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
Which protocol is supported by GlobalProtect Clientless VPN?

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

Answer: D

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

NEW QUESTION 3
When you import the configuration of an HA pair into Panorama, how do you prevent the import from affecting ongoing traffic?

A. Set the passive link state to shutdown".
B. Disable config sync.
C. Disable the HA2 link.
D. Disable HA.

Answer: B

Explanation:
To prevent the import from affecting ongoing traffic when you import the configuration of an HA pair into Panorama, you should disable config sync on both firewalls. Config sync is a feature that enables the firewalls in an HA pair to synchronize their configurations and maintain consistency. However, when you import the configuration of an HA pair into Panorama, you want to avoid any changes to the firewall configuration until you verify and commit the imported configuration on Panorama. Therefore, you should disable config sync before importing the configuration, and re-enable it after committing the changes on Panorama12. References: Migrate a Firewall HA Pair to Panorama Management, PCNSE Study Guide (page 50)

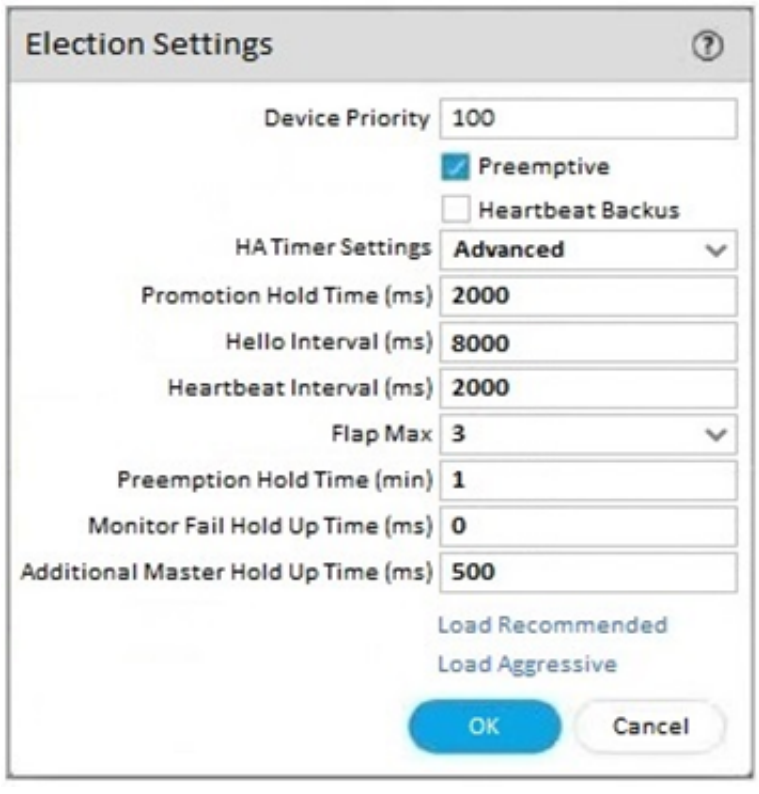
NEW QUESTION 4
Which statement about High Availability timer settings is true?

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 5
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 6
Which template values will be configured on the firewall if each template has an SSL to be deployed. The template stack should consist of four templates arranged according to the diagram.

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

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

Answer: D

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

NEW QUESTION 7
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 8
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 9
An engineer is configuring a firewall with three interfaces:
• MGT connects to a switch with internet access.
• Ethernet1/1 connects to an edge router.
• Ethernet1/2 connects to a visualization network.
The engineer needs to configure dynamic updates to use a dataplane interface for internet traffic. What should be configured in Setup > Services > Service Route Configuration to allow this traffic?

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

Answer: A

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

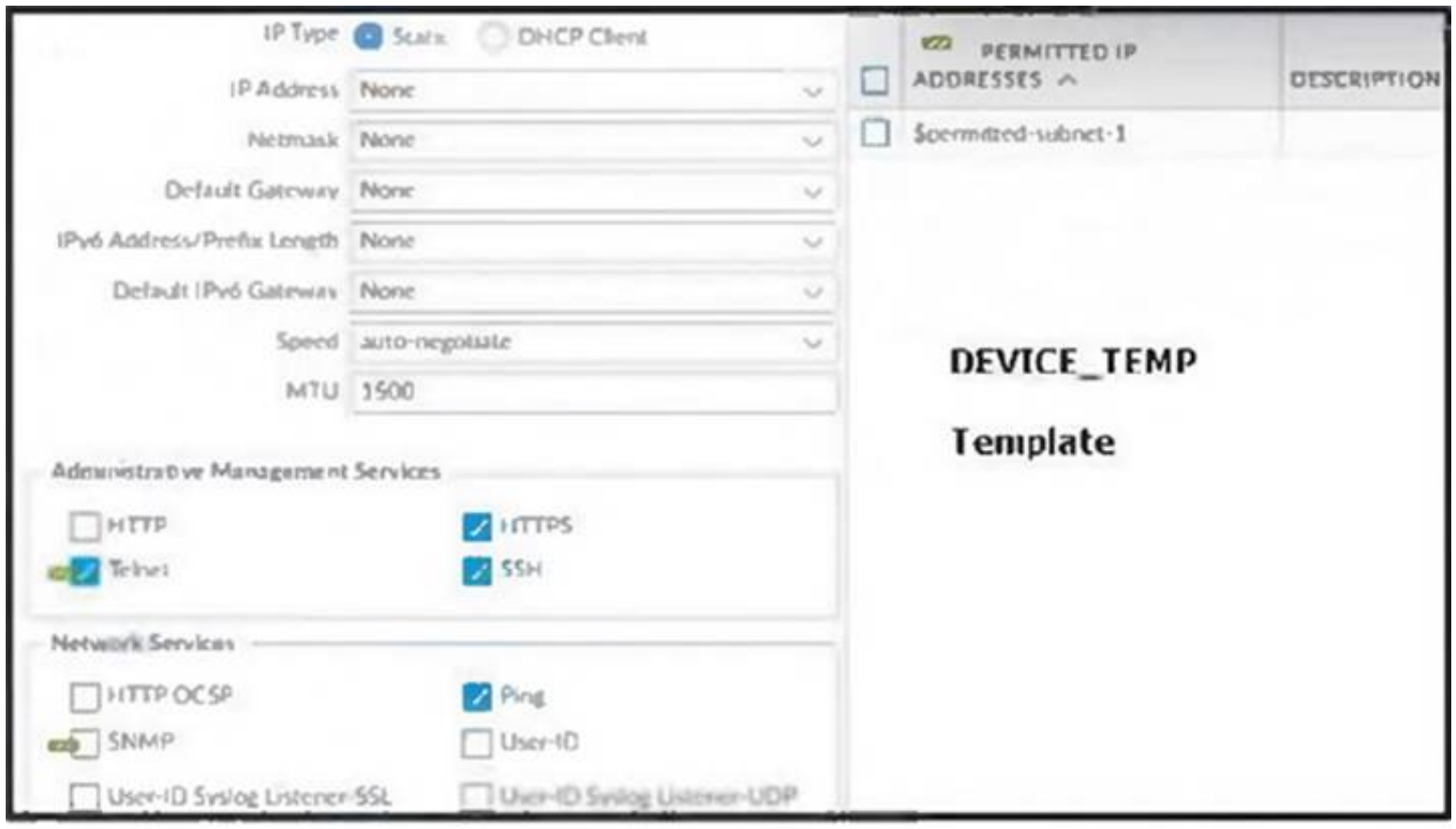
NEW QUESTION 10
An organization is interested in migrating from their existing web proxy architecture to the Web Proxy feature of their PAN-OS 11.0 firewalls. Currently. HTTP and SSL requests contain the c IP address of the web server and the client browser is redirected to the proxy
Which PAN-OS proxy method should be configured to maintain this type of traffic flow?

