Paloalto-Networks

Exam Questions PCNSE

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

NEW QUESTION 1
An engineer is troubleshooting a traffic-routing issue. What is the correct packet-flow sequence?

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

Answer: C

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

NEW QUESTION 2
A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours.
Which two steps are likely to mitigate the issue? (Choose TWO)

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

Answer: AC

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

NEW QUESTION 3
To ensure that a Security policy has the highest priority, how should an administrator configure a Security policy in the device group hierarchy?

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

Answer: D

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

NEW QUESTION 4
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
A firewall engineer creates a new App-ID report under Monitor > Reports > Application Reports > New Applications to monitor new applications on the network and better assess any Security policy updates the engineer might want to make.
How does the firewall identify the New App-ID characteristic?

A. It matches to the New App-IDs downloaded in the last 90 days.
B. It matches to the New App-IDs in the most recently installed content releases.
C. It matches to the New App-IDs downloaded in the last 30 days.
D. It matches to the New App-IDs installed since the last time the firewall was rebooted.

Answer: B

Explanation:

The New App-ID characteristic enables the firewall to monitor new applications on the network, so that the engineer can better assess the security policy updates they might want to make. The New App-ID characteristic always matches to only the new App-IDs in the most recently installed content releases. When a new content release is installed, the New App-ID characteristic automatically begins to match only to the new App-IDs in that content release version. This way, the engineer can see how the newly-categorized applications might impact security policy enforcement and make any necessary adjustments. References: Monitor New App-IDs

NEW QUESTION 6
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 7
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

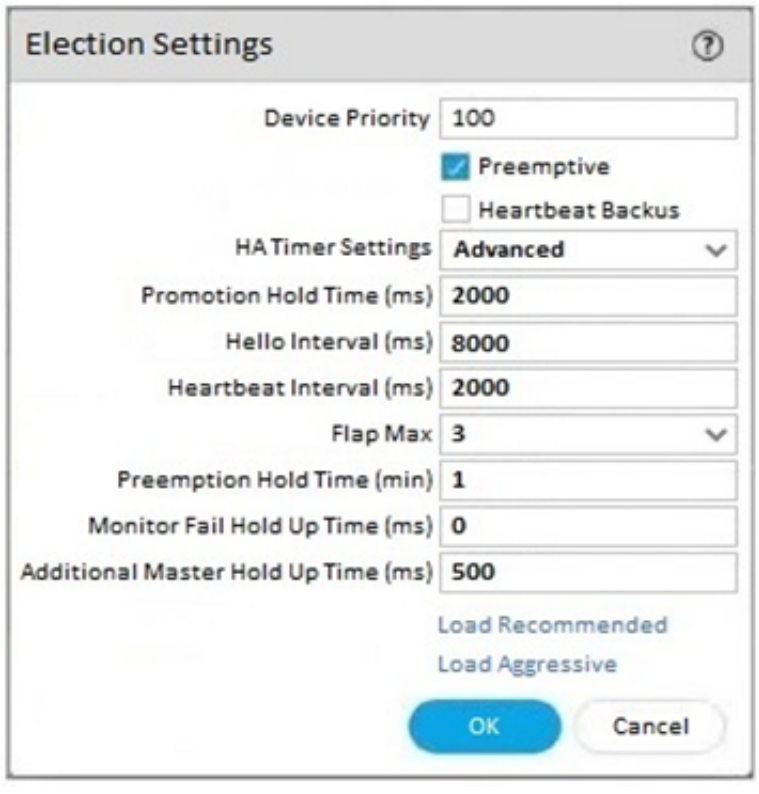
NEW QUESTION 8
A security engineer needs firewall management access on a trusted interface.
Which three settings are required on an SSL/TLS Service Profile to provide secure Web UI authentication? (Choose three.)

A. Minimum TLS version
B. Certificate
C. Encryption Algorithm
D. Maximum TLS version
E. Authentication Algorithm

Answer: ABD

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssltls-service

NEW QUESTION 9
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 10
An engineer is configuring a template in Panorama which will contain settings that need to be applied to all firewalls in production.
Which three parts of a template an engineer can configure? (Choose three.)

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

Answer: ACD

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

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

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

Answer: A

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

NEW QUESTION 13
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)

A. upload-onlys

B. install and reboot
C. upload and install
D. upload and install and reboot
E. verify and install

Answer: ACD

Explanation:
ttps://www.kareemccie.com/2021/05/palo-alto-firewall-packet-flow.html

NEW QUESTION 17
Which log type would provide information about traffic blocked by a Zone Protection profile?

A. Data Filtering
B. IP-Tag
C. Traffic
D. Threat

Answer: D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhzCAC
D is the correct answer because the threat log type would provide information about traffic blocked by a Zone Protection profile. This is because Zone Protection profiles are used to protect the network from attacks, including common flood, reconnaissance attacks, and other packet-based attacks1. These attacks are classified as threats by the firewall and are logged in the threat log2. The threat log displays information such as the source and destination IP addresses, ports, zones, applications, threat types, actions, and severity of the threats2.
Verified References:
1: Zone protection profiles - Palo Alto Networks Knowledge Base
2: Threat Log Fields - Palo Alto Networks

NEW QUESTION 18
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 19
What is the best definition of the Heartbeat Interval?

