Exam Code: PCNSE
Exam Name: Palo Alto Networks Certified Network Security Engineer

Exam A

QUESTION 1
Which statement regarding HA timer settings is true?

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

Correct Answer: A
Section:
Explanation:
The Recommended profile is the default profile that provides typical failover timer settings for most deployments. The other profiles are designed for specific scenarios where faster or slower failover isdesired. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high- availability/ha-concepts/ha-timers

QUESTION 2
While analyzing the Traffic log, you see that some entries show "unknown-tcp" in the Application column What best explains these occurrences?

A. A handshake took place, but no data packets were sent prior to the timeout.
B. A handshake took place; however, there were not enough packets to identify the application.
C. A handshake did take place, but the application could not be identified.
D. A handshake did not take place, and the application could not be identified.

Correct Answer: C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC#:~:text=un known%2Dtcp%3A,firewall%20does%20not%20have%20signatures.Unknown-tcp means the firewall captured the three-way TCP handshake, but the application was not identified. This may be due to the use of a custom application for which the firewall does not have signatures

QUESTION 3
A firewall should be advertising the static route 10.2.0.0/24 Into OSPF. The configuration on the neighbor is correct, but the route is not in the neighbor's routing table.
Which two configurations should you check on the firewall? (Choose two.)

A. In the OSFP configuration, ensure that the correct redistribution profile is selected in the OSPF Export Rules section.
B. Within the redistribution profile ensure that Redist is selected.
C. Ensure that the OSPF neighbor state Is "2-Way."
D. In the redistribution profile check that the source type is set to "ospf."

Correct Answer: A, B
Section:
Explanation:
A redistribution profile defines which routes from one routing protocol are redistributed into another routing protocol. In the OSPF configuration, the OSPF Export Rules section allows you to select which redistribution profiles to apply for exporting routes into OSPF. Within the redistribution profile, you need to select Redist as the option to redistribute the routes that match the profile filter. If you select No Redist, the routes that match the profile filter will not be redistributed.

Ensuring that the OSPF neighbor state is "2-Way" is not relevant for advertising a static route into OSPF, as this state indicates that the neighbor relationship is established but not synchronized. In the redistribution profile, the source type should be set to "static" if you want to redistribute a static route into OSPF, not "ospf". Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/route- redistribution/configure-route-redistribution https:// knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClfnCAC

QUESTION 4
Which statement best describes the Automated Commit Recovery feature?

A. It performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. It reverts the configuration changes on the firewall if the check fails.

B. It restores the running configuration on a firewall and Panorama if the last configuration commit fails.

C. It performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. It reverts the configuration changes on the firewall and on Panorama if the check fails.

D. It restores the running configuration on a firewall if the last configuration commit fails.

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer- panorama/enable-automated-commit-recoveryThe Automated Commit Recovery feature enables the firewall to automatically revert to a previous configuration if a commit operation causes connectivity loss between the firewall and Panorama. The feature performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. If the check fails, the firewall reverts to the last known good configuration and restores connectivity with Panorama. The feature does not restore the running configuration on a firewall or Panorama if the last commit fails, as this would require manual intervention. The feature does not revert the configuration changes on Panorama, as Panorama is not affected by the commit operation on the firewall. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-new-features/panorama- features/ automatic-panorama-connection-recovery https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/administer- panorama/enable-automated-commit-recovery

QUESTION 5
A firewall administrator wants to avoid overflowing the company syslog server with traffic logs.
What should the administrator do to prevent the forwarding of DNS traffic logs to syslog?

A. Disable logging on security rules allowing DNS.

B. Go to the Log Forwarding profile used to forward traffic logs to syslog. Then, under traffic logs match list, create a new filter with application not equal to DNS.

C. Create a security rule to deny DNS traffic with the syslog server in the destination

D. Go to the Log Forwarding profile used to forward traffic logs to syslog. Then, under traffic logs match list, create a new filter with application equal to DNS.

Correct Answer: B
Section:
Explanation:
A log forwarding profile defines which logs are forwarded to which destinations, such as syslog servers. By creating a filter with application not equal to DNS, the log forwarding profile will exclude DNS traffic logs from being forwarded to syslog. Disabling logging on security rules allowing DNS will prevent the firewall from generating any logs for DNS traffic, which may not be desirable. Creating a security rule to deny DNS traffic with the syslog server in the destination will block the communication between the firewall and the syslog server, which may affect other logs. Creating a filter with application equal to DNS will forward only DNS traffic logs to syslog, which is the opposite of what is required.
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-forwarding https://docs.paloaltonetworks.com/network-security/security-policy/objects/log-forwarding

QUESTION 6
An engineer is planning an SSL decryption implementation
Which of the following statements is a best practice for SSL decryption?

A. Use the same Forward Trust certificate on all firewalls in the network.

B. Obtain a certificate from a publicly trusted root CA for the Forward Trust certificate.

C. Obtain an enterprise CA-signed certificate for the Forward Trust certificate.

D. Use an enterprise CA-signed certificate for the Forward Untrust certificate.

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward- proxy(Best Practice) Enterprise CA-signed CertificatesóAn enterprise CA can issue a signing certificate that the firewall can use to sign the certificates for sites which require SSL decryption. When the firewall trusts the CA that signed the certificate of the destination server, the firewall can send a copy of the destination server certificate to the client, signed by the enterprise CA. This is a best practice because usually all network devices already trust the Enterprise CA (it is usually already installed in the devices' CA Trust storage), so you don't need to deploy the certificate on the endpoints, so therollout process is smoother. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os- admin/decryption/configure-ssl-forward-proxy.html

QUESTION 7
An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications QoS natively integrates with which feature to provide service quality?

A. certificate revocation
B. Content-ID
C. App-ID
D. port inspection

Correct Answer: C
Section:
Explanation:
QoS natively integrates with App-ID, which is a feature that identifies applications based on their unique characteristics and behaviors, regardless of port, protocol, encryption, or evasive tactics. By using App-ID, QoS can prioritize or limit traffic based on the application name, category, subcategory, technology, or risk level. Certificate revocation is a process of invalidating digital certificates that are no longer trusted or secure. Content-ID is a feature that scans content and data within allowed applications for threats and sensitive data. Port inspection is a method of identifying applications based on the TCP or UDP port numbers they use, which is not reliable or granular enough for QoS purposes. Reference:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/quality-of-service/configure-qos https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id

QUESTION 8
What can an engineer use with GlobalProtect to distribute user-specific client certificates to each GlobalProtect user?

A. Certificate profile
B. SSL/TLS Service profile
C. OCSP Responder
D. SCEP

Correct Answer: D
Section:
Explanation:
If you have a Simple Certificate Enrollment Protocol (SCEP) server in your enterprise PKI, you can configure a SCEP profile to automate the generation and distribution of unique client certificates.https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/obtain- certificates/deploy-certificates-using-scep

QUESTION 9
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices?
(Choose three.)

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

Correct Answer: A, B, D
Section:
Explanation:
Panorama can perform three actions when deploying PAN-OS images to its managed devices: upload-only, upload and install, and upload and install and reboot. Upload-only transfers the PAN-OS image from Panorama to the managed device without installing it. Upload and install transfers the PAN-OS image from Panorama to the managed device and installs it, but does not reboot the device.Upload and install and reboot transfers the PAN-OS image from Panorama to the managed device, installs it, and reboots the device. Verify and install is not a valid action for deploying PAN-OS images from Panorama. Install and reboot is not a valid action for deploying PAN-OS images from Panorama, as the image needs to be uploaded first. Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/panorama/panorama-device- deployment/manage-software-and-content-updates https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cles

QUESTION 10
During the implementation of SSL Forward Proxy decryption, an administrator imports the company's Enterprise Root CA and Intermediate CA certificates onto the firewall. The company's Root and Intermediate CA certificates are also distributed to trusted devices using Group Policy and GlobalProtect. Additional device certificates and/or Subordinate certificates requiring an Enterprise CA chain of trust are signed by the company's Intermediate CA.
Which method should the administrator use when creating Forward Trust and Forward Untrust certificates on the firewall for use with decryption?

A. Generate a single subordinate CA certificate for both Forward Trust and Forward Untrust.

B. Generate a CA certificate for Forward Trust and a self-signed CA for Forward Untrust.

C. Generate a single self-signed CA certificate for Forward Trust and another for Forward Untrust

D. Generate two subordinate CA certificates, one for Forward Trust and one for Forward Untrust.

Correct Answer: B
Section:
Explanation:
Generate a CA certificate for Forward Trust (step 2) a self-signed CA for Forward Untrust (step 4)https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward- proxy

QUESTION 11
When you navigate to Network: > GlobalProtect > Portals > Method section, which three options are available? (Choose three)

A. user-logon (always on)

B. pre-logon then on-demand

C. on-demand (manual user initiated connection)

D. post-logon (always on)

E. certificate-logon

Correct Answer: A, B, C
Section:
Explanation:
The Method section of the GlobalProtect portal configuration allows you to specify how users connect to the portal. The options are: user-logon (always on): The agent connects to the portal as soon as the user logs in to the endpoint. pre-logon then on-demand: The agent connects to the portal before the user logs in to the endpoint and then switches to on-demand mode after the user logs in. on-demand (manual user initiated connection): The agent connects to the portal only when the user initiates the connection manually. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan- os-admin/globalprotect/configure-the-globalprotect-portal/configure-the- agent/configure-the-app- tab.html

QUESTION 12
An engineer must configure the Decryption Broker feature
Which Decryption Broker security chain supports bi-directional traffic flow?

A. Layer 2 security chain

B. Layer 3 security chain

C. Transparent Bridge security chain

D. Transparent Proxy security chain

Correct Answer: B
Section:
Explanation:
Together, the primary and secondary interfaces form a pair of decryption forwarding interfaces. Only interfaces that you have enabled to be Decrypt Forward interfaces are displayed here. Your security chain type (Layer 3 or Transparent Bridge) and the traffic flow direction (unidirectional or bidirectional) determine which of the two interfaces forwards allowed, clear text traffic to the security chain, and which interface receives the traffic back from the security chain after it has undergone additional enforcement.

QUESTION 13
When configuring forward error correction (FEC) for PAN-OS SD-WAN, an administrator would turn on the feature inside which type of SD-WAN profile?

A. Certificate profile

B. Path Quality profile

C. SD-WAN Interface profile

D. Traffic Distribution profile

Correct Answer: C
Section:
Explanation:
To enable forward error correction (FEC) for PAN-OS SD-WAN, you need to create an SD-WAN Interface Profile that specifies Eligible for Error Correction Profile interface selection and apply the profile to one or more interfaces. Then you need to create an Error Correction Profile to implementFEC or packet duplication. Reference: https://docs.paloaltonetworks.com/sd-wan/2-0/sd-wan- admin/configure-sd-wan/create-an-error-correction-profile

QUESTION 14
What is the best description of the HA4 Keep-Alive Threshold (ms)?

A. the maximum interval between hello packets that are sent to verify that the HA functionality on the other firewall is operational.

B. The time that a passive or active-secondary firewall will wait before taking over as the active or active-primary firewall

C. the timeframe within which the firewall must receive keepalives from a cluster member to know that the cluster member is functional.

