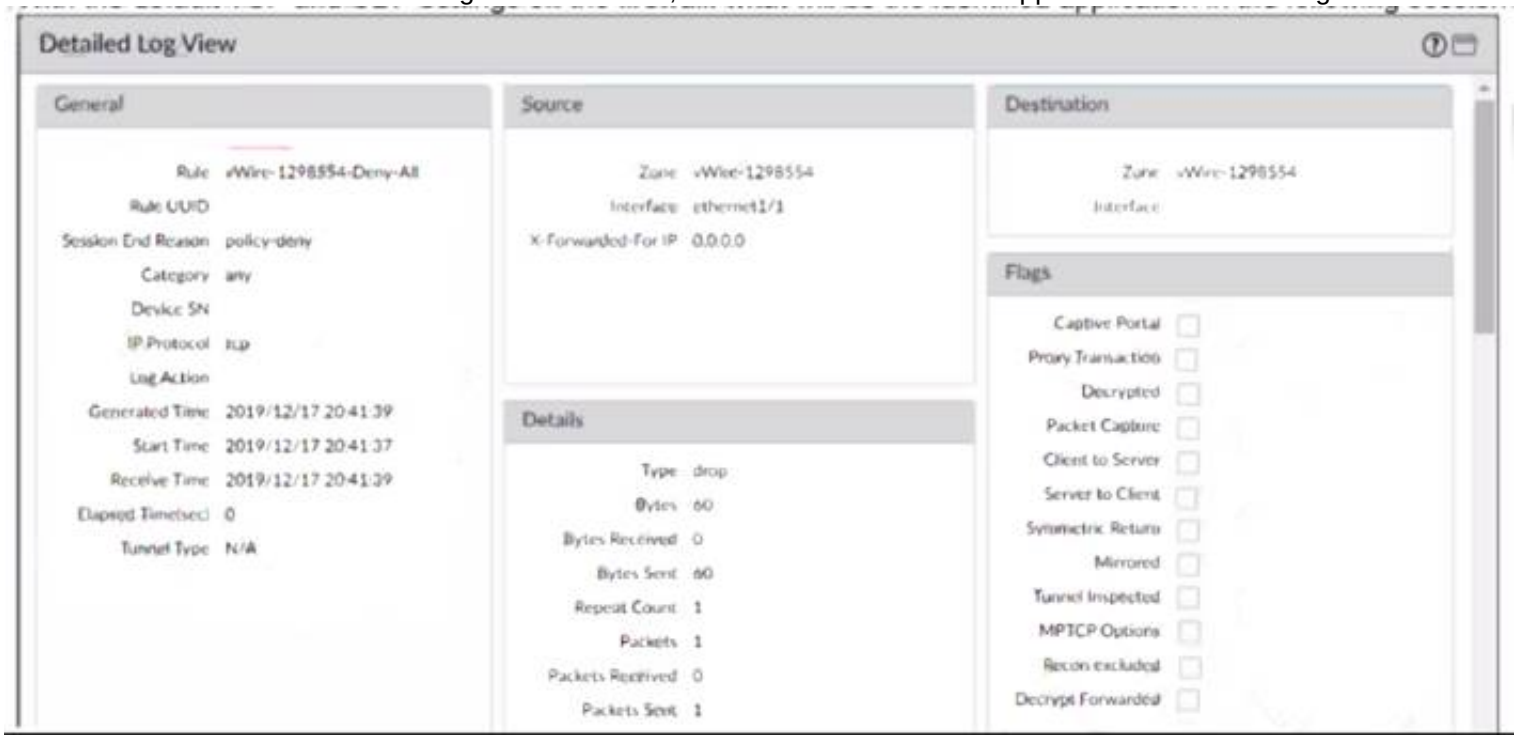
Paloalto-Networks

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?



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 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 3
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 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
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:

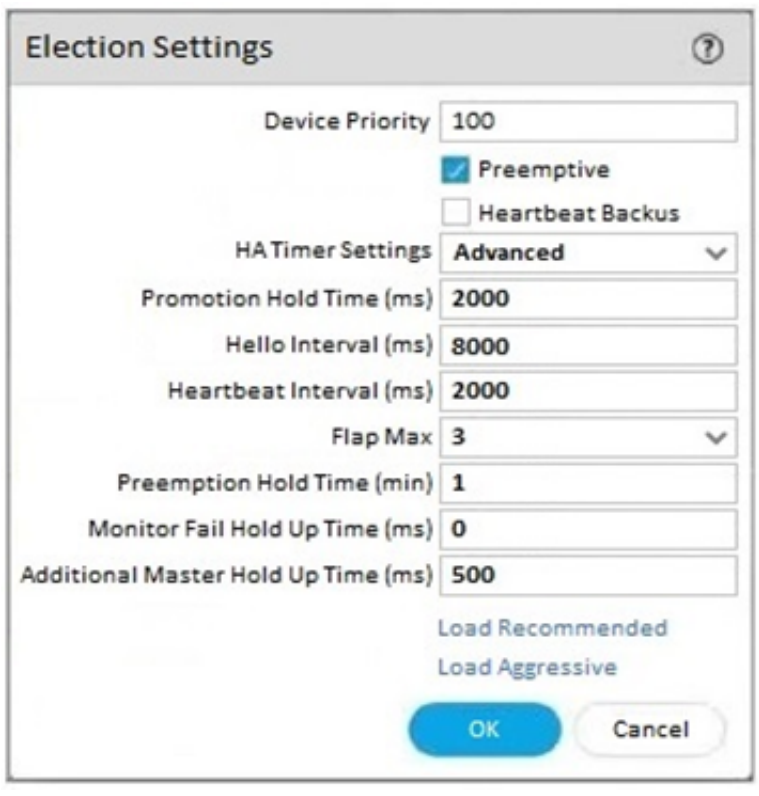
NEW QUESTION 6
An engineer needs to configure a standardized template for all Panorama-managed firewalls. These settings will be configured on a template named "Global" and will be included in all template stacks.
Which three settings can be configured in this template? (Choose three.)

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



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

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

Answer: D

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

How to Configure Ping Interval/Timeout Settings ... - Palo Alto Networks

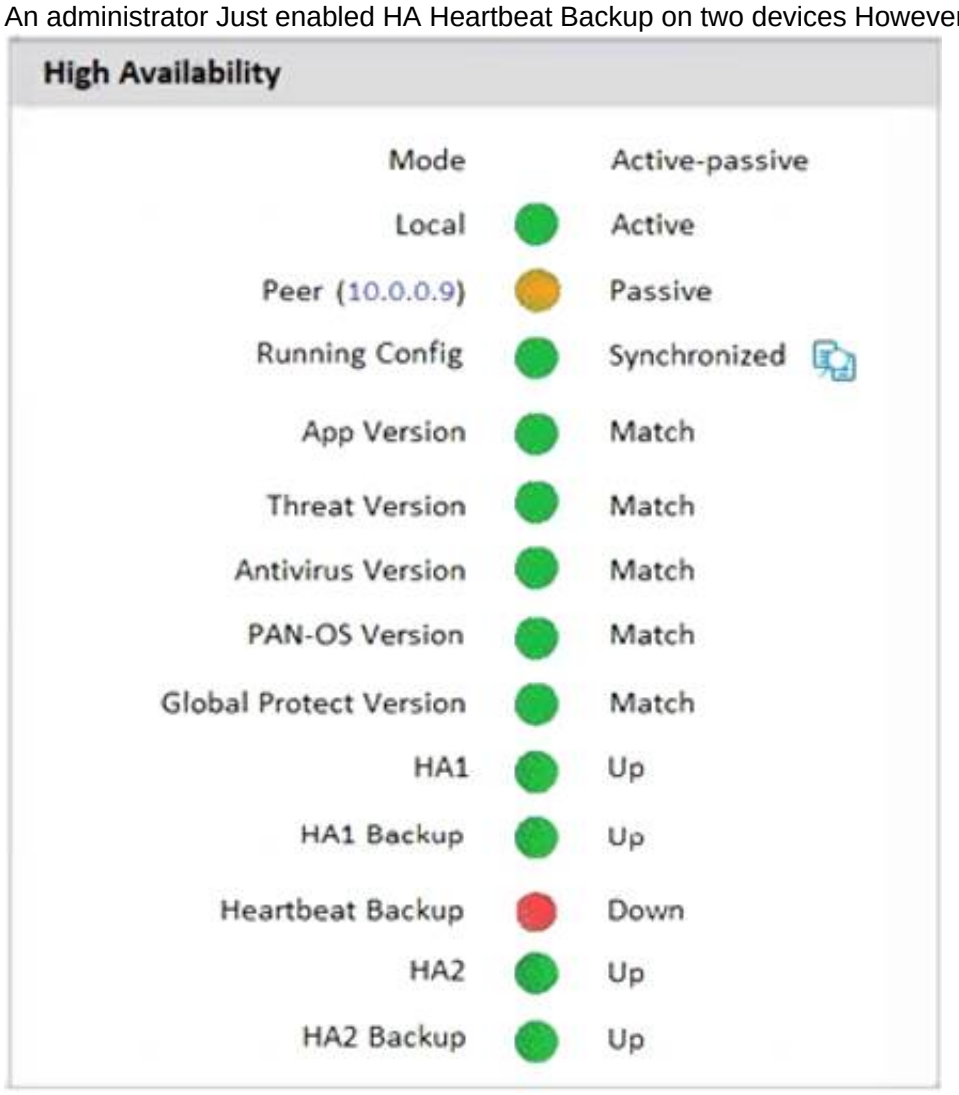
NEW QUESTION 8
In a security-first network, what is the recommended threshold value for apps and threats to be dynamically updated?

