic updates4. These settings can be configured in a template named “Global” and included in all template stacks. A template stack is a group of templates that Panorama pushes to managed firewalls in an ordered hierarchy4. References: Manage Templates and Template Stacks, PCNSE Study Guide (page 50)

NEW QUESTION 5
Given the following snippet of a WildFire submission log did the end-user get access to the requested information and why or why not?



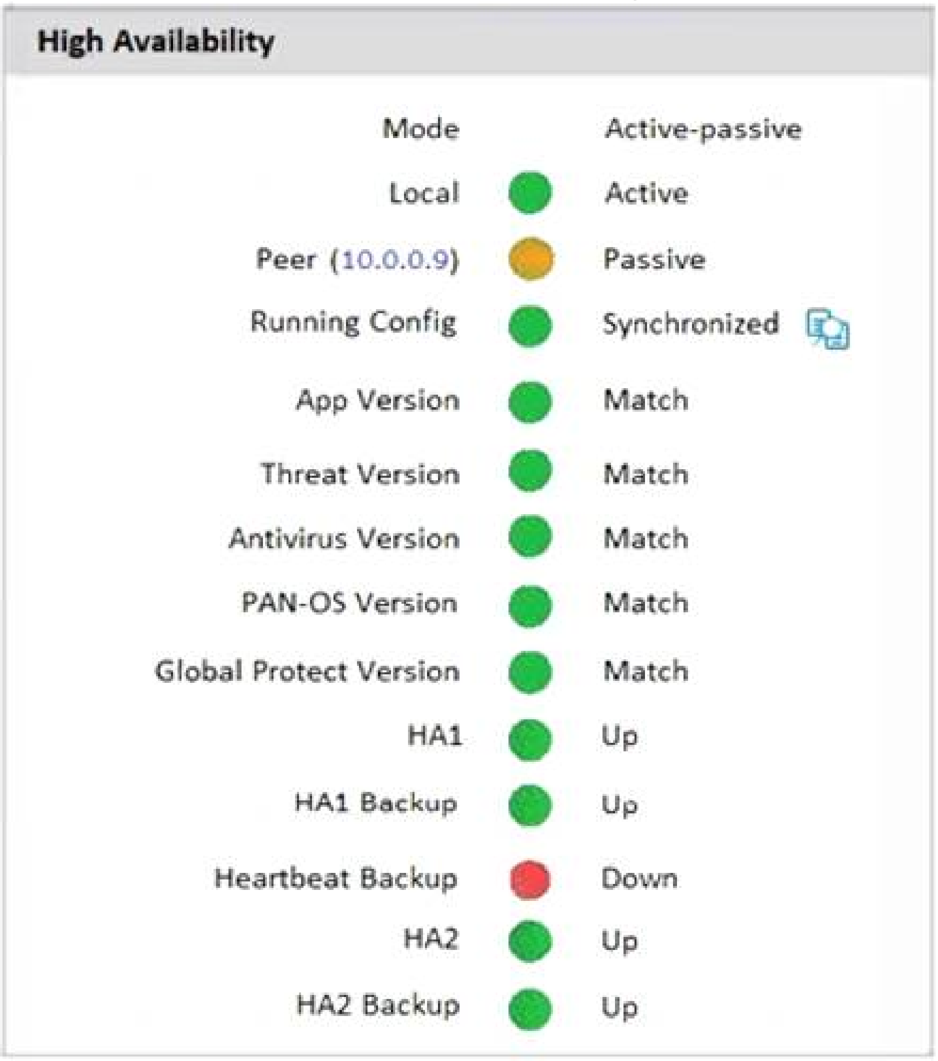
TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	web-browsing	allow	General Web Infrastructure	af55edec-93...		high			malicious
url	web-browsing	alert	General Web Infrastructure	af55edec-93...		informational	private-ip-addresses	private-ip-addresses	

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 6
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

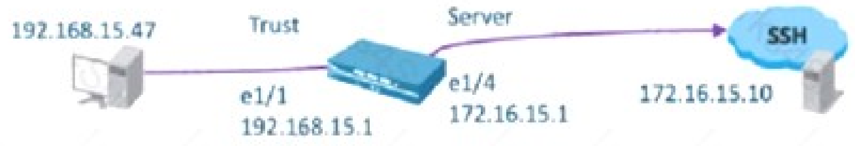
What could an administrator do to troubleshoot the issue?

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 7
Refer to the diagram. Users at an internal system want to ssh to the SSH server. The server is configured to respond only to the ssh requests coming from IP 172.16.16.1.
In order to reach the SSH server only from the Trust zone, which Security rule and NAT rule must be configured on the firewall?



A. NAT Rule:Source Zone: Trust - Source IP: Any - Destination Zone: Server Destination IP: 172.16.15.10 Source Translation: Static IP / 172.16.15.1 Security Rule:Source Zone: Trust - Source IP: Any - Destination Zone: Trust Destination IP: 172.16.15.10 - Application: ssh
B. NAT Rule:Source Zone: Trust Source IP: 192.168.15.0/24 Destination Zone: Trust - Destination IP: 192.168.15.1 Destination Translation: Static IP / 172.16.15.10 Security Rule:Source Zone: Trust Source IP: 192.168.15.0/24 Destination Zone: Server - Destination IP: 172.16.15.10 - Application: ssh
C. NAT Rule:Source Zone: Trust - Source IP: Any - Destination Zone: Trust Destination IP: 192.168.15.1 Destination Translation: Static IP /172.16.15.10 Security Rule:Source Zone: Trust - Source IP: Any - Destination Zone: Server Destination IP: 172.16.15.10 - Application: ssh
D. NAT Rule:Source Zone: Trust Source IP: Any - Destination Zone: Server Destination IP: 172.16.15.10 Source Translation: dynamic-ip-and-port / ethernet1/4 Security Rule:Source Zone: Trust - Source IP: Any - Destination Zone: Server Destination IP: 172.16.15.10 - Application: ssh

Answer: D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhwCAC https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/source-nat-and-destination-nat/sou

NEW QUESTION 8

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?

