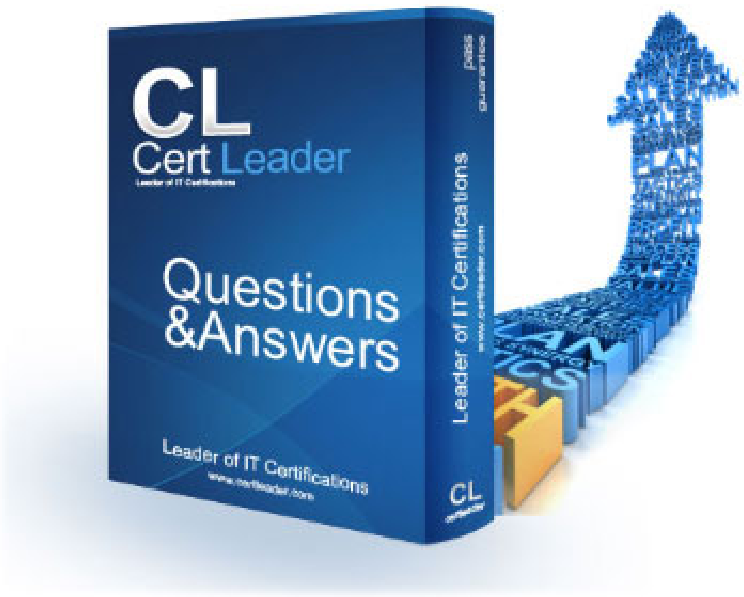
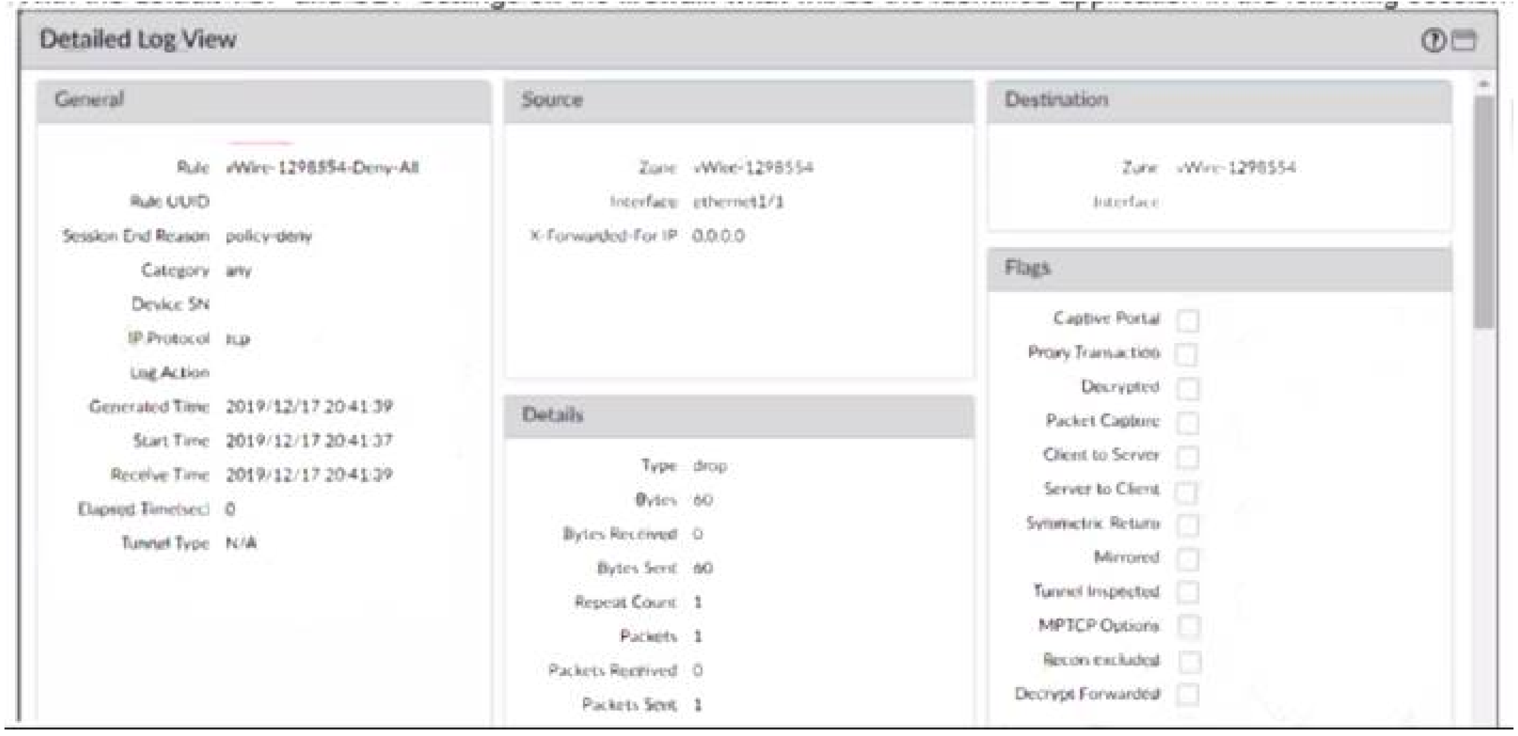
PCNSE Dumps