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

Answer: B

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

NEW QUESTION 9
An administrator Just enabled HA Heartbeat Backup on two devices However, the status on tie firewall's dashboard is showing as down High Availability.



What could an administrator do to troubleshoot the issue?

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

Answer: B

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

NEW QUESTION 10
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 10
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 12
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)

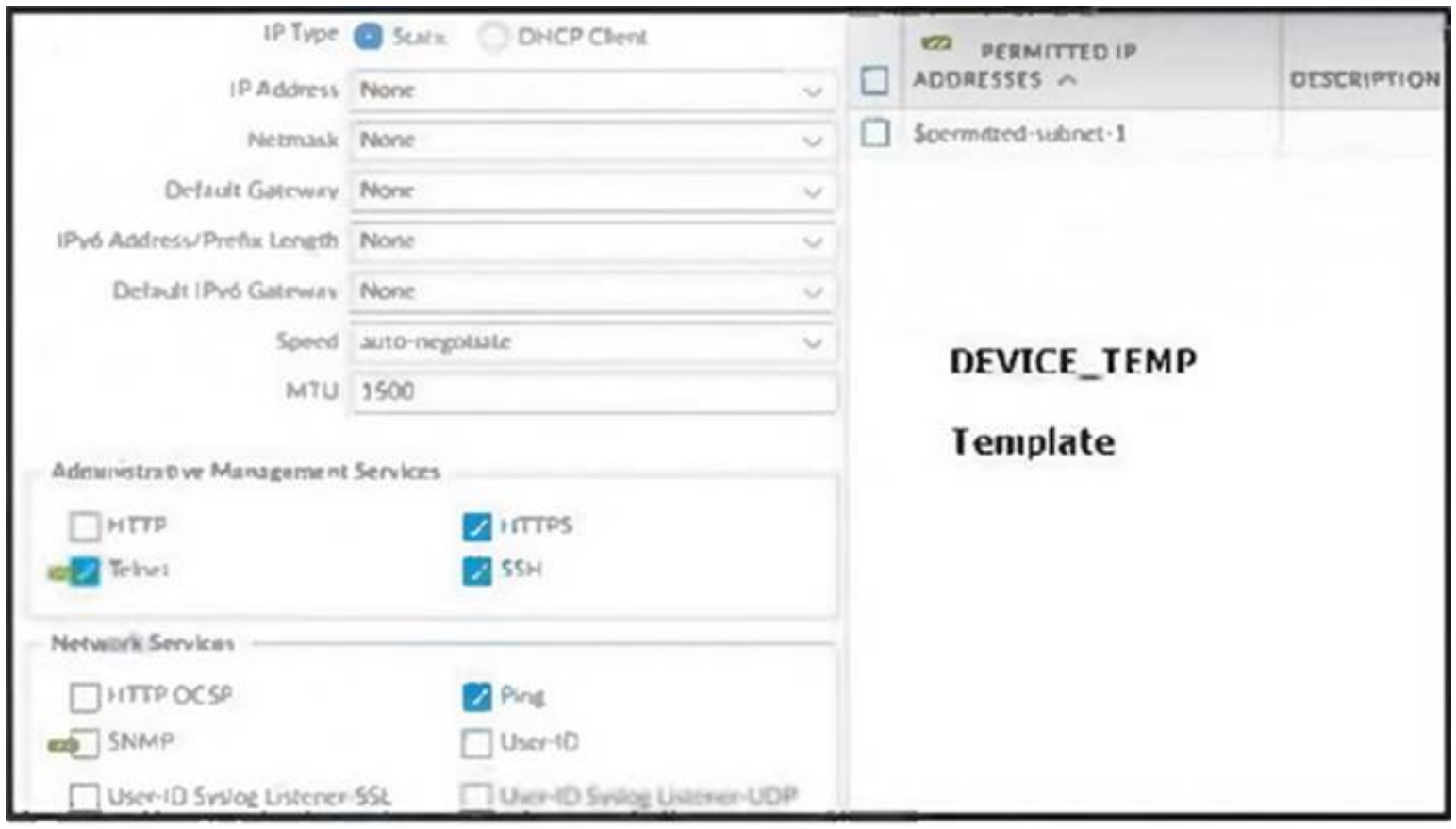
A. Configure the DNS server locally on the firewall.
B. Change the DNS server on the global template.
C. Override the DNS server on the template stack.
D. Configure a service route for DNS on a different interface.