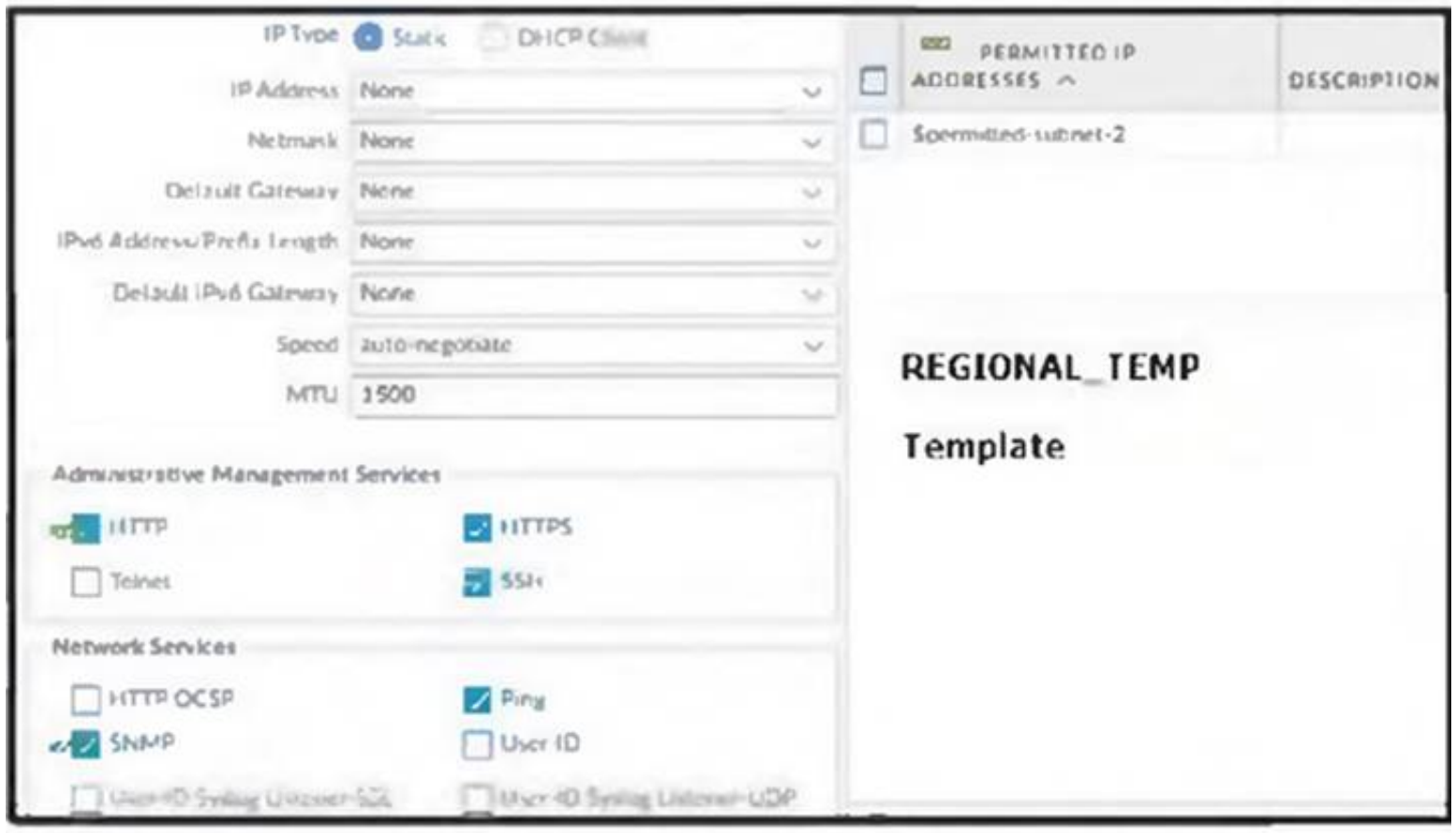
A. DNS proxy
B. Explicit proxy
C. SSL forward proxy
D. Transparent proxy

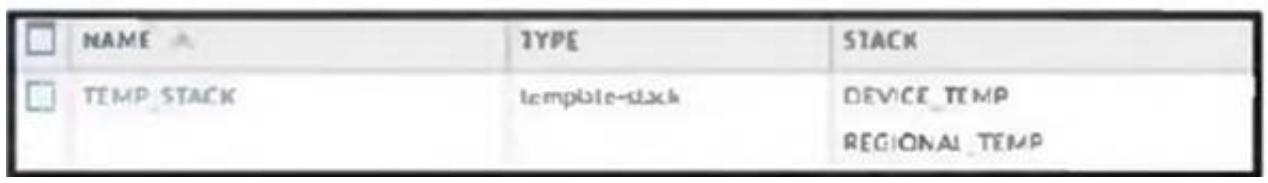
Answer: D

Explanation:
For the transparent proxy method, the request contains the destination IP address of the web server and the proxy transparently intercepts the client request (either by being in-line or by traffic steering). There is no client configuration and Panorama is optional. Transparent proxy requires a loopback interface, User-ID configuration in the proxy zone, and specific Destination NAT (DNAT) rules. Transparent proxy does not support X-Authenticated Users (XAU) or Web Cache Communications Protocol (WCCP). https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy

NEW QUESTION 10
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 15
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)

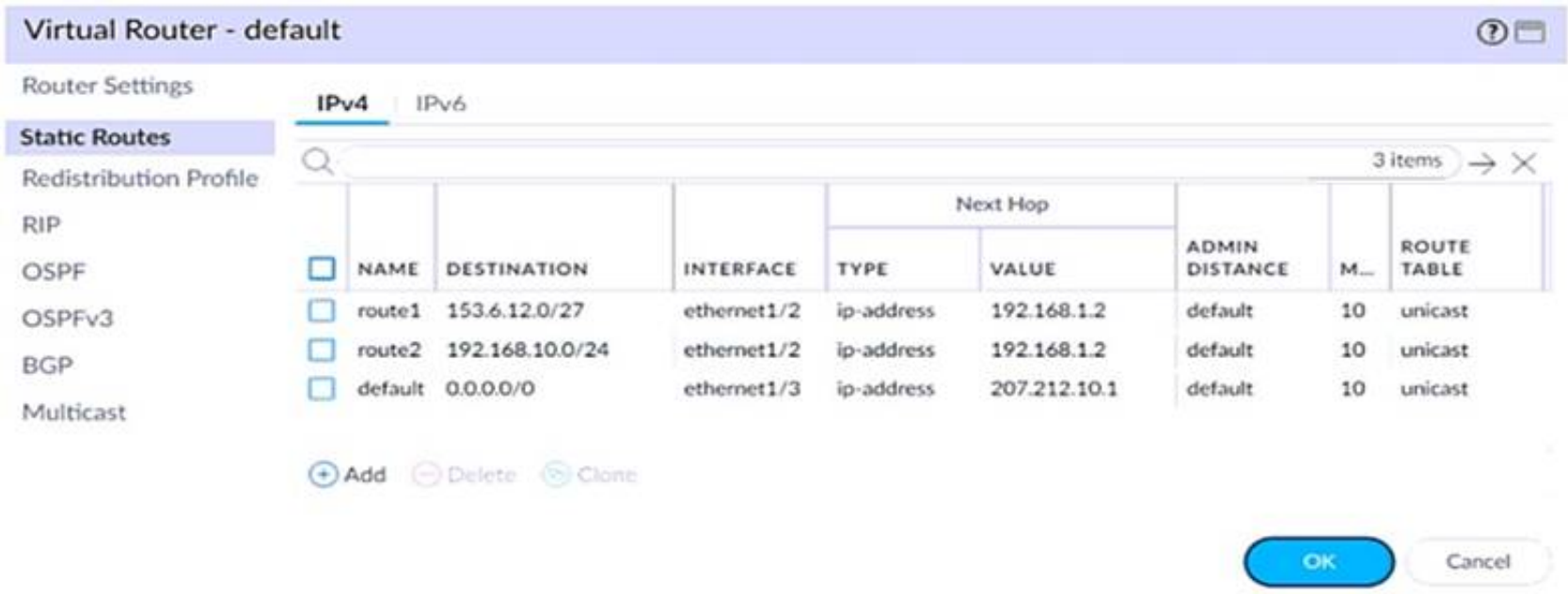
A. upload-onlys
B. install and reboot
C. upload and install
D. upload and install and reboot
E. verify and install

Answer: ACD

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

NEW QUESTION 20
A firewall engineer creates a destination static NAT rule to allow traffic from the internet to a webserver hosted behind the edge firewall. The pre-NAT IP address of the server is 153.6 12.10, and the post-NAT IP address is 192.168.10.10. Refer to the routing and interfaces information below.

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



What should the NAT rule destination zone be set to?

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

Answer: B

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

NEW QUESTION 23
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)

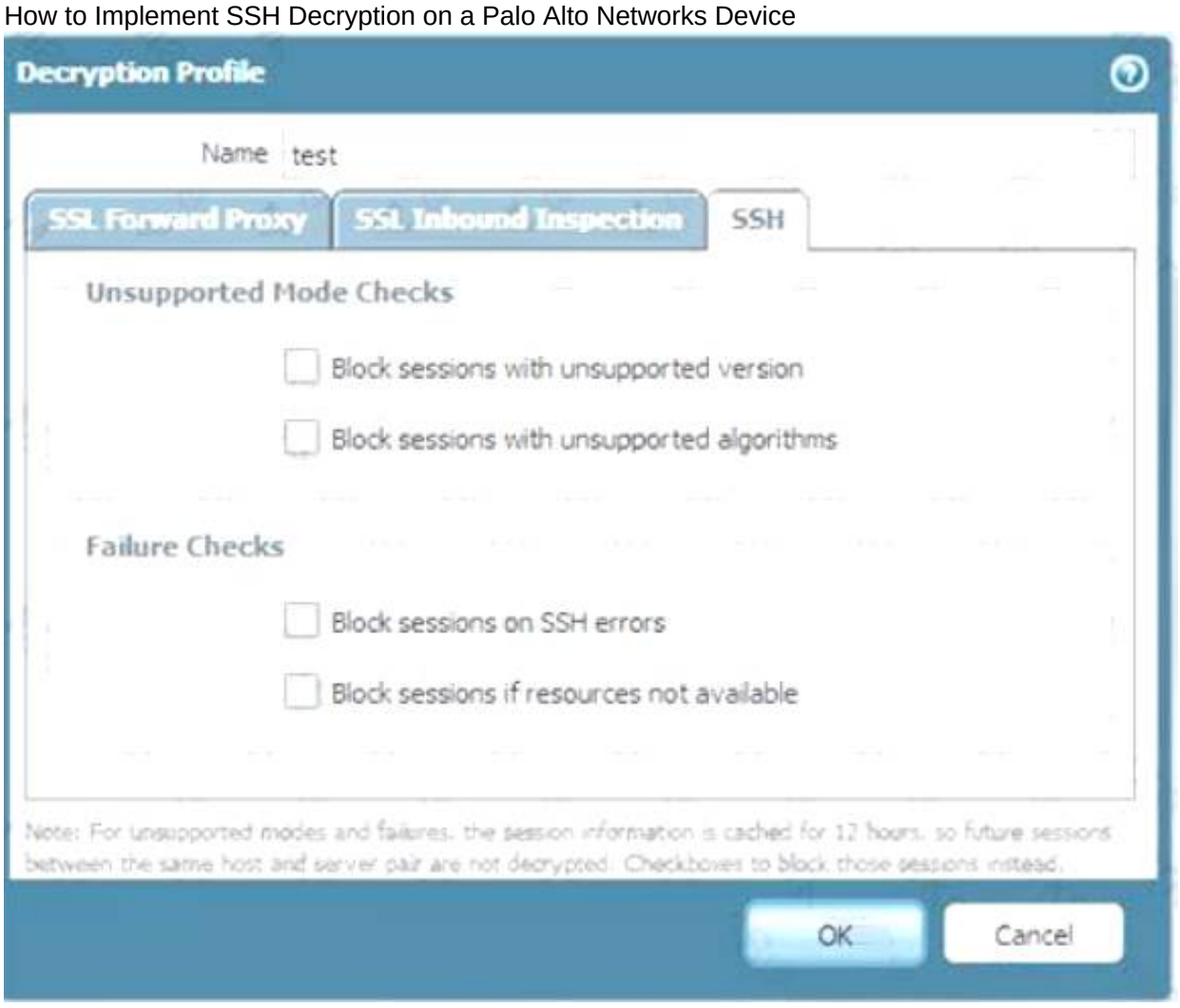
NEW QUESTION 27
An organization wants to begin decrypting guest and BYOD traffic.
Which NGFW feature can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted?