D. The timeframe that the local firewall wait before going to Active state when another cluster member is preventing the cluster from fully synchronizing.

Correct Answer: C
Section:

QUESTION 15
What happens when an A/P firewall cluster synchronies IPsec tunnel security associations (SAs)?

A. Phase 2 SAs are synchronized over HA2 links

B. Phase 1 and Phase 2 SAs are synchronized over HA2 links

C. Phase 1 SAs are synchronized over HA1 links

D. Phase 1 and Phase 2 SAs are synchronized over HA3 links

Correct Answer: A
Section:

QUESTION 16

A standalone firewall with local objects and policies needs to be migrated into Panoram a. What procedure should you use so Panorama is fully managing the firewall?

A. Use the "import Panorama configuration snapshot" operation, then perform a device-group commit push with "include device and network templates"
B. Use the "import device configuration to Panorama" operation, then "export or push device config bundle" to push the configuration
C. Use the "import Panorama configuration snapshot" operation, then "export or push device config bundle" to push the configuration
D. Use the "import device configuration to Panorama" operation, then perform a device-group commit push with "include device and network templates"

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/transition-afirewall-to-panorama-management/migrate-a-firewall-to-panorama-management.html

QUESTION 17
Before you upgrade a Palo Alto Networks NGFW, what must you do?

A. Make sure that the PAN-OS support contract is valid for at least another year
B. Export a device state of the firewall
C. Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.
D. Make sure that the firewall is running a supported version of the app + threat update

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/pan-os-upgrade- checklist#id53a2bc2b-f86e-4ee5-93d7-b06aff837a00 "Verify the minimum content release version."Before you upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OShttps://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRrCAK

QUESTION 18
A prospect is eager to conduct a Security Lifecycle Review (SLR) with the aid of the Palo Alto Networks NGFW.
Which interface type is best suited to provide the raw data for an SLR from the network in a way that is minimally invasive?

A. Layer 3
B. Virtual Wire
C. Tap
D. Layer 2

Correct Answer: C
Section:
Explanation:
A tap interface is best suited to provide the raw data for an SLR from the network in a way that is minimally invasive. A tap interface allows the firewall to passively monitor network traffic without affecting the flow of traffic. The firewall can analyze the traffic and generate reports based on the application, user, content, and threat information. Reference:https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/networking/configure-interfaces/configure-a-tap-interface

QUESTION 19
A remote administrator needs firewall access on an untrusted interface. Which two components are required on the firewall to configure certificate-based administrator authentication to the web Ul?
(Choose two)

A. client certificate
B. certificate profile

C. certificate authority (CA) certificate

D. server certificate

Correct Answer: B, C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/managefirewall-administrators/configure-administrative-accounts-and-authentication/configure-certificatebased-administrator-authentication-to-the-web-interface.html

QUESTION 20
When planning to configure SSL Froward Proxy on a PA 5260, a user asks how SSL decryption can be implemented using phased approach in alignment with Palo Alto Networks best practices What should you recommend?

A. Enable SSL decryption for known malicious source IP addresses

B. Enable SSL decryption for source users and known malicious URL categories

C. Enable SSL decryption for malicious source users

D. Enable SSL decryption for known malicious destination IP addresses

Correct Answer: B
Section:
Explanation:
According to the Palo Alto Networks best practices, one of the ways to implement SSL decryption using a phased approach is to enable SSL decryption for source users and known malicious URL categories. This will allow you to block or alert on traffic that is likely to be malicious or risky, while minimizing the impact on legitimate traffic and user privacy. Reference:https://docs.paloaltonetworks.com/best-practices/9-1/decryption-best-practices/decryption-best- practices/ deploy-ssl-decryption-using-a-phased-approach

QUESTION 21
What would allow a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain'?

A. a Security policy with 'known-user" selected in the Source User field

B. an Authentication policy with 'unknown' selected in the Source User field

C. a Security policy with 'unknown' selected in the Source User field

D. an Authentication policy with 'known-user' selected in the Source User field

Correct Answer: B
Section:
Explanation:
An Authentication policy with 'unknown' selected in the Source User field would allow a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain. This policy would prompt the user to enter their credentials when they access a web-based application or service that requires authentication. The firewall would then use User-ID to map the user to the device and apply the appropriate security policies based on theuser identity. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os- admin/authentication/configure-an-authentication-policy

QUESTION 22
What are three valid qualifiers for a Decryption Policy Rule match? (Choose three.)

A. Destination Zone

B. App-ID

C. Custom URL Category

D. User-ID

E. Source Interface

Correct Answer: A, C, D
Section:
Explanation:
The valid qualifiers for a Decryption Policy Rule match are: Source Zone Destination Zone Source Address Destination Address Source User Destination User Source Region Destination Region Service/URL Category Custom URL Category URL Filtering Profile Therefore, out of the options given, Destination Zone, Custom URL Category, and User-ID are valid qualifiers. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-decryption-policies.html

QUESTION 23
What are two common reasons to use a "No Decrypt" action to exclude traffic from SSL decryption?
(Choose two.)

A. the website matches a category that is not allowed for most users

B. the website matches a high-risk category

C. the web server requires mutual authentication

D. the website matches a sensitive category

Correct Answer: C, D
Section:
Explanation:

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryptionexclusions/palo-alto-networks-predefined-decryption-exclusions.htmlThe firewall provides a predefined SSL Decryption Exclusion list to exclude from decryptioncommonly used sites that break decryption because of technical reasons such as pinned certificatesand mutual authentication.

QUESTION 24
An administrator has a PA-820 firewall with an active Threat Prevention subscription The administrator is considering adding a WildFire subscription.
How does adding the WildFire subscription improve the security posture of the organization1?

A. Protection against unknown malware can be provided in near real-time

B. WildFire and Threat Prevention combine to provide the utmost security posture for the firewall

C. After 24 hours WildFire signatures are included in the antivirus update

D. WildFire and Threat Prevention combine to minimize the attack surface

Correct Answer: A
Section:
Explanation:
Adding a WildFire subscription can improve the security posture of the organization by providing protection against unknown malware in near real-time. With a WildFire subscription, the firewall can forward various file types for WildFire analysis, and can retrieve WildFire signatures for newly- discovered malware as soon as they are generated by the WildFire public cloud or a private cloud appliance. This reduces the exposure window and prevents further infection by the same malware.Reference: https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire- overview/wildfire-subscription

QUESTION 25
What are two valid deployment options for Decryption Broker? (Choose two)

A. Transparent Bridge Security Chain

B. Layer 3 Security Chain

C. Layer 2 Security Chain

D. Transparent Mirror Security Chain

Correct Answer: A, B
Section:

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption- broker/decryption-broker-concepts

QUESTION 26
An administrator needs to assign a specific DNS server to one firewall within a device group. Where would the administrator go to edit a template variable at the device level?

A. Variable CSV export under Panorama > templates

B. PDF Export under Panorama > templates

C. Manage variables under Panorama > templates

D. Managed Devices > Device Association

Correct Answer: C
Section:
Explanation:
To edit a template variable at the device level, you need to go to Manage variables under Panorama > templates. This allows you to override the default value of a variable for a specific device or device group. For example, you can assign a specific DNS server to one firewall within a device group by editing the ${dns-primary} variable for that device. Reference: https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage- templates/use-template-variables.html

QUESTION 27
A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)

A. Virtual router

B. Security zone

C. ARP entries

D. Netflow Profile

Correct Answer: A, B
Section:
Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interfacehelp/network/network-interfaces/pa-7000-series- layer-2-interface#idd2bcaacc-54b9-4ec9-a1dd-8064499f5b9d
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRqCAKVLAN interface is not necessary but in this scenario we assume it is. Create VLAN object, VLANinterface and VLAN Zone. Attach VLAN interface to VLAN object together with two L2 interfaces thenattach VLAN interface to virtual router. Without VLAN interface you can pass traffic betweeninterfaces on the same network and with VLAN interface you can route traffic to other networks.

QUESTION 28
A network administrator troubleshoots a VPN issue and suspects an IKE Crypto mismatch between peers. Where can the administrator find the corresponding logs after running a test command to initiate the VPN?

A. Configuration logs

B. System logs

C. Traffic logs

D. Tunnel Inspection logs

Correct Answer: B
Section:
Explanation:
According to the Palo Alto Networks documentation, "To view IKE and IPSec Crypto profiles in the logs, filter the System log for eventid equal to vpn (Monitor > Logs > System)."
Reference:https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/vpn/set-up-site-to-site-vpn/set-up- ike-crypto-profiles.html

QUESTION 29

An administrator is using Panorama to manage me and suspects an IKE Crypto mismatch between peers, from the firewalls to Panoram a. 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 ACC to consolidate the logs.

D. Use the scp logdb export command.

Correct Answer: A
Section:
Explanation:

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/use-the-cli/use-secure-copy-to-import-and-export-files/export-and-import-a-complete-log-database-logdb

QUESTION 30

A firewall administrator is trying to identify active routes learned via BGP in the virtual router runtime stats within the GUI. Where can they find this information?

A. routes listed in the routing table with flags Oi

B. routes listed in the routing table with flags A?B

C. under the BGP Summary tab

D. routes listed in the forwarding table with BGP in the Protocol column

Correct Answer: B
Section:
Explanation:
Flags
A?BóActive and learned via BGP
A CóActive and a result of an internal interface (connected) - Destination = network
A HóActive and a result of an internal interface (connected) - Destination = Host only
A RóActive and learned via RIP
A SóActive and static
SóInactive (because this route has a higher metric) and static
O1óOSPF external type-1
O2óOSPF external type-2
OióOSPF intra-area
OoóOSPF inter-area

QUESTION 31

A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named initcfg txt. The firewall is currently running PAN-OS 10.0 and using a lab config The contents of init-cfg txi in the USB flash drive are as follows:

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsys,jumbo-frame
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command:> request resort system Upon restart, the firewall fails to begin the bootstrapping process. The failure is caused because

A. Firewall must be in factory default state or have all private data deleted for bootstrapping
B. The hostname is a required parameter, but it is missing in init-cfg txt
C. The USB must be formatted using the ext3 file system, FAT32 is not supported
D. PANOS version must be 91.x at a minimum but the firewall is running 10.0.x
E. The bootstrap.xml file is a required file but it is missing

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive.html#id8378007f-d6e5-4f2d-84a4-5d50b0b3ad7d

QUESTION 32
A network security engineer wants to prevent resource-consumption issues on the firewall.
Which strategy is consistent with decryption best practices to ensure consistent performance?

A. Use RSA in a Decryption profile tor higher-priority and higher-risk traffic, and use less processorintensive decryption methods for lower-risk traffic
B. Use PFS in a Decryption profile for higher-priority and higher-risk traffic, and use less processorintensive decryption methods for tower-risk traffic
C. Use Decryption profiles to downgrade processor-intensive ciphers to ciphers that are less processor-intensive
D. Use Decryption profiles to drop traffic that uses processor-intensive ciphers

Correct Answer: C
Section:
Explanation:
According to the Palo Alto Networks documentation, "Decryption Profiles define the cipher suite settings the firewall accepts so you can protect against vulnerable, weak protocols and algorithms.You can also use Decryption Profiles to downgrade processor-intensive ciphers to ciphers that areless processor-intensive." Reference: https://docs.paloaltonetworks.com/best-practices/10-2/decryption-best-practices/decryption-best-practices/data-center-decryption-profile.html

QUESTION 33
An engineer is in the planning stages of deploying User-ID in a diverse directory services environment.
Which server OS platforms can be used for server monitoring with User-ID?