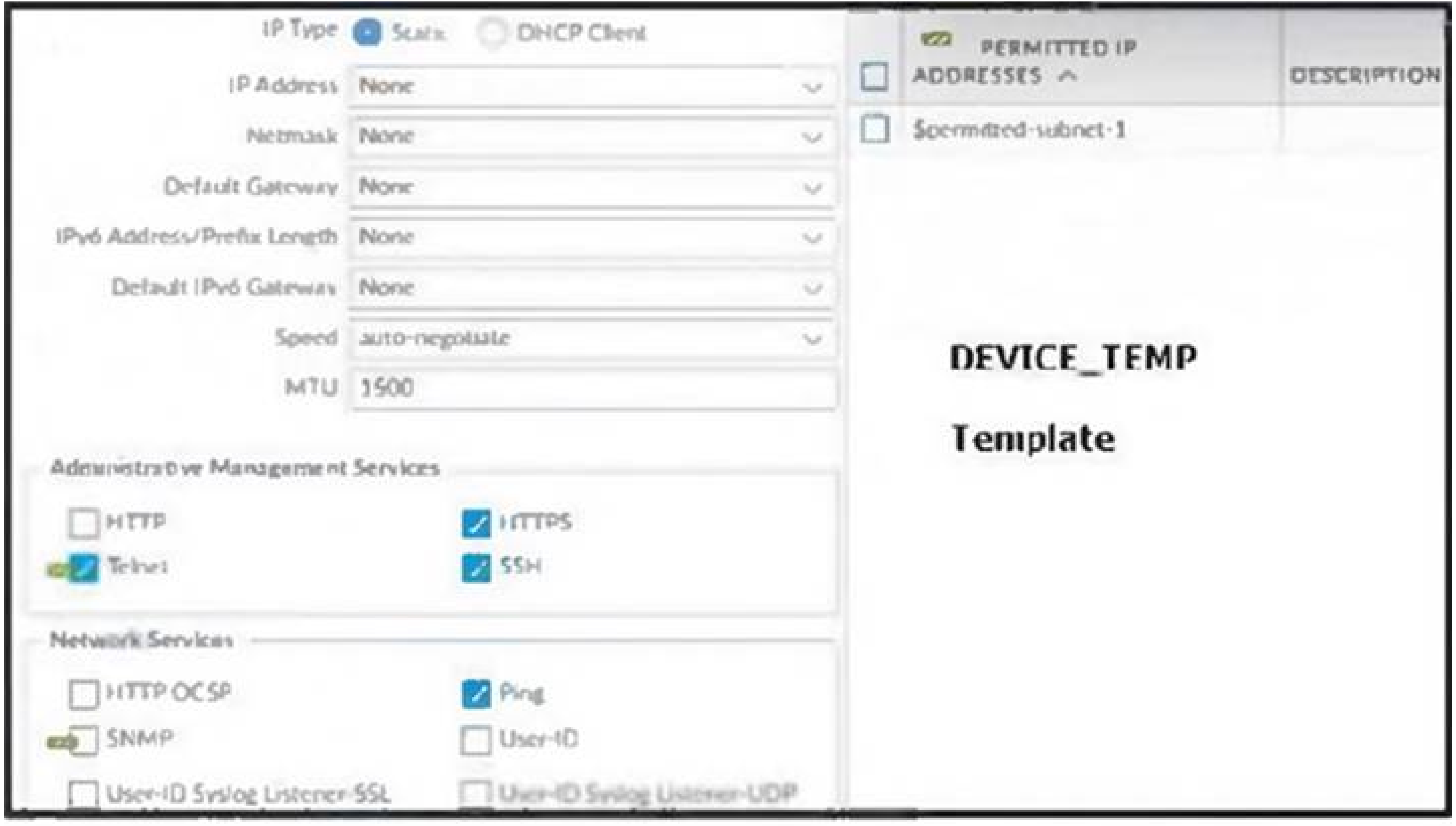
A. DNS proxy
B. Explicit proxy
C. SSL forward proxy
D. Transparent proxy

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 9

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

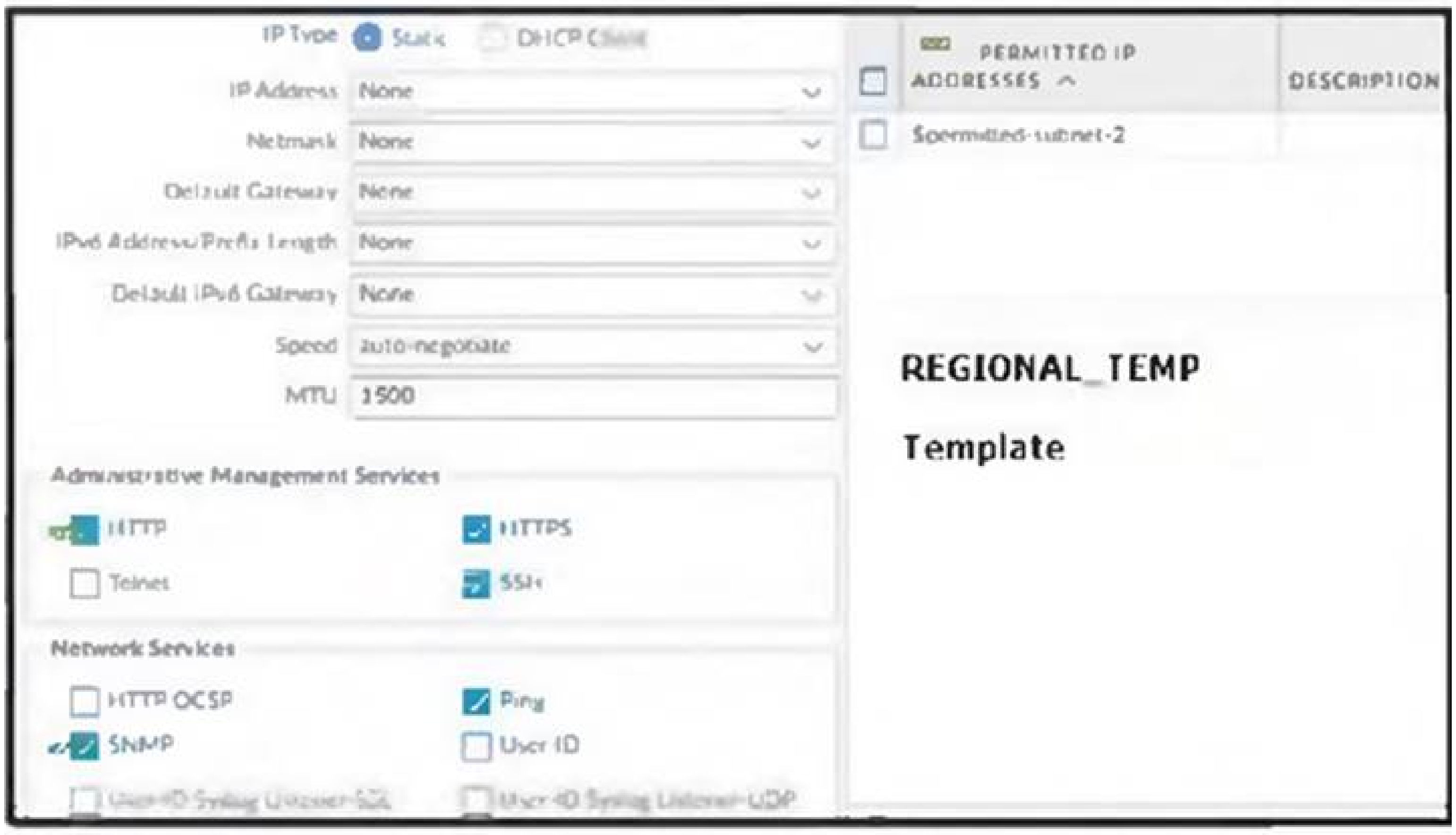
Network Services

□ 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

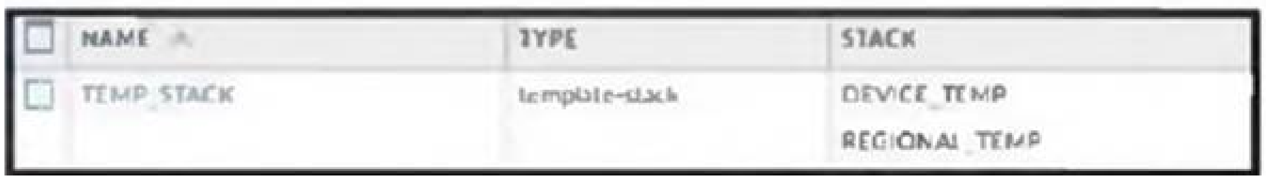
Network Services

□ 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 10
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

