Exam Questions PCNSE

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

https://www.2passeasy.com/dumps/PCNSE/

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 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 3
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 4
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 5
Which statement about High Availability timer settings is true?

A. Use the Critical timer for faster failover timer settings.

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

Answer: D

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

NEW QUESTION 6
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 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 8
Which two policy components are required to block traffic in real time using a dynamic user group (DUG)? (Choose two.)

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

Answer: AB

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

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-dynamic-user-groups-in-policy

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

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

Answer: AC

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

NEW QUESTION 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 15
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 17
A network security administrator has been tasked with deploying User-ID in their organization. What are three valid methods of collecting User-ID information in a network? (Choose three.)

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

Answer: ABC

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

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

NEW QUESTION 18
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 22
An administrator configures a site-to-site IPsec VPN tunnel between a PA-850 and an external customer on their policy-based VPN devices.
What should an administrator configure to route interesting traffic through the VPN tunnel?

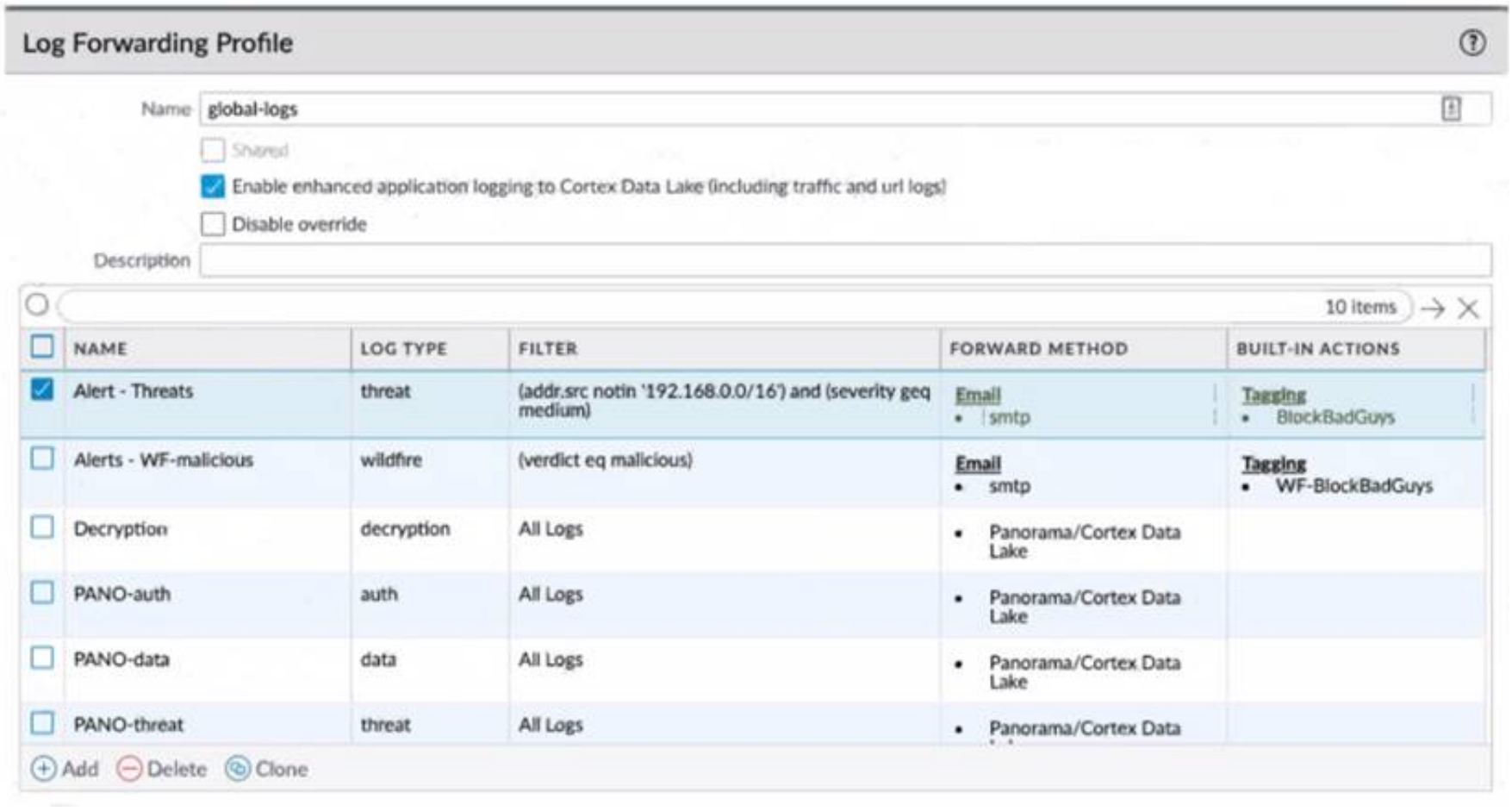
A. Proxy IDs
B. GRE Encapsulation
C. Tunnel Monitor
D. ToS Header