A. Microsoft Terminal Server, Red Hat Linux, and Microsoft Active Directory
B. Microsoft Active Directory, Red Hat Linux, and Microsoft Exchange
C. Microsoft Exchange, Microsoft Active Directory, and Novell eDirectory
D. Novell eDirectory, Microsoft Terminal Server, and Microsoft Active Directory

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/compatibility-matrix/user-id-agent/which-servers-can-the-user-id-agent-monitor

QUESTION 34
What are three reasons for excluding a site from SSL decryption? (Choose three.)

A. the website is not present in English

B. unsupported ciphers

C. certificate pinning

D. unsupported browser version

E. mutual authentication

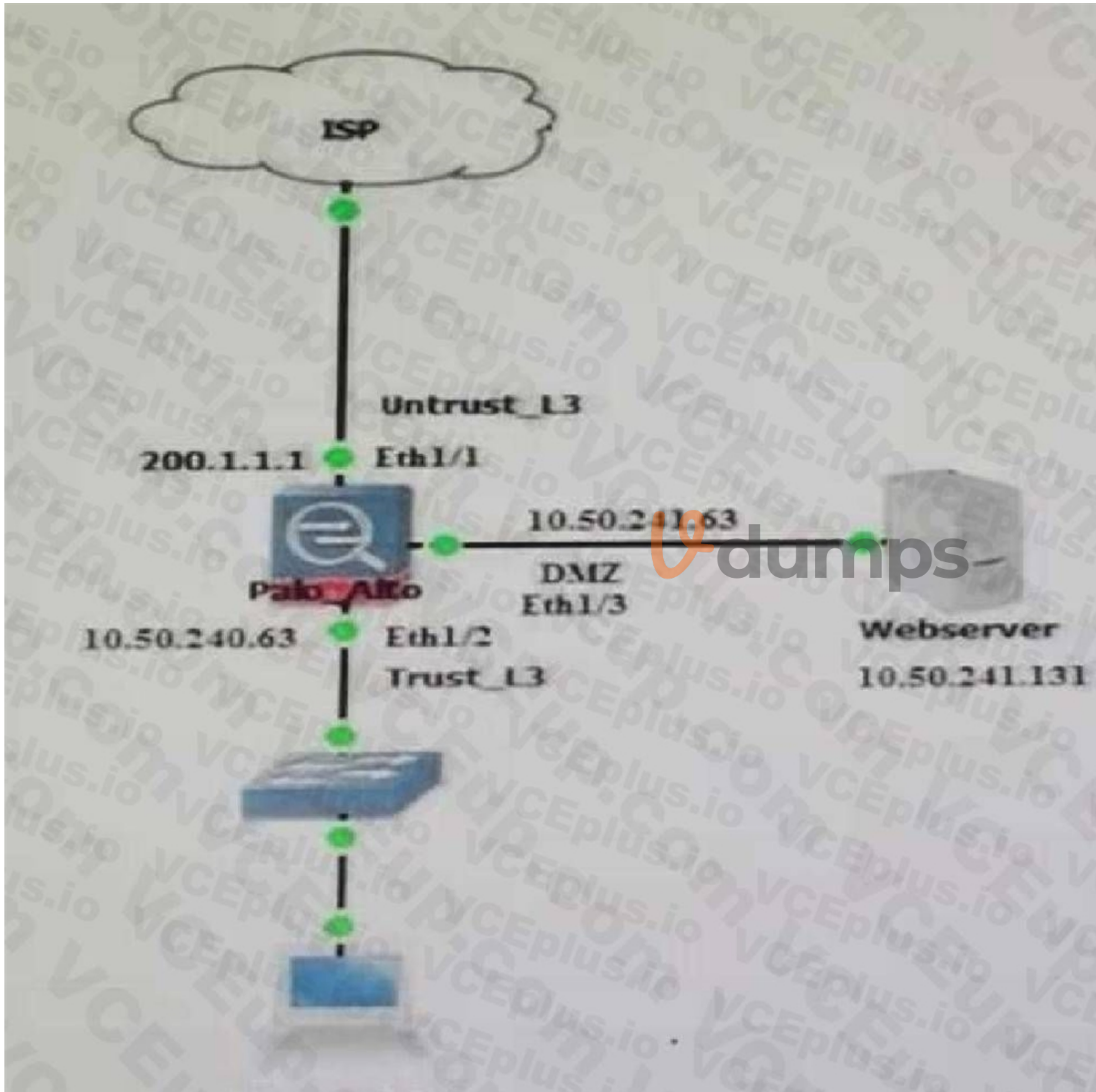**Correct Answer: B, C, E**
Section:
Explanation:
Reasons that sites break decryption technically include pinned certificates, client authentication, incomplete certificate chains, and unsupported ciphers. https://docs.paloaltonetworks.com/panos/ 10-1/pan-os-admin/decryption/decryption-exclusions/exclude-a-server-from-decryption.html

QUESTION 35
A user at an internal system queries the DNS server for their web server with a private IP of 10 250 241 131 in the. The DNS server returns an address of the web server's public address, 200.1.1.10.
In order to reach the web server, which security rule and U-Turn NAT rule must be configured on the firewall?

ISP

Untrust_L3

200.1.1.1   Eth1/1

10.50.241.63

Palo_Alto

DMZ
Eth1/3

Webserver

10.50.240.63   Eth1/2

10.50.241.131

Trust_L3

A.

NAT Rule:
Source Zone: Trust_L3
Source IP: Any
Destination Zone: Untrust_L3
Destination IP: 200.1.1.10
Destination Translation address: 10.250.241.131
Security Rule:
Source Zone: Trust-L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 200.1.1.10

B.

NAT Rule:
Source Zone: Untrust_L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 200.1.1.10
Destination Translation address: 10.250.241.131
Security Rule:
Source Zone: Trust-L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 10.250.241.131

C.

NAT Rule:
    Source Zone: Trust_L3
    Source IP: Any
    Destination Zone: DMZ
    Destination IP: 200.1.1.10
    Destination Translation address: 10.250.241.131
Security Rule:
    Source Zone: Untrust-L3
    Source IP: Any
    Destination Zone: DMZ
    Destination IP: 10.250.241.131

D.

NAT Rule:
    Source Zone: Untrust_L3
    Source IP: Any
    Destination Zone: Untrust_L3
    Destination IP: 200.1.1.10
    Destination Translation address: 10.250.241.131
Security Rule:
    Source Zone: Untrust-L3·
    Source IP: Any
    Destination Zone: DMZ
    Destination IP: 10.250.241.131

Correct Answer: A
Section:

QUESTION 36
An administrator device-group commit push is tailing due to a new URL category How should the administrator correct this issue?

A. verify that the URL seed Tile has been downloaded and activated on the firewall

B. change the new category action to alert" and push the configuration again

C. update the Firewall Apps and Threat version to match the version of Panorama

D. ensure that the firewall can communicate with the URL cloud

Correct Answer: C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNqw

QUESTION 37
Which GlobalProtect component must be configured to enable Clientless VPN?

A. GlobalProtect satellite

B. GlobalProtect app

C. GlobalProtect portal

D. GlobalProtect gateway

Correct Answer: C
Section:
Explanation:
Creating the GlobalProtect portal is as simple as letting it know if you have accessed it already. A new gateway for accessing the GlobalProtect portal will appear. Client authentication can be used with an existing one.
https://www.nstec.com/how-to-configure-clientless-vpn-in-palo-alto/#5

QUESTION 38
An administrator analyzes the following portion of a VPN system log and notices the following issue "Received local id 10 10 1 4/24 type IPv4 address protocol 0 port 0, received remote id 10.1.10.4/24 type IPv4 address protocol 0 port 0."
What is the cause of the issue?

A. IPSec crypto profile mismatch

B. IPSec protocol mismatch

C. mismatched Proxy-IDs

D. bad local and peer identification IP addresses in the IKE gateway

Correct Answer: C
Section:
Explanation:
According to the Palo Alto Networks documentation, "A successful phase 2 negotiation requires not only that the security proposals match, but also the proxy-ids on either peer, be a mirror image of each other. So it is mandatory to configure the proxy-IDs whenever you establish a tunnel between the Palo Alto Network firewall and the firewalls configured for policy-based VPNs." The log message indicates that the local and remote IDs are identical, which means they are not mirrored.Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClW8CAK

QUESTION 39
When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?

A. The interface must be used for traffic to the required services

B. You must enable DoS and zone protection

C. You must set the interface to Layer 2 Layer 3. or virtual wire

D. You must use a static IP address
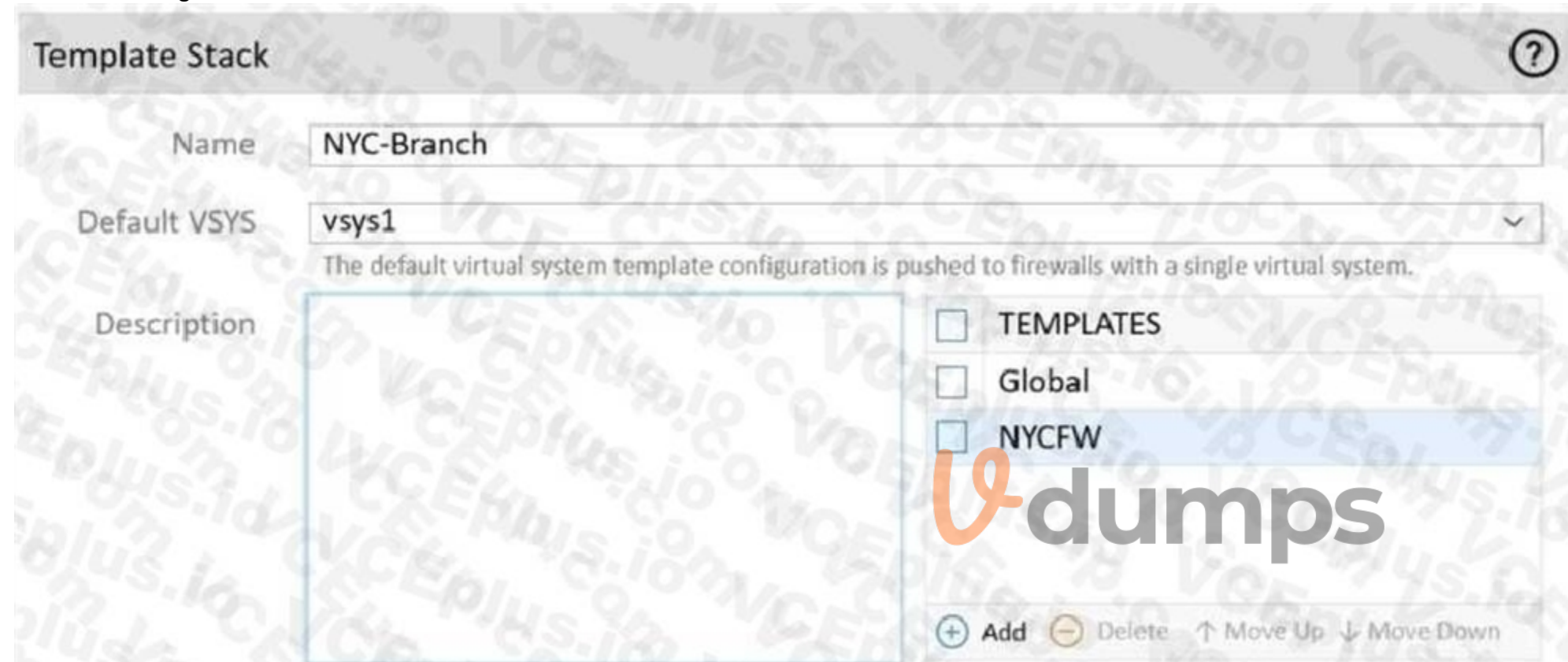
Correct Answer: D
Section:
Explanation:
According to the Palo Alto Networks documentation, "To configure a service route, you must specify a source interface and a source address. The source interface can be any data port (Ethernet interface) or a loopback interface. The source address must be a static IP address that is configured on the source interface." Reference: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/service-routes/service-routes-overview

QUESTION 40
Refer to the image.