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

https://www.certleader.com/PCNSE-dumps.html



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



Detailed Log View

General

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

Source

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

Details

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

Destination

Zone vWire-1298554
Interface

Flags

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

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

Answer: D

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

NEW QUESTION 2
A firewall engineer creates a NAT rule to translate IP address 1.1.1.10 to 192.168.1.10. The engineer also plans to enable DNS rewrite so that the firewall rewrites the IPv4 address in a DNS response based on the original destination IP address and translated destination IP address configured for the rule. The engineer wants the firewall to rewrite a DNS response of 1.1.1.10 to 192.168.1.10.
What should the engineer do to complete the configuration?

A. Create a U-Turn NAT to translate the destination IP address 192.168.1.10 to 1.1.1.10 with the destination port equal to UDP/53.
B. Enable DNS rewrite under the destination address translation in the Translated Packet section of the NAT rule with the direction Forward.
C. Enable DNS rewrite under the destination address translation in the Translated Packet section of the NAT rule with the direction Reverse.
D. Create a U-Turn NAT to translate the destination IP address 1.1.1.10 to 192.168.1.10 with the destination port equal to UDP/53.

Answer: B

Explanation:
If the DNS response matches the Original Destination Address in the rule, translate the DNS response using the same translation the rule uses. For example, if the rule translates IP address 1.1.1.10 to 192.168.1.10, the firewall rewrites a DNS response of 1.1.1.10 to 192.168.1.10.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/source-nat-and-destination-nat/desti

NEW QUESTION 3
A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours.
Which two steps are likely to mitigate the issue? (Choose TWO)

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

Answer: AC

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

NEW QUESTION 4
After implementing a new NGFW, a firewall engineer sees a VoIP traffic issue going through the firewall After troubleshooting the engineer finds that the firewall performs NAT on the voice packets payload and opens dynamic pinholes for media ports
What can the engineer do to solve the VoIP traffic issue?

A. Disable ALG under H.323 application
B. Increase the TCP timeout under H.323 application
C. Increase the TCP timeout under SIP application
D. Disable ALG under SIP application

Answer: D

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/disable-the-sip-application-level-gateway-a

NEW QUESTION 5
An administrator is attempting to create policies tor deployment of a device group and template stack. When creating the policies, the zone drop down list does not include the required zone.
What must the administrator do to correct this issue?

A. Specify the target device as the master device in the device group
B. Enable "Share Unused Address and Service Objects with Devices" in Panorama settings
C. Add the template as a reference template in the device group
D. Add a firewall to both the device group and the template

Answer: C

Explanation:
In order to see what is in a template, the device-group needs the template referenced. Even if you add the firewall to both the template and device-group, the device-group will not see what is in the template. The following link has a video that demonstrates that B is the correct answer.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNfeCAG

NEW QUESTION 6
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 7
Which statement about High Availability timer settings is true?