A. The interval in milliseconds between hello packets
B. The frequency at which the HA peers check link or path availability
C. The frequency at which the HA peers exchange ping
D. The interval during which the firewall will remain active following a link monitor failure

Answer: C

Explanation:
The firewalls exchange hello messages and heartbeats at configurable intervals to verify that the peer firewall is responsive and operational. Hello messages are sent from one peer to the other to verify the state of the firewall. The heartbeat is an ICMP ping to the HA peer. A response from the peer indicates that the firewalls are connected and responsive.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClUcCAK
"A "heartbeat-interval" CLI command was added to the election settings for HA, this interval has a 1000ms minimum for all Palo Alto Networks platforms and is an ICMP ping to the other device through the HA control link." https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClMaCAK

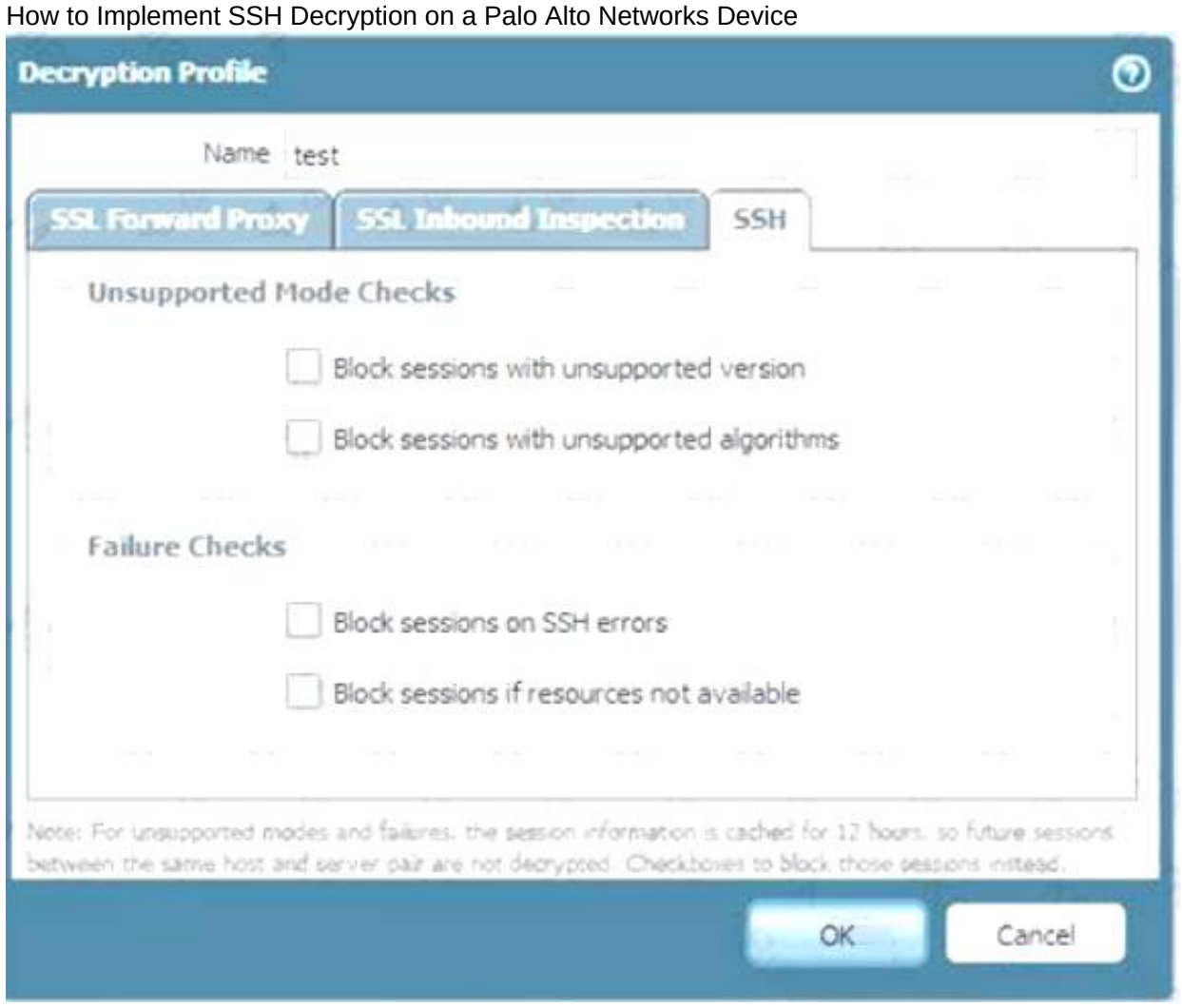
NEW QUESTION 24
An organization wants to begin decrypting guest and BYOD traffic.
Which NGFW feature can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted?

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 28
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 31
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 32
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 36
An engineer is tasked with deploying SSL Forward Proxy decryption for their organization. What should they review with their leadership before implementation?

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

Answer: D

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

NEW QUESTION 38
Which statement regarding HA timer settings is true?