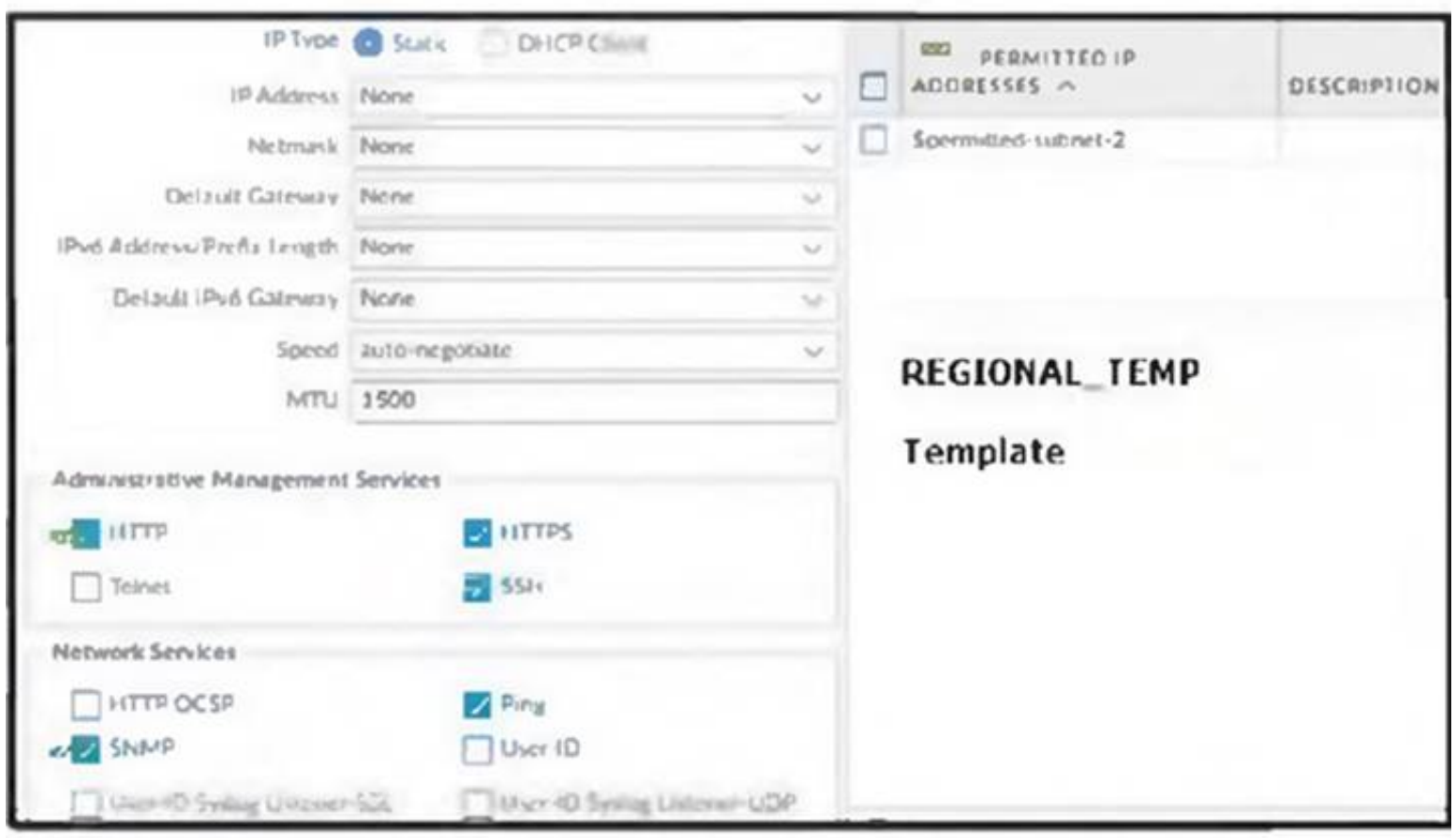
Answer: AC

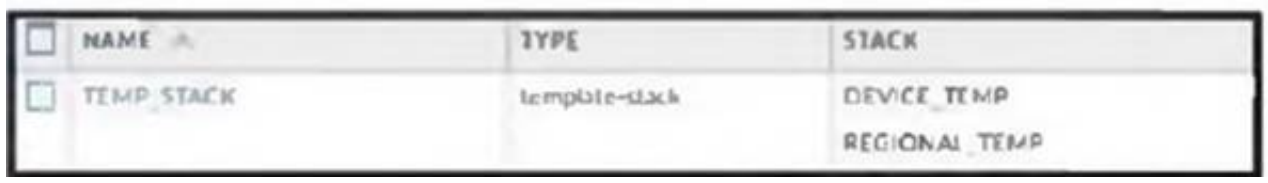
Explanation:
To override a device and network setting applied by a template, you can either configure the setting locally on the firewall or override the setting on the template stack. Configuring the setting locally on the firewall will
copy the setting to the local configuration of the device and will 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 16
Based on the screenshots above, and with no configuration inside the Template Stack itself, what access will the device permit on its Management port?







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 18
Where can a service route be configured for a specific destination IP?

A. Use Netw ork > Virtual Routers, select the Virtual Router > Static Routes > IPv4
B. Use Device > Setup > Services > Services