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



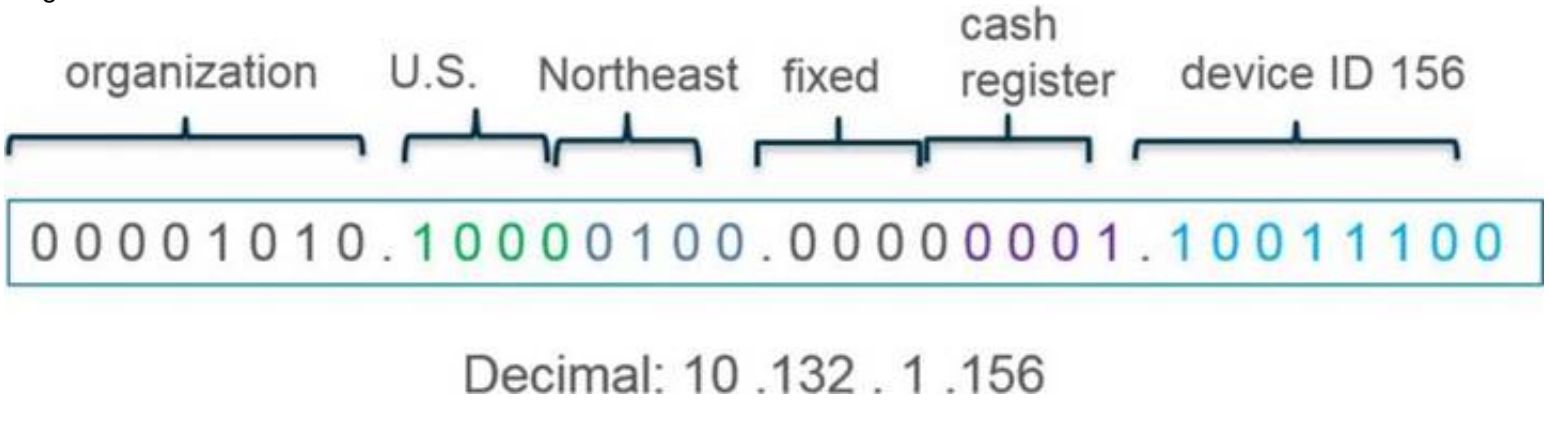
NEW QUESTION 28
Which two profiles should be configured when sharing tags from threat logs with a remote User-ID agent? (Choose two.)

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 31
What type of address object would be useful for internal devices where the addressing structure assigns meaning to certain bits in the address, as illustrated in the diagram?



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

Answer: B

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

NEW QUESTION 32
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 35
Which three options does Panorama offer for deploying dynamic updates to its managed devices? (Choose three.)

A. Check dependencies
B. Schedules
C. Verify
D. Revert content
E. Install

Answer: BDE

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-de https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-de

NEW QUESTION 40
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 44
Which Panorama feature protects logs against data loss if a Panorama server fails?

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

Answer: B

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

NEW QUESTION 46
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 51
An administrator has configured OSPF with Advanced Routing enabled on a Palo Alto Networks firewall running PAN-OS 10.2. After OSPF was configured, the administrator noticed that OSPF routes were not being learned.
Which two actions could an administrator take to troubleshoot this issue? (Choose two.)

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

Answer: AD

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

NEW QUESTION 55
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 59
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 62

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

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

Answer: AD

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

NEW QUESTION 66
What are three tasks that cannot be configured from Panorama by using a template stack? (Choose three.)

A. Change the firewall management IP address
B. Configure a device block list
C. Add administrator accounts
D. Rename a vsys on a multi-vsys firewall
E. Enable operational modes such as normal mode, multi-vsys mode, or FIPS-CC mode

Answer: ACE

NEW QUESTION 71
A company wants to add threat prevention to the network without redesigning the network routing. What are two best practice deployment modes for the firewall? (Choose two.)

A. VirtualWire
B. Layer3
C. TAP
D. Layer2

Answer: AD

Explanation:
- A and D are the best practice deployment modes for the firewall if the company wants to add threat prevention to the network without redesigning the network routing. This is because these modes allow the firewall to act as a transparent device that does not affect the existing network topology or routing1.
- A: VirtualWire mode allows the firewall to be inserted into any existing network segment without changing the IP addressing or routing of that segment2. The firewall inspects traffic between two interfaces that are configured as a pair, called a virtual wire. The firewall applies security policies to the traffic and forwards it to the same interface from which it was received2.
- D: Layer 2 mode allows the firewall to act as a switch that forwards traffic based on MAC addresses3.

The firewall inspects traffic between interfaces that are configured as Layer 2 interfaces and belong to the same VLAN. The firewall applies security policies to the traffic and forwards it to the appropriate interface based on the MAC address table3.
Verified References:
- 1: https://www.garlandtechnology.com/blog/whats-your-palo-alto-ngfw-deployment-plan
- 2: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/networking/configure-interfaces/virtual-wire
- 3: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/networking/configure-interfaces/layer-2.htm

NEW QUESTION 76
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 77
An engineer configures SSL decryption in order to have more visibility to the internal users' traffic when it is regressing the firewall.
Which three types of interfaces support SSL Forward Proxy? (Choose three.)