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

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-timers

NEW QUESTION 42
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
Which type of policy in Palo Alto Networks firewalls can use Device-ID as a match condition?

A. NAT
B. DOS protection
C. QoS
D. Tunnel inspection

Answer: C

Explanation:
The type of policy in Palo Alto Networks firewalls that can use Device-ID as a match condition is QoS. This is because Device-ID is a feature that allows the firewall to identify and classify devices on the network based on their characteristics, such as vendor, model, OS, and role1. QoS policies are used to allocate bandwidth and prioritize traffic based on various criteria, such as application, user, source, destination, and device2. By using Device-ID as a match condition in QoS policies, the firewall can apply different QoS actions to different types of devices, such as IoT devices, laptops, smartphones, etc3. This can help optimize the network performance and ensure the quality of service for critical applications and devices.

NEW QUESTION 46
An engineer is configuring a Protection profile to defend specific endpoints and resources against malicious activity.
The profile is configured to provide granular defense against targeted flood attacks for specific critical systems that are accessed by users from the internet.
Which profile is the engineer configuring?

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

Answer: D

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

NEW QUESTION 47
Which three items must be configured to implement application override? (Choose three)

A. Custom app
B. Security policy rule
C. Application override policy rule
D. Decryption policy rule
E. Application filter

Answer: ABC

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/policies/policies-application-override
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PPDrCAO

NEW QUESTION 49
You are auditing the work of a co-worker and need to verify that they have matched the Palo Alto Networks Best Practices for Anti-Spyware Profiles.
For which three severity levels should single-packet captures be enabled to meet the Best Practice standard? (Choose three.)

A. Low
B. High
C. Critical
D. Informational
E. Medium

Answer: BCE

Explanation:
https://docs.paloaltonetworks.com/best-practices/10-2/data-center-best-practices/data-center-best-practice-securi
The Palo Alto Networks Best Practices for Anti-Spyware Profiles recommend enabling single-packet captures (PCAP) for medium, high, and critical severity threats. This allows for capturing the first packet of the malicious traffic for further analysis and investigation. PCAP should not be enabled for low and informational severity threats, as they generate a relatively high volume of traffic and are not particularly useful compared to potential threats2. References: Create the Data Center Best Practice Anti-Spyware Profile, Security Profile Anti-Spyware, PCNSE Study Guide (page 57)

NEW QUESTION 51
A network security administrator wants to inspect HTTPS traffic from users as it egresses through a firewall to the Internet/Untrust zone from trusted network zones.
The security admin wishes to ensure that if users are presented with invalid or untrusted security certificates, the user will see an untrusted certificate warning.
What is the best choice for an SSL Forward Untrust certificate?

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

Answer: B

Explanation:
- B is the best choice for an SSL Forward Untrust certificate because a self-signed certificate generated on the firewall is not trusted by any client browsers by default1. This means that if the firewall observes an invalid or untrusted security certificate from the server, it will present the self-signed certificate to the client, which will trigger an untrusted certificate warning2. This way, the security admin can ensure that users are aware of any potential risks when accessing HTTPS sites with untrusted certificates.
- A web server certificate signed by the organization’s PKI (A) or a subordinate Certificate Authority certificate signed by the organization’s PKI © are not good choices for an SSL Forward Untrust certificate because they are trusted by the client browsers that have the organization’s root CA installed1. This means that if the firewall observes an invalid or untrusted security certificate from the server, it will present the web server or subordinate CA certificate to the client, which will not trigger an untrusted certificate warning2. This way, the security admin cannot ensure that users are aware of any potential risks when accessing HTTPS sites with untrusted certificates.
- A web server certificate signed by an external Certificate Authority (D) is not a good choice for an SSL Forward Untrust certificate because it is trusted by most client browsers that have the external CA in
their trust store1. This means that if the firewall observes an invalid or untrusted security certificate from the server, it will present the web server certificate to the client, which will not trigger an untrusted certificate warning2. This way, the security admin cannot ensure that users are aware of any potential
risks when accessing HTTPS sites with untrusted certificates.
Verified References:
- 1: How to Configure SSL Decryption - Palo Alto Networks Knowledge Base
- 2: How to Implement and Test SSL Decryption - Palo Alto Networks Knowledge Base

NEW QUESTION 54
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 55
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 58