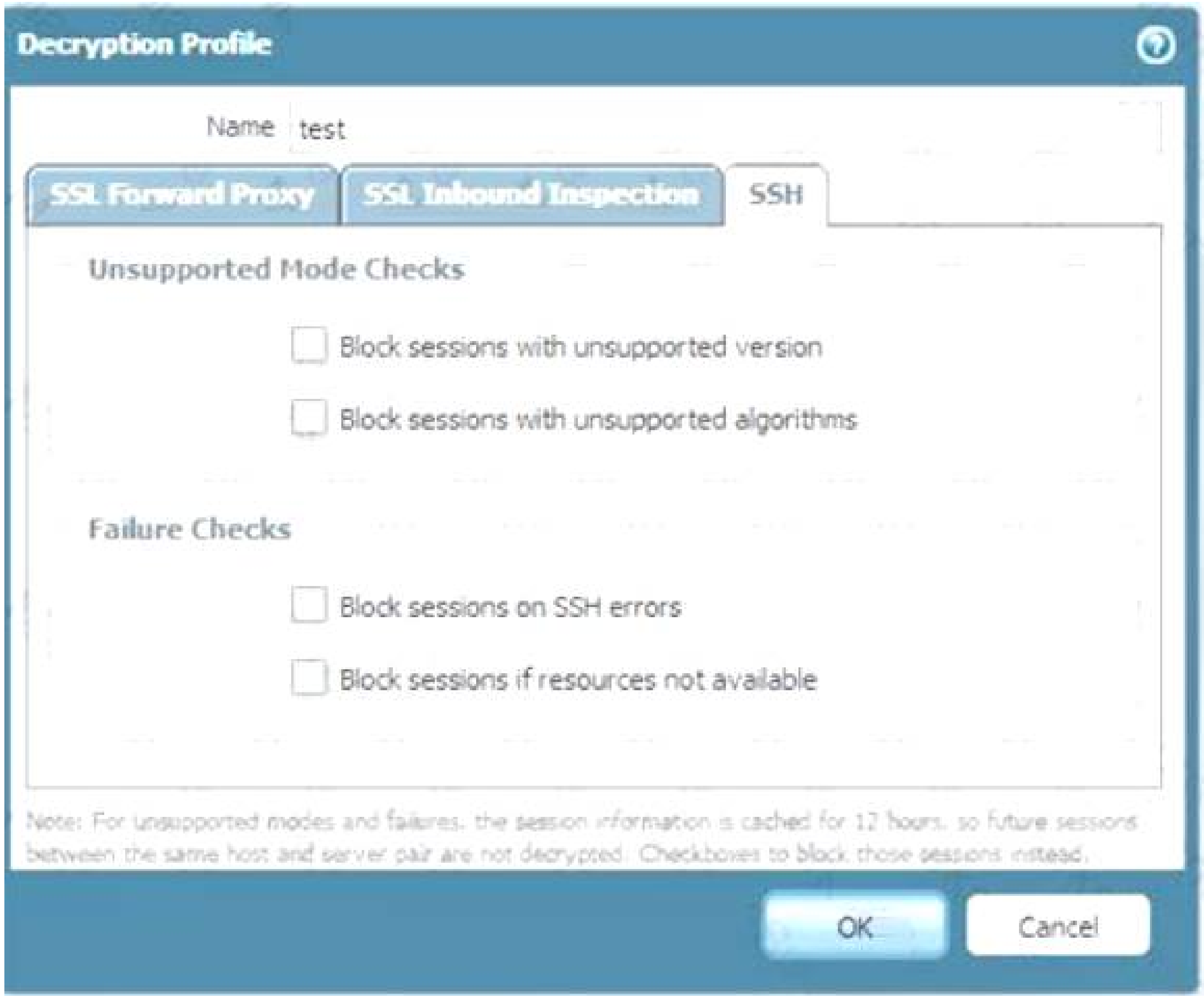
Explanation:
The firewalls exchange hello messages and heartbeats at configurable intervals to verify that the peer firewall is responsive and operational. Hello messages are sent from one peer to the other to verify the state of the firewall. The heartbeat is an ICMP ping to the HA peer. A response 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 10
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



Decryption Profile

Name test

SSL Forward Proxy | SSL Inbound Inspection | SSH

Unsupported Mode Checks

□ Block sessions with unsupported version

□ Block sessions with unsupported algorithms

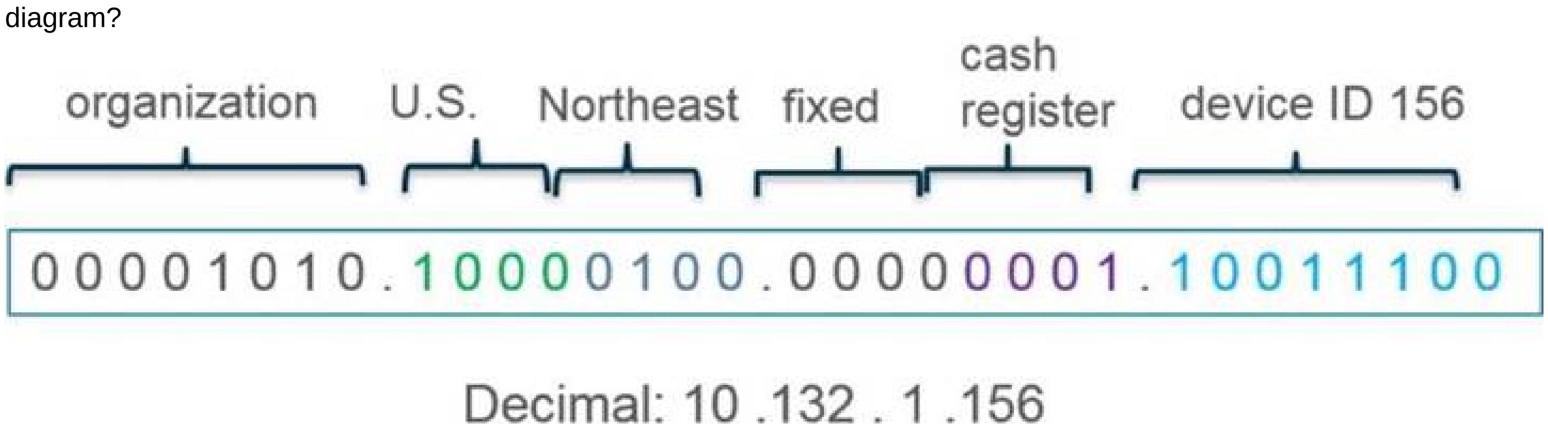
Failure Checks

□ 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 11
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