A. High availability (HA)
B. Layer 3
C. Layer 2

D. Tap
E. Virtual Wire

Answer: BCE

Explanation:
PAN-OS can decrypt and inspect SSL inbound and outbound connections going through the firewall. SSL decryption can occur on interfaces in virtual wire, Layer 2 or Layer 3 mode https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClmyCAC

NEW QUESTION 81
An engineer creates a set of rules in a Device Group (Panorama) to permit traffic to various services for a specific LDAP user group.
What needs to be configured to ensure Panorama can retrieve user and group information for use in these rules?

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

Answer: B

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

NEW QUESTION 83
Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

A. PAN-OS integrated User-ID agent
B. GlobalProtect
C. Windows-based User-ID agent
D. LDAP Server Profile configuration

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user-mapping/globalprote GlobalProtect is a VPN solution that provides secure remote access to corporate networks. When a user connects to GlobalProtect, their identity is verified against an LDAP server. This ensures that all IP address-to-user mappings are explicitly known.

NEW QUESTION 88
An engineer manages a high availability network and requires fast failover of the routing protocols. The engineer decides to implement BFD.
Which three dynamic routing protocols support BFD? (Choose three.)

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

Answer: ABC

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

NEW QUESTION 92
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 96
A company has recently migrated their branch office's PA-220S to a centralized Panorama. This Panorama manages a number of PA-7000 Series and PA-5200 Series devices All device group and template configuration is managed solely within Panorama
They notice that commit times have drastically increased for the PA-220S after the migration What can they do to reduce commit times?

A. Disable "Share Unused Address and Service Objects with Devices" in Panorama Settings.
B. Update the apps and threat version using device-deployment
C. Perform a device group push using the "merge with device candidate config" option

D. Use "export or push device config bundle" to ensure that the firewall is integrated with the Panorama config.

Answer: A

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

NEW QUESTION 100
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 104
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 106
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 108
Which three authentication types can be used to authenticate users? (Choose three.)

A. Local database authentication
B. PingID
C. Kerberos single sign-on
D. GlobalProtect client
E. Cloud authentication service

Answer: ACE

Explanation:
The three authentication types that can be used to authenticate users are:
- A: Local database authentication. This is the authentication type that uses the local user database on the firewall or Panorama to store and verify user credentials1.
- C: Cloud authentication service. This is the authentication type that uses a cloud-based identity provider such as Okta, PingOne, or PingFederate, to authenticate users and provide SAML assertions to the firewall or Panorama2.
- E: Kerberos single sign-on. This is the authentication type that uses the Kerberos protocol to authenticate users who are logged in to a Windows domain and provide them with seamless access to resources on the firewall or Panorama3.

NEW QUESTION 110
A firewall engineer reviews the PAN-OS GlobalProtect application and sees that it implicitly uses web-browsing and depends on SSL.
When creating a new rule, what is needed to allow the application to resolve dependencies?

A. Add SSL and web-browsing applications to the same rule.
B. Add web-browsing application to the same rule.
C. Add SSL application to the same rule.
D. SSL and web-browsing must both be explicitly allowed.

Answer: C

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

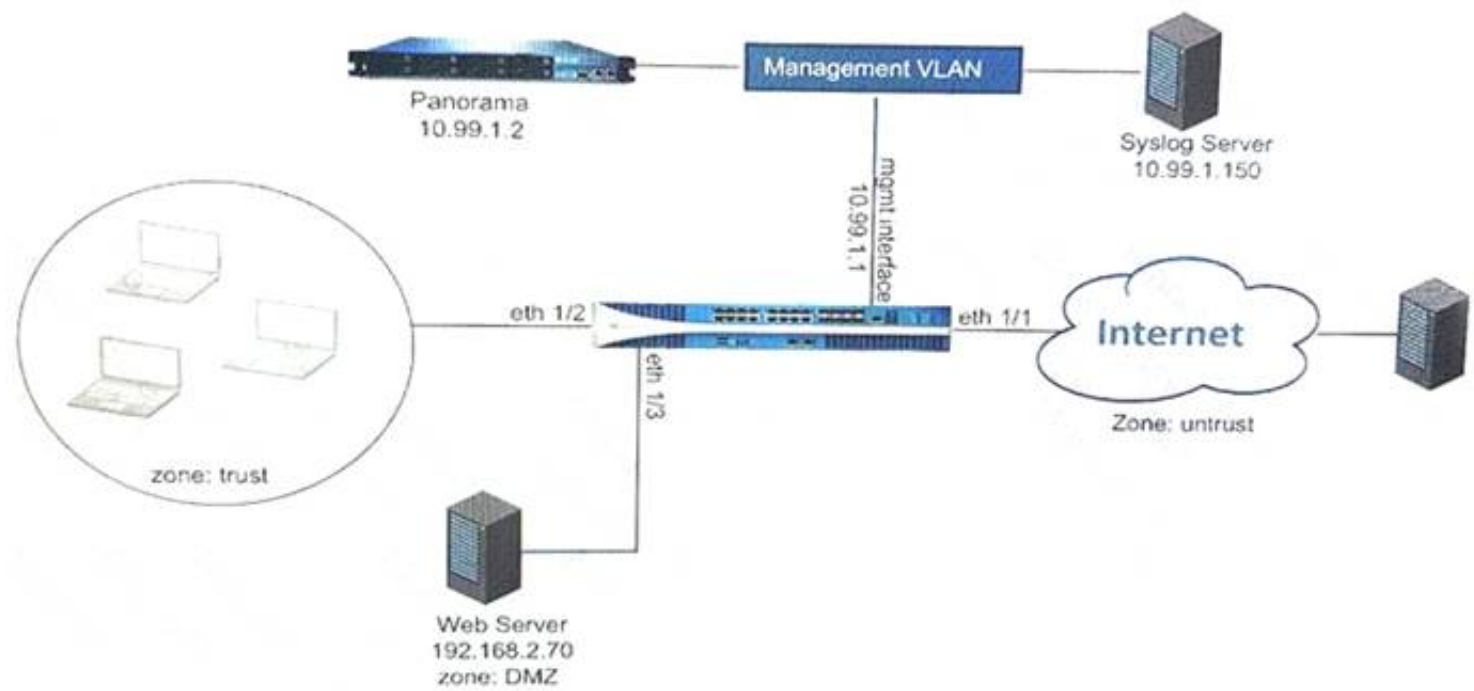
NEW QUESTION 111
An administrator troubleshoots an issue that causes packet drops.
Which log type will help the engineer verify whether packet buffer protection was activated?