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

Answer: D

Explanation:
Recommended: Use for typical failover timer settings. Unless you're sure that you need different settings, the best practice is to use the Recommended settings.
Aggressive: Use for faster failover timer settings.
Advanced: Allows you to customize the values to suit your network requirement for each of the following timers:

NEW QUESTION 8
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)

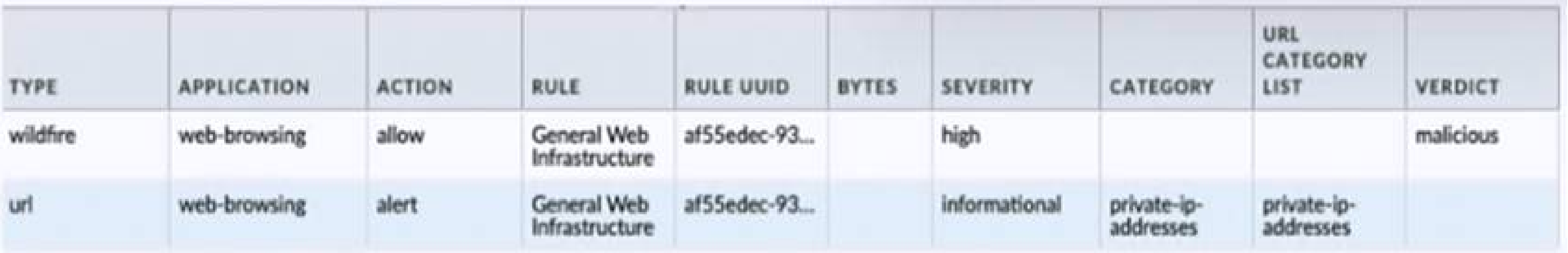
NEW QUESTION 9
In a security-first network, what is the recommended threshold value for apps and threats to be dynamically updated?

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 10
Given the following snippet of a WildFire submission log did the end-user get access to the requested information and why or why not?



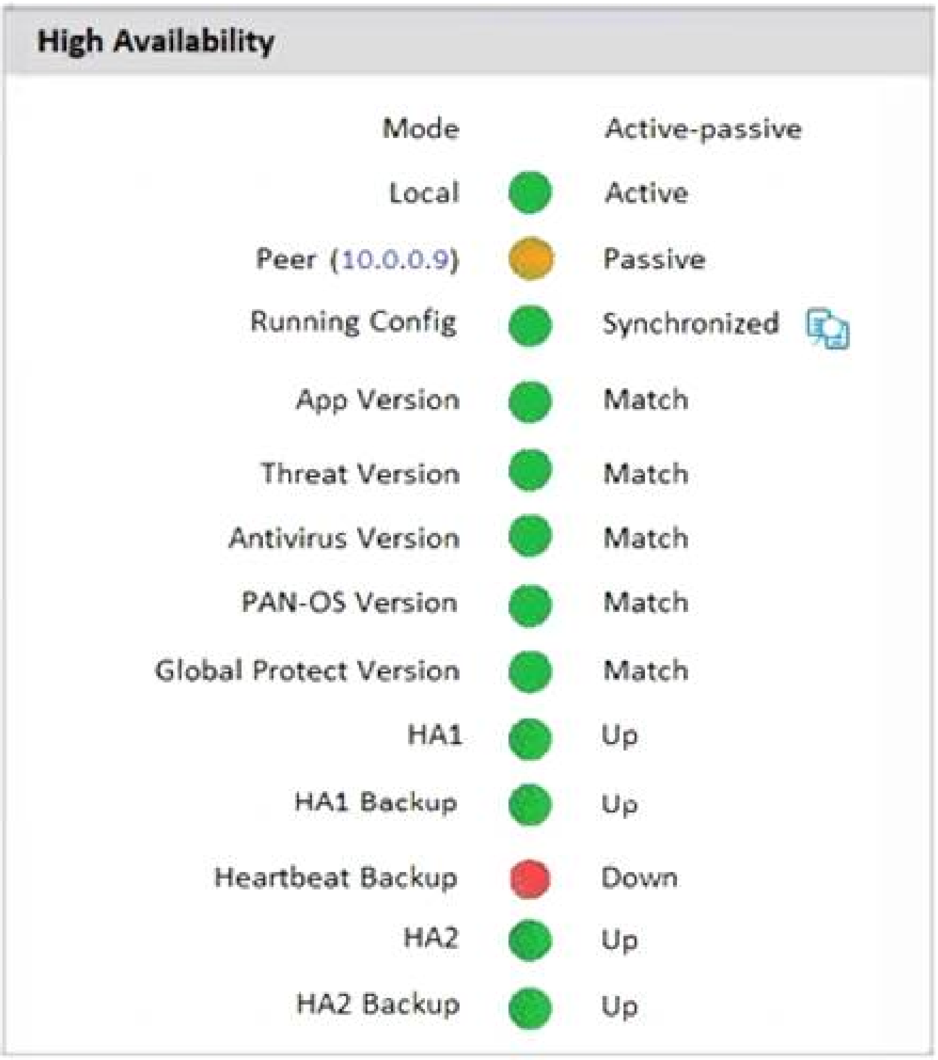
TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	web-browsing	allow	General Web Infrastructure	af55edec-93...		high			malicious
url	web-browsing	alert	General Web Infrastructure	af55edec-93...		informational	private-ip-addresses	private-ip-addresses	