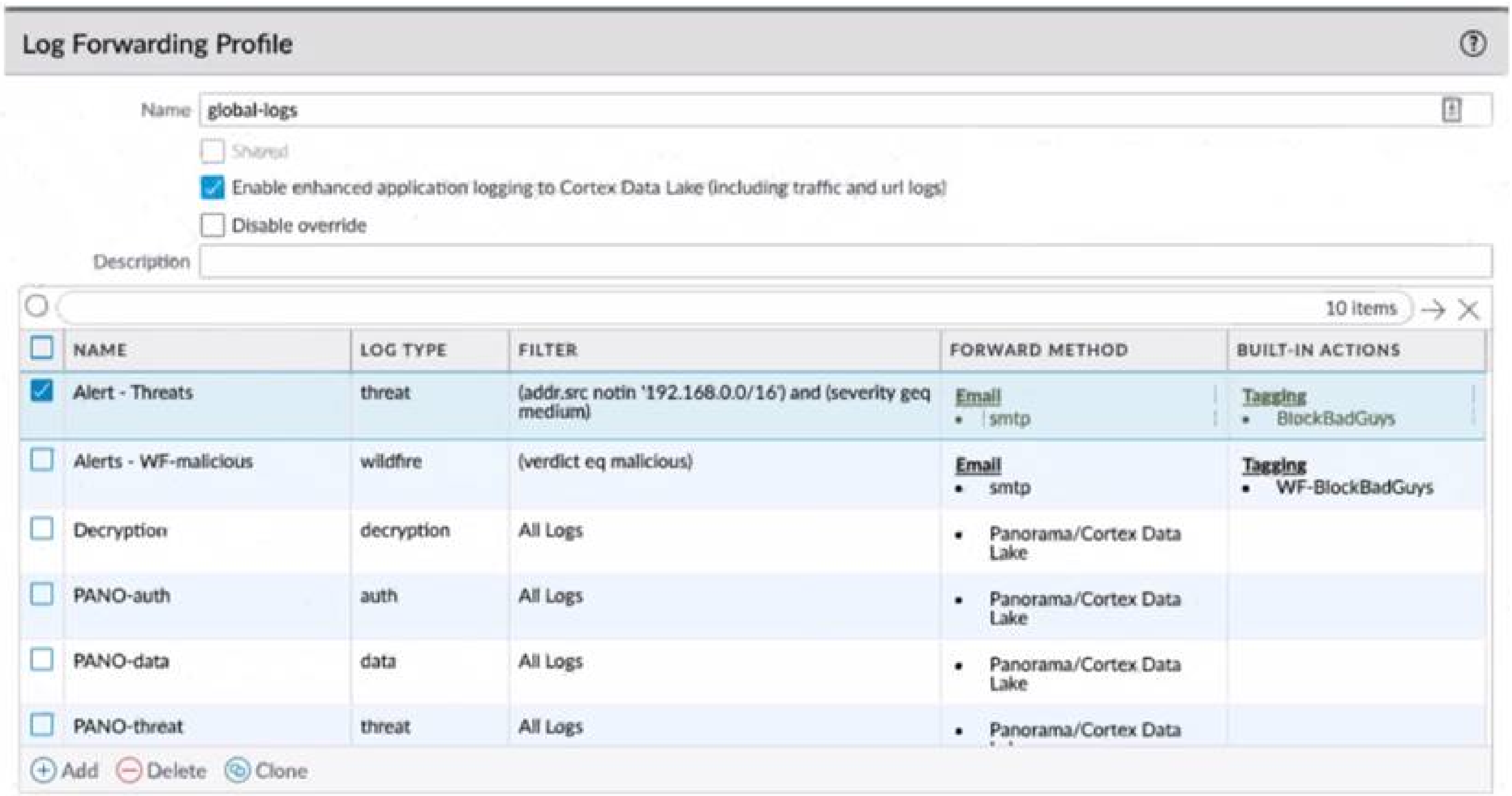
NEW QUESTION 14
An administrator has two pairs of firewalls within the same subnet. Both pairs of firewalls have been configured to use High Availability mode with Active/Passive.
The ARP tables for upstream routes display the same MAC address being shared for some of these firewalls.
What can be configured on one pair of firewalls to modify the MAC addresses so they are no longer in conflict?

A. Configure a floating IP between the firewall pairs.
B. Change the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet.
C. Change the interface type on the interfaces that have conflicting MAC addresses from L3 to VLAN.
D. On one pair of firewalls, run the CLI command: set network interface vlan arp.

Answer: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCAS
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCAS

NEW QUESTION 18
Review the images.



Log Forwarding Profile

Name: global-logs

□ Shared

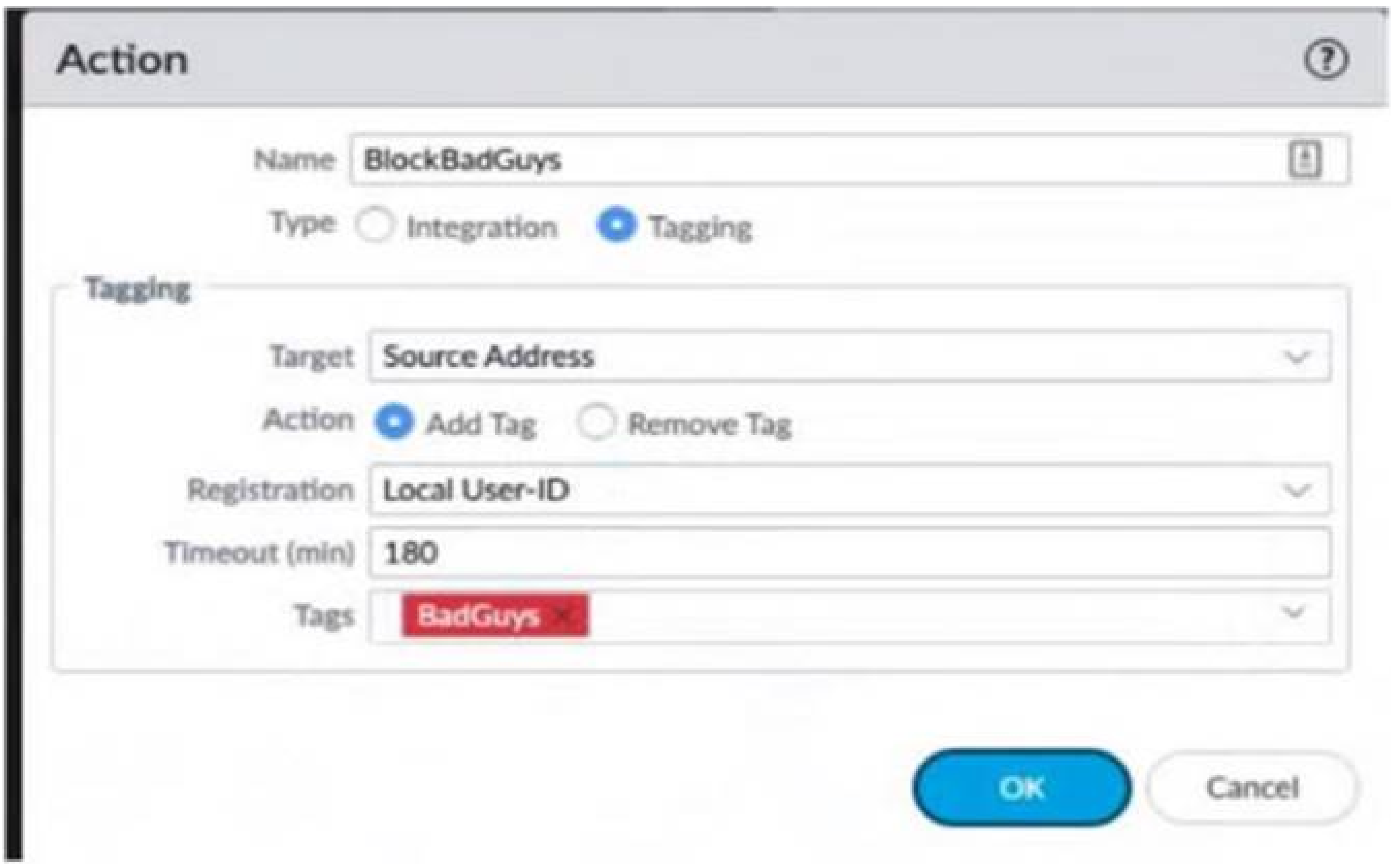
☑ Enable enhanced application logging to Cortex Data Lake (including traffic and url logs)