A. Data Filtering
B. Configuration
C. Threat
D. Traffic

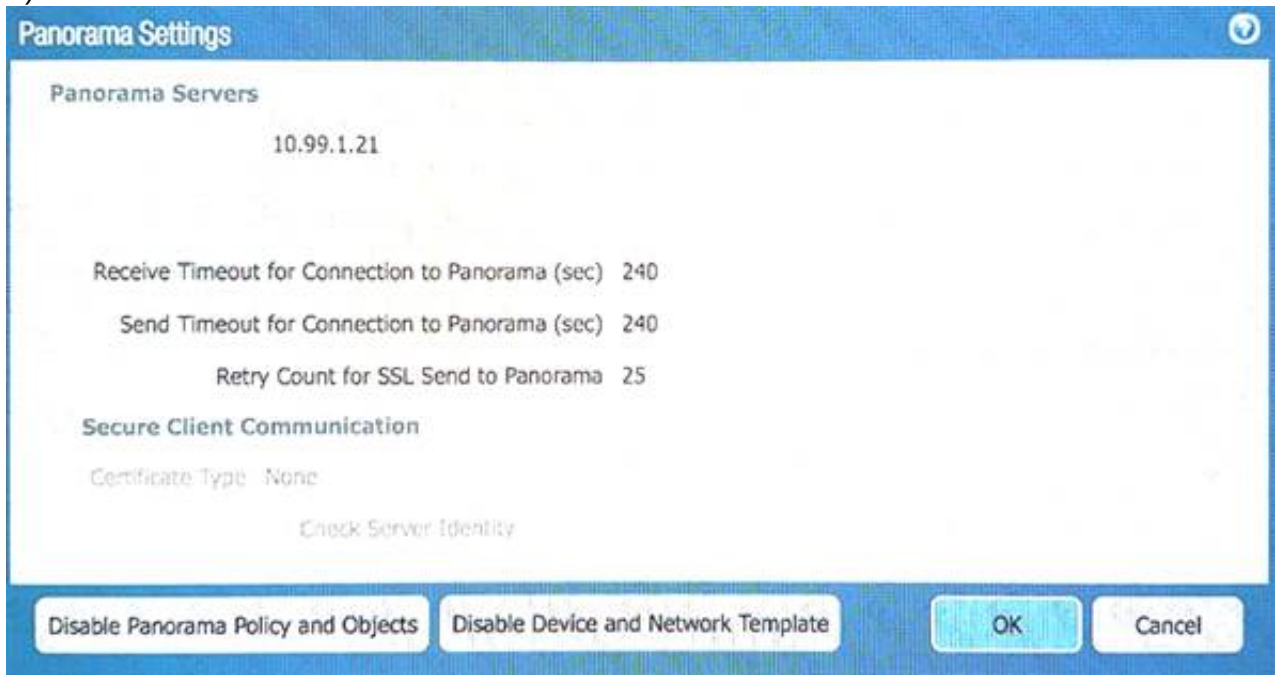
Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNGFCA4

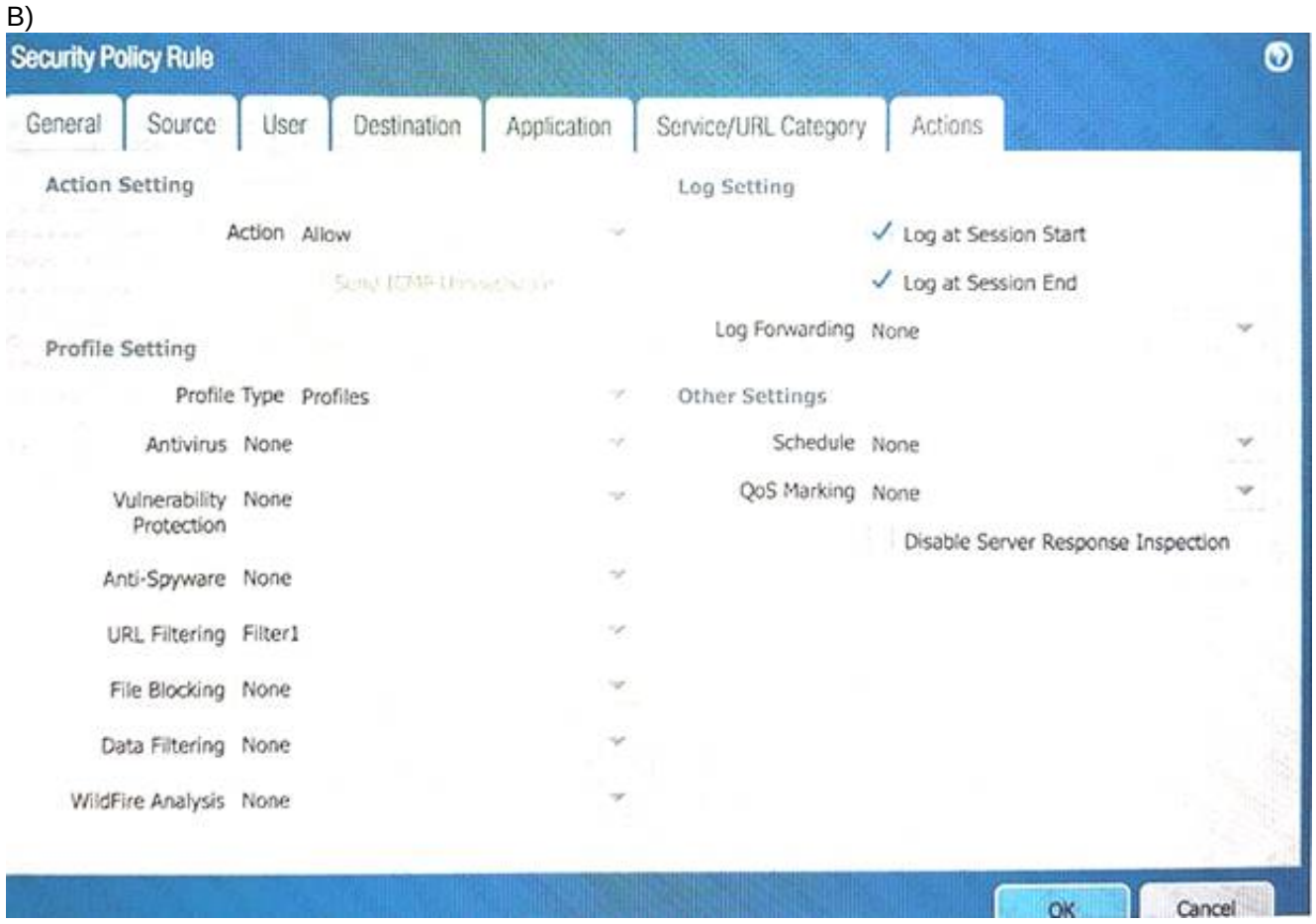
NEW QUESTION 112
Refer to Exhibit:



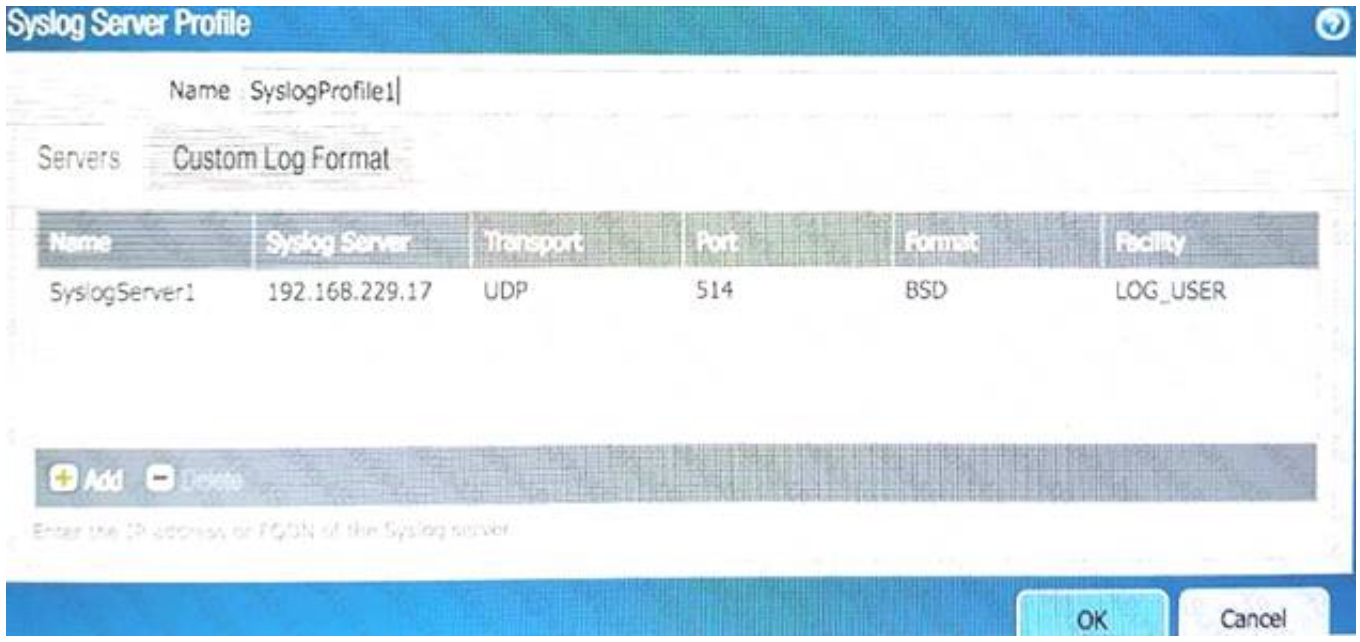
An administrator can not see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall.
Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?
A)



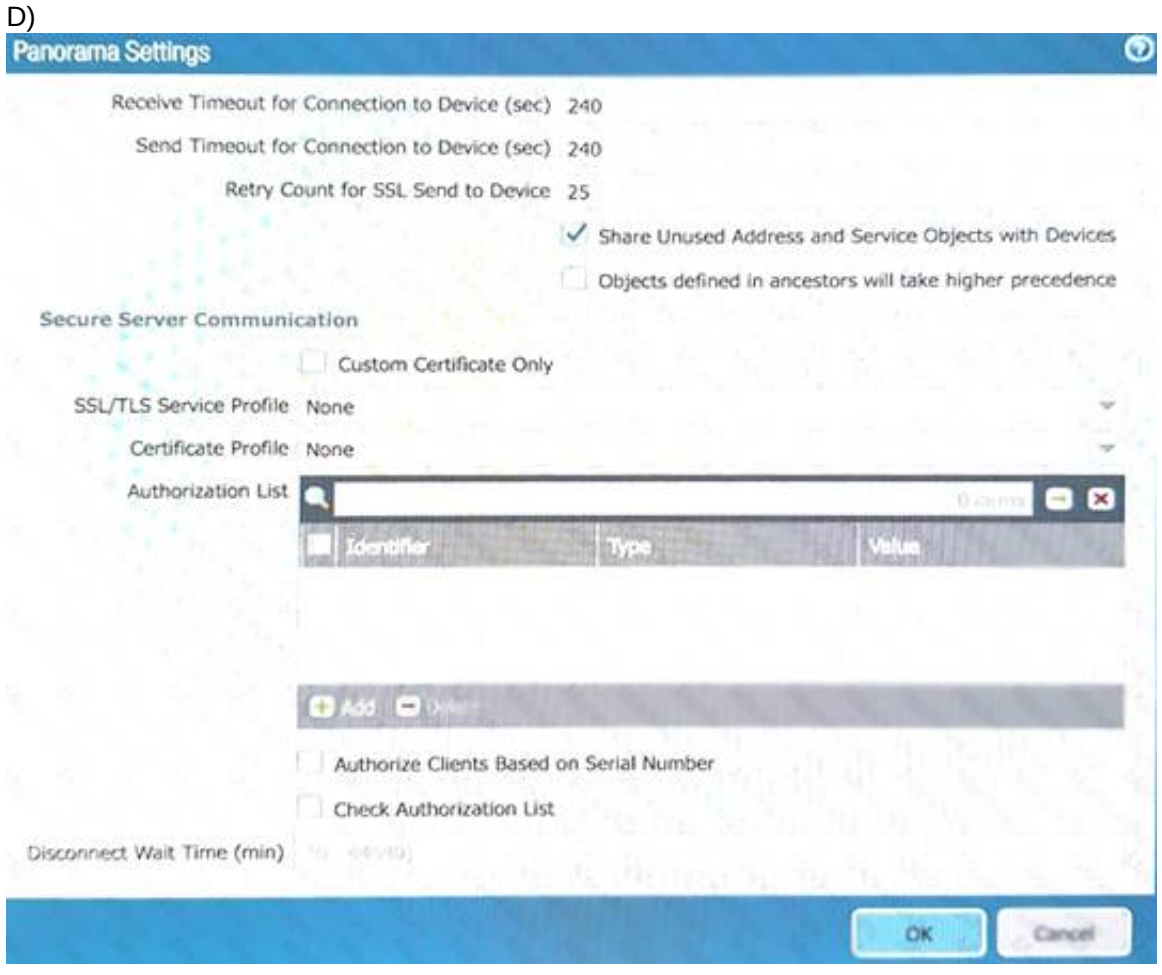
B)