C. Use Device > Setup > Services > Service Route Configuration > Customize > Destination
D. Use Device > Setup > Services > Service Route Configuration > Customize > IPv4

Answer: C

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

NEW QUESTION 23
Which three multi-factor authentication methods can be used to authenticate access to the firewall? (Choose three.)

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

Answer: CDE

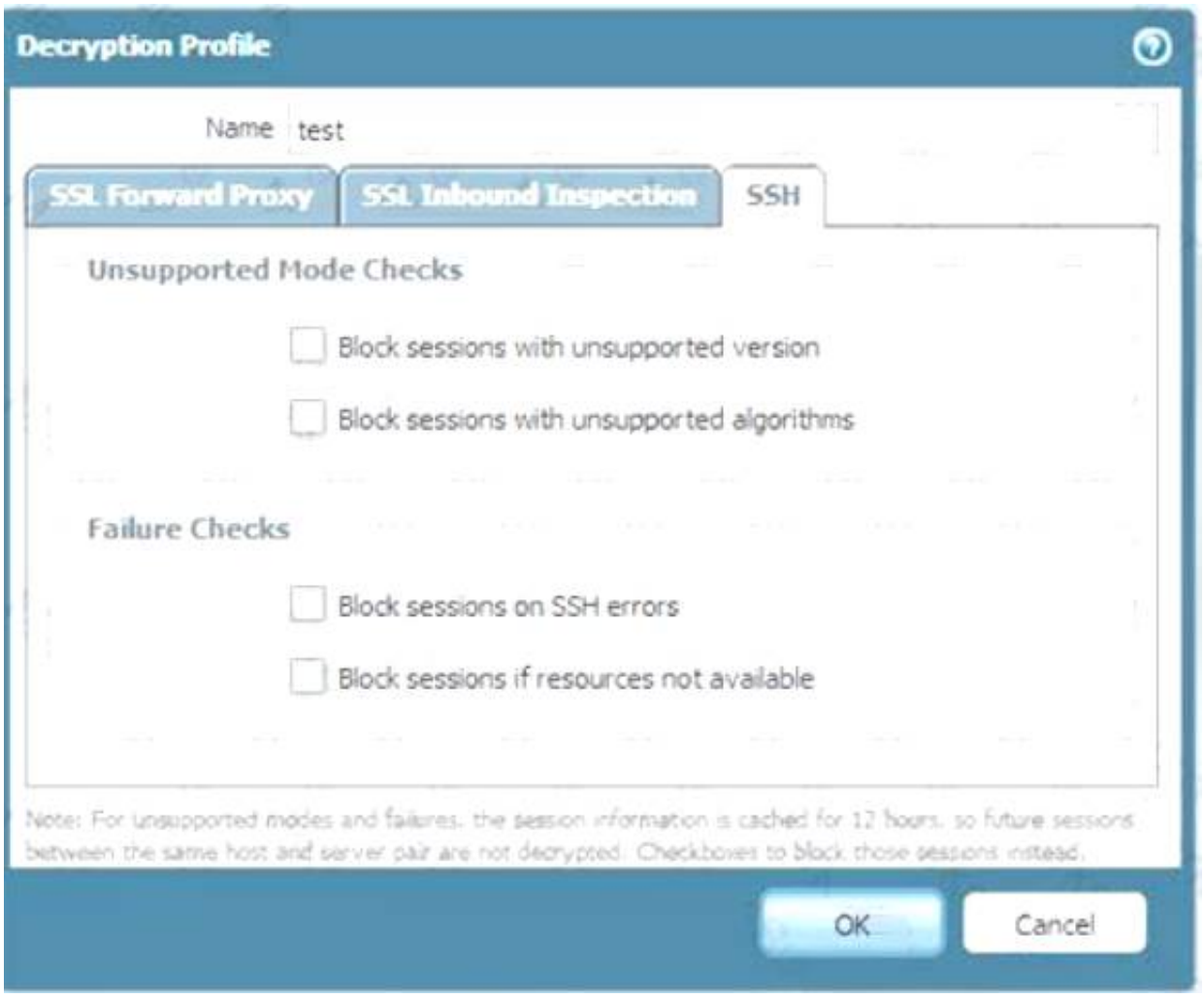
Explanation:
The firewall can use three multi-factor authentication methods to authenticate access to the firewall: SMS, user certificate, and one-time password. These methods can be used in combination with other authentication factors, such as username and password, to provide stronger security for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