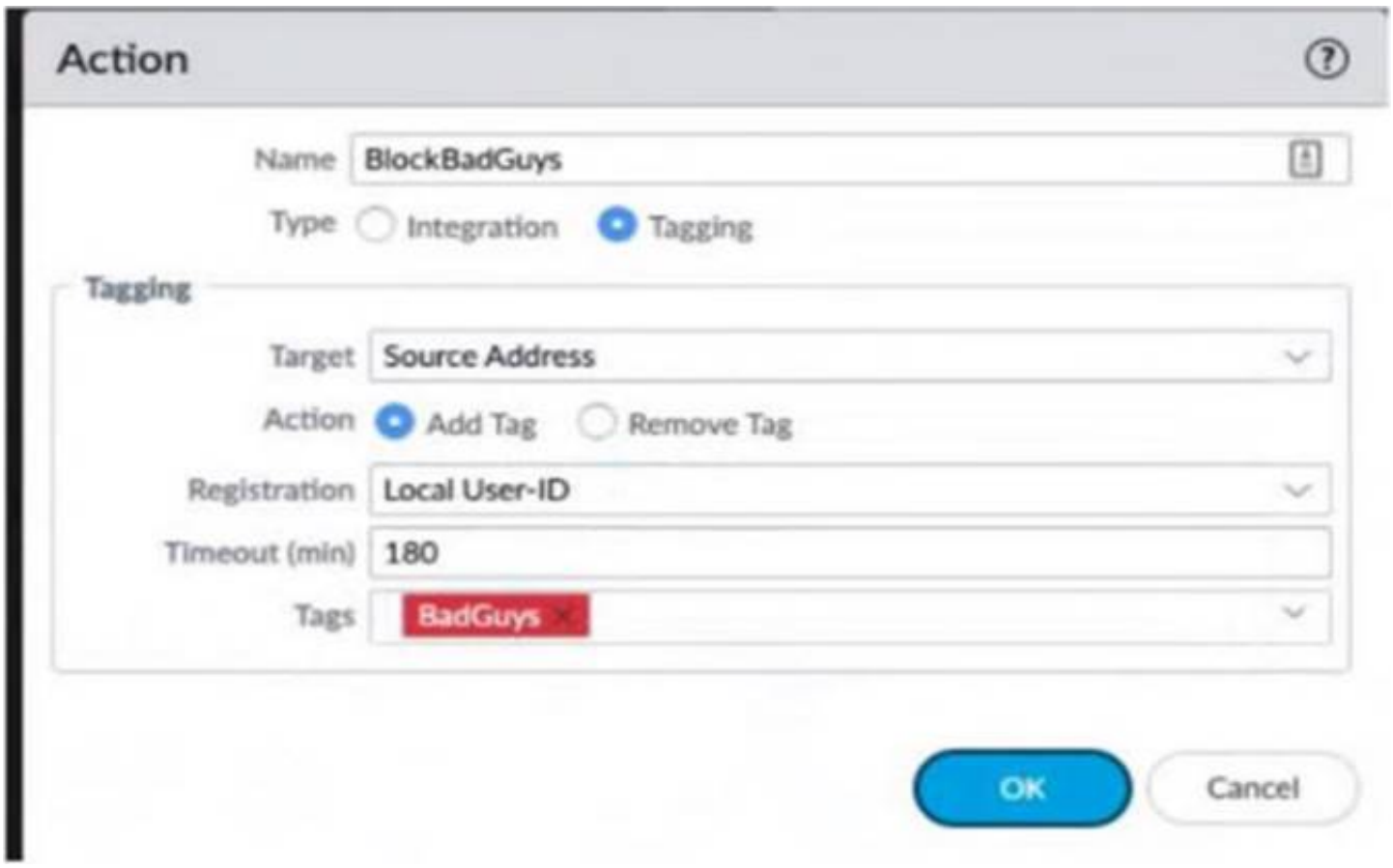
Answer: A

Explanation:
An administrator should configure proxy IDs to route interesting traffic through the VPN tunnel when the peer device is a policy-based VPN device. Proxy IDs are used to identify the traffic that belongs to a particular IPSec VPN and to direct it to the appropriate tunnel. Proxy IDs consist of a local IP address, a remote IP address, and an application (protocol and port numbers). Each proxy ID is considered to be a VPN tunnel and is counted towards the IPSec VPN tunnel capacity of the firewall. Proxy IDs are required for IKEv1 VPNs and optional for IKEv2 VPNs. If the proxy ID is not configured, the firewall uses the default values of source IP: 0.0.0.0/0, destination IP: 0.0.0.0/0, and application: any, which may not match the peer's policy and result in a failure to establish the VPN connection.
References:

- Proxy ID for IPSec VPN
- Set Up an IPSec Tunnel

NEW QUESTION 25
Review the images.





A firewall policy that permits web traffic includes the global-logs policy is depicted What is the result of traffic that matches the "Alert - Threats" Profile Match List?

A. The source address of SMTP traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.
B. The source address of traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.
C. The source address of traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.
D. The source address of SMTP traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.

Answer: C

NEW QUESTION 30
During the process of developing a decryption strategy and evaluating which websites are required for corporate users to access, several sites have been identified that cannot be decrypted due to technical reasons. In this case, the technical reason is unsupported ciphers Traffic to these sites will therefore be blocked if decrypted.
How should the engineer proceed?

A. Install the unsupported cipher into the firewall to allow the sites to be decrypted
B. Allow the firewall to block the sites to improve the security posture.
C. Add the sites to the SSL Decryption Exclusion list to exempt them from decryption.
D. Create a Security policy to allow access to those sites.