C)



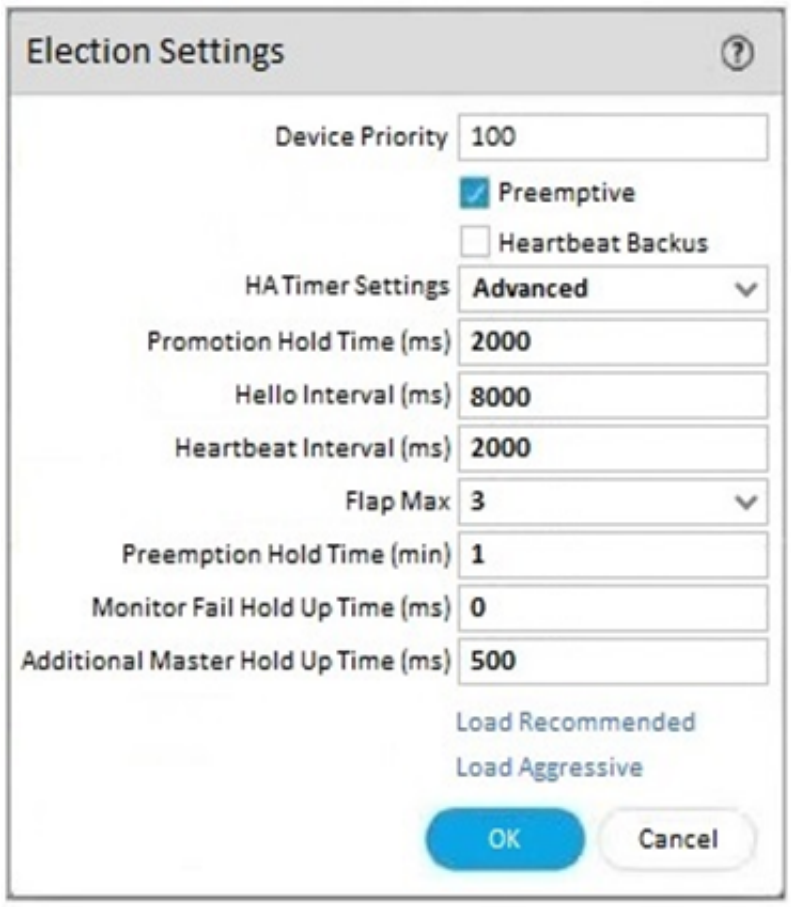
D)



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

Answer: C

NEW QUESTION 114
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 116
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 120
Which new PAN-OS 11.0 feature supports IPv6 traffic?

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

Answer: A

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

NEW QUESTION 121
An administrator has purchased WildFire subscriptions for 90 firewalls globally. What should the administrator consider with regards to the WildFire infra-structure?

A. To comply with data privacy regulations, WildFire signatures and ver-dicts are not shared globally.
B. Palo Alto Networks owns and maintains one global cloud and four WildFire regional clouds.
C. Each WildFire cloud analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds.
D. The WildFire Global Cloud only provides bare metal analysis.

Answer: C

Explanation:
https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts Each WildFire cloud—global (U.S.), regional, and private—analyzes samples and generates WildFire verdicts independently of the other WildFire clouds. With the exception of WildFire private cloud verdicts, WildFire verdicts are shared globally, enabling WildFire users to access a worldwide database of threat data.
https://docs.paloaltonetworks.com/wildfire/10-1/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts.ht

NEW QUESTION 123
An engineer must configure a new SSL decryption deployment.
Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

A. A Decryption profile must be attached to the Decryption policy that the traffic matches.
B. A Decryption profile must be attached to the Security policy that the traffic matches.
C. There must be a certificate with only the Forward Trust option selected.
D. There must be a certificate with both the Forward Trust option and Forward Untrust option selected.

Answer: A

Explanation:
To use PAN-OS multi-factor authentication (MFA) to secure access to critical assets, the enterprise should configure a Captive Portal authentication policy that uses an authentication sequence. An authentication sequence is a feature that allows the firewall to enforce multiple authentication methods (factors) for users who access sensitive services or applications. An authentication sequence can include up to four factors, such as login and password, Voice, SMS, Push, or One-time Password (OTP) authentication. The firewall can integrate with MFA vendors through RADIUS or vendor APIs to provide the additional factors12.
To configure an authentication sequence, the enterprise needs to create an authentication profile for each factor and then add them to the sequence in the desired order. The enterprise also needs to create a Captive Portal authentication policy that matches the traffic that requires MFA and applies the authentication sequence to it. The Captive Portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The Captive Portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button34.
When a user tries to access a service or application that matches the Captive Portal authentication policy, the firewall redirects the user to the Captive Portal web form for the first factor. After the user successfully authenticates for the first factor, the firewall prompts the user for the second factor through RADIUS or vendor API integration. The firewall repeats this process until all factors in the sequence are completed or until one factor fails. If all factors are completed successfully, the firewall allows the user to access the service or application. If one factor fails, the firewall denies access and logs an event56.
Configuring a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile is not sufficient to use PAN-OS MFA. This option only provides one factor of authentication through RADIUS integration with an MFA vendor. To use multiple factors of authentication, an authentication sequence is required.
Creating an authentication profile and assigning another authentication factor to be used by a Captive Portal authentication policy is not correct to use PAN-OS MFA. This option does not specify how to create or apply an authentication sequence, which is necessary for enforcing multiple factors of authentication.
Using a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns is not relevant to use PAN-OS MFA. This option is a feature of Palo Alto Networks Cortex XDR™ that helps
protect endpoints from credential theft by malicious actors. It does not provide any MFA functionality for accessing critical assets7.
References: Authentication Sequence, Configure Multi-Factor Authentication, Configure an Authenticatio Portal, Create an Authentication Profile, Create an Authentication Sequence, Create a Captive Portal Authentication Policy, Credential Phishing Agent

NEW QUESTION 127
.....

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