NEW QUESTION 26
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



NEW QUESTION 31
Which two profiles should be configured when sharing tags from threat logs with a remote User-ID agent? (Choose two.)

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

Answer: BC

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

NEW QUESTION 33
A network security administrator has been tasked with deploying User-ID in their organization. What are three valid methods of collecting User-ID information in a network? (Choose three.)

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

Answer: ABC

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

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

NEW QUESTION 36
An engineer is designing a deployment of multi-vsys firewalls.
What must be taken into consideration when designing the device group structure?

A. Only one vsys or one firewall can be assigned to a device group, and a multi-vsys firewall can have each vsys in a different device group.
B. Multiple vsys and firewalls can be assigned to a device group, and a multi-vsys firewall can have each vsys in a different device group.
C. Only one vsys or one firewall can be assigned to a device group, except for a multi-vsys firewall, which must have all its vsys in a single device group.
D. Multiple vsys and firewalls can be assigned to a device group, and a multi-vsys firewall must have all its vsys in a single device group.

Answer: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClETCA0
A device group is a logical grouping of firewalls that share the same security policy rules. A device group can contain multiple vsys and firewalls, including multi-vsys firewalls. A multi-vsys firewall can have each vsys in a different device group, depending on the desired security policy for each vsys. This allows for granular control and flexibility in managing multi-vsys firewalls with Panorama1. References: Device Group Push to Multi-VSYS Firewall, Configure Virtual Systems, PCNSE Study Guide (page 50)