Answer: C

Explanation:
If some sites cannot be decrypted due to technical reasons, such as unsupported ciphers, and blocking them is not an option, then the engineer should add the sites to the SSL Decryption Exclusion list to exempt them from decryption. The SSL Decryption Exclusion list is a predefined list of sites that are not subject to SSL decryption by the firewall. The list includes sites that use certificate pinning, mutual authentication, or unsupported cipher suites. The engineer can also add custom sites to the list if they have a valid business reason or technical limitation for not decrypting them34. Adding the sites to the SSL Decryption Exclusion list will allow the traffic to pass through without being decrypted or blocked by the firewall. References: SSL Decryption Exclusion, Troubleshoot Unsupported Cipher Suites

NEW QUESTION 34
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 36
An organization conducts research on the benefits of leveraging the Web Proxy feature of PAN-OS 11.0. What are two benefits of using an explicit proxy method versus a transparent proxy method? (Choose two.)

A. No client configuration is required for explicit proxy, which simplifies the deployment complexity.
B. Explicit proxy supports interception of traffic using non-standard HTTPS ports.
C. It supports the X-Authenticated-User (XAU) header, which contains the authenticated username in the outgoing request.
D. Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy.

Answer: CD

Explanation:
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-us https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy

NEW QUESTION 40
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 41
A network security administrator has an environment with multiple forms of authentication. There is a network access control system in place that authenticates and restricts access for wireless users, multiple Windows domain controllers, and an MDM solution for company-provided smartphones. All of these devices have their authentication events logged.
Given the information, what is the best choice for deploying User-ID to ensure maximum coverage?

A. Captive portal
B. Standalone User-ID agent
C. Syslog listener
D. Agentless User-ID with redistribution

Answer: C

Explanation:
A syslog listener is the best choice for deploying User-ID to ensure maximum coverage in an environment with multiple forms of authentication. A syslog listener is a feature that enables the firewall or Panorama to receive syslog messages from other systems and parse them for IP address-to-username mappings. A syslog listener can collect user mapping information from a variety of sources, such as network access control systems, domain controllers, MDM solutions, VPN gateways, wireless controllers, proxies, and more2. A syslog listener can also support multiple platforms and operating systems, such as Windows, Linux, macOS, iOS, Android, etc3. Therefore, a syslog listener can provide a comprehensive and flexible solution for User-ID deployment in a large-scale network. References: Configure a Syslog Listener for User Mapping, User-ID Agent Deployment Guide, PCNSE Study Guide (page 48)

NEW QUESTION 43
An engineer is deploying multiple firewalls with common configuration in Panorama. What are two benefits of using nested device groups? (Choose two.)

A. Inherit settings from the Shared group
B. Inherit IPSec crypto profiles
C. Inherit all Security policy rules and objects
D. Inherit parent Security policy rules and objects

Answer: AD

Explanation:

https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-conf

NEW QUESTION 46
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 49
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."

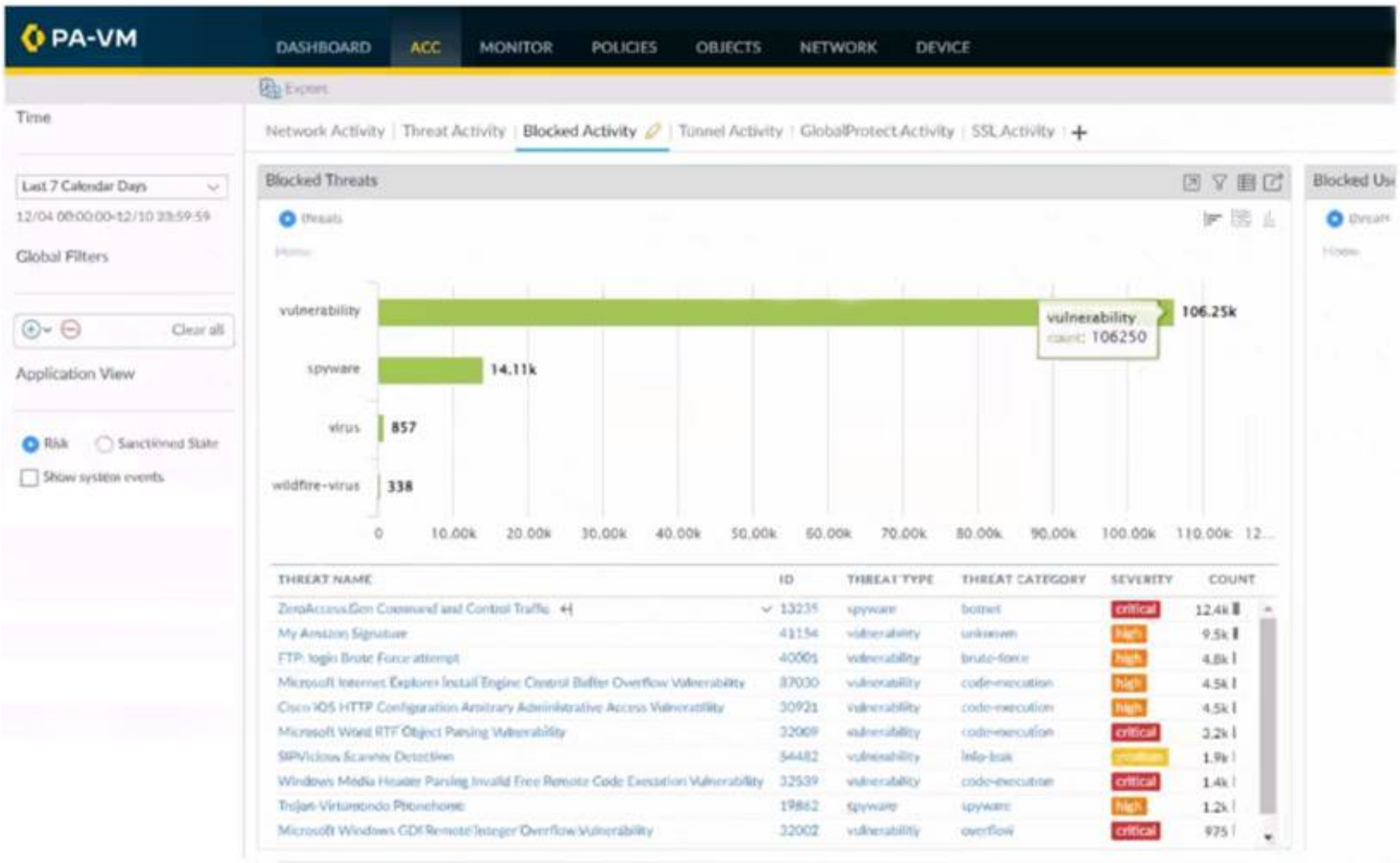
NEW QUESTION 51
Which type of policy in Palo Alto Networks firewalls can use Device-ID as a match condition?