□ 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 19

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

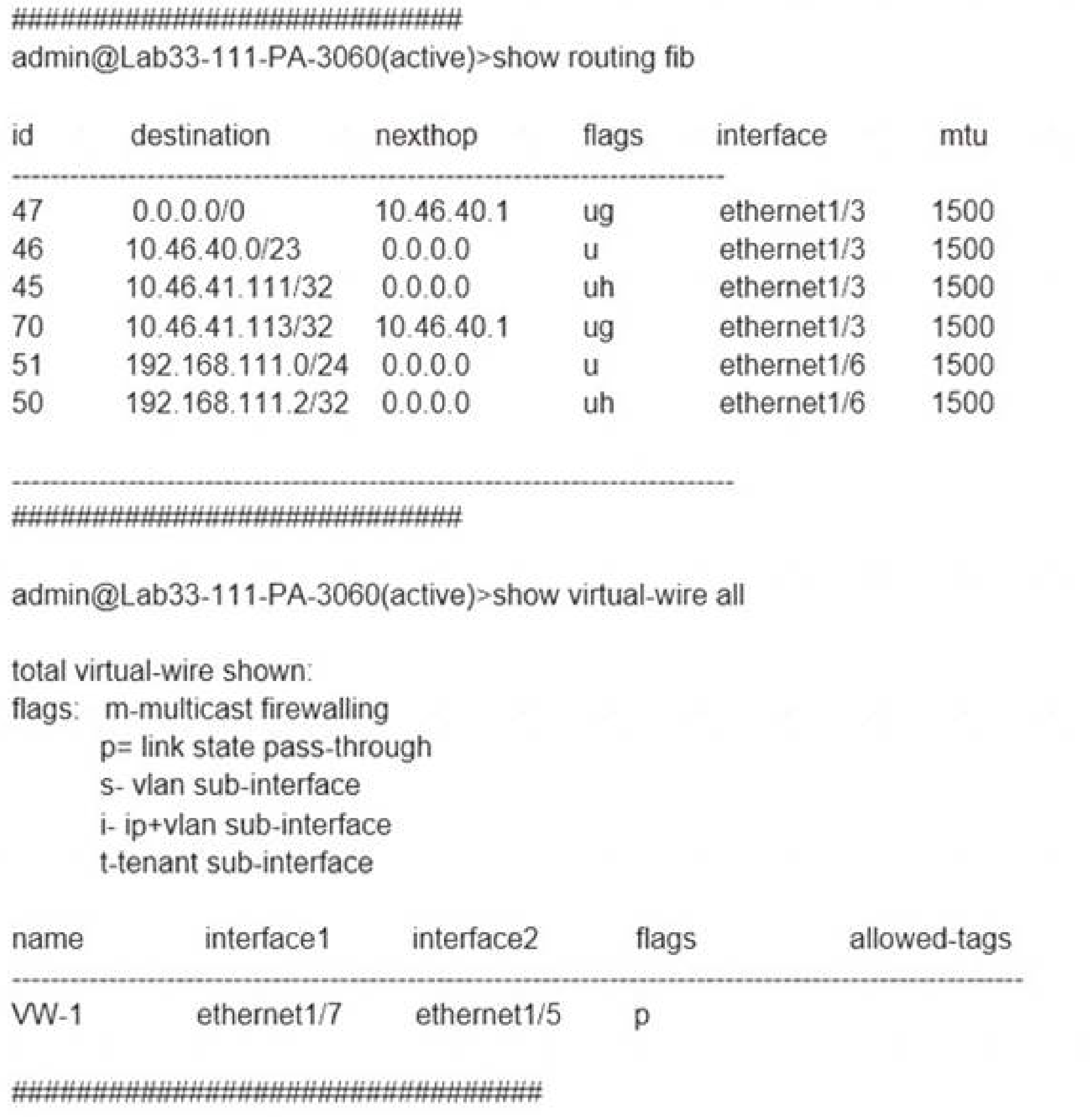
NEW QUESTION 21
A company has configured a URL Filtering profile with override action on their firewall. Which two profiles are needed to complete the configuration? (Choose two)

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 22
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

