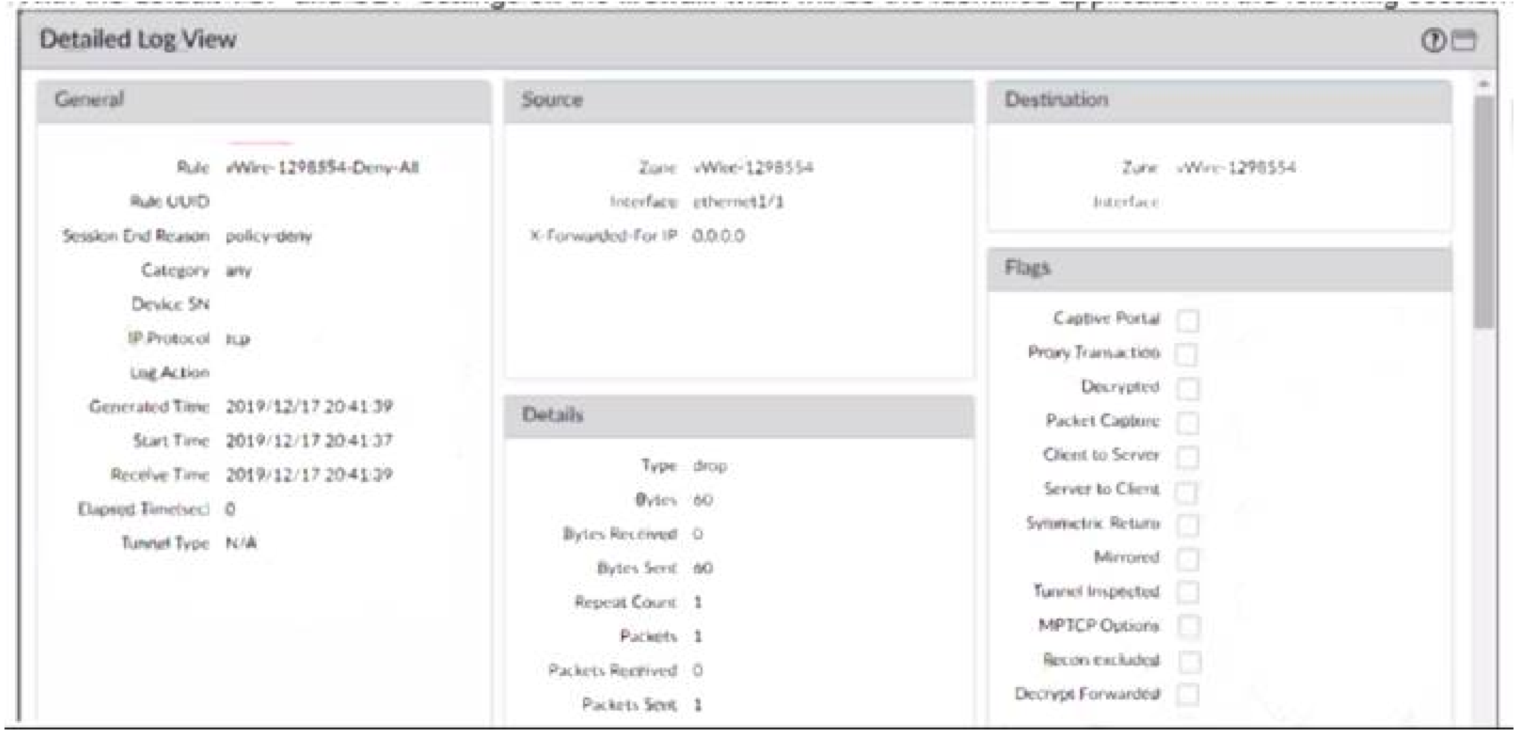
Paloalto-Networks

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
An engineer is troubleshooting a traffic-routing issue. What is the correct packet-flow sequence?

A. PBF > Zone Protection Profiles > Packet Buffer Protection
B. BGP > PBF > NAT
C. PBF > Static route > Security policy enforcement
D. NAT > Security policy enforcement > OSPF

Answer: C

Explanation:
The correct packet-flow sequence is C. PBF > Static route > Security policy enforcement. This sequence describes the order of operations that the firewall performs when processing a packet. PBF stands for
Policy-Based Forwarding, which is a feature that allows the firewall to override the routing table and forward
traffic based on the source and destination addresses, application, user, or service. PBF is evaluated before the static route lookup, which is the default method of forwarding traffic based on the destination address and the longest prefix match. Security policy enforcement is the stage where the firewall applies the security policy rules to allow or block traffic based on various criteria, such as zone, address, port, user, application, etc12. References: Policy-Based Forwarding, Packet Flow Sequence in PAN-OS

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

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

Answer: C

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

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

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

Answer: D

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

NEW QUESTION 5
A network administrator is trying to prevent domain username and password submissions to phishing sites on some allowed URL categories
Which set of steps does the administrator need to take in the URL Filtering profile to prevent credential phishing on the firewall?

A. Choose the URL categories in the User Credential Submission column and set action to block Select the User credential Detection tab and select Use Domain Credential Filter Commit
B. Choose the URL categories in the User Credential Submission column and set action to block Select the User credential Detection tab and select use IP User Mapping Commit
C. Choose the URL categories on Site Access column and set action to block Click the User credential Detection tab and select IP User Mapping Commit
D. Choose the URL categories in the User Credential Submission column and set action to block Select the URL filtering settings and enable Domain Credential Filter Commit

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-u https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/prevent-credential-phishing/set-up-cre

NEW QUESTION 6
Which type of zone will allow different virtual systems to communicate with each other?

A. Tap
B. External
C. Virtual Wire
D. Tunnel

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/virtual-systems/communication-between-virtual-s

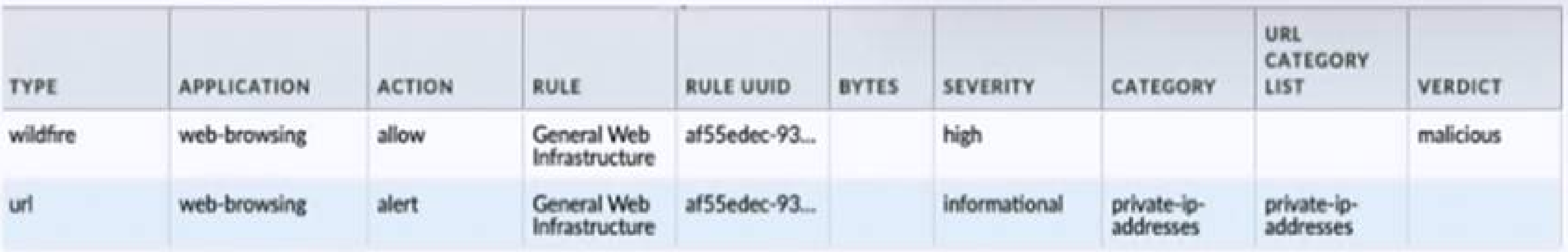
NEW QUESTION 7
In a security-first network, what is the recommended threshold value for apps and threats to be dynamically updated?

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

Answer: B

Explanation:
Schedule content updates so that they download-and-install automatically. Then, set a Threshold that determines the amount of time the firewall waits before installing the latest content. In a security-first network, schedule a six to twelve hour threshold.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-thr
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/software-and-content-updates/best-practices-for

NEW QUESTION 8
Given the following snippet of a WildFire submission log did the end-user get access to the requested information and why or why not?



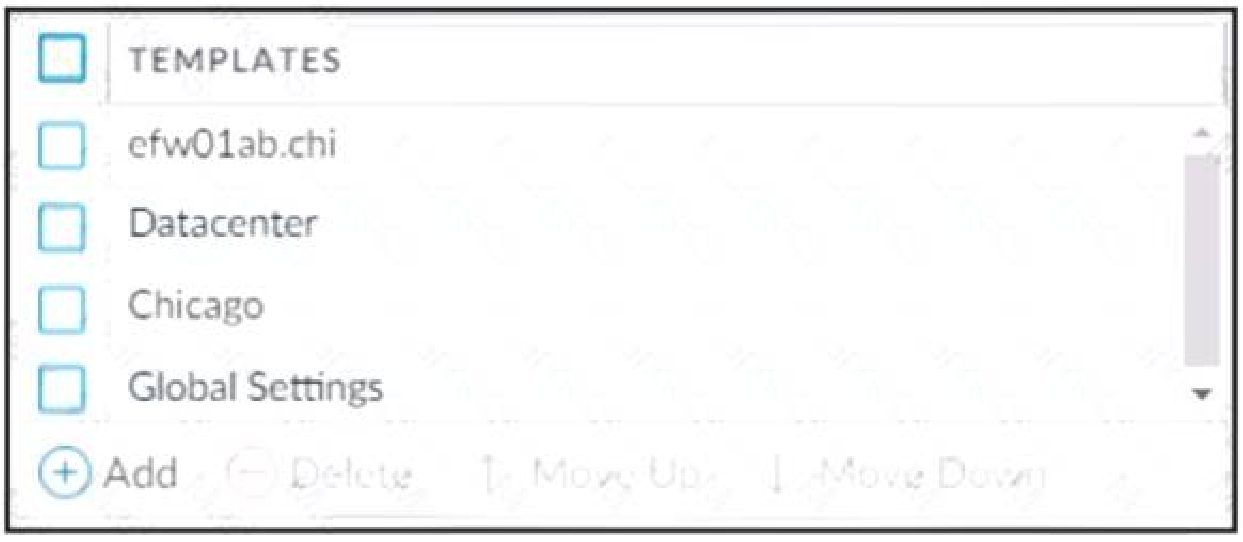
TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	web-browsing	allow	General Web Infrastructure	af55edec-93...		high			malicious
url	web-browsing	alert	General Web Infrastructure	af55edec-93...		informational	private-ip-addresses	private-ip-addresses	

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 9
Which template values will be configured on the firewall if each template has an SSL to be deployed. The template stack should consist of four templates arranged according to the diagram.