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

Answer: D

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

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



High Availability

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

What could an administrator do to troubleshoot the issue?

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

Answer: B

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

NEW QUESTION 13
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 15
Which two policy components are required to block traffic in real time using a dynamic user group (DUG)? (Choose two.)

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

Answer: AB

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

NEW QUESTION 16
An engineer is configuring a firewall with three interfaces:
• MGT connects to a switch with internet access.
• Ethernet1/1 connects to an edge router.
• Ethernet1/2 connects to a visualization network.
The engineer needs to configure dynamic updates to use a dataplane interface for internet traffic. What should be configured in Setup > Services > Service Route Configuration to allow this traffic?

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

Answer: A

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

NEW QUESTION 21
An engineer troubleshoots a Panorama-managed firewall that is unable to reach the DNS servers configured via a global template. As a troubleshooting step, the engineer needs to configure a local DNS server in place of the template value.
Which two actions can be taken to ensure that only the specific firewall is affected during this process? (Choose two)

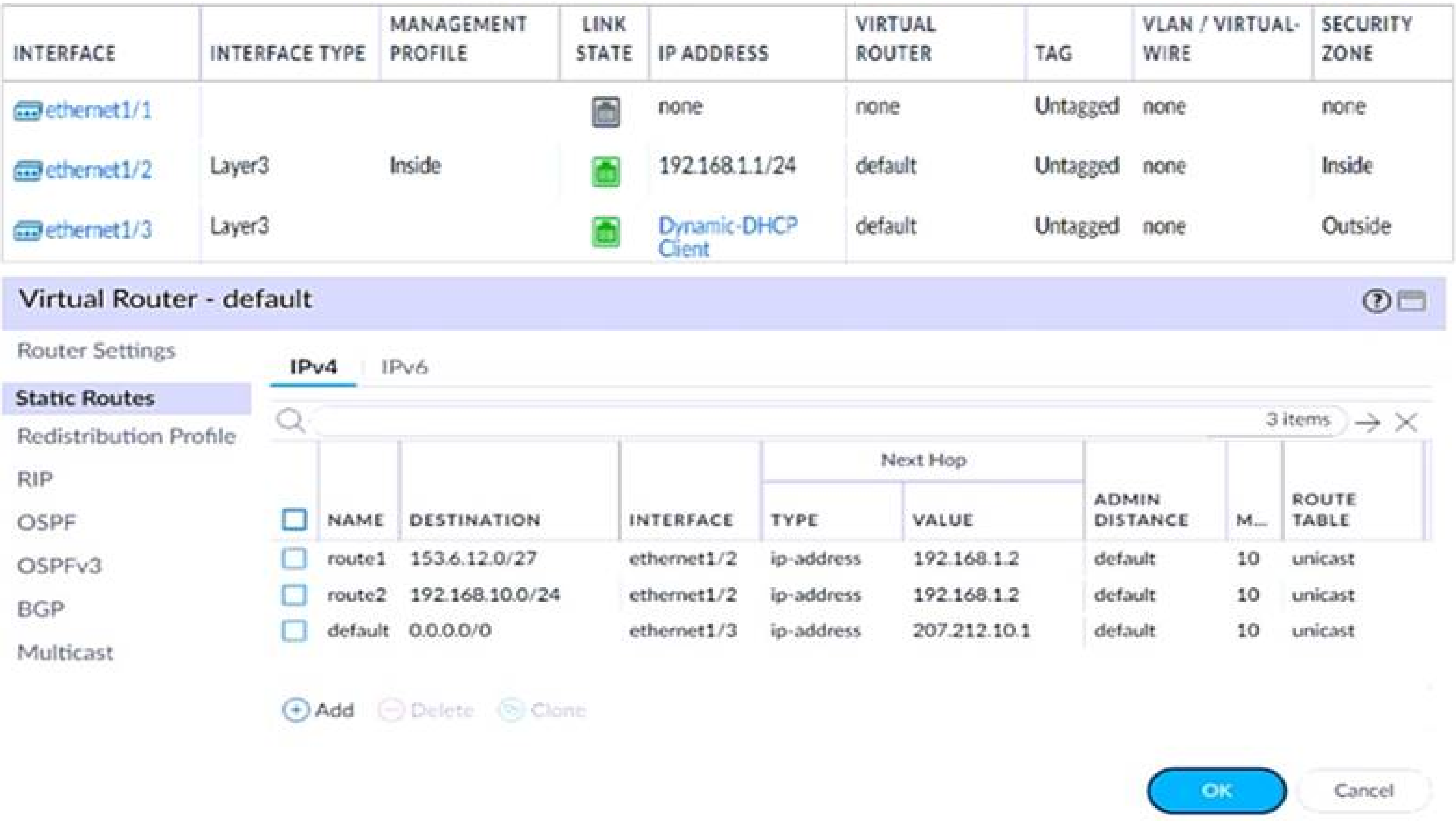
A. Configure the DNS server locally on the firewall.
B. Change the DNS server on the global template.
C. Override the DNS server on the template stack.
D. Configure a service route for DNS on a different interface.

Answer: AC

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

- Override a Template Setting
- Overriding Panorama Template settings

NEW QUESTION 22
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 23
A network administrator wants to deploy SSL Forward Proxy decryption. What two attributes should a forward trust certificate have? (Choose two.)