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

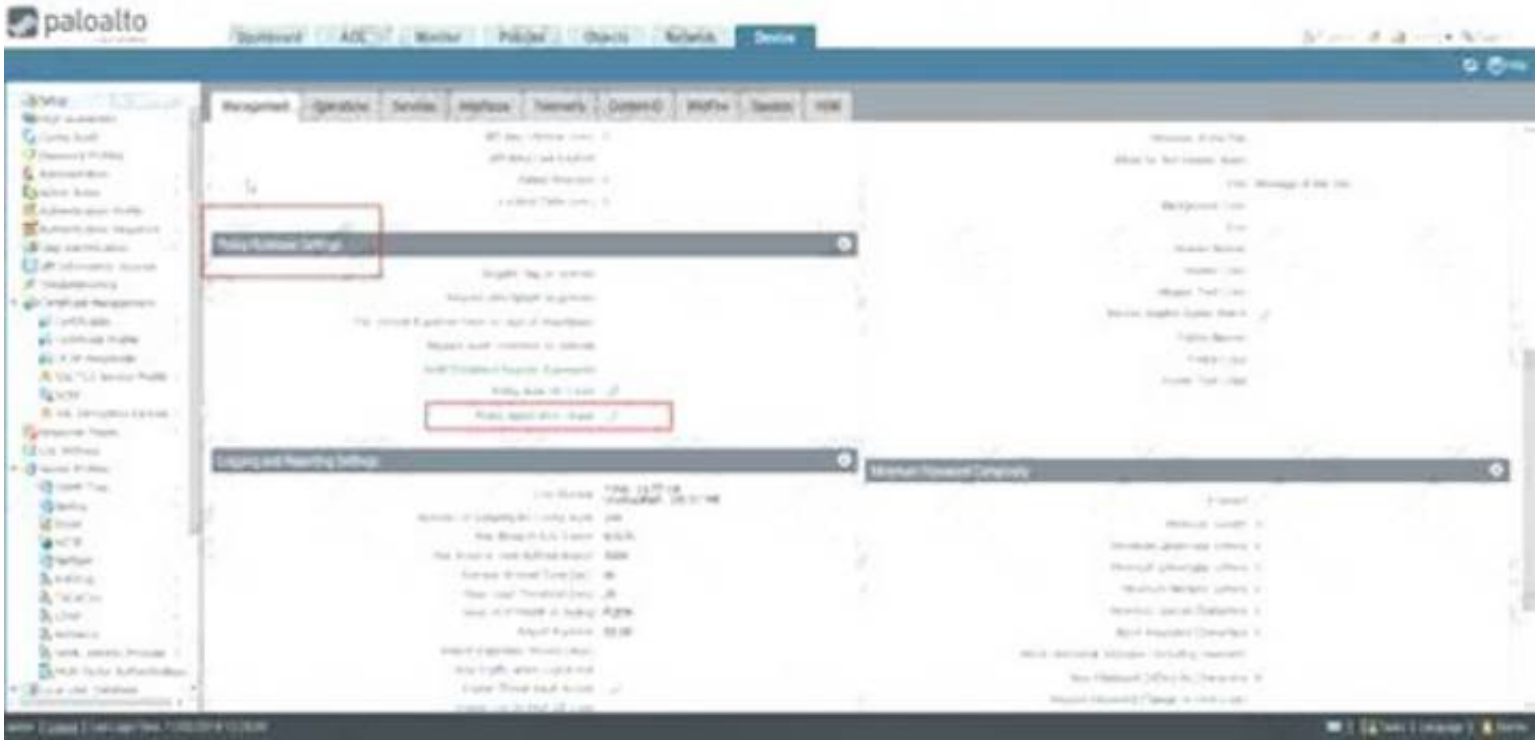
Explanation:
Traffic view in the Monitor tab of the firewall GUI can display the information about the NAT policy that is in use for a traffic flow, if the Source or Destination NAT columns are included and reviewed in the detailed log view1. The Source NAT column shows the translated source IP address 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 61
In the New App Viewer under Policy Optimizer, what does the compare option for a specific rule allow an administrator to compare?

A. The running configuration with the candidate configuration of the firewall
B. Applications configured in the rule with applications seen from traffic matching the same rule
C. Applications configured in the rule with their dependencies
D. The security rule with any other security rule selected

Answer: B

Explanation:
The compare option for a specific rule in the New App Viewer under Policy Optimizer allows an administrator to compare the applications configured in the rule with the applications seen from traffic matching the same rule. This helps the administrator to identify any new applications that are not explicitly defined in the rule, but are implicitly allowed by the firewall based on the dependencies of the configured applications. The compare option also shows the usage statistics and risk levels of the applications, and provides suggestions for optimizing the rule by adding, removing, or replacing applications12. References: New App Viewer (Policy Optimizer), PCNSE Study Guide (page 47)
Why use Security Policy Optimizer and what are the benefits?