□ TEMPLATES
□ efw01ab.chi
□ Datacenter
□ Chicago
□ Global Settings

Which template values will be configured on the firewall if each template has an SSL/TLS Service profile configured named Management?

A. Values in Datacenter
B. Values in efwOlab.chi
C. Values in Global Settings
D. Values in Chicago

Answer: D

Explanation:
The template stack should consist of four templates arranged according to the diagram. The template values that will be configured on the firewall if each template has an SSL/TLS Service profile configured named Management will be the values in Chicago. This is because the SSL/TLS Service profile is configured in the Chicago template, which is the highest priority template in the stack. The firewall will inherit the settings from the highest priority template that has the setting configured, and ignore the settings from the lower priority templates that have the same setting configured. Therefore, the values in Datacenter, efwOlab.chi, and Global Settings will not be applied to the firewall. References:

- [Template Stack Configuration]
- [Template Stack Priority]

NEW QUESTION 10
An engineer is configuring a template in Panorama which will contain settings that need to be applied to all firewalls in production.
Which three parts of a template an engineer can configure? (Choose three.)

A. NTP Server Address
B. Antivirus Profile
C. Authentication Profile
D. Service Route Configuration
E. Dynamic Address Groups

Answer: ACD

Explanation:

- A, C, and D are the correct answers because they are the parts of a template that an engineer can configure in Panorama. A template is a collection of device and network settings that can be pushed to multiple firewalls from Panorama1. A template can contain settings such as2:
- A: NTP Server Address: This is the address of the Network Time Protocol server that synchronizes the time on the firewall.
- C: Authentication Profile: This is the profile that defines how the firewall authenticates users and administrators.
- D: Service Route Configuration: This is the configuration that specifies which interface and source IP address the firewall uses to access external services, such as DNS, email, syslog, etc.

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

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

Answer: A

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

NEW QUESTION 12
Why would a traffic log list an application as "not-applicable”?

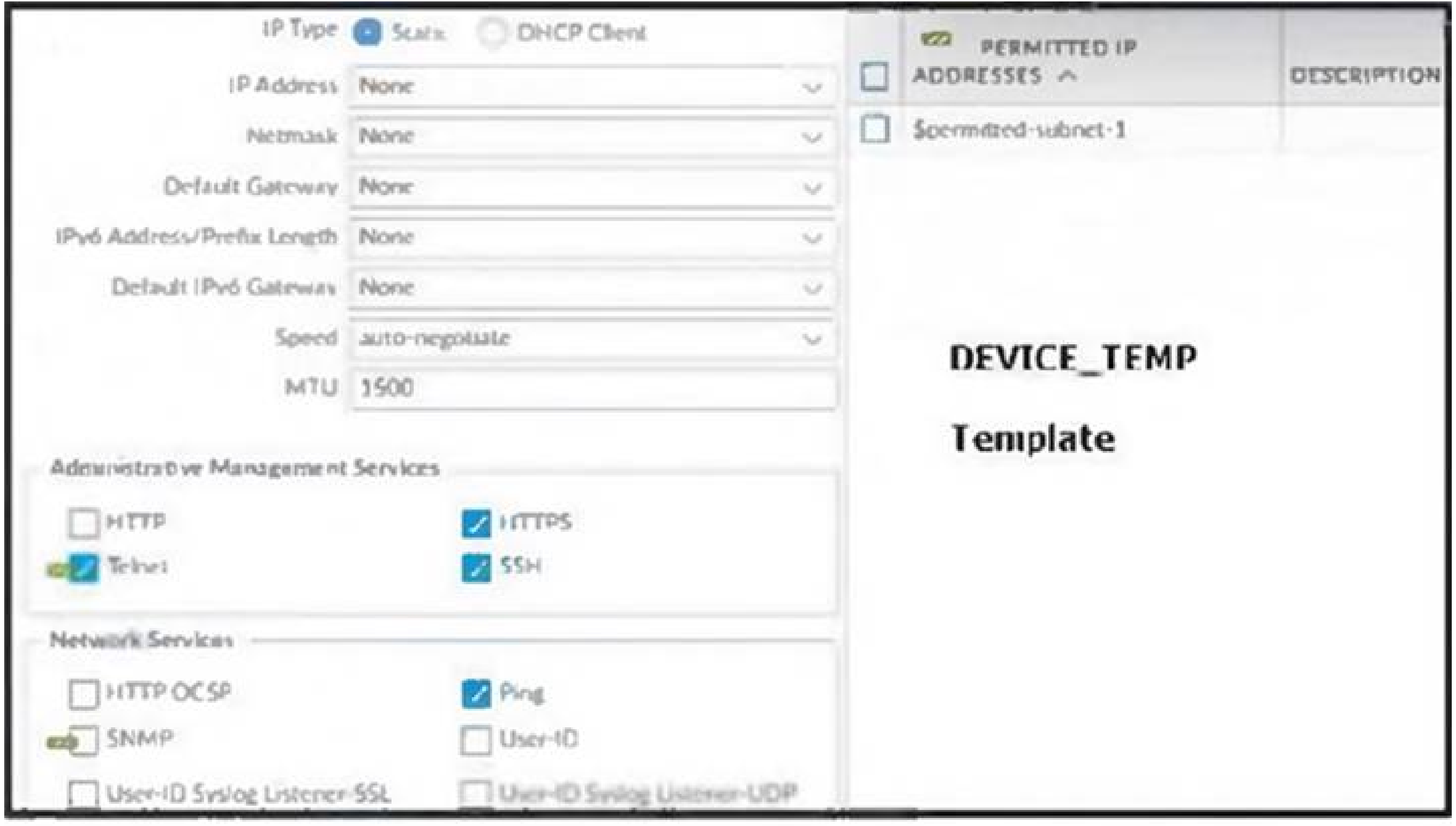
A. The firewall denied the traffic before the application match could be performed.
B. The TCP connection terminated without identifying any application data

C. There was not enough application data after the TCP connection was established
D. The application is not a known Palo Alto Networks App-ID.

Answer: A

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

NEW QUESTION 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

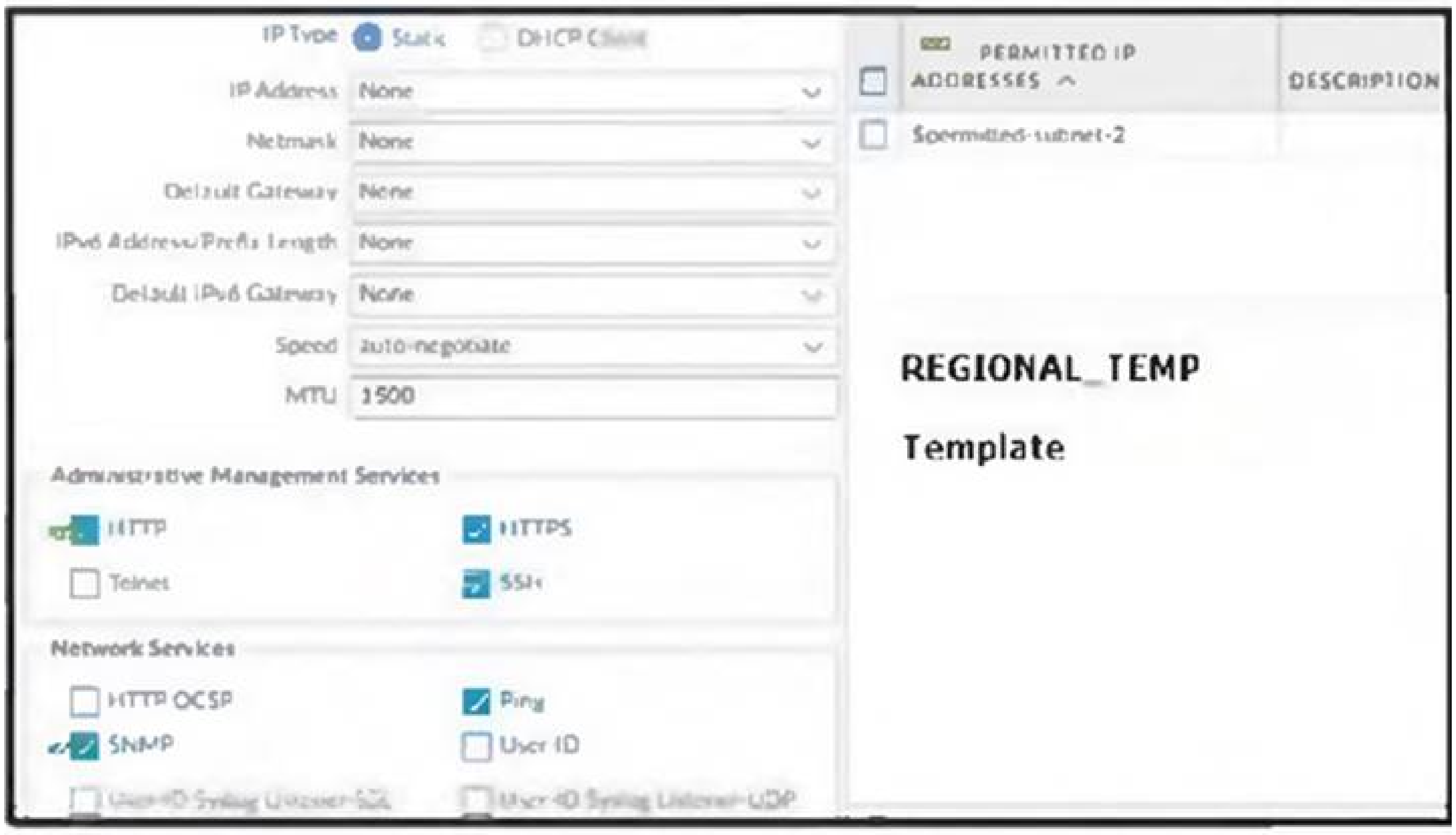
Administrative Management Services
☐ HTTP ☑ HTTPS
☑ Telnet ☑ SSH