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 54
Refer to the exhibit.



Using the above screenshot of the ACC, what is the best method to set a global filter, narrow down Blocked User Activity, and locate the user(s) that could be compromised by a botnet?

A. Click the hyperlink for the Zero Access.Gen threat.
B. Click the left arrow beside the Zero Access.Gen threat.
C. Click the source user with the highest threat count.
D. Click the hyperlink for the hotport threat Category.

Answer: B

Explanation:
Hover over an attribute in the table below the chart and click the arrow icon to the right of the attribute. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-the-application-command-center/int

NEW QUESTION 56
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 59
Based on the graphic which statement accurately describes the output shown in the Server Monitoring panel?

A. The User-ID agent is connected to a domain controller labeled lab-client
B. The host lab-client has been found by a domain controller
C. The host lab-client has been found by the User-ID agent.
D. The User-ID aaent is connected to the firewall labeled lab-client

Answer: A

NEW QUESTION 64
What must be configured to apply tags automatically based on User-ID logs?

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

Answer: B

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

NEW QUESTION 67
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

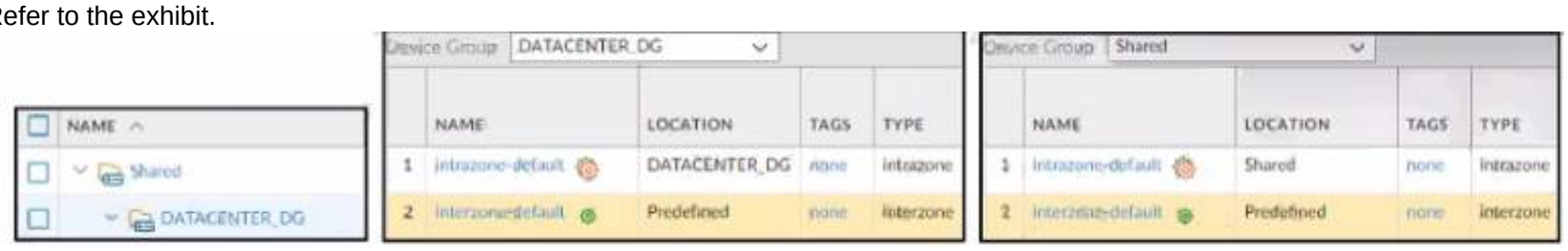
NEW QUESTION 70
A company has recently migrated their branch office's PA-220S to a centralized Panorama. This Panorama manages a number of PA-7000 Series and PA-5200 Series devices All device group and template configuration is managed solely within Panorama
They notice that commit times have drastically 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 71
Refer to the exhibit.



Based on the screenshots above what is the correct order in which the various rules are deployed to firewalls inside the DATACENTER_DG device group?

A. shared pre-rules DATACENTER DG pre rulesrules configured locally on the firewall shared post-rules DATACENTER_DG post-rules DATACENTER.DG default rules
B. shared pre-rules DATACENTER_DG pre-rulesrules configured locally on the firewall shared post-rulesDATACENTER.DG post-rules shared default rules
C. shared pre-rules DATACENTER_DG pre-rulesrules configured locally on the firewall DATACENTER_DG post-rules shared post-rulesshared default rules
D. shared pre-rules DATACENTER_DG pre-rulesrules configured locally on the firewall DATACENTER_DG post-rules shared post-rules DATACENTER_DG default rules

Answer: A

NEW QUESTION 76
The decision to upgrade PAN-OS has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when attempting the install.
When performing an upgrade on Panorama to PAN-OS. what is the potential cause of a failed install?