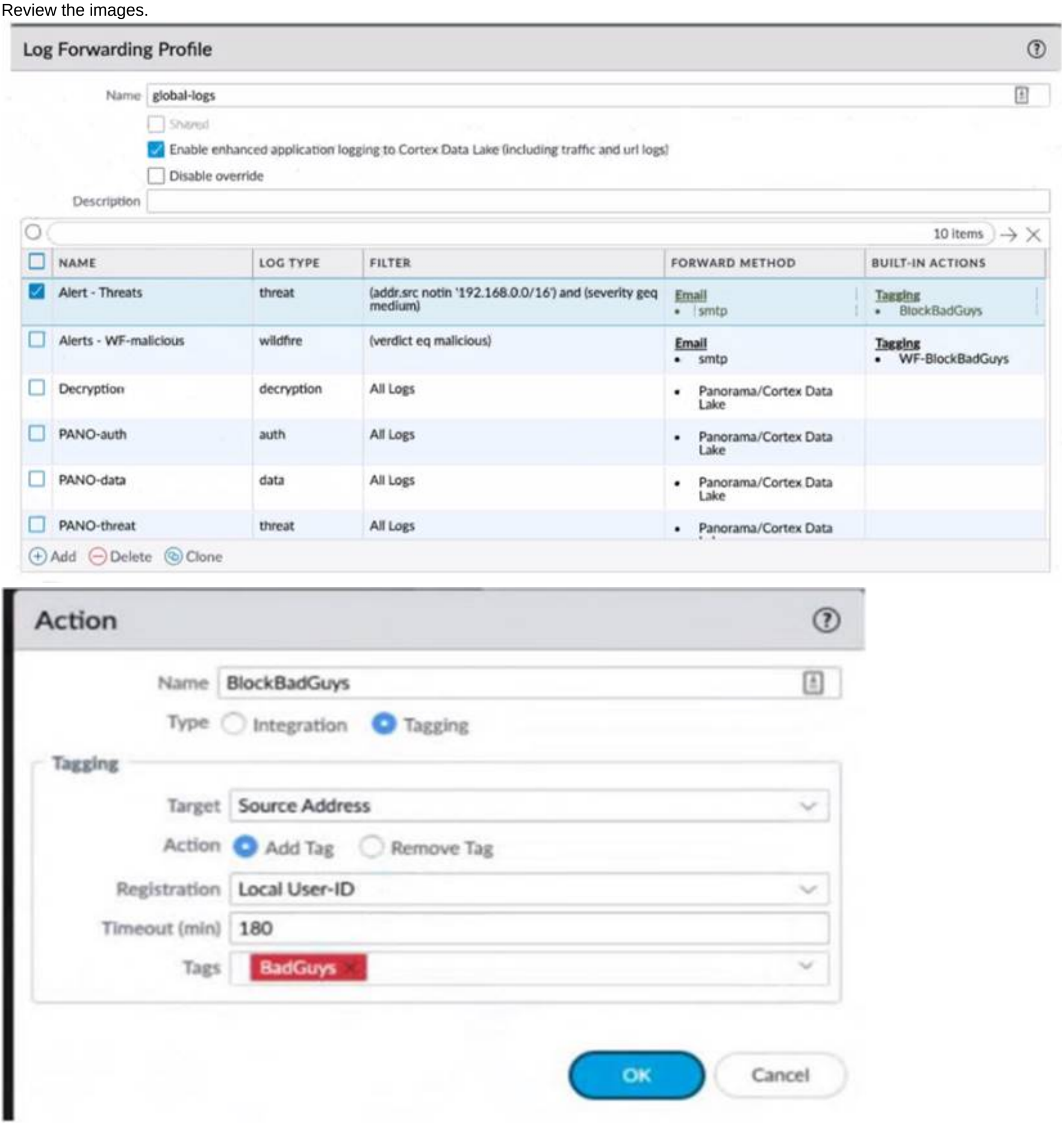
NEW QUESTION 37
An administrator has two pairs of firewalls within the same subnet. Both pairs of firewalls have been configured to use High Availability mode with Active/Passive. The ARP tables for upstream routes display the same MAC address being shared for some of these firewalls.
What can be configured 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 41
Review the images.



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 42
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 44
Which two key exchange algorithms consume the most resources when decrypting SSL traffic? (Choose two.)

A. ECDSA
B. ECDHE
C. RSA
D. DHE

Answer: BD

Explanation:
The two key exchange algorithms that consume the most resources when decrypting SSL traffic are ECDHE and DHE. These are both Diffie-Hellman based algorithms that enable perfect forward secrecy (PFS), which means that they generate a new and unique session key for each SSL/TLS session, and do not reuse any previous keys. This enhances the security of the encrypted communication, but also increases the computational cost and complexity of the key exchange process. ECDHE stands for Elliptic Curve Diffie-Hellman Ephemeral, which uses elliptic curve cryptography (ECC) to generate the session key. DHE stands for Diffie-Hellman Ephemeral, which uses modular arithmetic to generate the session key. Both ECDHE and DHE require more CPU and memory resources than RSA, which is a non-PFS algorithm that uses public and private keys to encrypt and decrypt the session key123. References: Key Exchange Algorithms, Best Practices for Enabling SSL Decryption, PCNSE Study Guide (page 60)

NEW QUESTION 48
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 50
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 51
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 54
An administrator is troubleshooting why video traffic is not being properly classified. If this traffic does not match any QoS classes, what default class is assigned?

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

Answer: D

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

NEW QUESTION 56
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 61
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.)