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

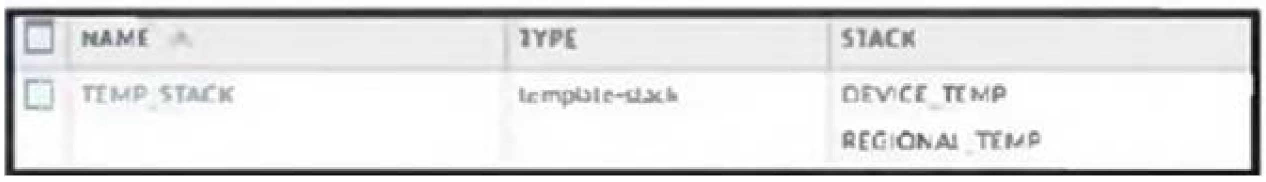
Administrative Management Services
☑ HTTP ☑ HTTPS
☐ Telnet ☑ SSH

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

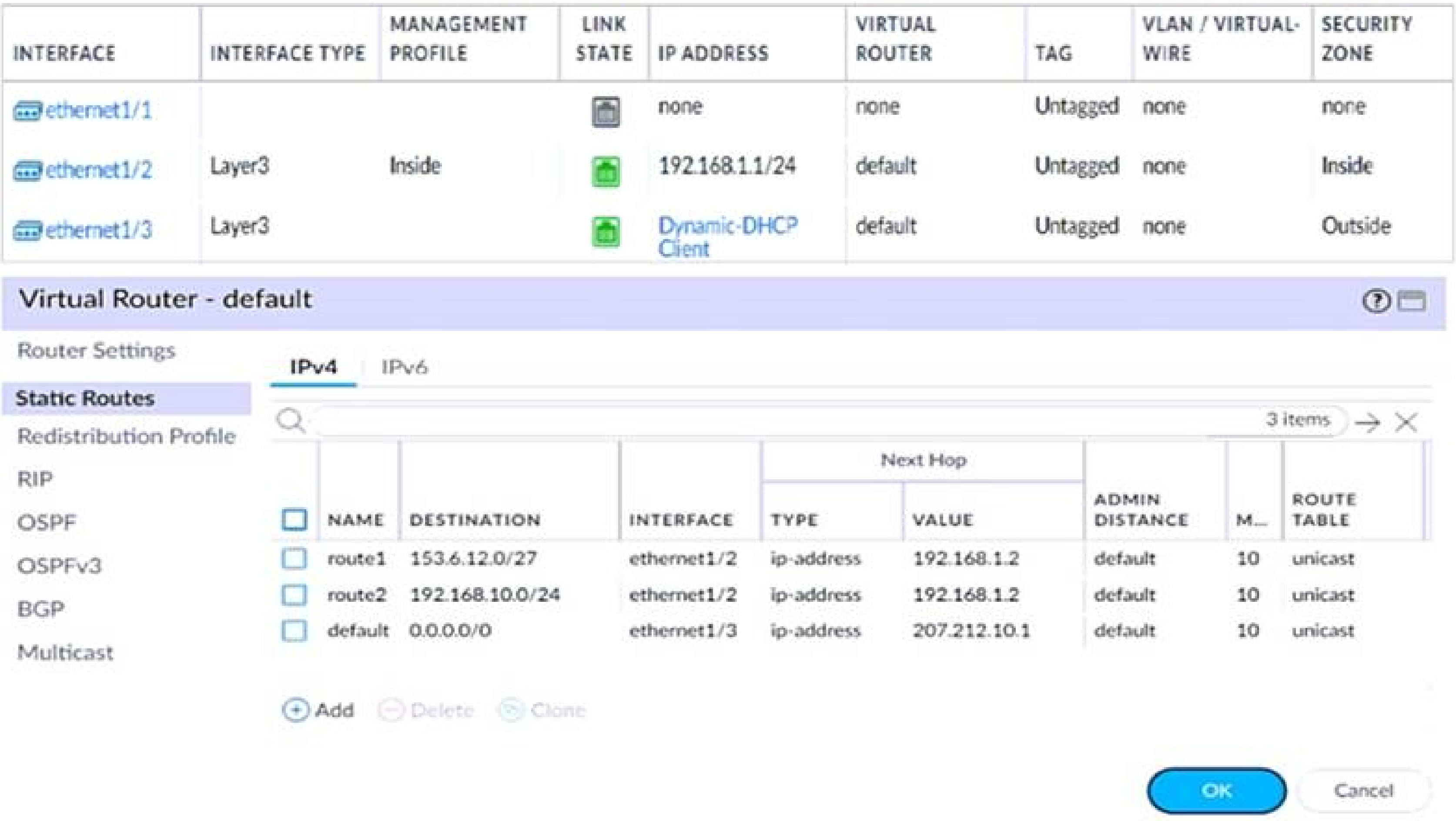
A. The firewall will allow HTTP Telnet, HTTPS, SSH, and Ping from IP addresses defined as$permitted-subnet-1.
B. The firewall will allow HTTP Telnet, HTTPS, SSH, and Ping from IP addresses defined as$permitted-subnet-2.
C. The firewall will allow HTTP, Telnet, SNMP, HTTPS, SSH and Ping from IP addresses 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 19
A firewall engineer creates a destination static NAT rule to allow traffic from the internet to a webserver hosted behind the edge firewall. The pre-NAT IP address of the server is 153.6 12.10, and the post-NAT IP address is 192.168.10.10. Refer to the routing and interfaces information below.



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1			▨	none	none	Untagged	none	none
ethernet1/2	Layer3	Inside	🟩	192.168.1.1/24	default	Untagged	none	Inside
ethernet1/3	Layer3		🟩	Dynamic-DHCP Client	default	Untagged	none	Outside

Virtual Router - default

				Next Hop				
□	NAME	DESTINATION	INTERFACE	TYPE	VALUE	ADMIN DISTANCE	M...	ROUTE TABLE
□	route1	153.6.12.0/27	ethernet1/2	ip-address	192.168.1.2	default	10	unicast
□	route2	192.168.10.0/24	ethernet1/2	ip-address	192.168.1.2	default	10	unicast
□	default	0.0.0.0/0	ethernet1/3	ip-address	207.212.10.1	default	10	unicast

What should the NAT rule destination zone be set to?

A. None
B. Outside
C. DMZ
D. Inside

Answer: B

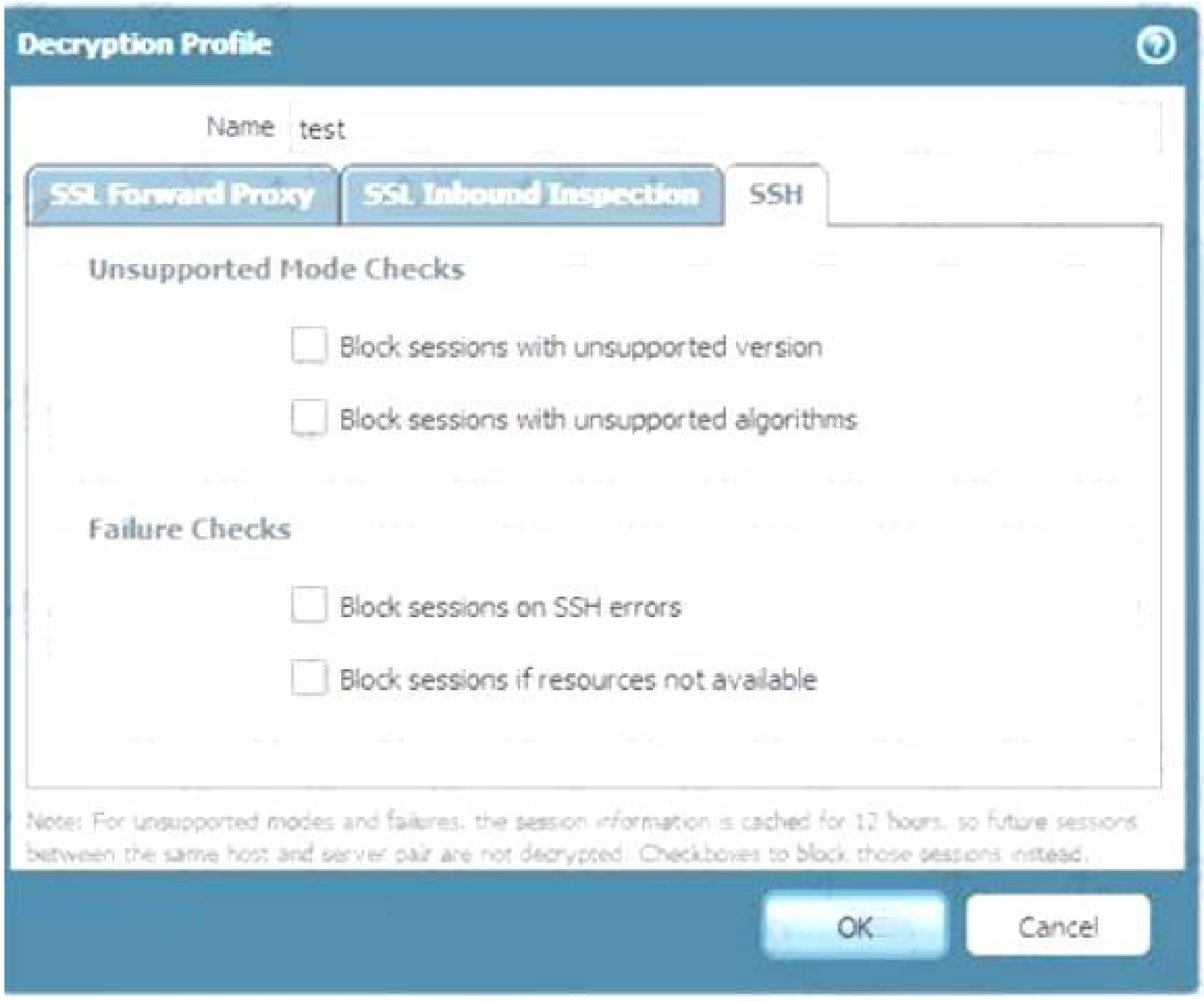
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/nat-configuration-examples/destin