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

Answer: A

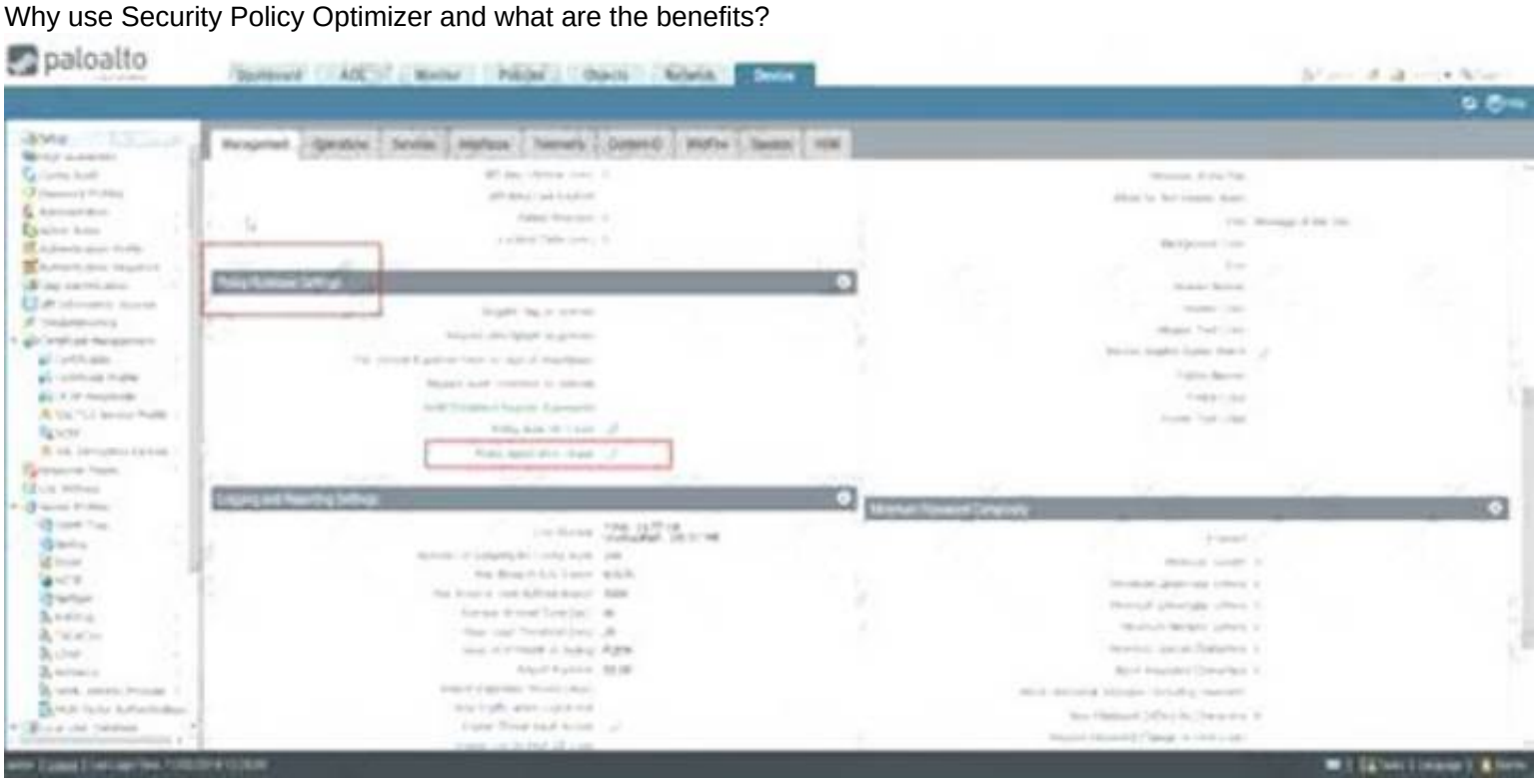
Explanation:
One of the potential causes of a failed install when upgrading Panorama to PAN-OS is having outdated plugins. Plugins are software extensions that enable Panorama to interact with Palo Alto Networks cloud services and third-party services. Plugins have dependencies on specific PAN-OS versions,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

NEW QUESTION 78
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 81
Which three authentication types can be used to authenticate users? (Choose three.)