An administrator is tasked with correcting an NTP service configuration for firewalls that cannot use the Global template NTP servers. The administrator needs to change the IP address to a preferable server for this template stack but cannot impact other template stacks.
How can the issue be corrected?

A. Override the value on the NYCFW template.

B. Override a template value using a template stack variable.

C. Override the value on the Global template.

D. Enable "objects defined in ancestors will take higher precedence" under Panorama settings.

Correct Answer: B
Section:
Explanation:
Both templates and template stacks support variables. Variables allow you to create placeholder objects with their value specified in the template or template stack based on your configuration needs. Create a template or template stack variable to replace IP addresses, Group IDs, and interfaces in your configurations. https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/override-a-template-setting.html

QUESTION 41
You need to allow users to access the office-suite applications of their choice. How should you configure the firewall to allow access to any office-suite application?

A. Create an Application Group and add Office 365, Evernote Google Docs and Libre Office
B. Create an Application Group and add business-systems to it.
C. Create an Application Filter and name it Office Programs, then filter it on the office programs subcategory.
D. Create an Application Filter and name it Office Programs then filter on the business-systems category.

Correct Answer: C
Section:
Explanation:
According to the Palo Alto Networks documentation, "Application filters enable you to create groups of applications based on specific characteristics such as subcategory, technology, risk factor, and so on. You can then use these groups in Security policy rules to allow or block access to the applications.For example, you can create an application filter that includes all applications in the office-programs subcategory and use it in a Security policy rule to allow access to any office-suite application." Reference: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/manage- applications-in-a-policy/use-application-filters-in-policy

QUESTION 42
A customer is replacing their legacy remote access VPN solution The current solution is in place to secure only internet egress for the connected clients Prisma Access has been selected to replace the current remote access VPN solution
During onboarding the following options and licenses were selected and enabled
- Prisma Access for Remote Networks 300Mbps
- Prisma Access for Mobile Users 1500 Users
- Cortex Data Lake 2TB
- Trusted Zones trust
- Untrusted Zones untrust
- Parent Device Group shared
How can you configure Prisma Access to provide the same level of access as the current VPN solution?

A. Configure mobile users with trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet
B. Configure mobile users with a service connection and trust-to-trust Security policy rules to allow the desired traffic outbound to the internet
C. Configure remote networks with a service connection and trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet
D. Configure remote networks with trust-to-trust Security policy rules to allow the desired traffic outbound to the internet

Correct Answer: A
Section:
Explanation:
To provide the same level of access as the current VPN solution, which is to secure only Internet egress for the connected clients, you can configure mobile users with trust-to-untrust Security policy rules to allow the desired traffic outbound to the Internet. This way, the mobile users will beassigned an IP address from a pool that belongs to the trust zone, and they will be able to access the Internet through Prisma Access using a gateway that belongs to the untrust zone1. You do not need to configure a service connection for this scenario, as a service connection is used to enable access between mobile users and remote networks or private apps2. You also do not need to configure trust-to-trust Security policy rules, as they are used to enable access between mobile users and other trusted resources3. Reference: 1: https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/service-connection- overview/create-a-service-connection-to-enable-access-between-users-and-networks 2: https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/prisma-access-service-connections 3: https://docs.paloaltonetworks.com/prisma/prisma- access/prisma-access-cloud-managed-admin/prisma-access-mobile-users/mobile-users-globalprotect/globalprotect-features-for-prisma-access.html

QUESTION 43
What is the best description of the HA4 Keep-Alive Threshold (ms)?

A. the maximum interval between hello packets that are sent to verify that the HA functionality on the other firewall is operational.
B. The time that a passive or active-secondary firewall will wait before taking over as the active or active-primary firewall
C. the timeframe within which the firewall must receive keepalives from a cluster member to know that the cluster member is functional.
D. The timeframe that the local firewall wait before going to Active state when another cluster member is preventing the cluster from fully synchronizing.

Correct Answer: C
Section:

QUESTION 44
What is the function of a service route?

A. The service route is the method required to use the firewall's management plane to provide services to applications
B. The service packets enter the firewall on the port assigned from the external service. The server sends its response to the configured destination interface and destination IP address
C. The service packets exit the firewall on the port assigned for the external service. The server sends its response to the configured source interface and source IP address
D. Service routes provide access to external services such as DNS servers external authentication servers or Palo Alto Networks services like the Customer Support Portal

Correct Answer: D
Section:
Explanation:
A service route is the path from an interface on the firewall to a service on a server. Service routesprovide access to external services such as DNS servers, external authentication servers or Palo Alto Networks services like the Customer Support Portal1. By default, the firewall uses the management (MGT) interface to access these services, but you can configure a data port (a regular interface) as analternative2. A service route is not related to the firewall's management plane or the port assignedfor the external service. A service route does not affect how the server sends its response to the firewall. Reference: 1: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking- admin/service-routes/ service-routes-overview 2: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/service-routes/configure-service-routes

QUESTION 45
Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

A. link requirements
B. the name of the ISP
C. IP Addresses
D. branch and hub locations

Correct Answer: A, C, D
Section:
Explanation:
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration

QUESTION 46
What is considered the best practice with regards to zone protection?

A. Review DoS threat activity (ACC > Block Activity) and look for patterns of abuse
B. Use separate log-forwarding profiles to forward DoS and zone threshold event logs separately from other threat logs
C. If the levels of zone and DoS protection consume too many firewall resources, disable zone protection
D. Set the Alarm Rate threshold for event-log messages to high severity or critical severity

Correct Answer: A
Section:
Explanation:
The best practice with regards to zone protection is to review DoS threat activity (ACC > BlockActivity) and look for patterns of abuse. This way, you can identify the sources and types of DoS attacks that target your network zones and adjust your zone protection profiles and policies accordingly1. You can also use the DoS Protection dashboard widget to monitor the number of sessions that match DoS protection policies2. You do not need to use separate log-forwarding profiles to forward DoS and zone threshold event logs separately from other threat logs, as you can use a single log-forwarding profile to forward different types of logs to different destinations3. You shouldnot disable zone protection if the levels of zone and DoS protection consume too many firewall resources, as this would expose your network zones to potential DoS attacks. Instead, you shouldoptimize your zone protection profiles and policies to reduce the resource consumption4. You shouldnot set the Alarm Rate threshold for event-log messages to high severity or critical severity, as this would limit the visibility into DoS attacks

that have lower severity levels. Instead, you should set theAlarm Rate threshold to a value that is appropriate for your network environment and traffic patterns. Reference: 1: https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection- best-practices/dos-and-zone-protection-best-practices/follow-post-deployment-dos-and-zone- protection-best-practices 2: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-the-acc-to-monitor-network-activity/use-the-acc-to-monitor-dos- protection 3: https:// docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/configure-log-forwarding/log-forwarding-profiles 4: https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-best-practices : https://docs.paloaltonetworks.com/pan-os/10-2/pan-os- admin/networking/network-profiles/zone-protection-profiles/configure-a-zone-protection-profile

QUESTION 47

In the screenshot above which two pieces of information can be determined from the ACC configuration shown? (Choose two)

A. The Network Activity tab will display all applications, including FTP.

B. Threats with a severity of "high" are always listed at the top of the Threat Name list

C. Insecure-credentials, brute-force and protocol-anomaly are all a part of the vulnerability Threat Type

D. The ACC has been filtered to only show the FTP application

Correct Answer: C, D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/threat-signature

QUESTION 48
A firewall has been assigned to a new template stack that contains both "Global" and "Local" templates in Panorama, and a successful commit and push has been performed. While validating the configuration on the local firewall, the engineer discovers that some settings are not being applied as intended.
The setting values from the "Global" template are applied to the firewall instead of the "Local" template that has different values for the same settings.
What should be done to ensure that the settings in the "Local" template are applied while maintaining settings from both templates?

A. Move the "Global" template above the "Local" template in the template stack.

B. Perform a commit and push with the "Force Template Values" option selected.

C. Move the "Local" template above the "Global" template in the template stack.

D. Override the values on the local firewall and apply the correct settings for each value.

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama- overview/centralized-firewall-configuration-and-update-management/templates-and-template- stacks

QUESTION 49
WildFire will submit for analysis blocked files that match which profile settings?

A. files matching Anti-Spyware signatures
B. files that are blocked by URL filtering
C. files that are blocked by a File Blocking profile
D. files matching Anti-Virus signatures

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud- features/wildfire-analysis-of-blocked-files

QUESTION 50
An administrator needs to build Security rules in a Device Group that allow traffic to specific users and groups defined in Active Directory What must be configured in order to select users and groups for those rules from Panorama?

A. The Security rules must be targeted to a firewall in the device group and have Group Mapping configured
B. A master device with Group Mapping configured must be set in the device group where the Security rules are configured
C. User-ID Redistribution must be configured on Panorama to ensure that all firewalls have the same mappings
D. A User-ID Certificate profile must be configured on Panorama

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web- interface/panorama-device-groups

QUESTION 51
A network administrator wants to use a certificate for the SSL/TLS Service Profile.
Which type of certificate should the administrator use?

A. certificate authority (CA) certificate
B. client certificate
C. machine certificate
D. server certificate

Correct Answer: D
Section:
Explanation:
Use only signed certificates, not CA certificates, in SSL/TLS service profiles.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configurean-ssltls-service-profile.html
A server certificate is used for the SSL/TLS Service Profile. The server certificate identifies the firewall to clients that initiate SSL/TLS connections to it. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate- management/certificates-and-keys/server-certificates

QUESTION 52
Using multiple templates in a stack to manage many firewalls provides which two advantages?
(Choose two.)