NEW QUESTION 21
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

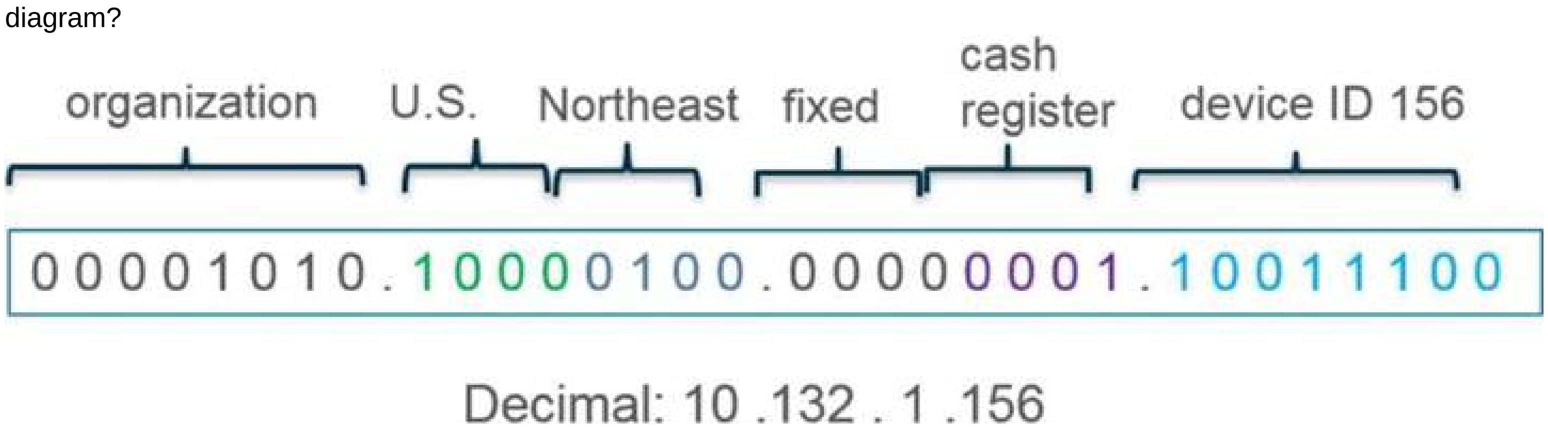
□ Block sessions if resources not available

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.

OK Cancel

NEW QUESTION 24

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?

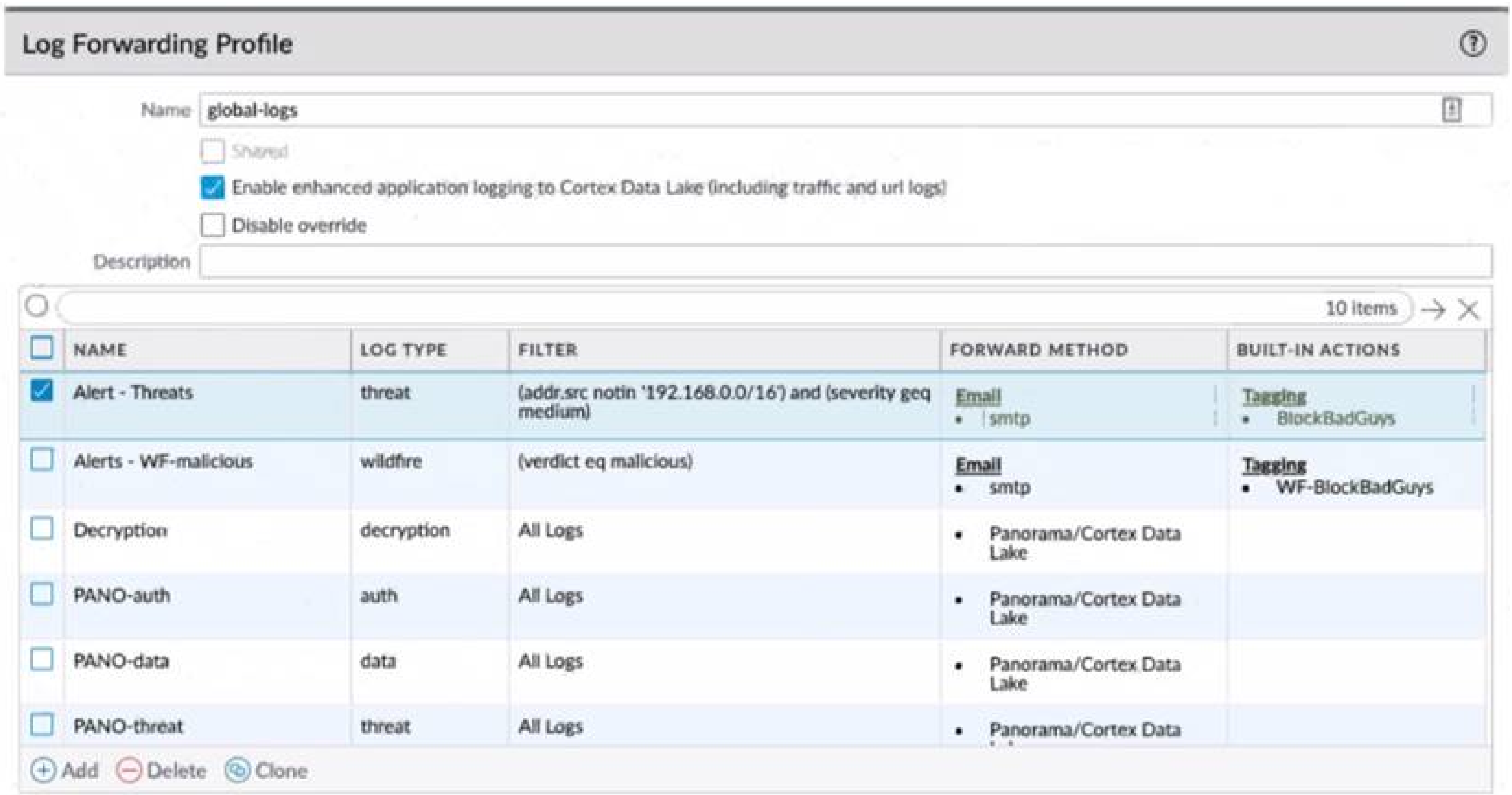


A. IP Netmask
B. IP Wildcard Mask
C. IP Address
D. IP Range

Answer: B

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

NEW QUESTION 28
Review the images.