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

Answer: BD

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

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

NEW QUESTION 25
A network security administrator has been tasked with deploying User-ID in their organization. What are three valid methods of collecting User-ID information in a network? (Choose three.)

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

Answer: ABC

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

- A: Windows User-ID agent: A software agent that runs on a Windows server and collects user information from Active Directory domain controllers, Exchange servers, or eDirectory servers2. The agent then sends the user information to the firewall or Panorama for user mapping2.
- B: GlobalProtect: A software agent that runs on the endpoints and provides secure VPN access to the network3. GlobalProtect also collects user information from the endpoints and sends it to the firewall or Panorama for user mapping4.
- C: XMLAPI: An application programming interface that allows external systems or scripts to send user information to the firewall or Panorama in XML format.

The XMLAPI can be used to integrate with third-party systems, such as identity providers, captive portals, or custom applications.

NEW QUESTION 26
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 30
A network administrator configured a site-to-site VPN tunnel where the peer device will act as initiator None of the peer addresses are known
What can the administrator configure to establish the VPN connection?

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

Answer: B

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

NEW QUESTION 34
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 36
An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Link and Path Monitoring is enabled with the Failure Condition set to "any." There is one link group configured containing member interfaces ethernet1/1 and ethernet1/2 with a Group Failure Condition set to "all."
Which HA state will the Active firewall go into if ethernet1/1 link goes down due to a failure?'