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

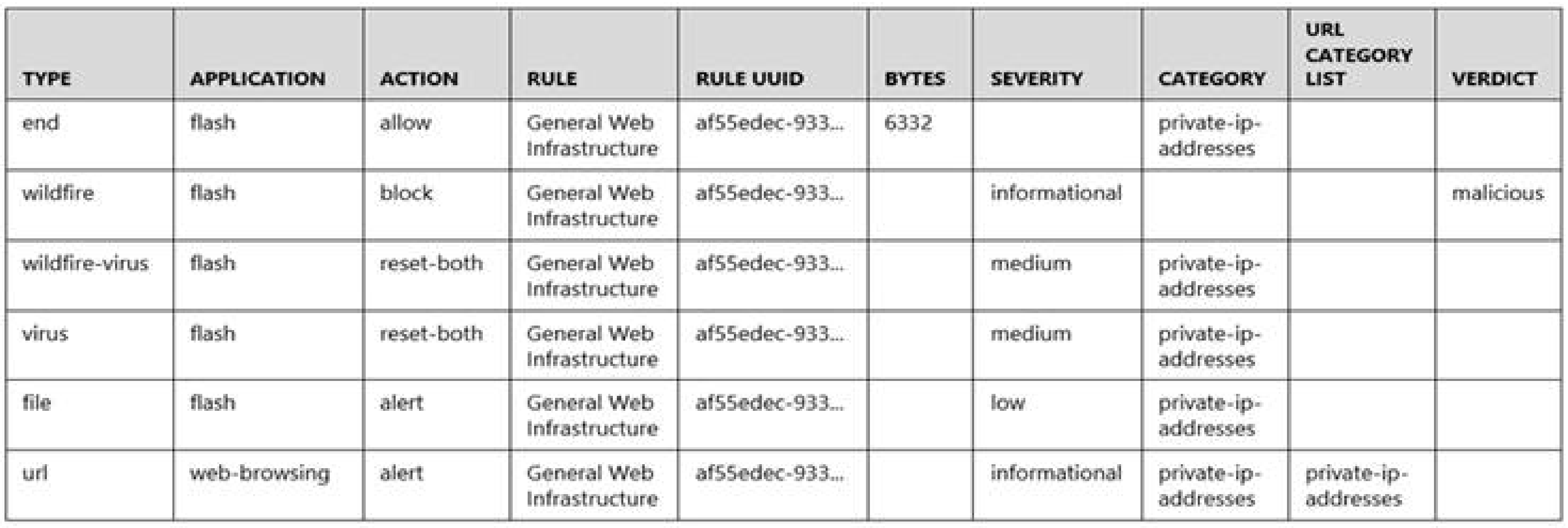
Which will be the egress interface if the traffic's ingress interface is ethernet1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

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 26
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 31
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 35
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 36
Information Security is enforcing group-based policies by using security-event monitoring on Windows User-ID agents for IP-to-User mapping in the network. During the rollout, Information Security identified a gap for users authenticating to their VPN and wireless networks.
Root cause analysis showed that users were authenticating via RADIUS and that authentication events were not captured on the domain controllers that were being monitored Information Security found that authentication events existed on the Identity Management solution (IDM). There did not appear to be direct integration between PAN-OS and the IDM solution
How can Information Security extract and learn iP-to-user mapping information from authentication events for VPN and wireless users?

A. Add domain controllers that might be missing to perform security-event monitoring for VPN and wireless users.
B. Configure the integrated User-ID agent on PAN-OS to accept Syslog messages over TLS.
C. Configure the User-ID XML API on PAN-OS firewalls to pull the authentication events directly fromthe IDM solution
D. Configure the Windows User-ID agents to monitor the VPN concentrators and wireless controllers for IP-to-User mapping.

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-i

NEW QUESTION 40
An administrator has configured OSPF with Advanced Routing enabled on a Palo Alto Networks firewall running PAN-OS 10.2. After OSPF was configured, the administrator noticed that OSPF routes were not being learned.
Which two actions could an administrator take to troubleshoot this issue? (Choose two.)

A. Run the CLI command show advanced-routing ospf neighbor
B. In the WebUI, view the Runtime Stats in the virtual router
C. Look for configuration problems in Network > virtual router > OSPF
D. In the WebUI, view Runtime Stats in the logical router

Answer: AD

Explanation:
A:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-virtual-routers/more
D:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/cli-cheat-sheets/cli-cheat-sheet-networking

NEW QUESTION 44
An administrator notices that an interface configuration has been overridden locally on a firewall. They require all configuration to be managed from Panorama and overrides are not allowed. What is one way the administrator can meet this requirement?

A. Perform a commit force from the CLI of the firewall.
B. Perform a template commit push from Panorama using the "Force Template Values" option.
C. Perform a device-group commit push from Panorama using the "Include Device and Network Templates" option.
D. Reload the running configuration and perform a Firewall local commit.

Answer: B

Explanation:
The best way for the administrator to meet the requirement of managing all configuration from Panorama and preventing local overrides is B: Perform a template commit push from Panorama using the “Force Template Values” option. This option allows the administrator to overwrite any local configuration on the firewall with the values defined in the template1. This way, the administrator can ensure that the interface configuration and any other

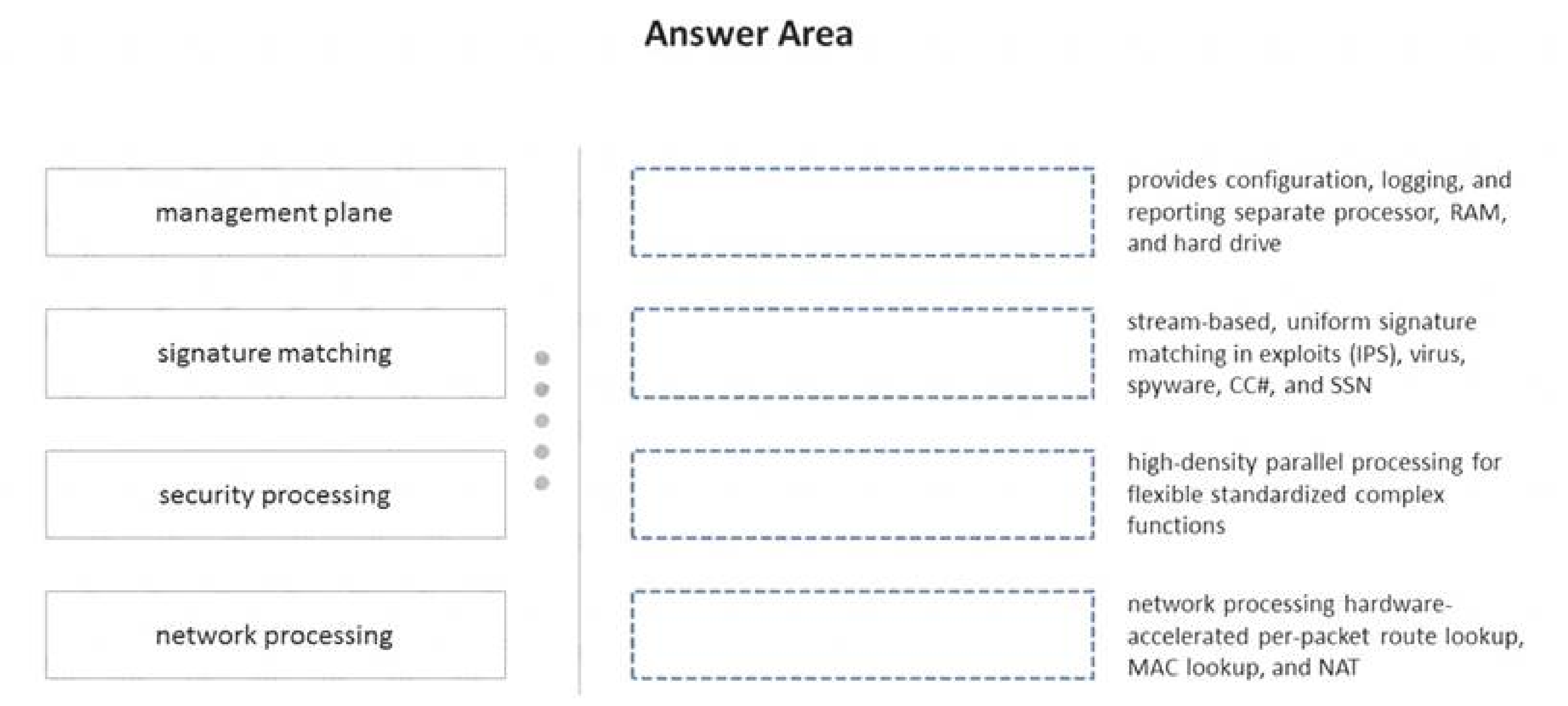
NEW QUESTION 49
An engineer is configuring a Protection profile to defend specific endpoints and resources against malicious activity.
The profile is configured to provide granular defense against targeted flood attacks for specific critical systems that are accessed by users from the internet.
Which profile is the engineer configuring?