Log Forwarding Profile

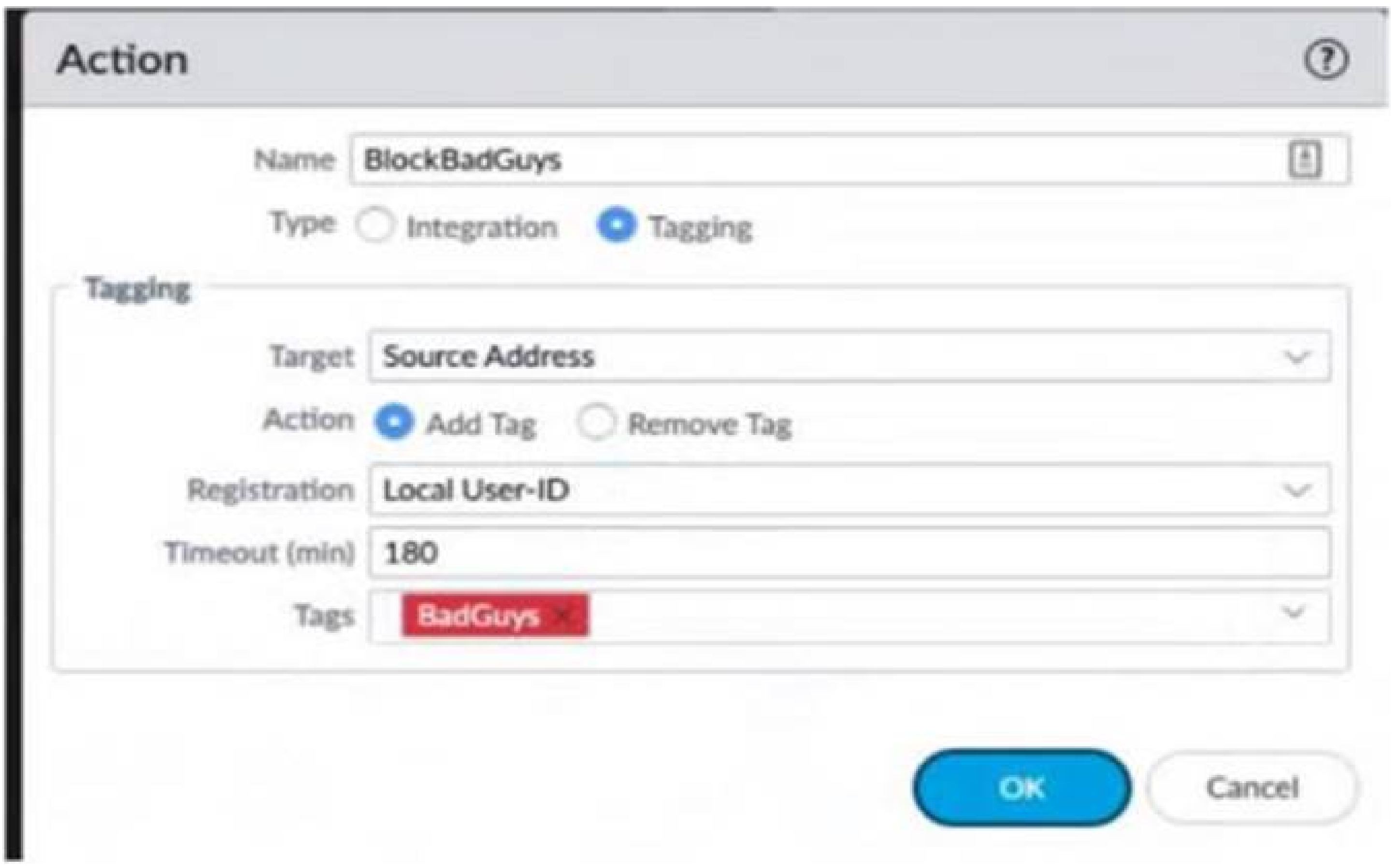
Name: global-logs

☐ 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 33
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

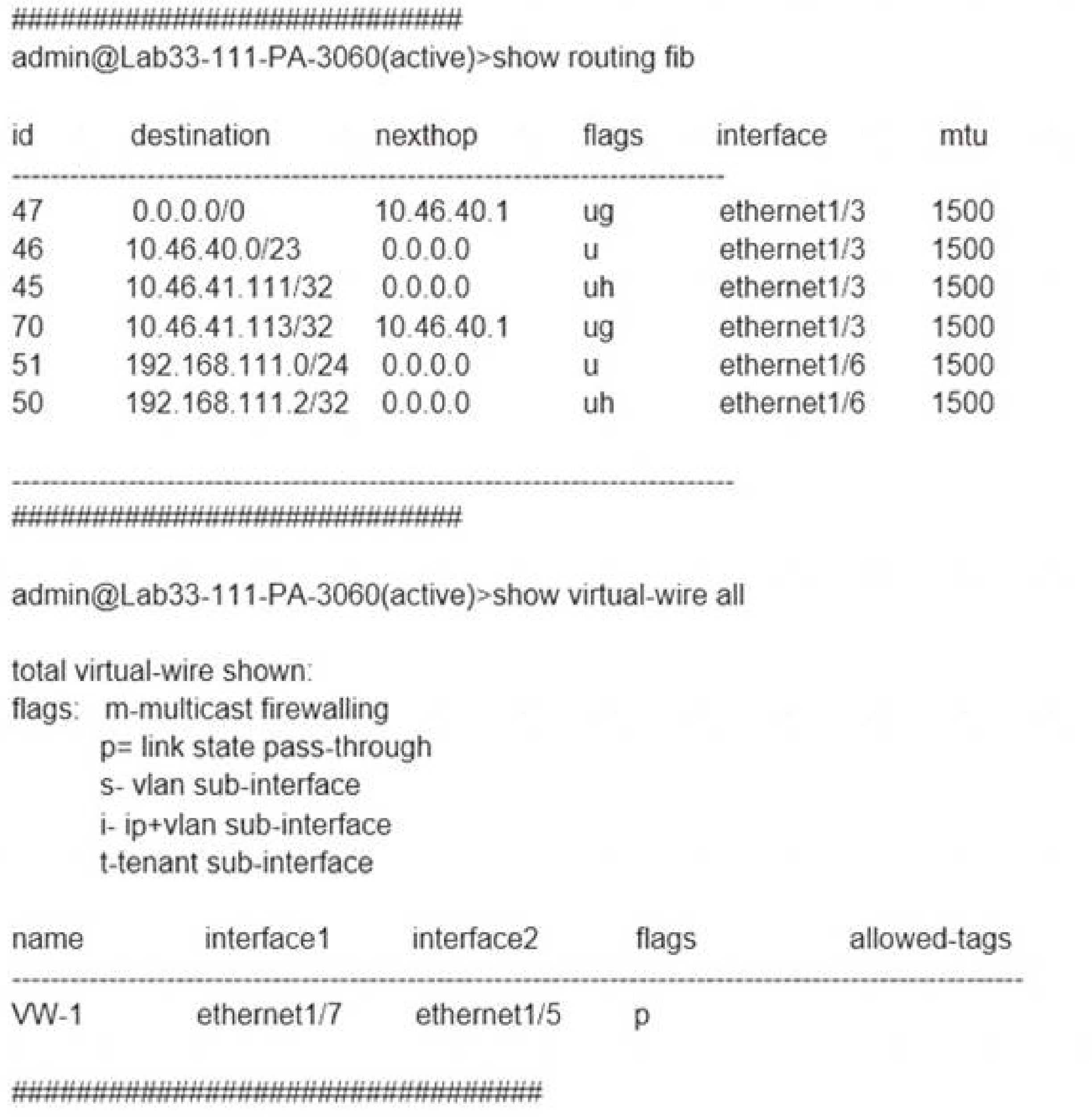
NEW QUESTION 35
A company has configured a URL Filtering profile with override action on their firewall. Which two profiles are needed to complete the configuration? (Choose two)

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 37
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 41
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 44
Which Panorama feature protects logs against data loss if a Panorama server fails?

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

Answer: B

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

NEW QUESTION 45
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 46
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 48
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 52
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 55
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 58
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 63
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 64
What must be configured to apply tags automatically based on User-ID logs?

A. Device ID
B. Log Forwarding profile
C. Group mapping
D. Log settings

Answer: B

Explanation:
To apply tags automatically based on User-ID logs, the engineer must configure a Log Forwarding profile that specifies the criteria for matching the logs and the tags to apply. The Log Forwarding profile can be attached to a security policy rule or a decryption policy rule to enable auto-tagging for the traffic that matches the rule. The tags can then be used for dynamic address groups, policy enforcement, or
reporting1. References: Use Auto-Tagging to Automate Security Actions, PCNSE Study Guide (page 49)

NEW QUESTION 68
Phase two of a VPN will not establish a connection. The peer is using a policy-based VPN configuration. What part of the configuration should the engineer verify?

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

Answer: C

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

NEW QUESTION 72
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.

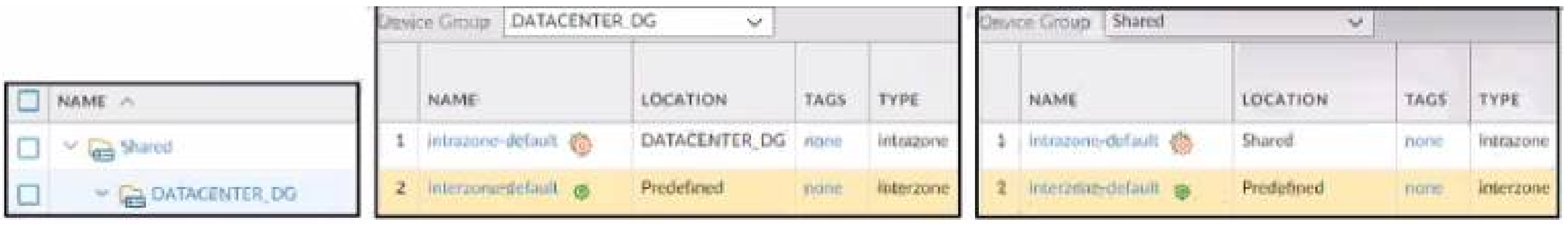
NEW QUESTION 73
A company has recently migrated their branch office's PA-220S to a centralized Panorama. This Panorama manages a number of PA-7000 Series and PA-5200 Series devices All device group and template configuration is managed solely within Panorama
They notice that commit times have drastically increased for the PA-220S after the migration What can they do to reduce commit times?

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

Answer: A

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

NEW QUESTION 78
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 82
The decision to upgrade PAN-OS has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when attempting the install.
When performing an upgrade on Panorama to PAN-OS. what is the potential cause of a failed install?