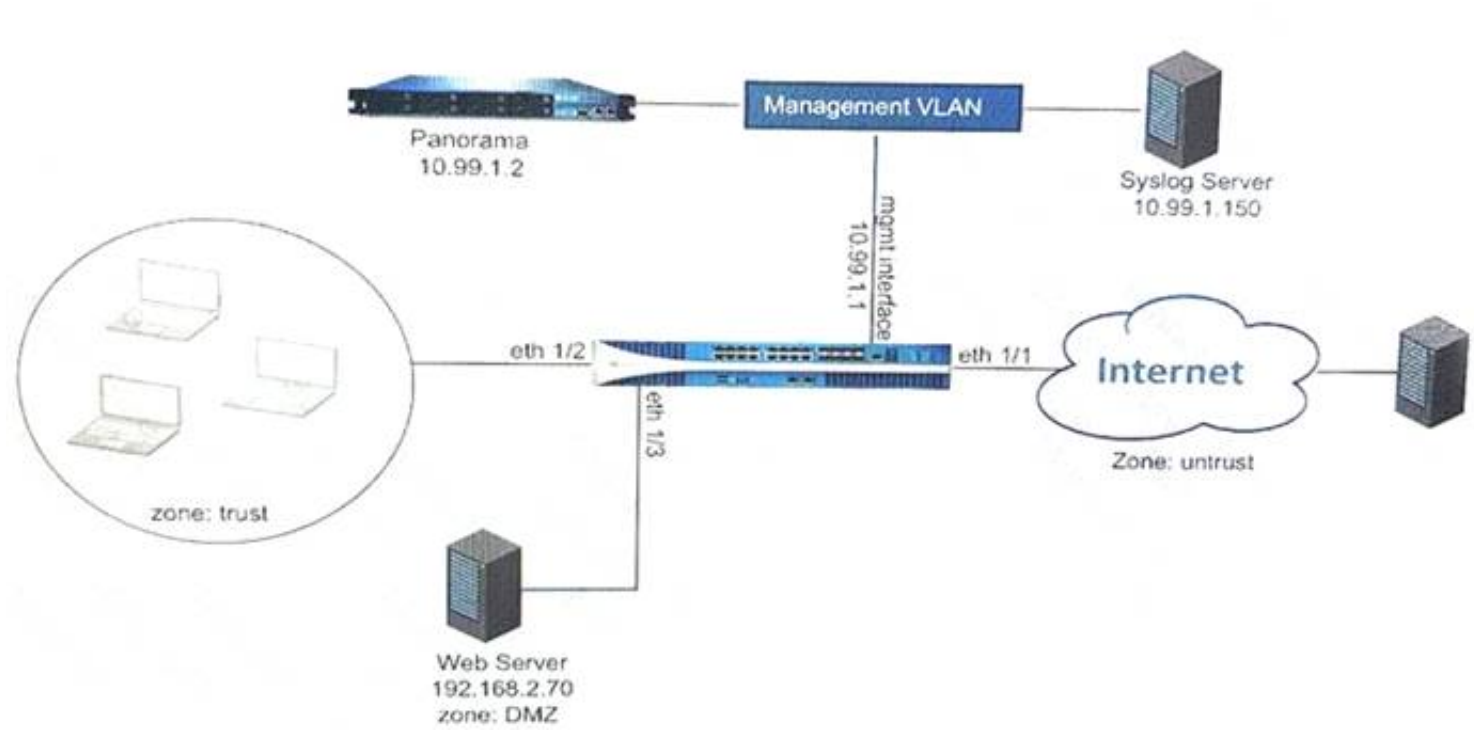
NEW QUESTION 63
During the implementation of SSL Forward Proxy decryption, an administrator imports the company's Enterprise Root CA and Intermediate CA certificates onto the firewall. The company's Root and Intermediate CA certificates are also distributed to trusted devices using Group Policy and GlobalProtect. 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.

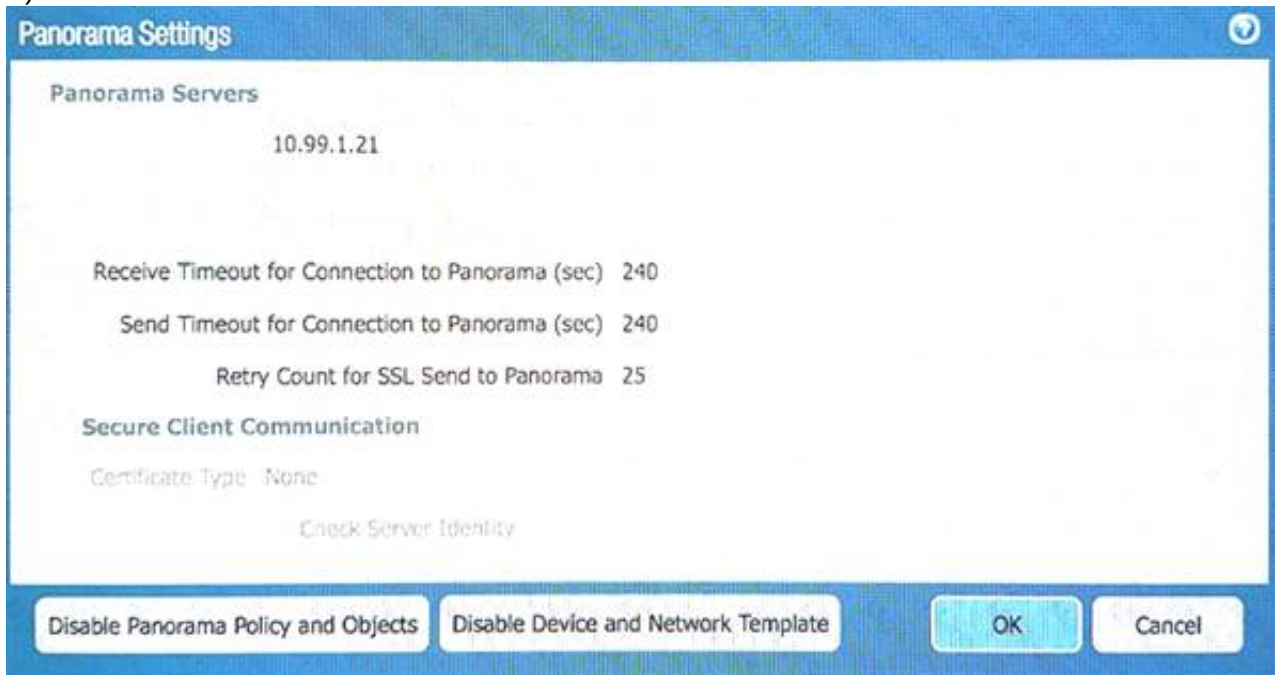
Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy

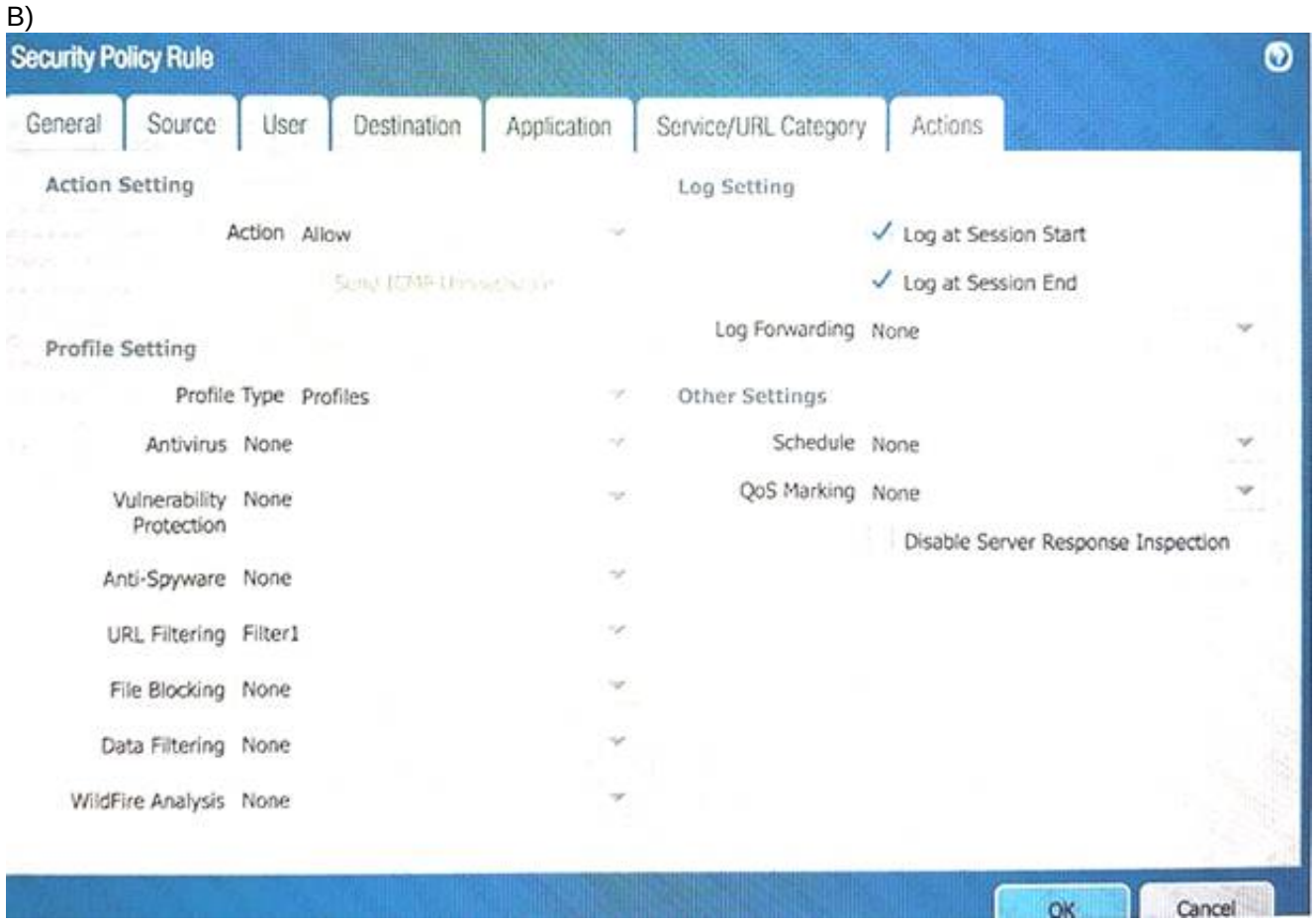
NEW QUESTION 68
Refer to Exhibit:



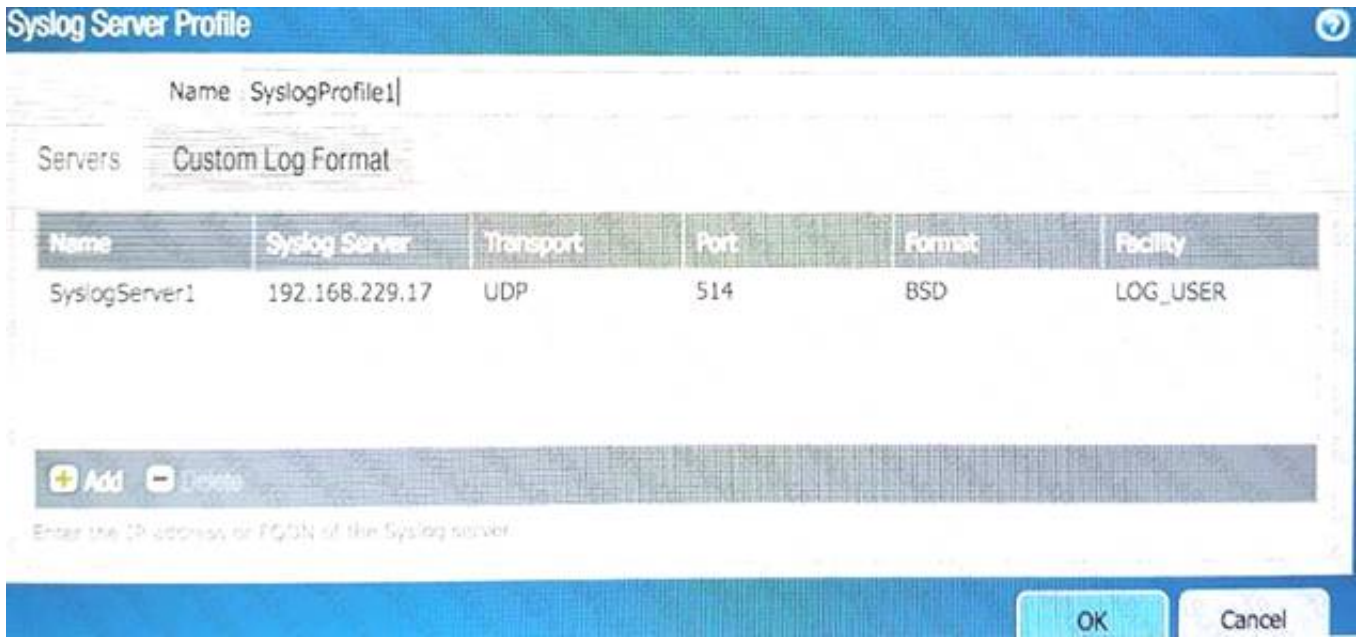
An administrator can not see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall.
Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?
A)



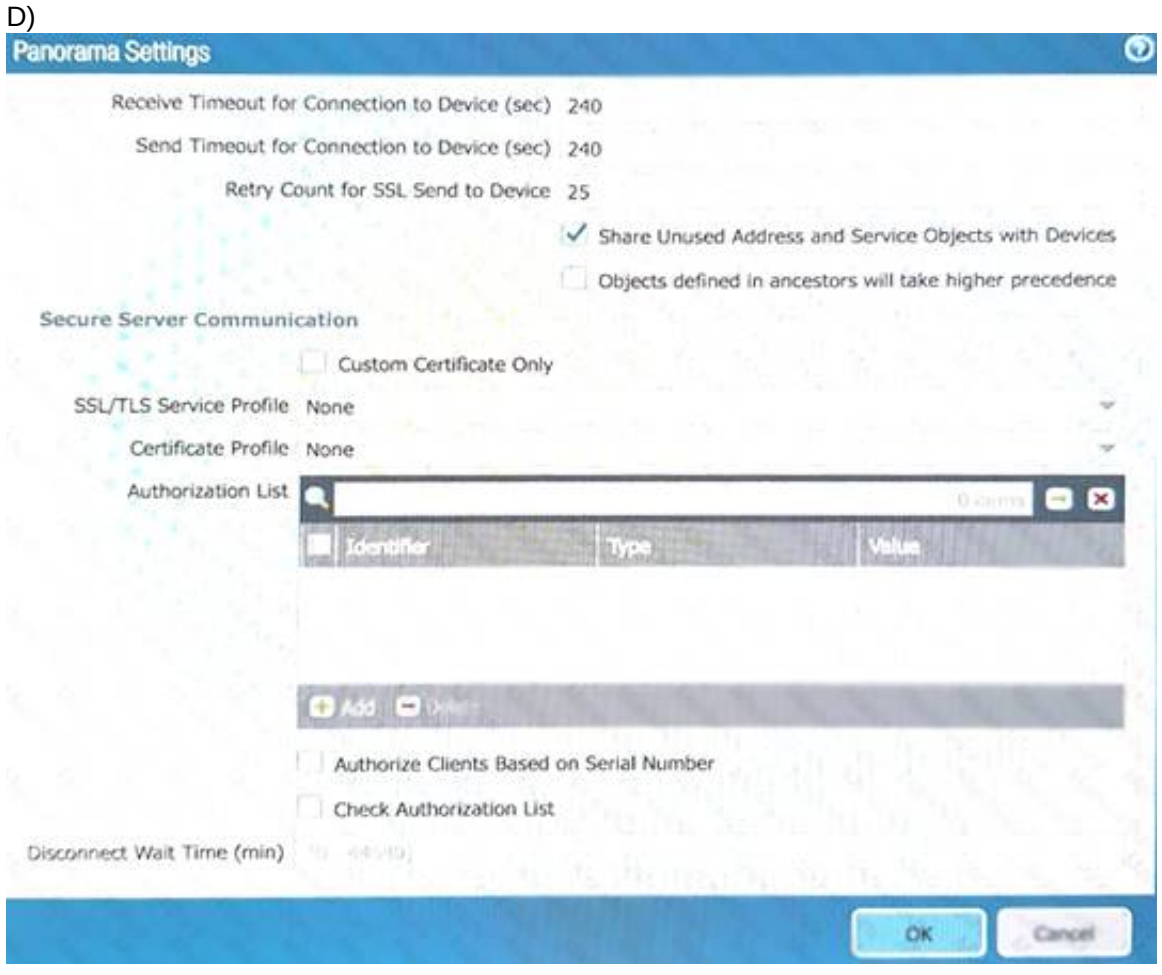
B)