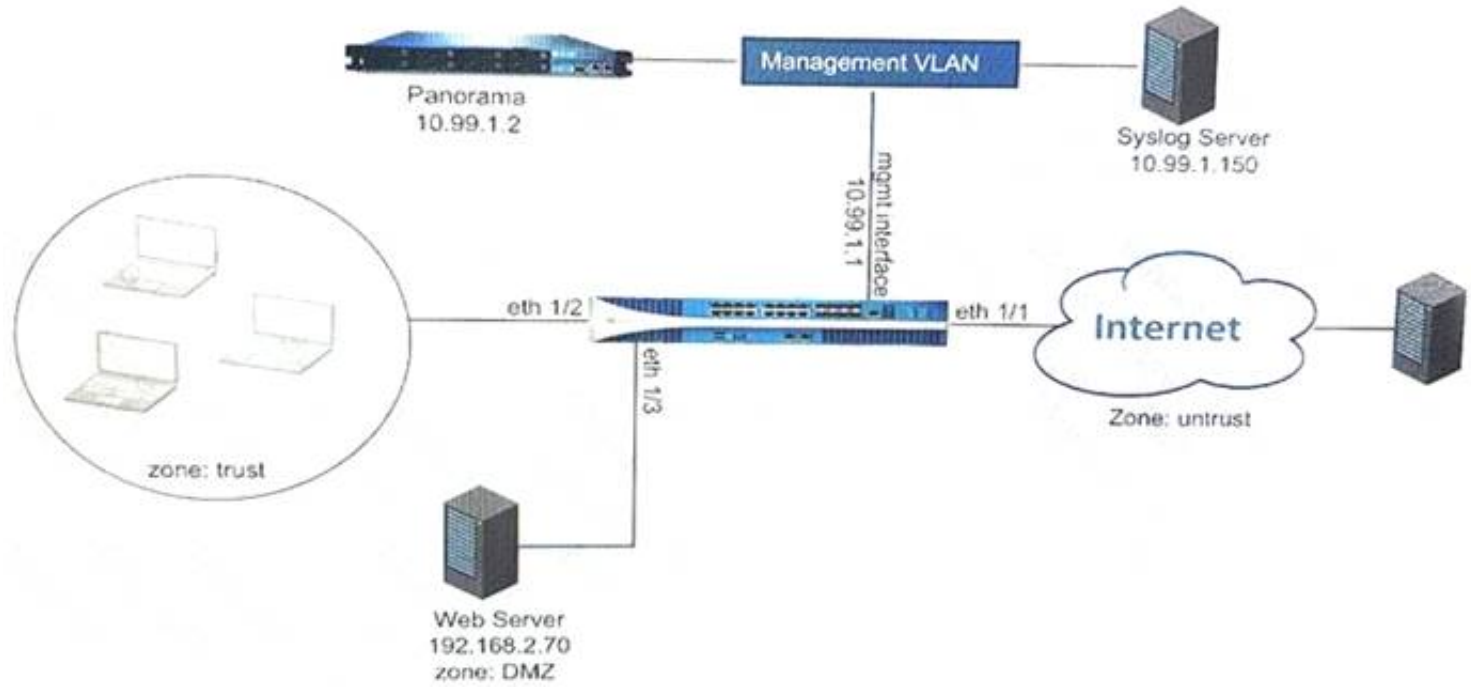
A. Local database authentication
B. PingID
C. Kerberos single sign-on
D. GlobalProtect client
E. Cloud authentication service

Answer: ACE

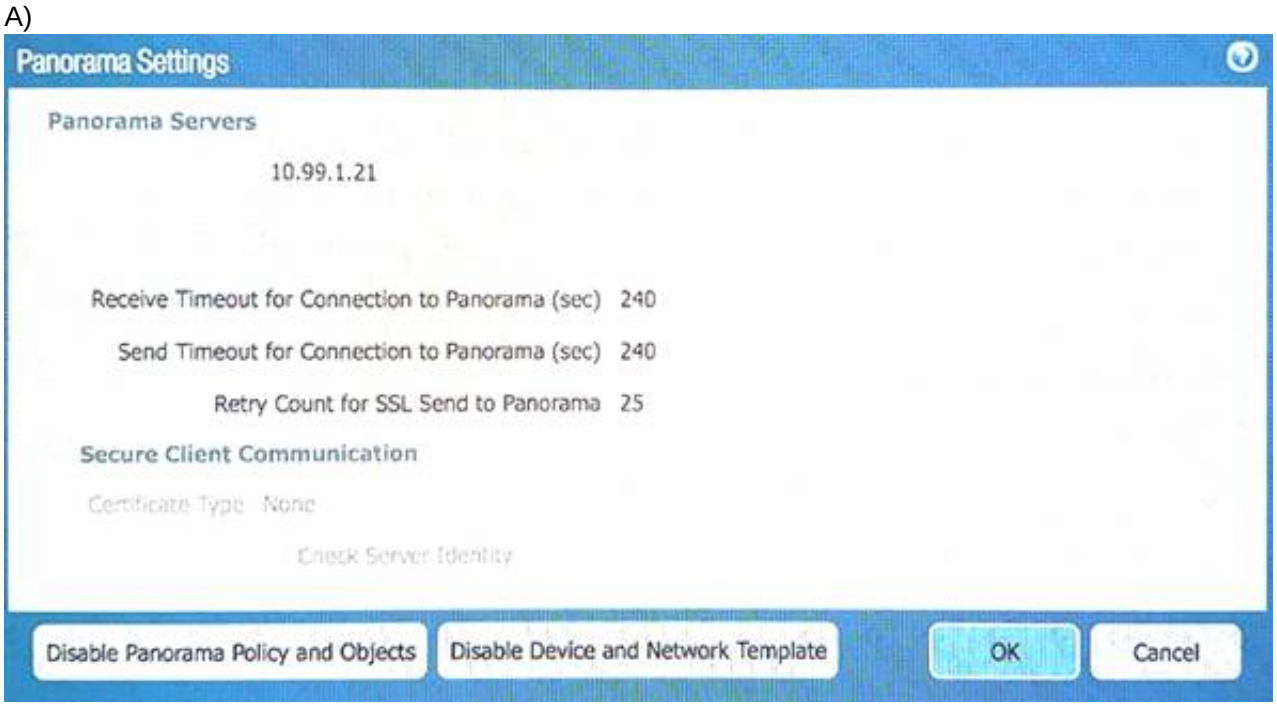
Explanation:
The three authentication types that can be used to authenticate users are:

- 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.