A. Active-Secondary
B. Non-functional
C. Passive
D. Active

Answer: D

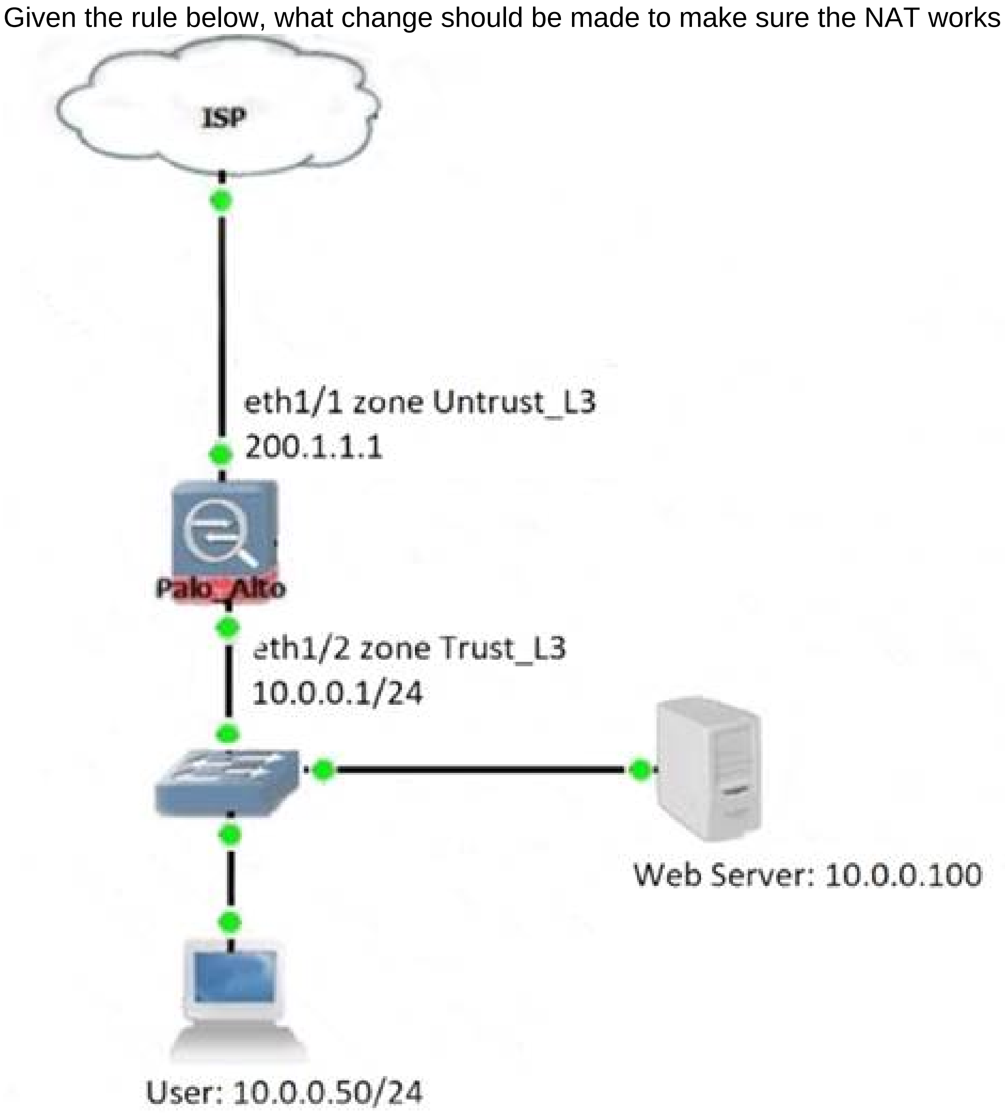
NEW QUESTION 40
An administrator has configured OSPF with Advanced Routing enabled on a Palo Alto Networks firewall running PAN-OS 10.2. After OSPF was configured, the administrator noticed that OSPF routes were not being learned.
Which two actions could an administrator take to troubleshoot this issue?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