A. inherit address-objects from templates

B. define a common standard template configuration for firewalls

C. standardize server profiles and authentication configuration across all stacks

D. standardize log-forwarding profiles for security polices across all stacks

Correct Answer: B, C
Section:
Explanation:
Using multiple templates in a stack to manage many firewalls provides the advantages of defining a common standard template configuration for firewalls and standardizing server profiles and authentication configuration across all stacks.
A template stack is a container for multiple templates that you can assign to firewalls and firewall groups. The templates in a stack are prioritized so that the settings in a higher-priority template override the same settings in a lower-priority template.This allows you to create a hierarchy of templates that define common settings for all firewalls and specific settings for different groups of firewalls.
Reference:https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/ manage-firewalls/manage- templates-and-template-stacks

QUESTION 53
A network security engineer is attempting to peer a virtual router on a PAN-OS firewall with an external router using the BGP protocol. The peer relationship is not establishing.
What command could the engineer run to see the current state of the BGP state between the two devices?

A. show routing protocol bgp state

B. show routing protocol bgp peer

C. show routing protocol bgp summary

D. show routing protocol bgp rib-out

Correct Answer: C
Section:
Explanation:
The show routing protocol bgp summary command displays the current state of the BGP peer relationship between the firewall and other BGP routers. The output includes the peer IP address, AS number, uptime, prefix count, state, and status codes. Reference:https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-cli-quick-start/use-the-cli/show-the- routing-table-and-statistics

QUESTION 54
A network security engineer must implement Quality of Service policies to ensure specific levels of delivery guarantees for various applications in the environment They want to ensure that they know as much as they can about QoS before deploying.
Which statement about the QoS feature is correct?

A. QoS is only supported on firewalls that have a single virtual system configured

B. QoS can be used in conjunction with SSL decryption

C. QoS is only supported on hardware firewalls

D. QoS can be used on firewalls with multiple virtual systems configured

Correct Answer: D
Section:
Explanation:
The correct answer is D - QoS can be used on firewalls with multiple virtual systems configured. QoS is a feature that enables network administrators to prioritize and manage network traffic to ensure that critical applications receive the necessary bandwidth and quality of service. This feature can be used on firewalls with multiple virtual systems, allowing administrators to configure policies on a per-Virtual System basis. Additionally, QoS can be

used in conjunction with SSL decryption to ensure that applications running over SSL receive appropriate treatment.

QUESTION 55
What can you use with Global Protect to assign user-specific client certificates to each GlobalProtect user?

A. SSL/TLS Service profile

B. Certificate profile

C. SCEP

D. OCSP Responder

Correct Answer: C
Section:
Explanation:
If you have a Simple Certificate Enrollment Protocol (SCEP) server in your enterprise PKI, you can configure a SCEP profile to automate the generation and distribution of unique client certificates.https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/obtain- certificates/deploy-certificates-using-scep

QUESTION 56
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. Allow the firewall to block the sites to improve the security posture

B. Add the sites to the SSL Decryption Exclusion list to exempt them from decryption

C. Install the unsupported cipher into the firewall to allow the sites to be decrypted

D. Create a Security policy to allow access to those sites

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-exclusions Traffic that breaks decryption for technical reasons, such as using a pinned certificate, an incomplete certificate chain, unsupported ciphers, or mutual authentication (attempting to decrypt the traffic results in blocking the traffic). Palo Alto Networks provides a predefined SSL Decryption Exclusion list (DeviceCertificate ManagementSSL Decryption Exclusion) that excludes hosts with applications and services that are known to break decryption technically from SSL Decryption by default. If you encounter sites that break decryption technically and are not on the SSL Decryption Exclusion list, you can add them to list manually by server hostname. The firewall blocks sites whose applications and services break decryption technically unless you add them to the SSL Decryption Exclusion list.

QUESTION 57
An administrator has configured the Palo Alto Networks NGFW's management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.
Which configuration setting or step will allow the firewall to get automatic application signature updates?

A. A scheduler will need to be configured for application signatures.

B. A Security policy rule will need to be configured to allow the update requests from the firewall to the update servers.

C. A Threat Prevention license will need to be installed.

D. A service route will need to be configured.

Correct Answer: A
Section:
Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates

QUESTION 58

Before an administrator of a VM-500 can enable DoS and zone protection, what actions need to be taken?

A. Measure and monitor the CPU consumption of the firewall data plane to ensure that each firewall is properly sized to support DoS and zone protection
B. Create a zone protection profile with flood protection configured to defend an entire egress zone against SYN. ICMP ICMPv6, UDP. and other IP flood attacks
C. Add a WildFire subscription to activate DoS and zone protection features
D. Replace the hardware firewall because DoS and zone protection are not available with VM-Series systems

Correct Answer: A
Section:
Explanation:
1 - https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-bestpractices.html#:~:text=DoS%20and%20Zone%20Protection%20help,device%20at%20the%20internet%20perimeter.
2 - https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dosprotection/zone-defense/take-baseline-cps-measurements-for-setting-flood-thresholds/how-to-measure-cps.html
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dosprotection.html

QUESTION 59
An engineer wants to implement the Palo Alto Networks firewall in VWire mode on the internet gateway and wants to be sure of the functions that are supported on the vwire interface What are three supported functions on the VWire interface? (Choose three)

A. NAT
B. QoS
C. IPSec
D. OSPF
E. SSL Decryption

Correct Answer: A, B, E
Section:
Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/virtual-wire-interfaces"The virtual wire supports blocking or allowing traffic based on virtual LAN (VLAN) tags, in addition to supporting security policy rules, App-ID, Content-ID, User-ID, decryption, LLDP, active/passive and active/active HA, QoS, zone protection (with some exceptions), non-IP protocol protection, DoS protection, packet buffer protection, tunnel content inspection, and NAT."

QUESTION 60
Where is information about packet buffer protection logged?

A. Alert entries are in the Alarms log. Entries for dropped traffic, discarded sessions, and blocked IP address are in the Threat log
B. All entries are in the System log
C. Alert entries are in the System log. Entries for dropped traffic, discarded sessions and blocked IP addresses are in the Threat log
D. All entries are in the Alarms log

Correct Answer: D
Section:
Explanation:

WHICH SYSTEM LOGS AND THREAT LOGS ARE GENERATED WHEN PACKET BUFFER PROTECTION

Created On 10/29/19 15:51 PM - Last Modified 04/27/20 22:13 PM

ZONE PROTECTION   ZONE AND DOS PROTECTION   8.1   8.0   9.0   HARDWARE

Question
Which system logs and threat logs are generated when packet buffer protection is enabled?

Environment
- PAN-OS 8.x
- PBP

Answer
The firewall records alert events in the System log and events for dropped traffic, discarded sessions, and blocked IP address in the Threat log.
- System logs:

Logs:
Monitor>System
Packet buffer congestion
Severity: informational

- Threat logs:

QUESTION 61
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.

Panorama Settings   ⑦

Receive Timeout for Connection to Device (sec) 240

Send Timeout for Connection to Device (sec) 240

Retry Count for SSL Send to Device 25

☐ Share Unused Address and Service Objects with Devices

☐ Objects defined in ancestors will take higher precedence

☐ Enable reporting and filtering on groups

When enabled Panorama will locally store users and groups from

Master Devices

OK   Cancel

C.

Syslog Server Profile   ⑦

Name SyslogProfile1

Servers   Custom Log Format

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

⊕ Add ⊖ Delete

Enter the IP address or FQDN of the Syslog server

OK   Cancel

D.

E. Option A
F. Option B
G. Option C
H. Option D

Correct Answer: C
Section:

QUESTION 62
Which statement is true regarding a Best Practice Assessment?

A. It shows how your current configuration compares to Palo Alto Networks recommendations
B. It runs only on firewalls
C. When guided by an authorized sales engineer, it helps determine the areas of greatest risk where you should focus prevention activities.
D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Correct Answer: A
Section:
Explanation:
The Best Practice Assessment (BPA) tool compares the configuration of firewalls and Panorama to the Palo Alto Networks best practice recommendations. Run the BPA periodically to identify security weaknesses, see the best practice settings, and implement them to improve your security posture.https://docs.paloaltonetworks.com/best-practices/10-2/bpa-getting-started

QUESTION 63
A network administrator plans a Prisma Access deployment with three service connections, each with a BGP peering to a CPE. The administrator needs to minimize the BGP configuration and management overhead on on-prem network devices.
What should the administrator implement?

A. target service connection for traffic steering

B. summarized BGP routes before advertising

C. hot potato routing

D. default routing

Correct Answer: B
Section:
Explanation:
The best way to minimize the BGP configuration and management overhead on on-prem network devices is to summarize BGP routes before advertising them. Route summarization is a technique that reduces the number of routes in a routing table by aggregating multiple routes into a single route with a less specific prefix. This reduces the size of routing updates and the memory and CPUusage of routers. Prisma Access supports route summarization for service connections and remotenetwork connections that use BGP routing1. You should not implement target service connection for traffic steering, as this is a feature that allows you to select a specific service connection for traffic from a remote network connection or a mobile user based on destination IP address orapplication. This does not affect the BGP configuration or management on on-prem networkdevices2. You should not implement hot potato routing, as this is a routing technique that selects the closest exit point to the destination network based on the number of hops or the lowest IGPmetric. This does not affect the BGP configuration or management on on-prem network devices3.You should not implement default routing, as this is a routing technique that uses a default route to forward packets to an unknown destination. This does not affect the BGP configuration ormanagement on on-prem network devices, and it may not provide optimal routing for Prisma Access traffic4. Reference: 1: https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access- panorama-admin/prepare-the-prisma-access-infrastructure/service-connection-overview/configure- route-summarization-for-service-connections 2: https://docs.paloaltonetworks.com/prisma/prisma- access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/service- connection-overview/target-service-connection-for-traffic-steering 3: https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed- admin/prisma-access-service-connections/service-connection-routing 4:https://docs.paloaltonetworks.com/prisma/prisma-access/ prisma-access-cloud-managed- admin/prisma-access-service-connections/service-connection-routing/routing-for-service- connection-traffic-cloud-management.html

QUESTION 64
Which function is handled by the management plane (control plane) of a Palo Alto Networks firewall?

A. signature matching for content inspection

B. IPSec tunnel standup

C. Quality of Service

D. logging

Correct Answer: D
Section:
Explanation:
Logging is a function that is handled by the management plane (control plane) of a Palo Alto Networks firewall. The management plane is responsible for managing and configuring the firewall, as well as generating and storing logs and reports. The management plane communicates with the data plane (also known as the packet forwarding plane) through an internal backplane interface.Signature matching for content inspection, IPSec tunnel standup, and Quality of Service are functions that are handled by the data plane of a Palo Alto Networks firewall. The data plane is responsible for processing and forwarding packets, as well as applying security policies and features to the traffic.The data plane consists of multiple dedicated hardware components, such as the Single-Pass Parallel Processing (SP3) engine, the Security Processing Unit (SPU), and the Network Processing Unit (NPU).Reference: : https://docs.paloaltonetworks.com/ pan-os/10-2/pan-os-admin/firewall- administration/manage-firewall-administrators/firewall-management-interfaces :https://docs.paloaltonetworks.com/pan-os/10-2/pan-os- admin/firewall-administration/firewall- concepts/firewall-overview

QUESTION 65
In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)

A. wildcard server certificate

B. enterprise CA certificate

C. client certificate

D. server certificate

E. self-signed CA certificate

Correct Answer: B, E
Section:

Explanation:

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-forward-proxy.html

QUESTION 66

An organization wishes to roll out decryption but gets some resistance from engineering leadership regarding the guest network.
What is a common obstacle for decrypting traffic from guest devices?