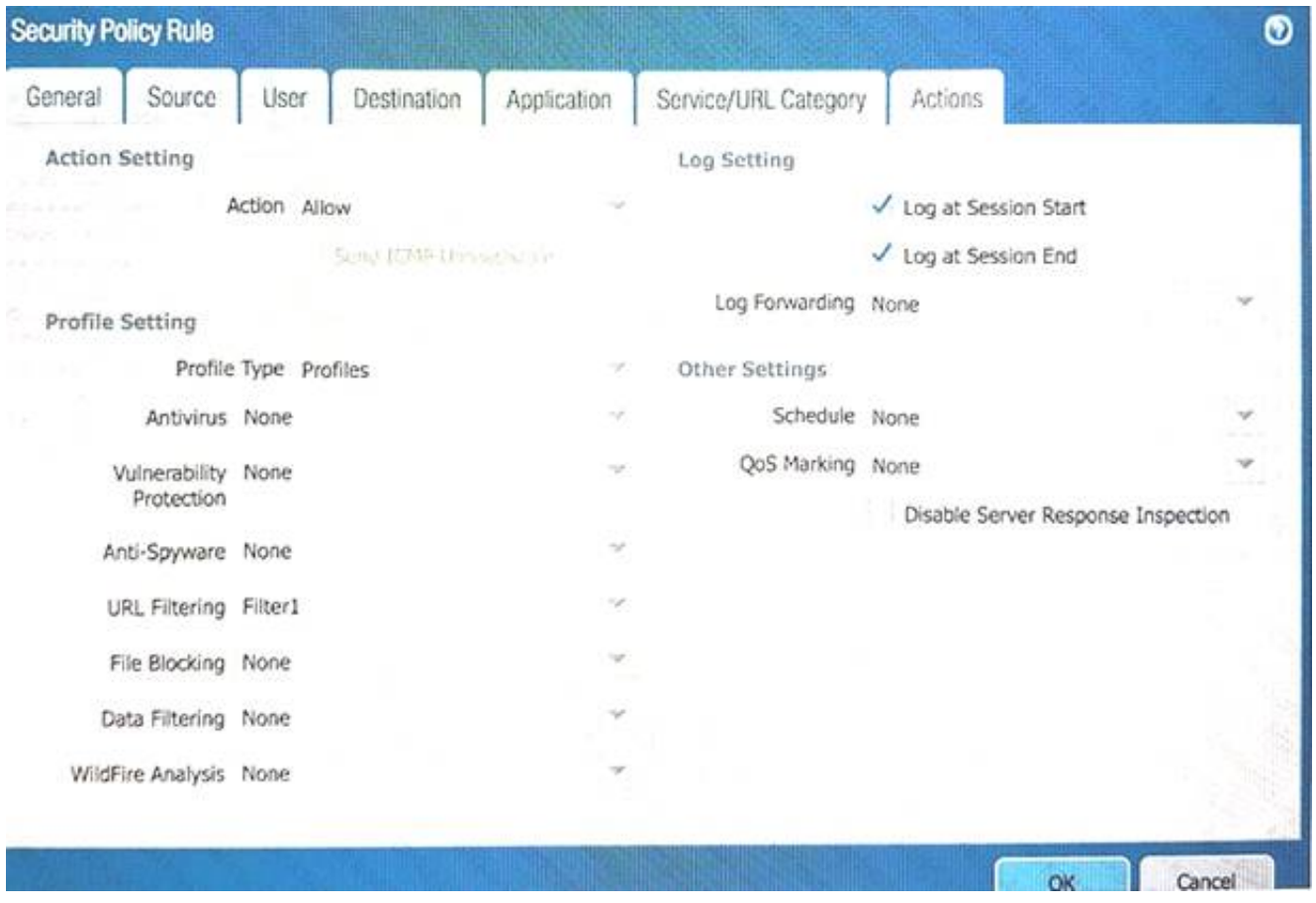
NEW QUESTION 82
Refer to Exhibit:



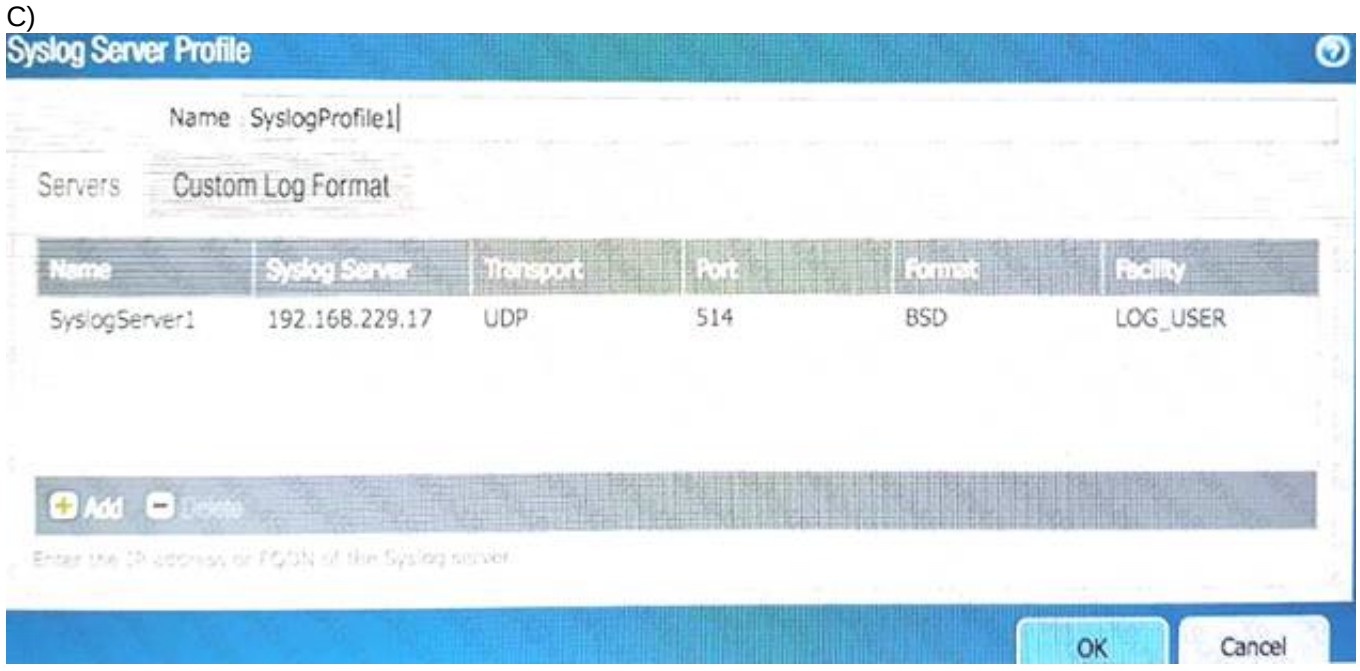
An administrator can not see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall.
Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?
A)