A. Outdated plugins
B. Global Protect agent version
C. Expired certificates
D. Management only mode

Answer: A

Explanation:
One of the potential causes of a failed install when upgrading Panorama to PAN-OS is having outdated plugins. Plugins are software extensions that enable Panorama to interact with Palo Alto Networks cloud services and third-party services. Plugins have dependencies on specific PAN-OS versions, so they must be updated before or after upgrading Panorama, depending on the plugin compatibility matrix2. If the plugins are not updated accordingly, the upgrade process may fail or cause issues with Panorama
functionality3. References: Panorama Plugins Upgrade/Downgrade Considerations, Troubleshoot Your Panorama Upgrade, PCNSE Study Guide (page 54)

NEW QUESTION 86
Which two factors should be considered when sizing a decryption firewall deployment? (Choose two.)

A. Encryption algorithm
B. Number of security zones in decryption policies
C. TLS protocol version
D. Number of blocked sessions

Answer: AC

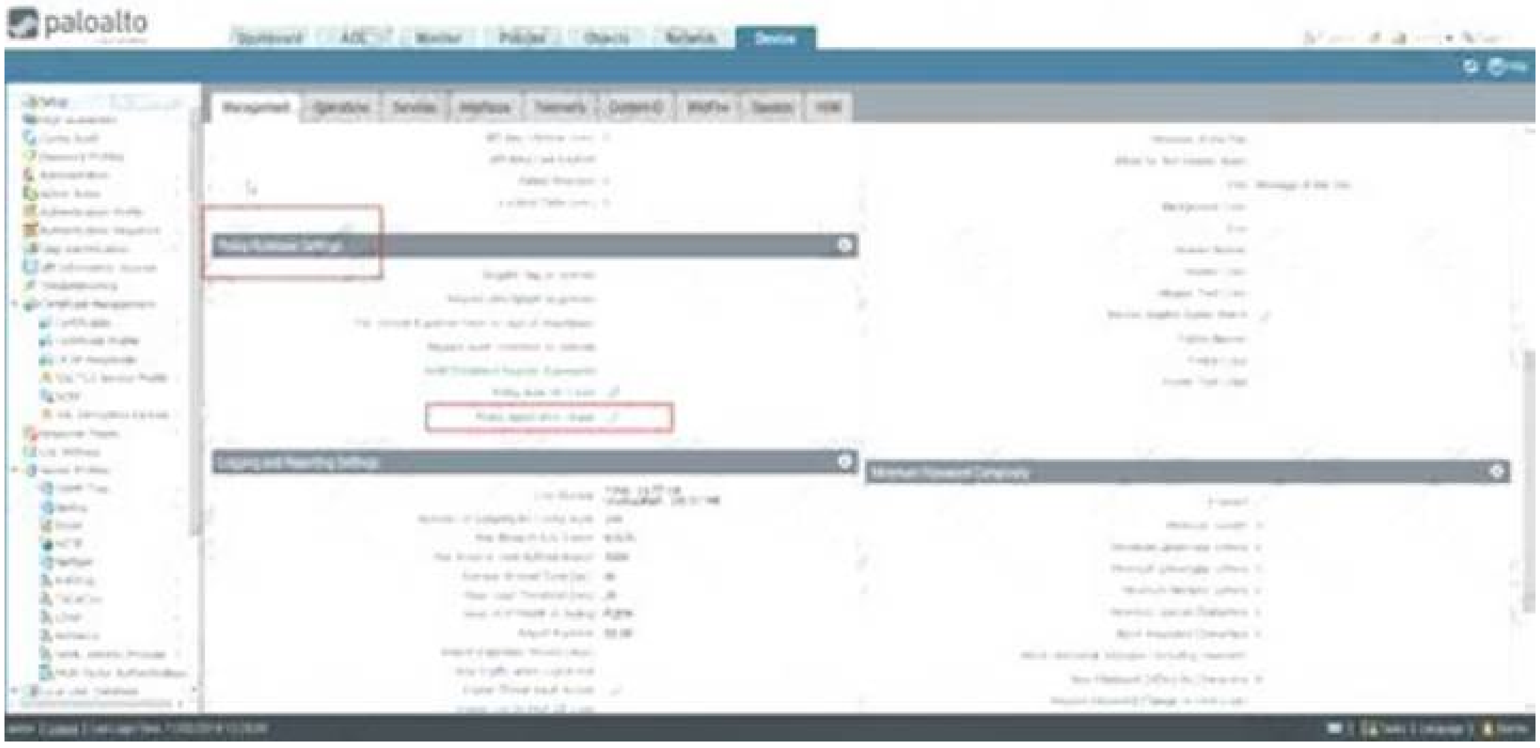
Explanation:
When sizing a decryption firewall deployment, two factors that should be considered are the encryption algorithm and the TLS protocol version. These factors affect the amount of resources and processing power that the firewall needs to decrypt and inspect SSL/TLS traffic.
The encryption algorithm is the method that the server and the client use to encrypt and decrypt the data exchanged in an SSL/TLS session. Different encryption algorithms have different levels of security and performance. For example, AES is a symmetric encryption algorithm that is faster and more efficient than RSA, which is an asymmetric encryption algorithm. However, RSA is more secure than AES because it uses public and private keys to encrypt and decrypt data, while AES uses a single shared key. The firewall must support the encryption algorithms that are used by the servers and clients that it decrypts, and it must have enough CPU and memory resources to handle the decryption workload12.
The TLS protocol version is the standard that defines how the server and the client establish and maintain an SSL/TLS session. Different TLS protocol versions have different features and requirements for encryption algorithms, cipher suites, certificates, handshake messages, etc. For example, TLS 1.3 is the latest and most secure version of TLS, which supports only strong encryption algorithms and cipher suites, such as AES-GCM and ChaCha20-Poly1305, and requires elliptic curve certificates. The firewall must support the TLS protocol versions that are used by the servers and clients that it decrypts, and it must have enough hardware acceleration resources to handle the decryption speed34.
The number of security zones in decryption policies and the number of blocked sessions are not relevant factors for sizing a decryption firewall deployment. The number of security zones in decryption policies only affects how the firewall matches traffic to decryption rules based on source and destination zones, but it does not affect the decryption performance or resource consumption. The number of blocked sessions only indicate how many sessions are denied by the firewall based on security policy or decryption policy rules, but it does not affect the decryption capacity or throughput56.
References: Encryption Algorithms, TLS Protocol Versions, Decryption Policy, PCNSE Study Guide (pag 60)

NEW QUESTION 91
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 92
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

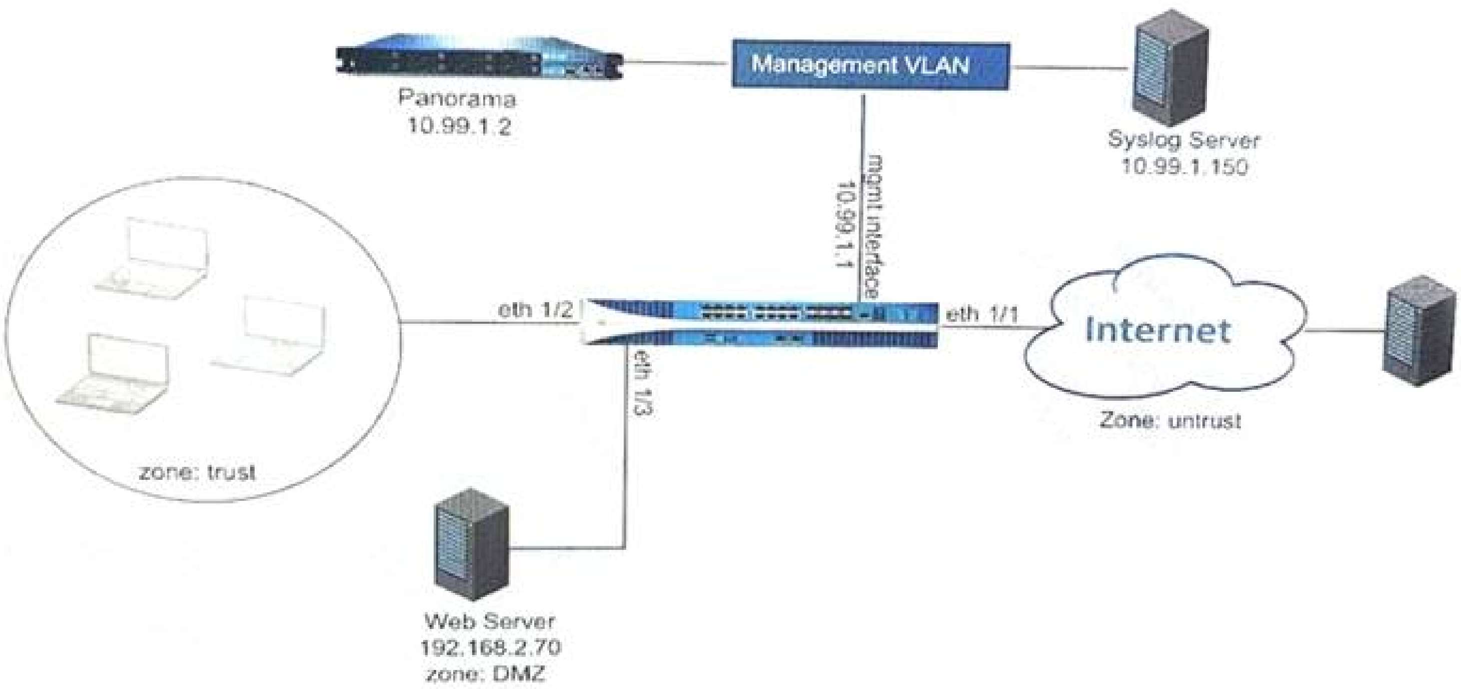
NEW QUESTION 94
A firewall engineer reviews the PAN-OS GlobalProtect application and sees that it implicitly uses web-browsing and depends on SSL.
When creating a new rule, what is needed to allow the application to resolve dependencies?