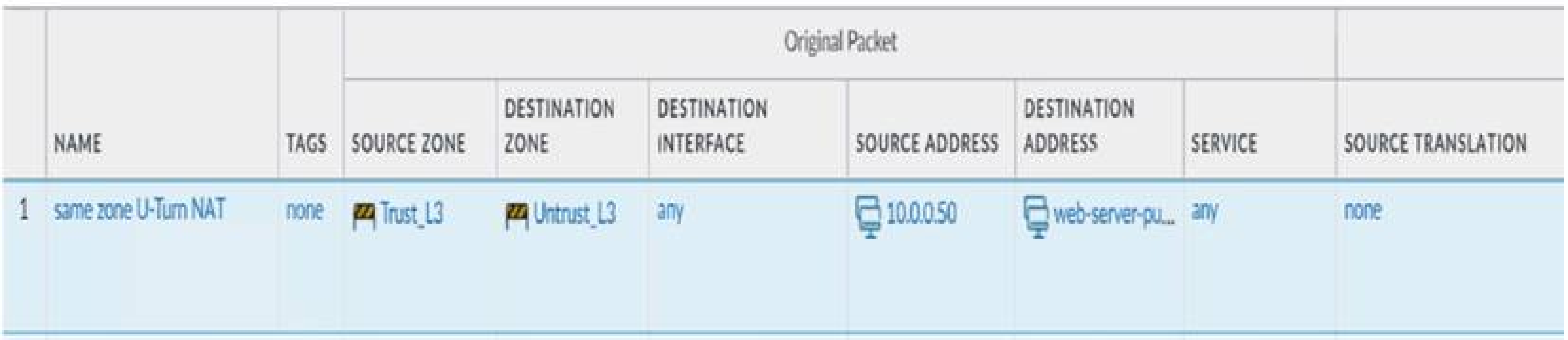
A. Run the CLI command show advanced-routing ospf neighbor
B. In the WebUI, view the Runtime Stats in the virtual router
C. Look for configuration problems in Network > virtual router > OSPF
D. In the WebUI, view Runtime Stats in the logical router

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 42
Review the information below. A firewall engineer creates a U-NAT rule to allow users in the trust zone access to a server in the same zone by using an external, public NAT IP for that server.
Given the rule below, what change should be made to make sure the NAT works as expected?





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

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

Answer: D

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

NEW QUESTION 43
An administrator is receiving complaints about application performance degradation. After checking the ACC, the administrator observes that there is an excessive amount of VoIP traffic.
Which three elements should the administrator configure to address this issue? (Choose three.)

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

Answer: BDE

Explanation:
To address the issue of application performance degradation due to excessive VoIP traffic, the administrator should configure QoS on the egress interface for the traffic flows and a QoS profile defining traffic classes. QoS stands for Quality of Service, which is a feature that allows the firewall to manage bandwidth usage and