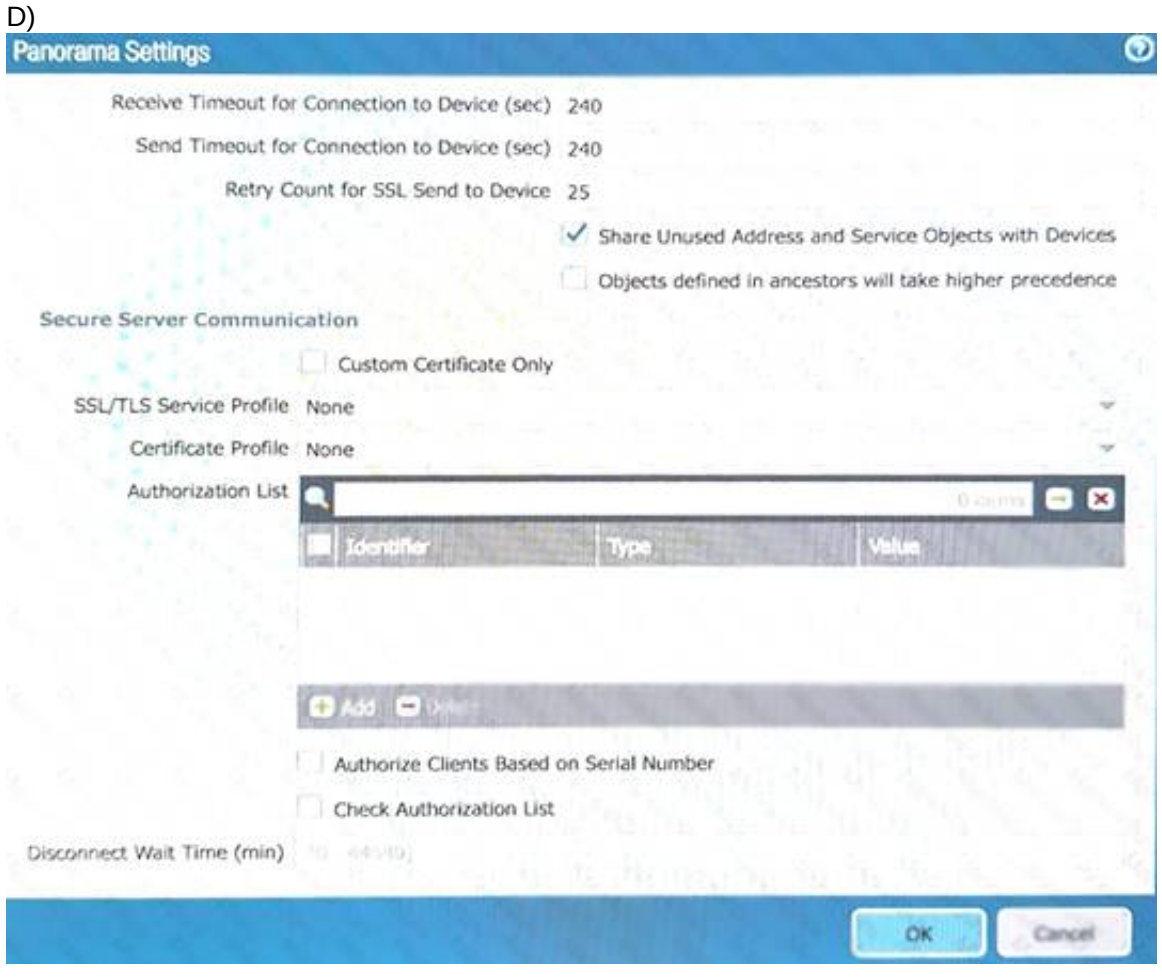
B)



C)



D)



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

Answer: C

NEW QUESTION 87
Review the screenshot of the Certificates page.

An administrator for a small LLC has created a series of certificates as shown, to use for a planned Decryption roll out. The administrator has also installed the self-signed root certificate in all client systems.
When testing, they noticed that every time a user visited an SSL site, they received unsecured website warnings.
What is the cause of the unsecured website warnings?

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

Answer: D

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

NEW QUESTION 91
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 93
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCNSE Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PCNSE Product From:

https://www.2passeasy.com/dumps/PCNSE/

Money Back Guarantee

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