A. Guest devices may not trust the CA certificate used for the forward untrust certificate.

B. Guests may use operating systems that can't be decrypted.

C. The organization has no legal authority to decrypt their traffic.

D. Guest devices may not trust the CA certificate used for the forward trust certificate.

Correct Answer: D
Section:
Explanation:

https://docs.paloaltonetworks.com/best-practices/10-2/decryption-best-practices/decryption-best- practices/plan-ssl-decryption-best-practice-deployment https://live.paloaltonetworks.com/t5/general-topics/decrypt-guest-network-traffic/td-p/119388

QUESTION 67

An existing NGFW customer requires direct interne! access offload locally at each site and iPSec connectivity to all branches over public internet. One requirement is mat no new SD-WAN hardware be introduced to the environment.
What is the best solution for the customer?

A. Configure a remote network on PAN-OS

B. Upgrade to a PAN-OS SD-WAN subscription

C. Deploy Prisma SD-WAN with Prisma Access

D. Configure policy-based forwarding

Correct Answer: B
Section:
Explanation:
According to the Palo Alto Networks documentation, "The PAN-OS software now includes a native SD-WAN subscription to provide intelligent and dynamic path selection on top of the industry- leading security that PAN-OS software" already delivers. Key features of the SD-WAN implementation include centralized configuration management, automatic VPN topology creation, traffic distribution, monitoring, and troubleshooting." Reference: https:// docs.paloaltonetworks.com/sd-wan

QUESTION 68

An administrator wants to configure the Palo Alto Networks Windows User-ID agent to map IP addresses to usernames. The company uses four Microsoft Active Directory servers and two Microsoft Exchange servers, which can provide logs for login events.
All six servers have IP addresses assigned from the following subnet: 192.168 28.32/27. The Microsoft Active Directory servers reside in 192.168.28.32/28. and the Microsoft Exchange servers resideL in 192.168.28 48/28
What information does the administrator need to provide in the User Identification > Discovery section?

A. The IP-address and corresponding server type (Microsoft Active Directory or Microsoft Exchange) for each of the six servers

B. Network 192 168.28.32/28 with server type Microsoft Active Directory and network 192.168.28.48/28 with server type Microsoft Exchange

C. Network 192 168 28.32/27 with server type Microsoft

D. One IP address of a Microsoft Active Directory server and "Auto Discover" enabled to automatically obtain all five of the other servers

Correct Answer: A
Section:

Explanation:

The administrator needs to provide the IP address and corresponding server type (Microsoft Active Directory or Microsoft Exchange) for each of the six servers in the User Identification > Discovery section. The administrator should enter the network address of 192.168.28.32/28 and select "Microsoft Active Directory" as the server type for the four Active Directory servers and enter the network address of 192.168.28.48/28 and select "Microsoft Exchange" as the server type for the two Exchange servers. This will allow the User-ID agent to discover and map the IP address of each server to the corresponding username.

QUESTION 69

Which three statements accurately describe Decryption Mirror? (Choose three.)

A. Decryption Mirror requires a tap interface on the firewall

B. Use of Decryption Mirror might enable malicious users with administrative access to the firewall to harvest sensitive information that is submitted via an encrypted channel

C. Only management consent is required to use the Decryption Mirror feature.

D. Decryption, storage, inspection, and use of SSL traffic are regulated in certain countries.

E. You should consult with your corporate counsel before activating and using Decryption Mirror in a production environment.

Correct Answer: B, D, E

Section:

Explanation:

Decryption Mirror is a feature that allows a Palo Alto Networks firewall to send a copy of decrypted traffic to an external security device or tool for further analysis. The potential risk associated with Decryption Mirror is that if the firewall administrator's credentials are compromised, a malicious user could potentially access sensitive decrypted information. Hence, it's advised to be cautious and ensure proper handling of this feature.

Additionally, laws and regulations regarding the decryption, storage, inspection, and use of SSL/TLS encrypted traffic vary by country and industry. It is crucial to ensure compliance with relevant laws and best practices when using Decryption Mirror. This often requires consultation with corporate legal counsel to understand the implications and ensure that the use of such features does not violate privacy laws or regulatory requirements.

The need for administrative consent and the legal implications of using Decryption Mirror features are outlined in Palo Alto Networks' 'PAN-OS Administrator's Guide' and best practice documentation. It is not specifically required to have a tap interface to use Decryption Mirror, which eliminates option A. Option C is incorrect because it is not just management consent but legal compliance that needs to be considered.

QUESTION 70

A network security engineer needs to enable Zone Protection in an environment that makes use of Cisco TrustSec Layer 2 protections
What should the engineer configure within a Zone Protection profile to ensure that the TrustSec packets are identified and actions are taken upon them?

A. TCP Fast Open in the Strip TCP options

B. Ethernet SGT Protection

C. Stream ID in the IP Option Drop options

D. Record Route in IP Option Drop options

Correct Answer: B

Section:

Explanation:

Cisco TrustSec technology uses Security Group Tags (SGTs) to enforce access controls on Layer 2 traffic. When implementing Zone Protection on a Palo Alto Networks firewall in an environment with Cisco TrustSec, you should configure Ethernet SGT Protection. This setting ensures that the firewall can recognize SGTs in Ethernet frames and apply the appropriate actions based on the configured policies. The use of Ethernet SGT Protection in conjunction with TrustSec is covered in advanced firewall configuration documentation and in interoperability guides between Palo Alto Networks and Cisco systems.

QUESTION 71

When a new firewall joins a high availability (HA) cluster, the cluster members will synchronize all existing sessions over which HA port?

A. HA1

B. HA3

C. HA2

D. HA4

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/high-availability/ha-clustering-overview

QUESTION 72
Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

A. link requirements
B. the name of the ISP
C. IP Addresses
D. branch and hub locations

Correct Answer: A, C, D
Section:
Explanation:
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration

QUESTION 73
An engineer needs to redistribute User-ID mappings from multiple data centers. Which data flow best describes redistribution of user mappings?

A. Domain Controller to User-ID agent
B. User-ID agent to Panorama
C. User-ID agent to firewall
D. firewall to firewall

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/deploy-user-id-in-a-large- scale-network/redistribute-user-mappings-and-authentication-timestamps/firewall-deployment-for- user-id-redistribution#ide3661b46-4722-4936-bb9b-181679306809

QUESTION 74
An engineer is configuring Packet Buffer Protection on ingress zones to protect from single-session DoS attacks Which sessions does Packet Buffer Protection apply to?

A. It applies to existing sessions and is not global
B. It applies to new sessions and is global
C. It applies to new sessions and is not global
D. It applies to existing sessions and is global

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos- protection/zone-defense/packet-buffer-protection

QUESTION 75
The administrator for a small company has recently enabled decryption on their Palo Alto Networks firewall using a self-signed root certificate. They have also created a Forward Trust and Forward Untrust certificate and set them as such

The admin has not yet installed the root certificate onto client systems What effect would this have on decryption functionality?

A. Decryption will function and there will be no effect to end users
B. Decryption will not function because self-signed root certificates are not supported
C. Decryption will not function until the certificate is installed on client systems
D. Decryption will function but users will see certificate warnings for each SSL site they visit

Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEZCA0

QUESTION 76
A firewall has Security policies from three sources

A. locally created policies
B. shared device group policies as pre-rules
C. the firewall's device group as post-rules
   How will the rule order populate once pushed to the firewall?
D. shared device group policies, firewall device group policies. local policies.
E. firewall device group policies, local policies. shared device group policies
F. shared device group policies. local policies, firewall device group policies
G. local policies, firewall device group policies, shared device group policies

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage- device-groups/manage-the-rule-hierarchy

QUESTION 77
Which three use cases are valid reasons for requiring an Active/Active high availability deployment?
(Choose three)

A. The environment requires real, full-time redundancy from both firewalls at all times
B. The environment requires Layer 2 interfaces in the deployment
C. The environment requires that both firewalls maintain their own routing tables for faster dynamic routing protocol convergence
D. The environment requires that all configuration must be fully synchronized between both members of the HA pair
E. The environment requires that traffic be load-balanced across both firewalls to handle peak traffic spikes

Correct Answer: A, C, E
Section:
Explanation:
Active/Active high availability is a deployment mode that allows both firewalls in an HA pair to actively process traffic and share the load. Active/Active HA is suitable for environments that require real, full-time redundancy from both firewalls at all times, as there is no failover time or session loss in case of a firewall failure. Active/Active HA is also suitable for environments that require that both firewalls maintain their own routing tables for faster dynamic routing protocol convergence, as each firewall can run its own routing protocols and exchange routes with other routers independently.Active/Active HA is also suitable for environments that require that traffic be load-balanced across both firewalls to handle peak traffic spikes, as each firewall can process a portion of the traffic and increase the overall throughput and performance. Active/Active HA is not suitable for environments that require Layer 2 interfaces in the deployment, as Layer 2 interfaces are not supported in Active/Active HA mode. Active/Active HA is also not suitable for environments that require that all configuration must be fully

synchronized between both members of the HA pair, as some configuration settings are not synchronized in Active/Active HA mode, such as virtual router configuration, virtual wire configuration, and QoS configuration.
Reference: : https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activeactive-ha : https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up- activeactive-ha/determine-your-activeactive-use-case

QUESTION 78
An administrator is building Security rules within a device group to block traffic to and from malicious locations How should those rules be configured to ensure that they are evaluated with a high priority?

A. Create the appropriate rules with a Block action and apply them at the top of the Default Rules

B. Create the appropriate rules with a Block action and apply them at the top of the Security Post- Rules.

C. Create the appropriate rules with a Block action and apply them at the top of the local firewall Security rules.

D. Create the appropriate rules with a Block action and apply them at the top of the Security Pre- Rules

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web- interface/defining-policies-on-panorama

QUESTION 79
A company requires that a specific set of ciphers be used when remotely managing their Palo Alto Networks appliances. Which profile should be configured in order to achieve this?

A. SSH Service profile

B. SSL/TLS Service profile

C. Decryption profile

D. Certificate profile

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure- an-ssh-service-profile

QUESTION 80
A company is using wireless controllers to authenticate users. Which source should be used for User- ID mappings?

A. Syslog

B. XFF headers

C. server monitoring

D. client probing

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/user-id-overview

QUESTION 81
An engineer is configuring SSL Inbound Inspection for public access to a company's application.
Which certificate(s) need to be installed on the firewall to ensure that inspection is performed successfully?