C)



D)



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

Answer: C

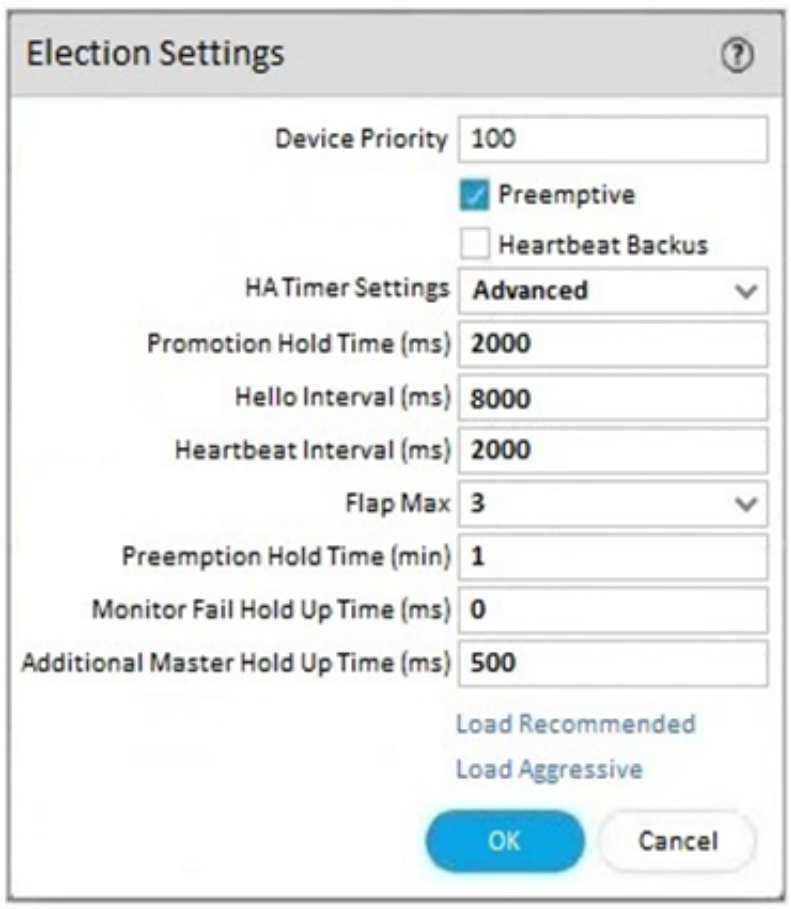
NEW QUESTION 73
An administrator would like to determine which action the firewall will take for a specific CVE. Given the screenshot below, where should the administrator navigate to view this information?

A. The profile rule action
B. CVE column
C. Exceptions lab
D. The profile rule threat name

Answer: C

Explanation:
The Exceptions settings allows you to change the response to a specific signature. For example, you can block all packets that match a signature, except for the selected one, which generates an alert. The Exception tab supports filtering functions.
If you not believed, then login the firewall go to Vulnerability > Exceptions and select "Show all signatures". From there you will see all threat information including specific actions.
More detail: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm4yCAC

NEW QUESTION 77
An engineer reviews high availability (HA) settings to understand a recent HA failover event. Review the screenshot below.



Which timer determines the frequency at which the HA peers exchange messages in the form of an ICMP (ping)

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

Answer: B

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/ha-timers

NEW QUESTION 79
Which DoS Protection Profile detects and prevents session exhaustion attacks against specific destinations?

A. Resource Protection
B. TCP Port Scan Protection
C. Packet Based Attack Protection
D. Packet Buffer Protection

Answer: A

Explanation:
IP flood thresholds, you can also use DoS Protection profiles to detect and prevent session exhaustion attacks in which a large number of hosts (bots) establish as many sessions as possible to consume a target's resources. On the profile's Resources Protection tab, you can set the maximum number of concurrent sessions that the device(s) defined in the DoS Protection policy rule to which you apply the profile can receive. When the number of concurrent sessions reaches its maximum limit, new sessions are dropped.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/

NEW QUESTION 80
Which statement is correct given the following message from the PanGPA log on the GlobalProtect app? Failed to connect to server at port:47 67

A. The PanGPS process failed to connect to the PanGPA process on port 4767
B. The GlobalProtect app failed to connect to the GlobalProtect Portal on port 4767
C. The PanGPA process failed to connect to the PanGPS process on port 4767
D. The GlobalProtect app failed to connect to the GlobalProtect Gateway on port 4767

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/kCSArticleDetail?id=kA10g000000PMiD

NEW QUESTION 83
.....

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