A. Packet Buffer Protection
B. Zone Protection
C. Vulnerability Protection
D. DoS Protection

Answer: D

Explanation:
The engineer is configuring a DoS Protection profile to defend specific endpoints and resources against malicious activity. A DoS Protection profile is a feature that enables the firewall to detect and prevent denial-of-service (DoS) attacks that attempt to overwhelm network resources or disrupt services. A DoS Protection profile can provide granular defense against targeted flood attacks for specific critical systems that are accessed by users from the internet, such as web servers, DNS servers, or VPN gateways. A DoS Protection profile can be applied to a security policy rule that matches the traffic to and from the protected systems, and can specify the thresholds and actions for different types of flood attacks, such as SYN, UDP, ICMP, or other IP floods12. References: DoS Protection, PCNSE Study Guide (page 58)

NEW QUESTION 53
Match the terms to their corresponding definitions



Answer Area

management plane

signature matching

security processing

network processing

provides configuration, logging, and reporting separate processor, RAM, and hard drive

stream-based, uniform signature matching in exploits (IPS), virus, spyware, CC#, and SSN

high-density parallel processing for flexible standardized complex functions

network processing hardware-accelerated per-packet route lookup, MAC lookup, and NAT

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A close-up of a computer screen Description automatically generated
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnse-study-guide.p page 83

NEW QUESTION 58
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 63
A network engineer has discovered that asymmetric routing is causing a Palo Alto Networks firewall to drop traffic. The network architecture cannot be changed to correct this.
Which two actions can be taken on the firewall to allow the dropped traffic permanently? (Choose two.)

A. Navigate to Network > Zone Protection Click AddSelect Packet Based Attack Protection > TCP/IP Drop Set "Reject Non-syn-TCP" to No Set "Asymmetric Path" to Bypass
B. > set session tcp-reject-non-syn no
C. Navigate to Network > Zone Protection Click AddSelect Packet Based Attack Protection > TCP/IP Drop Set "Reject Non-syn-TCP" to Global Set "Asymmetric Path" to Global
D. # set deviceconfig setting session tcp-reject-non-syn no

Answer: AD

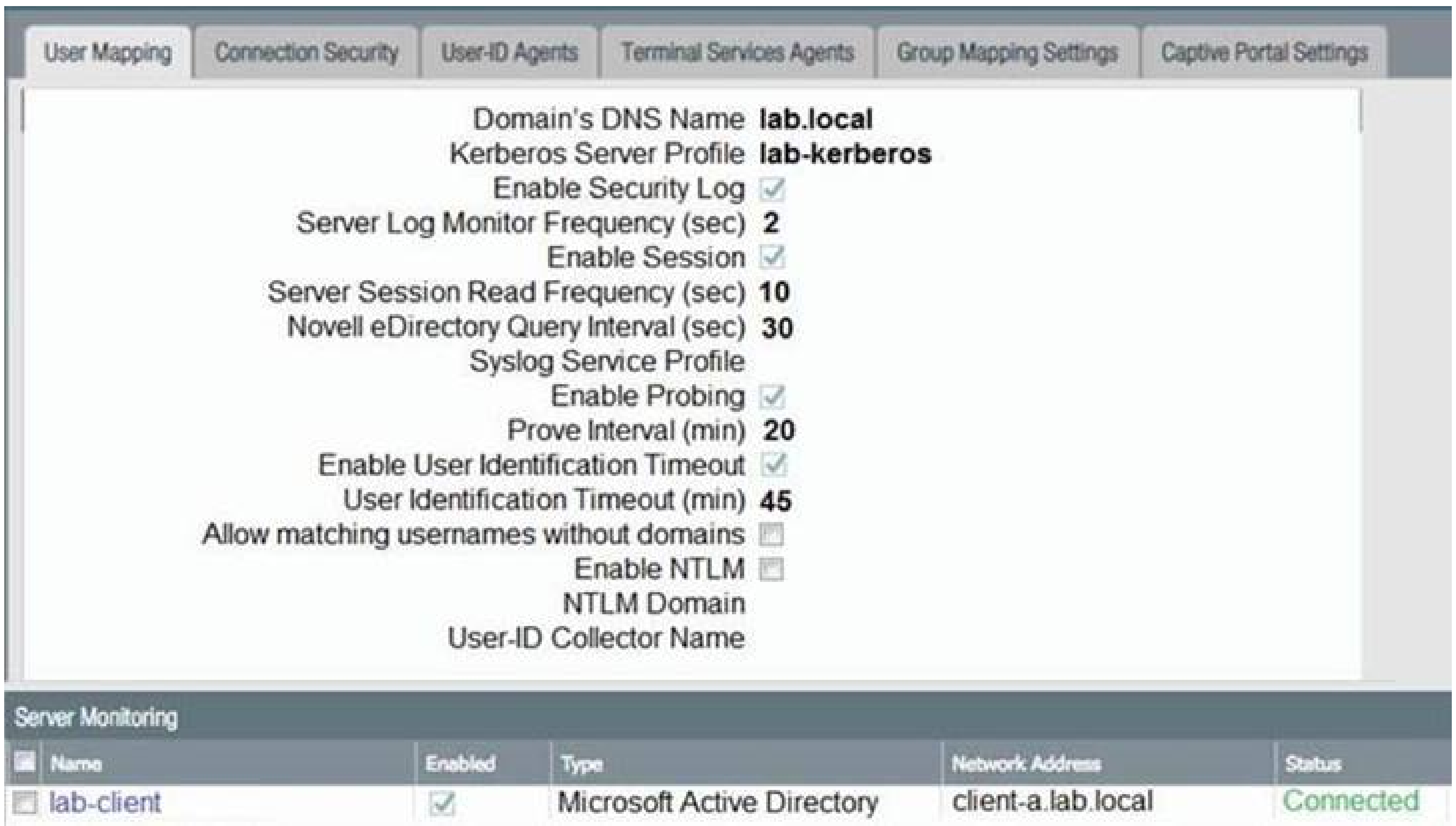
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClG2CAK

NEW QUESTION 64
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 66
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