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

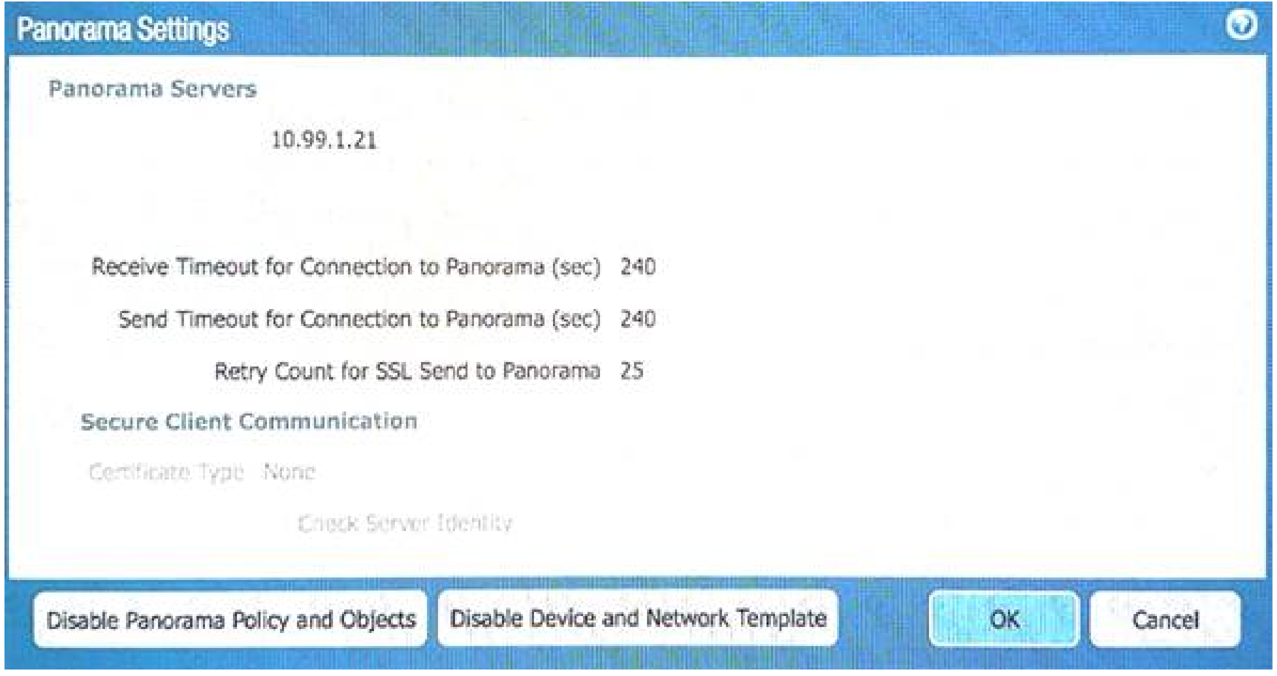
Explanation:
'Implicitly Uses' has web-browsing listed. This means that if you allow facebook-posting, that it will also be allowing the web-browsing application implicitly.. In our case, we dont know which APP the question referes too but 'Implicitly means already uses HTTP.

NEW QUESTION 97
Refer to Exhibit:



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

A)



Panorama Settings

Panorama Servers

10.99.1.21

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

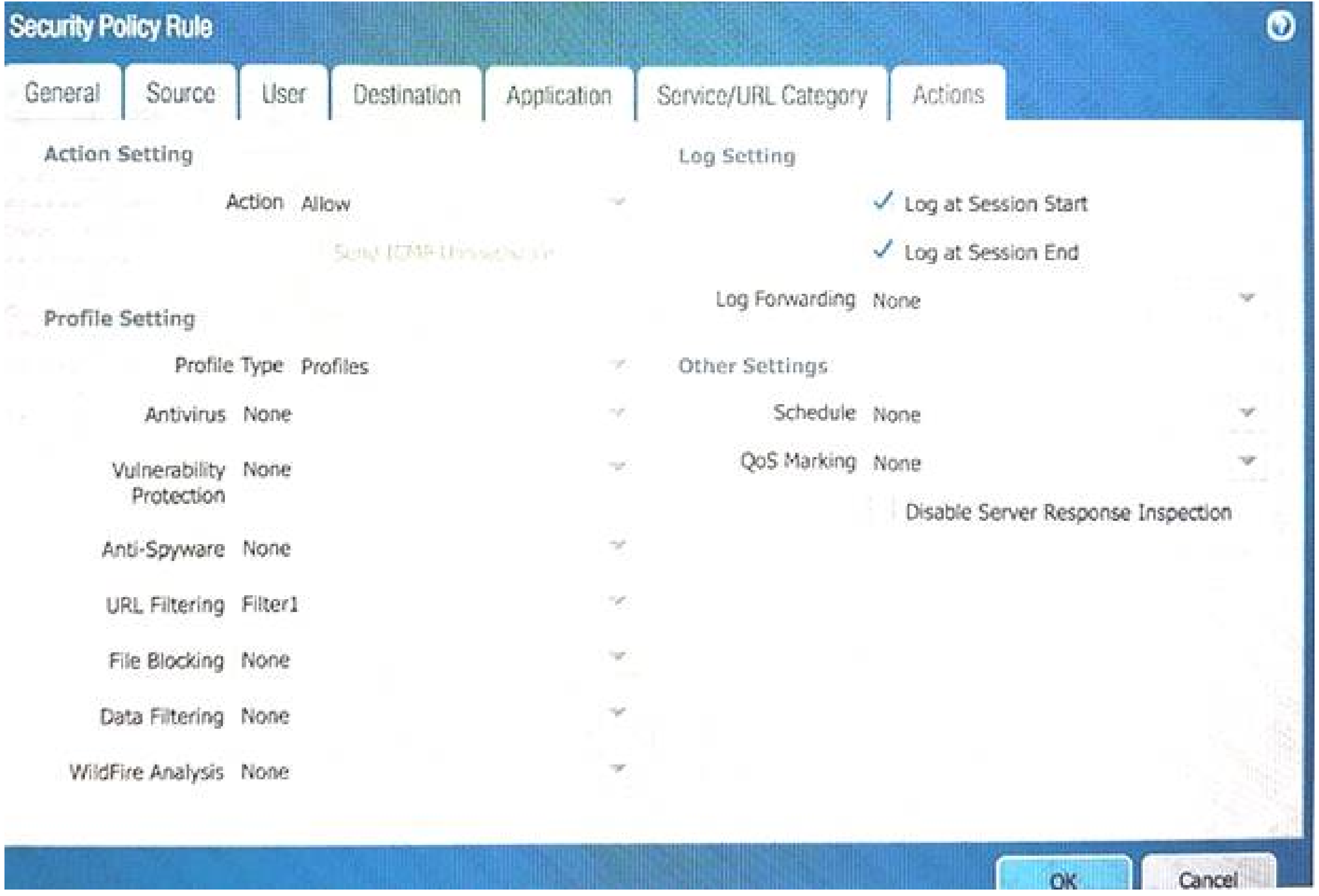
Secure Client Communication

Certificate Type None

Check Server Identity

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

B)



Security Policy Rule

Action Setting

Action Allow

Send ICMP Unreachable

Profile Setting

Profile Type Profiles

Antivirus None

Vulnerability Protection None

Anti-Spyware None

URL Filtering Filter1

File Blocking None

Data Filtering None

WildFire Analysis None

Log Setting

✓ Log at Session Start

✓ Log at Session End

Log Forwarding None

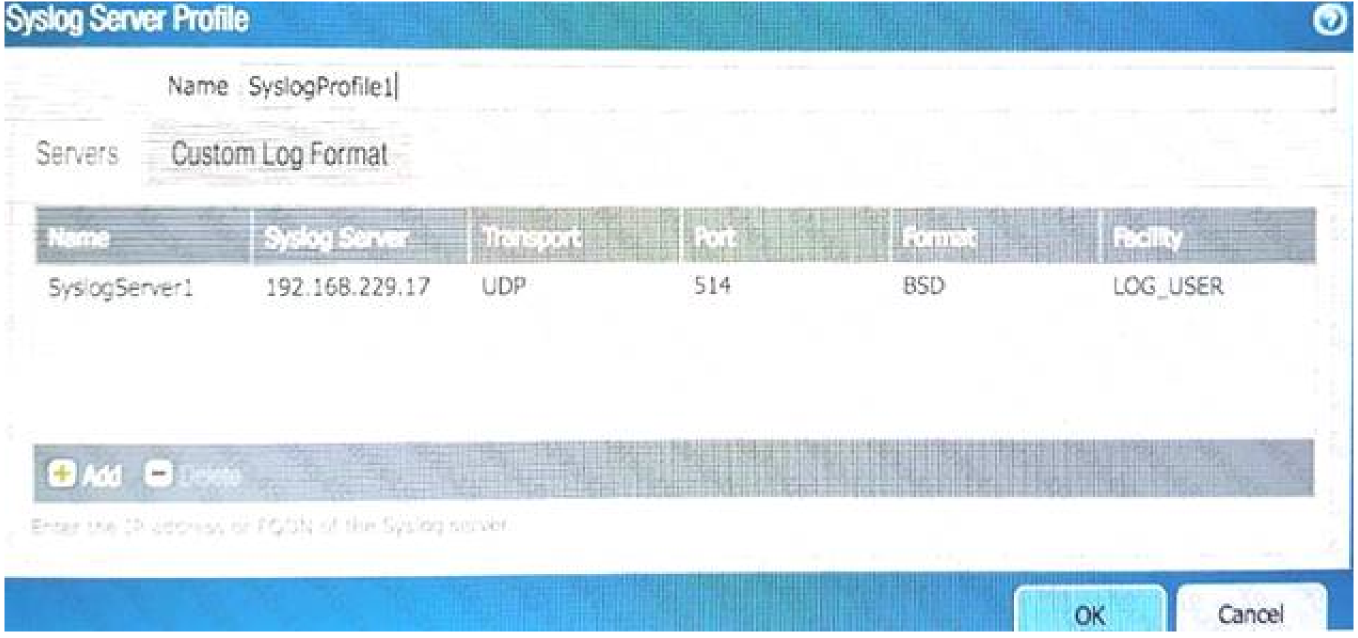
Other Settings

Schedule None

QoS Marking None

□ Disable Server Response Inspection

C)