A. Self-signed CA and End-entity certificate

B. Root CA and Intermediate CA(s)

C. Self-signed certificate with exportable private key

D. Intermediate CA (s) and End-entity certificate

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-inbound- inspection We recommend uploading a certificate chain (a single file) to the firewall if your end- entity (leaf) certificate is signed by one or more intermediate certificates and your web server supports TLS 1.2 and Rivest, Shamir, Adleman (RSA) or Perfect Forward Secrecy (PFS) key exchange algorithms. Uploading the chain avoids client-side server certificate authentication issues. You should arrange the certificates in the file as follows: End-entity (leaf) certificate Intermediate certificates (in issuing order) (Optional) Root certificate

QUESTION 82
A firewall administrator needs to be able to inspect inbound HTTPS traffic on servers hosted in theirDMZ to prevent the hosted service from being exploited. Which combination of features can allowPAN-OS to detect exploit traffic in a session with TLS encapsulation?

A. Decryption policy and a Data Filtering profile

B. a WildFire profile and a File Blocking profile

C. Vulnerability Protection profile and a Decryption policy

D. a Vulnerability Protection profile and a QoS policy

Correct Answer: C
Section:
Explanation:
A vulnerability protection profile enables the firewall to detect and prevent exploit attempts against known vulnerabilities in network protocols and applications. A decryption policy allows the firewall to decrypt and inspect inbound HTTPS traffic for potential threats. A data filtering profile is used for detecting and controlling the transfer of sensitive data such as credit card numbers or social security numbers. A WildFire profile is used for submitting unknown files or email links to the WildFire cloud for analysis and verdict. A file blocking profile is used for blocking or allowing the transfer of files based on their type, direction, or application. A QoS policy is used for managing the bandwidth allocation and priority of network traffic based on various criteria. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-concepts/ssl- inbound-inspection https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/set-up- vulnerability-protection.html