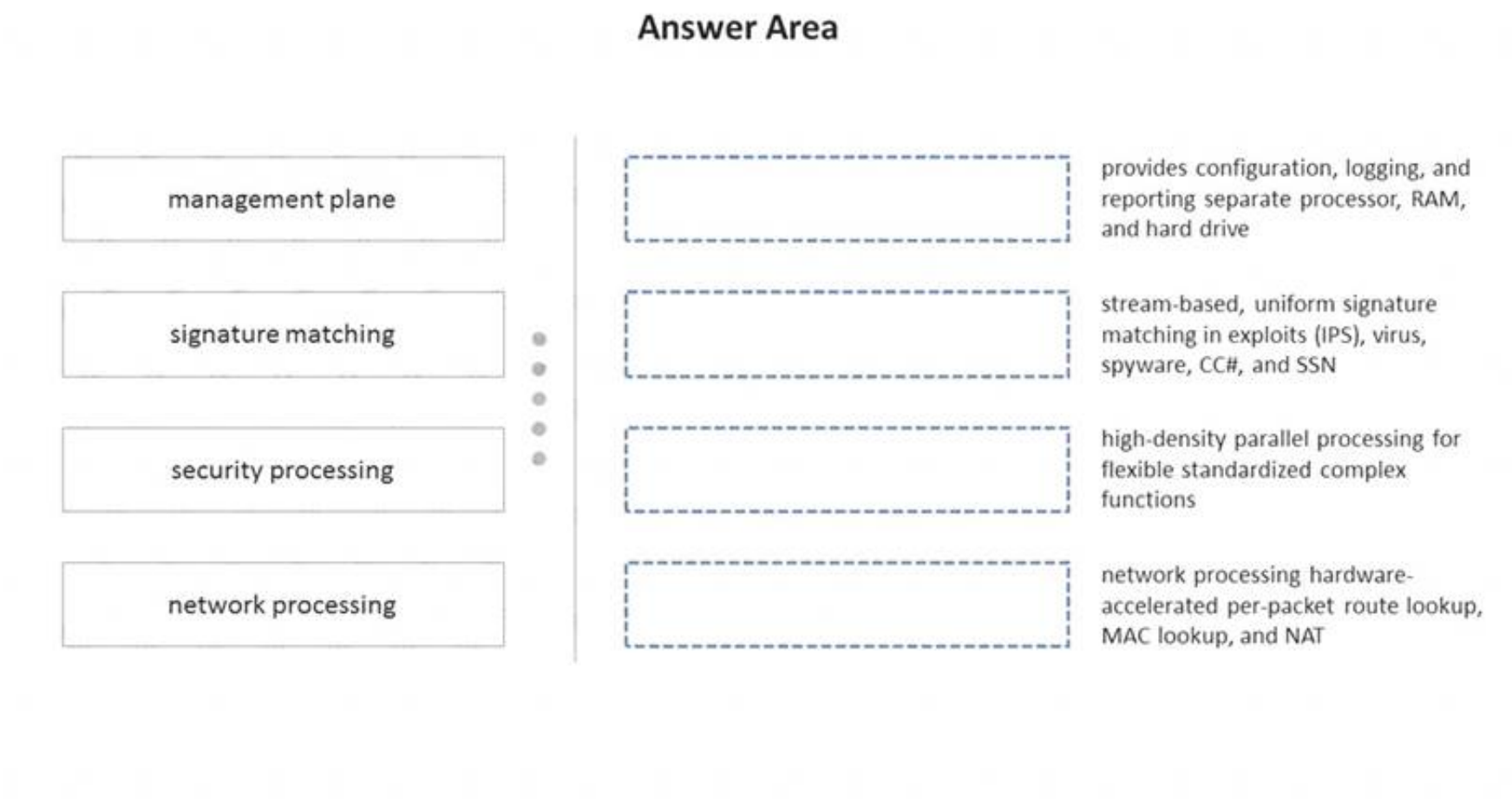
A. An Application Override policy for the SIP traffic
B. QoS on the egress interface for the traffic flows
C. QoS on the ingress interface for the traffic flows
D. A QoS profile defining traffic classes
E. A QoS policy for each application ID

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 63
Match the terms to their corresponding definitions



A. Mastered
B. Not Mastered

Answer: A

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

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

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

Answer: B

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

NEW QUESTION 72
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 74
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 77
Which three external authentication services can the firewall use to authenticate admins into the Palo Alto Networks NGFW without creating administrator account on the firewall? (Choose three.)

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

Answer: ABE

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

NEW QUESTION 78
Which operation will impact the performance of the management plane?

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

Answer: B

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

NEW QUESTION 83
Which two statements correctly describe Session 380280? (Choose two.)

```
> show session id 380280

Session          380280

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

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

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

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

Answer: AC

NEW QUESTION 87
An administrator needs to identify which NAT policy is being used for internet traffic.
From the Monitor tab of the firewall GUI, how can the administrator identify which NAT policy is in use for a traffic flow?

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

Answer: C

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

NEW QUESTION 92
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 95
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 99
An administrator has been tasked with configuring decryption policies, Which decryption best practice should they consider?

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

Answer: A

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

NEW QUESTION 100
An administrator is required to create an application-based Security policy rule to allow Evernote. The Evernote application implicitly uses SSL and web browsing. What is the minimum the administrator needs to configure in the Security rule to allow only Evernote?

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

Answer: D

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

NEW QUESTION 105
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PCNSE Practice Exam Features:

* PCNSE Questions and Answers Updated Frequently

* PCNSE Practice Questions Verified by Expert Senior Certified Staff

* PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year