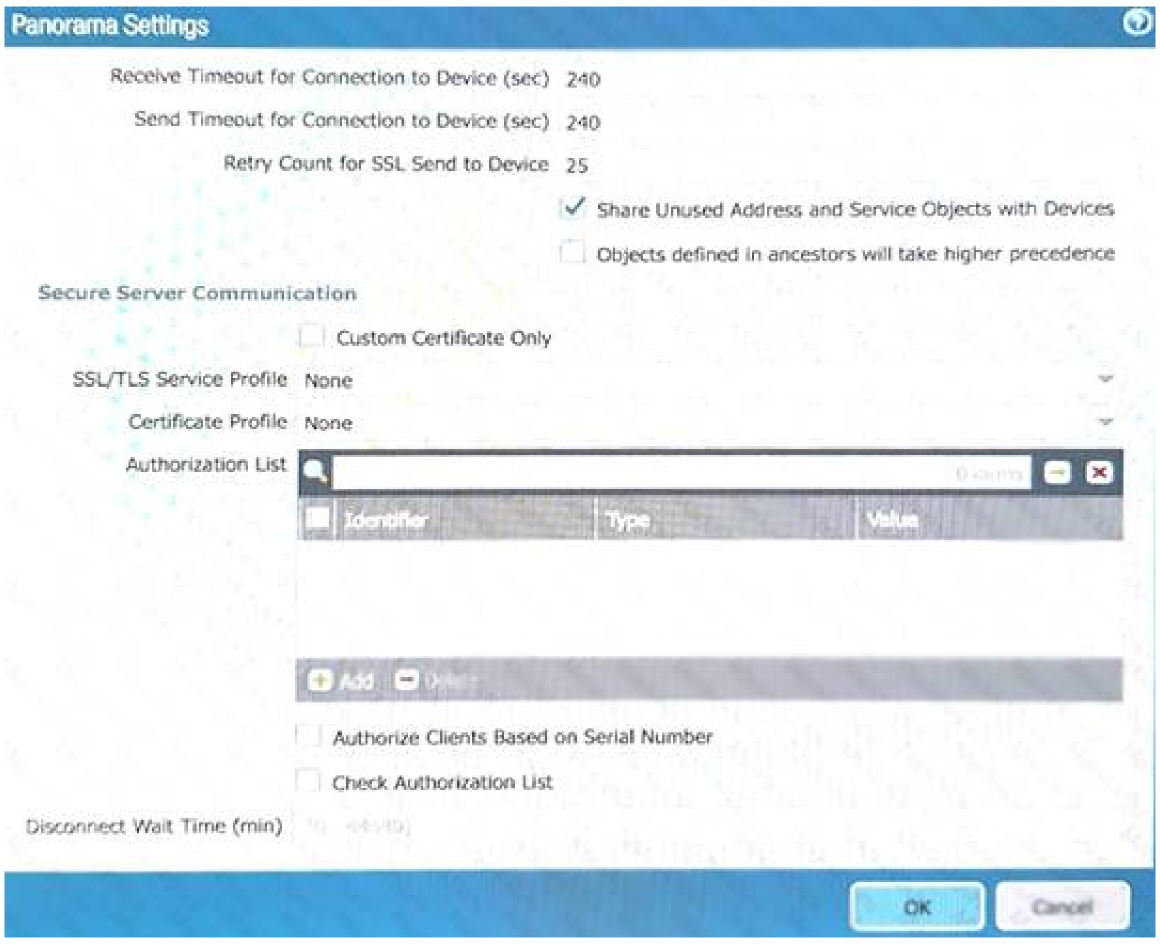
Syslog Server Profile

Name SyslogProfile1

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

Enter the IP address or FQDN of the Syslog server

D)



Panorama Settings

Receive Timeout for Connection to Device (sec) 240

Send Timeout for Connection to Device (sec) 240

Retry Count for SSL Send to Device 25

☑ Share Unused Address and Service Objects with Devices

□ Objects defined in ancestors will take higher precedence

Secure Server Communication

□ Custom Certificate Only

SSL/TLS Service Profile None

Certificate Profile None

Authorization List

□	Identifier	Type	Value

□ Authorize Clients Based on Serial Number

□ Check Authorization List

Disconnect Wait Time (min)

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

Answer: C

NEW QUESTION 101
Which new PAN-OS 11.0 feature supports IPv6 traffic?

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

Answer: A

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

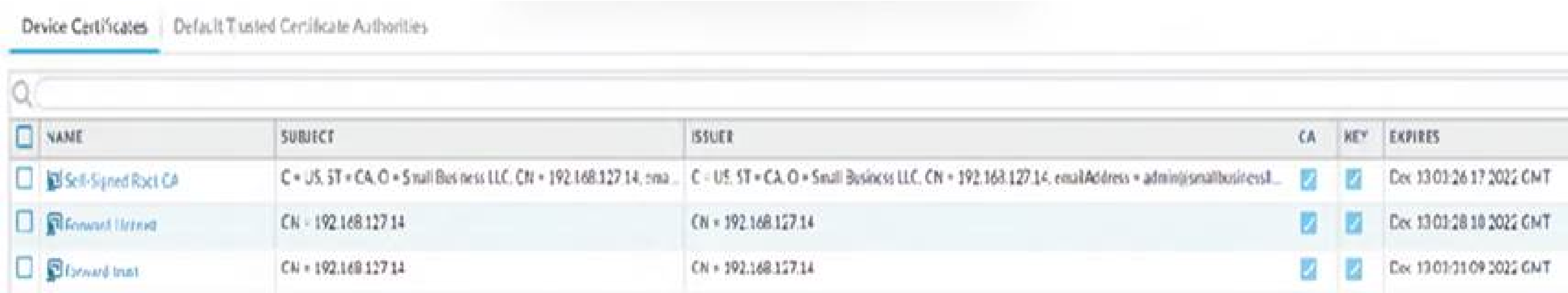
NEW QUESTION 103
An administrator has purchased WildFire subscriptions for 90 firewalls globally. What should the administrator consider with regards to the WildFire infra-structure?

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 108
Review the screenshot of the Certificates page.



Device Certificates | Default Trusted Certificate Authorities

□	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES
□	Self-Signed Root CA	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.14, ema...	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.14, emailAddress = admin@smallbusinessll...	☑	☑	Dec 13 03:26:17 2022 GMT
□	Forward Untrust	CN = 192.168.127.14	CN = 192.168.127.14	☑	☑	Dec 13 03:28:10 2022 GMT
□	Forward trust	CN = 192.168.127.14	CN = 192.168.127.14	☑	☑	Dec 13 03:31:09 2022 GMT

An administrator for a small LLC has created a series of certificates as shown, to use for a planned Decryption roll out. The administrator has also installed the self-signed root certificate in all client systems.

When testing, they noticed that every time a user visited an SSL site, they received unsecured website warnings.
What is the cause of the unsecured website warnings?

A. The forward untrust certificate has not been signed by the self-singed root CA certificate.
B. The forward trust certificate has not been installed in client systems.
C. The self-signed CA certificate has the same CN as the forward trust and untrust certificates.
D. The forward trust certificate has not been signed by the self-singed root CA certificate.

Answer: D

Explanation:
The cause of the unsecured website warnings is that the forward trust certificate has not been signed by the self-signed root CA certificate. The forward trust certificate is used by the firewall to generate a copy of the server certificate for outbound SSL decryption (SSL Forward Proxy). The firewall signs the copy with the forward trust certificate and presents it to the client. The client then verifies the signature using the public key of the CA that issued the forward trust certificate. If the client does not trust the CA, it will display a warning message. Therefore, the forward trust certificate must be signed by a CA that is trusted by the client. In this case, the administrator has installed the self-signed root CA certificate in all client systems, so this CA should be used to sign the forward trust certificate. However, as shown in the screenshot, the forward trust certificate has a different issuer than the self-signed root CA certificate, which means it has not been signed by it. This causes the client to reject the signature and show a warning message. To fix this issue, the administrator should generate a new forward trust certificate and sign it with the self-signed root CA certificate12. References: Keys and Certificates for Decryption Policies, How to Configure SSL Decryptio

NEW QUESTION 109
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 111
......