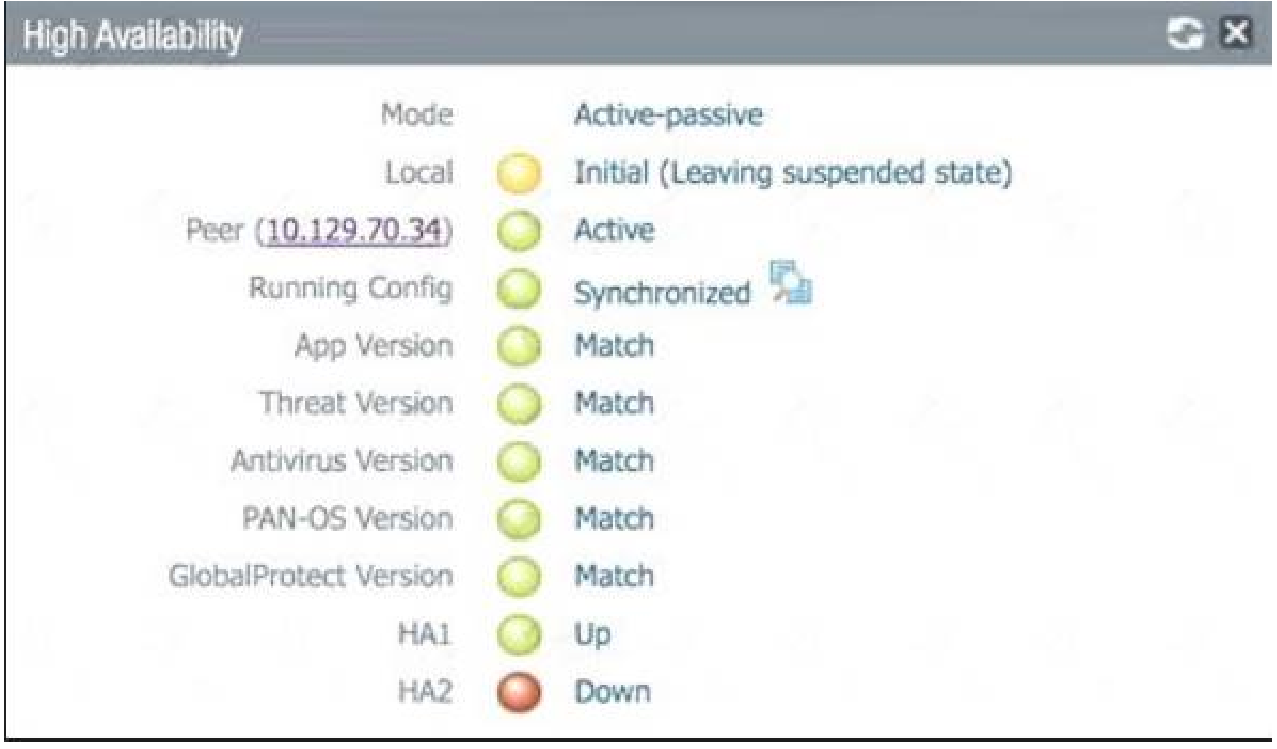
prioritize traffic based on various criteria, such as application, user, service, etc. QoS can help improve the performance and quality of latency-sensitive applications, such as VoIP, by guaranteeing them sufficient bandwidth and priority over other traffic1.
To enable QoS on the firewall, the administrator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

NEW QUESTION 45
An engineer is monitoring an active/active high availability (HA) firewall pair.
Which HA firewall state describes the firewall that is experiencing a failure of a monitored path?

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

Answer: B

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



High Availability

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

NEW QUESTION 49
A network security administrator wants to begin inspecting bulk user HTTPS traffic flows egressing out of the internet edge firewall. Which certificate is the best choice to configure as an SSL Forward Trust certificate?

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

Answer: D

Explanation:
Regardless of whether you generate Forward Trust certificates from your Enterprise Root CA or use a
self-signed certificate generated on the firewall, generate a separate subordinate Forward Trust CA certificate for each firewall. The flexibility of using separate subordinate CAs enables you to revoke one certificate when you decommission a device (or device pair) without affecting the rest of the deployment and reduces the impact in any situation in which you need to revoke a certificate. Separate Forward Trust CAs on each firewall also helps troubleshoot issues because the CA

error message the user sees includes information about the firewall the traffic is traversing. If you use the same Forward Trust CA on every firewall, you lose the granularity of that information.
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy

NEW QUESTION 51
An administrator receives the following error message:
"IKE phase-2 negotiation failed when processing Proxy ID. Received local id 192.168 33 33/24 type IPv4 address protocol 0 port 0, received remote id 172.16 33.33/24 type IPv4 address protocol 0 port 0."
How should the administrator identify the root cause of this error message?

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

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-me The VPN peer on one end is using policy-based VPN. You must configure a Proxy ID on the Palo Alto
Networks firewall.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-me

NEW QUESTION 52
An engineer creates a set of rules in a Device Group (Panorama) to permit traffic to various services for a specific LDAP user group.
What needs to be configured to ensure Panorama can retrieve user and group information for use in these rules?

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

Answer: B

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

NEW QUESTION 57
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 58
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 60
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 65
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 67
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 68
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 72
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 73
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 75
......