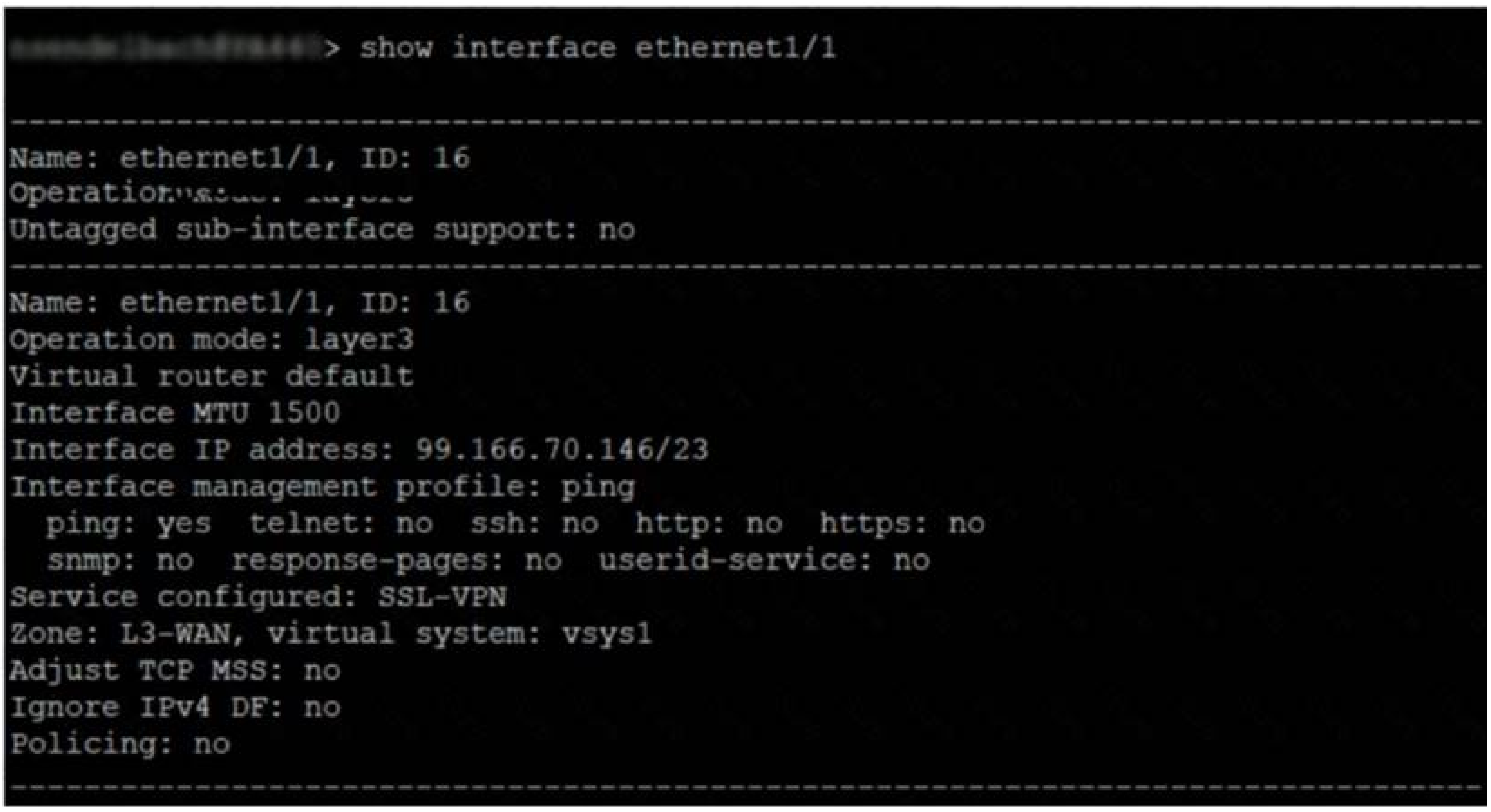
NEW QUESTION 71
An engineer manages a high availability network and requires fast failover of the routing protocols. The engineer decides to implement BFD.
Which three dynamic routing protocols support BFD? (Choose three.)

A. OSPF
B. RIP
C. BGP
D. IGRP
E. OSPFv3 virtual link

Answer: ABC

Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/bfd/bfd-overview/bfd-for-dynamic-ro

NEW QUESTION 75
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
Operatio[illegible]
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
-------------------------------------------------------------------------------
```

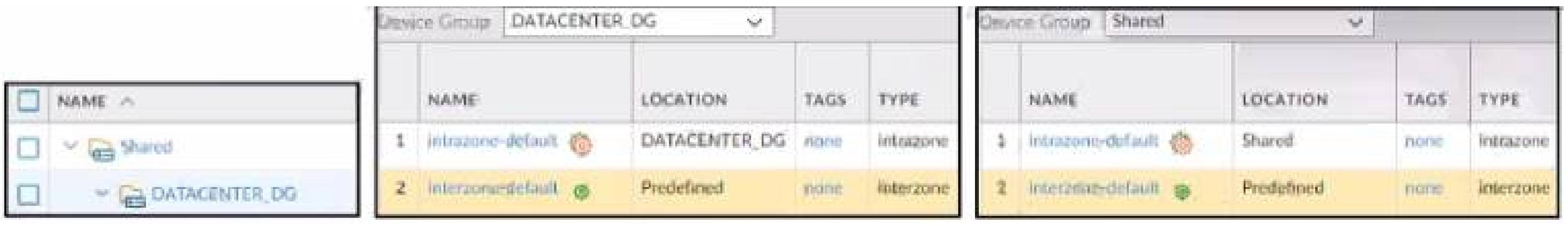
Which setting should be modified on ethernet1/1 to remedy this problem?

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 76
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 79
What is the best description of the Cluster Synchronization Timeout (min)?

A. The maximum time that the local firewall waits before going to Active state when another cluster member is preventing the cluster from fully synchronizing
B. The time that a passive or active-secondary firewall will wait before taking over as the active or active-primary firewall
C. The timeframe within which the firewall must receive keepalives from a cluster member to know that the cluster member is functional
D. The maximum interval between hello packets that are sent to verify that the HA functionality on theother firewall is operational

Answer: A

Explanation:
The best description of the Cluster Synchronization Timeout (min) is the maximum time that the local firewall waits before going to Active state when another cluster member is preventing the cluster from fully synchronizing. This is a parameter that can be configured in an HA cluster, which is a group of firewalls that share session state and provide high availability and scalability. The Cluster Synchronization Timeout (min) determines how long the local firewall will wait for the cluster to reach a stable state before it decides to become Active and process traffic. A stable state means that all cluster members are either Active or Passive, and have synchronized their sessions with each other. If there is another cluster member that is in an unknown or unstable state, such as Initializing, Non-functional, or Suspended, then it may prevent the cluster from fully synchronizing and cause a delay in traffic processing. The Cluster Synchronization Timeout (min) can be set to a value between 0 and 30 minutes, with a default of 0. If it is set to 0, then the local firewall will not wait for any other cluster member and will immediately go to Active state. If it is set to a positive value, then the local firewall will wait for that amount of time before going to Active state, unless the cluster reaches a stable state earlier12. References: Configure HA Clustering, PCNSE Study Guide (page 53)
How to Set Session, TCP, and UDP Timeout Values - Palo Alto Networks ...

NEW QUESTION 82
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 86
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 91
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 94
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 98

......