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

```
> show session id 380280

session          380280

    c2s flow:
            source:     172.17.149.129 [L3-Trust]
            dst:        104.154.89.105
            proto:      6
            sport:      60597           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)             : 13698
    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.

Correct Answer: A, C
Section:
Explanation:
The session went through SSL decryption processing because the Decryption column shows a green check mark, indicating that the firewall decrypted the traffic and applied security policies. The application has been identified as web-browsing because the Application column shows web- browsing as the application name. The session has not ended yet because the Session End Reason column shows N/A, indicating that the session is still active. The session did go through SSL decryption processing, so option D is incorrect. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/monitor/monitor- network/monitor-sessions

QUESTION 84
How would an administrator configure a Bidirectional Forwarding Detection profile for BGP after enabling the Advance Routing Engine run on PAN-OS 10.2?

A. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Virtual Router > BGP > BFD
B. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Virtual Router > BGP > General > Global BFD Profile
C. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Routing > Logical Routers > BGP > General > Global BFD Profile
D. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Routing > Logical Routers > BGP > BFD

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClivCAC
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/advanced- routing/create-bfd-profiles#idf2ccda44-0678-4df3-ad1d-2ec8f47cec7b then https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/advanced- routing/configure-bgp-on-an-advanced-routing-engine

QUESTION 85
Which User-ID mapping method should be used in a high-security environment where all IP addressto- 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

Correct Answer: B
Section:
Explanation:
Because GlobalProtect users must authenticate to gain access to the network, the IP address-to- username mapping is explicitly known. This is the best solution in sensitive environments where you must be certain of who a user is in order to allow access to an application or service.https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user- mapping/globalprotect.html

QUESTION 86
What can be used to create dynamic address groups?

A. dynamic address
B. region objects
C. tags
D. FODN addresses

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/monitor-changes-in-the- virtual-environment/use-dynamic-address-groups-in-policy

QUESTION 87

A firewall administrator has been tasked with ensuring that all Panorama configuration is committed and pushed to the devices at the end of the day at a certain time. How can they achieve this?

A. Use the Scheduled Config Export to schedule Commit to Panorama and also Push to Devices.

B. Use the Scheduled Config Push to schedule Push lo Devices and separately schedule an API call to commit all Panorama changes.

C. Use the Scheduled Config Export to schedule Push to Devices and separately schedule an API call to commit all Panorama changes.

D. Use the Scheduled Config Push to schedule Commit to Panorama and also Push to Devices.

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/schedule-a- configuration-push-to-managed-firewalls Log in to the Panorama Web Interface. Create a scheduled configuration push. Select PanoramaScheduled Config Push and Add a new scheduled configuration push. You can also schedule a configuration push to managed firewalls when you push to devices (CommitPush to Devices).

QUESTION 88

Which statement accurately describes service routes and virtual systems?

A. Virtual systems that do not have specific service routes configured inherit the global service and service route settings for the firewall.

B. Virtual systems can only use one interface for all global service and service routes of the firewall.

C. Virtual systems cannot have dedicated service routes configured; and virtual systems always use the global service and service route settings for the firewall.

D. The interface must be used for traffic to the required external services.

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/virtual-systems/customize-service- routes-for-a-virtual-system "When a firewall is enabled for multiple virtual systems, the virtual systems inherit the global service and service route settings. For example, the firewall can use a shared email server to originate email alerts to all virtual systems. In some scenarios, you'd want to create different service routes for each virtual system."

QUESTION 89

You have upgraded Panorama to 10.2 and need to upgrade six Log Collectors. When upgrading Log Collectors to 10.2, you must do what?

A. Upgrade the Log Collectors one at a time.

B. Add Panorama Administrators to each Managed Collector.

C. Add a Global Authentication Profile to each Managed Collector.

D. Upgrade all the Log Collectors at the same time.

Correct Answer: D
Section:
Explanation:
You must upgrade all Log Collectors in a collector group at the same time to avoid losing log data https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-panorama/deploy- updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/deploy-an-update-to- log-collectors-when-panorama-is-internet-connected

QUESTION 90

Which configuration is backed up using the Scheduled Config Export feature in Panorama?

A. Panorama running configuration

B. Panorama candidate configuration

C. Panorama candidate configuration and candidate configuration of all managed devices

D. Panorama running configuration and running configuration of all managed devices

Correct Answer: D
Section:
Explanation:

https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer- panorama/manage-panorama-and-firewall-configuration-backups

QUESTION 91
Cortex XDR notifies an administrator about grayware on the endpoints. There are no entries about grayware in any of the logs of the corresponding firewall. Which setting can the administrator configure on the firewall to log grayware verdicts?

A. within the log forwarding profile attached to the Security policy rule

B. within the log settings option in the Device tab

C. in WildFire General Settings, select "Report Grayware Files"

D. in Threat General Settings, select "Report Grayware Files"

Correct Answer: C
Section:
Explanation:

https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/monitor-wildfire-activity/use-the- firewall-to-monitor-malware/configure-wildfire-submissions-log-settings/enable-logging-for-benign- and-grayware-samples

QUESTION 92
You have upgraded your Panorama and Log Collectors lo 10.2 x. Before upgrading your firewalls using Panorama, what do you need do?

A. Refresh your licenses with Palo Alto Network Support - Panorama/Licenses/Retrieve License Keys from License Server.

B. Re-associate the firewalls in Panorama/Managed Devices/Summary.

C. Commit and Push the configurations to the firewalls.

D. Refresh the Mastor Key in Panorama/Master Key and Diagnostic

Correct Answer: C
Section:
Explanation:

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the- firewall-pan-os/upgrade-firewalls-using-panorama

QUESTION 93
Which Panorama mode should be used so that all logs are sent to, and only stored in. Cortex Data Lake?

A. Legacy

B. Log Collector

C. Panorama

D. Management Only

Correct Answer: D
Section:
Explanation:

https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama- overview/panorama-modelsManagement Only mode is the only Panorama mode that allows all logs to be sent to and only stored in Cortex Data Lake.
In this mode, Panorama does not store any logs locally and only acts as a management interface for the firewalls and Cortex Data Lake. The other modes either store somelogs locally (Legacy and Log Collector) or do not support Cortex Data Lake

QUESTION 94
An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Link and Path Monitoring Is enabled with the Failure Condition set to "any." There is one link group configured containing member interfaces ethernet1/1 and ethernet1/2 with a Group Failure Condition set to "all." Which HA state will the Active firewall go into if ethernet1/1 link goes down due to a failure?

A. Non-functional

B. Passive

C. Active-Secondary

D. Active

Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClG7CAK

QUESTION 95
An engineer is pushing configuration from Panorama lo a managed firewall.
What happens when the pushed Panorama configuration has Address Object names that duplicate the Address Objects already configured on the firewall?

A. The firewall rejects the pushed configuration, and the commit fails.

B. The firewall renames the duplicate local objects with "-1" at the end signifying they are clones; it will update the references to the objects accordingly and fully commit the pushed configuration.

C. The firewall fully commits all of the pushed configuration and overwrites its locally configured objects

D. The firewall ignores only the pushed objects that have the same name as the locally configured objects, and it will commit the rest of the pushed configuration.

Correct Answer: A
Section:
Explanation:
it fails the commit should the local FW has the same object as the Panorama. on this docs it say"shared" https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage- firewalls/transition-a-firewall-to-panorama-management/ plan-the-transition-to-panorama- management

QUESTION 96
What is a correct statement regarding administrative authentication using external services with a local authorization method?

A. Prior to PAN-OS 10.2. an administrator used the firewall to manage role assignments, but access domains have not been supported by this method.

B. Starting with PAN-OS 10.2. an administrator needs to configure Cloud Identity Engine to use external authentication services for administrative authentication.

C. The administrative accounts you define locally on the firewall serve as references to the accounts defined on an external authentication server.

D. The administrative accounts you define on an external authentication server serve as references to the accounts defined locally on the firewall.
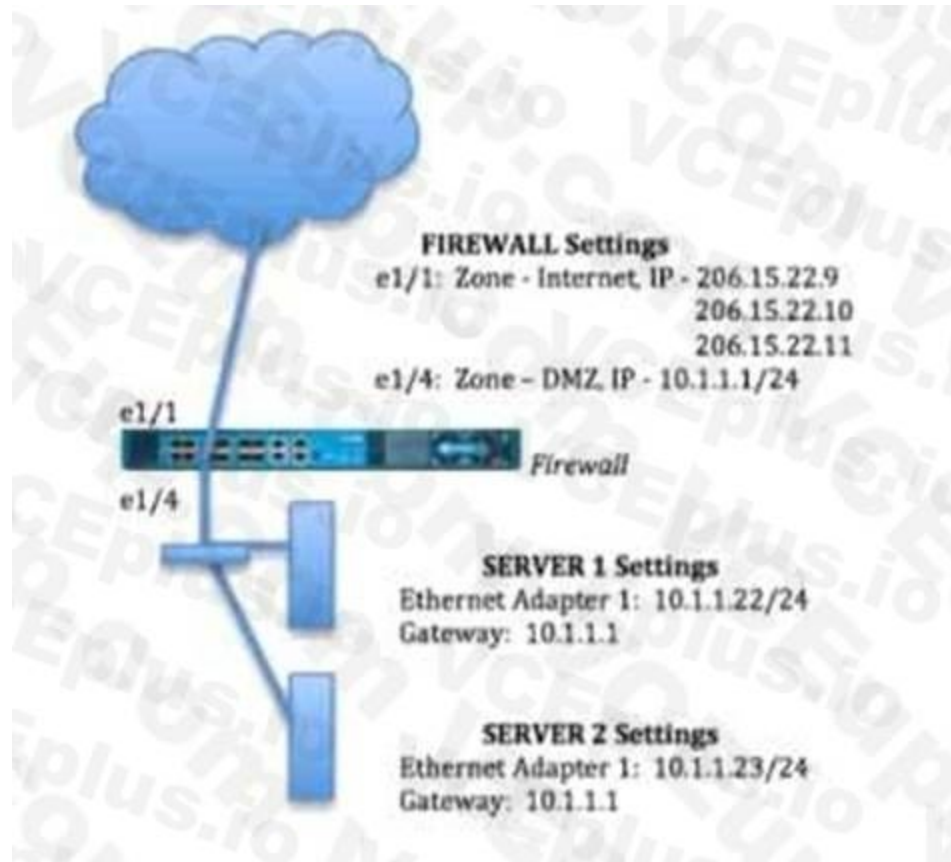
Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage- firewall-administrators/administrative-authentication

QUESTION 97
An administrator wants multiple web servers In the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22.
Based on the image, which NAT rule will forward web-browsing traffic correctly?

FIREWALL Settings
e1/1: Zone - Internet, IP - 206.15.22.9
206.15.22.10
206.15.22.11
e1/4: Zone - DMZ, IP - 10.1.1.1/24

SERVER 1 Settings
Ethernet Adapter 1: 10.1.1.22/24
Gateway: 10.1.1.1

SERVER 2 Settings
Ethernet Adapter 1: 10.1.1.23/24
Gateway: 10.1.1.1

A.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 80/TCP

B.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: None

C.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

D.

Source IP: Any

Destination IP: 206.15.22.9

Source Zone: Internet

Destination Zone: DMZ

Destination Service: 80/TCP

Action: Destination NAT

Translated IP: 10.1.1.22

Translated Port: 80/TCP

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration- examples/destination-nat-exampleone-to-one-mapping.html

QUESTION 98
An engineer is tasked with enabling SSL decryption across the environment. What are three valid parameters of an SSL Decryption policy? (Choose three.)

A. URL categories

B. source users

C. source and destination IP addresses

D. App-ID

E. GlobalProtect HIP

Correct Answer: A, B, C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEZCA0 https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/define-traffic-to- decrypt/create-a-decryption-policy-rule

QUESTION 99
A firewall administrator has been tasked with ensuring that all Panorama-managed firewalls forward traffic logs to Panoram a. In which section is this configured?

A. Panorama > Managed Devices

B. Monitor > Logs > Traffic

C. Device Groups > Objects > Log Forwarding

D. Templates > Device > Log Settings

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-log- collection/configure-log-forwarding-to-panorama

QUESTION 100
An administrator discovers that a file blocked by the WildFire inline ML feature on the firewall is a false-positive action. How can the administrator create an exception for this particular file?

A. Add partial hash and filename in the file section of the WildFire inline ML tab of the Antivirus profile.

B. Set the WildFire inline ML action to allow for that protocol on the Antivirus profile.

C. Add the related Threat ID in the Signature exceptions tab of the Antivirus profile.

D. Disable the WildFire profile on the related Security policy.

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/wildfire-inline- ml/configure-wildfire-inline-ml"The File Exceptions table allows you to define specific files that you do not want analyzed, such as false-positives.
To create a new file exception entry, Add a new entry and provide the partial hash, filename, and description of the file that you want to exclude from enforcement." https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/objects/objects- security-profiles-antivirus

QUESTION 101
A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443 A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.
Which combination of service and application, and order of Security policy rules, needs to be configured to allow cJeartext web-browsing traffic to this server on tcp/443?

A. Rule #1 application: web-browsing; service application-default; action: allow Rule #2- application: ssl; service: application-default; action: allow

B. Rule #1: application; web-browsing; service: service-https; action: allow Rule #2 application: ssl;service: application-default, action: allow

C. Rule #1: application: web-browsing; service: service-http; action: allow Rule #2: application: ssl;service: application-default; action: allow

D. Rule tf1 application: ssl; service: application-default; action: allow Rule #2 application; webbrowsing; service application-default; action: allow

Correct Answer: B
Section:
Explanation:
This combination of service and application, and order of Security policy rules, allows clear-text web- browsing traffic to the server on tcp/443. The first rule matches the web-browsing application on the service-https service, which is a predefined service object that includes tcp/443 as the default port.The second rule matches the ssl application on the application-default service, which is a dynamic service object that includes the default ports for each application. This rule is needed to allow the decrypted ssl traffic to pass through the firewall after the Forward Proxy rule. The order of the rules is important because the firewall evaluates the rules from top to bottom and applies the first matching rule. https://live.paloaltonetworks.com/t5/general-topics/web-browsing-default-port-application/td- p/228859

QUESTION 102
The firewall identifies a popular application as an unKnown-tcp.
Which two options are available to identify the application? (Choose two.)

A. Create a custom application.
B. Submit an App-ID request to Palo Alto Networks.
C. Create a custom object for the application server.
D. Create a Security policy to identify the custom application.

Correct Answer: A, B
Section:
Explanation:
You can create a custom app: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app- id/use-application-objects-in-policy/create-a-custom-application or submit a request to PANhttps://www.paloaltonetworks.com/blog/submit-an-application/

QUESTION 103
An administrator is required to create an application-based Security policy rule to allow Evernote.
The Evernote application implicitly uses SSL and web browsing. What is the minimum the administrator needs to configure in the Security rule to allow only Evernote?

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

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/applications-with-implicit- supportion:

QUESTION 104
A firewall engineer creates a new App-ID report under Monitor > Reports > Application Reports > New Application 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 30 days.
B. It matches to the New App-IDs downloaded in the last 90 days
C. It matches to the New App-IDs installed since the last time the firewall was rebooted
D. It matches to the New App-IDs in the most recently installed content releases.

Correct Answer: D
Section:
Explanation:
When creating a new App-ID report under Monitor > Reports > Application Reports > New Application, the firewall identifies new applications based on the New App-IDs in the most recently installed content releases. The New App-IDs are the application signatures that have been added in the latest content release, which can be found under Objects > Security Profiles > Application. This allows the engineer to monitor any new applications that have been added to the firewall's database and evaluate whether to allow or block them with a Security policy update.

QUESTION 105
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 allows for easier troubleshooting, since the client browser is aware of the existence of the proxy.
C. Explicit proxy supports interception of traffic using non-standard HTTPS ports.
D. It supports the X-Authenticated-User (XAU) header, which contains the authenticated username in the outgoing request

Correct Answer: B, C
Section:
Explanation:
B. Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy12. This means that the client can see the proxy's IP address and port number, and can use tools like ping or traceroute to check connectivity and latency issues. Transparent proxies are invisible to the client browser, which makes it harder to diagnose problems.
C. Explicit proxy supports interception of traffic using non-standard HTTPS ports3. This means that the proxy can handle HTTPS requests that use ports other than 443, which may be required by some applications or websites. Transparent proxies can only intercept HTTPS traffic on port 443, which limits their functionality.

QUESTION 106
What is the best definition of the Heartbeat Interval?

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

Correct Answer: A
Section:
Explanation:
According to the Palo Alto Networks Knowledge Base12, the best definition of the Heartbeat Interval is A. The interval in milliseconds between hello packets.
The Heartbeat Interval is a CLI command that configures how often an HA peer sends an ICMP ping to its partner through the HA control link. The ping verifies network connectivity and ensures that the peer kernel is responsive. The default value is 1000ms for all Palo Alto Networks platforms.

QUESTION 107
SAML SLO is supported for which two firewall features? (Choose two.)

A. GlobalProtect Portal
B. CaptivePortal
C. WebUI
D. CLI

Correct Answer: A, B
Section:
Explanation:
SSO is available to administrators who access the web interface and to end users who access applications through GlobalProtect or Captive Portal. SLO is available to administrators and GlobalProtect end users, but not to Captive Portal end users.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/authentication-types/saml
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/device/device-server-profiles-saml-identity-provider

QUESTION 108
The manager of the network security team has asked you to help configure the company's Security Profiles according to Palo Alto Networks best practice As part of that effort, the manager has assigned you the Vulnerability Protection profile for the internet gateway firewall.
Which action and packet-capture setting for items of high severity and critical severity best matches Palo Alto Networks best practice?

A. action 'reset-both' and packet capture 'extended-capture'

B. action 'default' and packet capture 'single-packet'

C. action 'reset-both' and packet capture 'single-packet'

D. action 'reset-server' and packet capture 'disable'

Correct Answer: C
Section:

QUESTION 109
The following objects and policies are defined in a device group hierarchy

Dallas-Branch has Dallas-FW as a member of the Dallas-Branch device-group
NYC-DC has NYC-FW as a member of the NYC-DC device-group
What objects and policies will the Dallas-FW receive if "Share Unused Address and Service Objects" is enabled in Panorama?

A.

Address Objects
- Shared Address1
- Shared Address2
- Branch Address1

Policies
- Shared Policy1
- Branch Policy1

B.

Address Objects

- Shared Address1
- Shared Address2
- Branch Address1
- DC Address1

Policies

- Shared Policy1
- Shared Policy2
- Branch Policy1

C. Address Objects
   -Shared Address 1
   -Branch Address2 Policies
   -Shared Polic1 l
   -Branch Policy1

D. Address Objects -Shared Addressl -Shared Address2 -Branch Addressl Policies -Shared Policyl -Shared Policy2 -Branch Policy1

Correct Answer: A
Section:

QUESTION 110
An administrator is attempting to create policies tor deployment of a device group and template stack. When creating the policies, the zone drop down list does not include the required zone.
What must the administrator do to correct this issue?

A. Specify the target device as the master device in the device group

B. Enable "Share Unused Address and Service Objects with Devices" in Panorama settings

C. Add the template as a reference template in the device group

D. Add a firewall to both the device group and the template

Correct Answer: C
Section:
Explanation:
Short According to the Palo Alto Networks documentation, "To use a template stack for a device group, you must add the template stack as a reference template in the device group. This enables you to use zones and interfaces defined in the template stack when creating policies for the device group." Reference: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-templates-and-template-stacks

QUESTION 111
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

Correct Answer: A, C, E
Section:
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.

QUESTION 112
An administrator has been tasked with configuring decryption policies,
Which decryption best practice should they consider?

A. Consider the local, legal, and regulatory implications and how they affect which traffic can be decrypted.

B. Decrypt all traffic that traverses the firewall so that it can be scanned for threats.

C. Place firewalls where administrators can opt to bypass the firewall when needed.

D. Create forward proxy decryption rules without Decryption profiles for unsanctioned applications.

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

QUESTION 113
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.

Correct Answer: B
Section:
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.Reference:Migrate a Firewall HA Pair to Panorama Management, PCNSE Study Guide (page 50)

QUESTION 114
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

Correct Answer: C
Section:
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.Reference:Policy-Based Forwarding,Packet Flow Sequence in PAN-OS

QUESTION 115
A consultant advises a client on designing an explicit Web Proxy deployment on PAN-OS 11 0 The client currently uses RADIUS authentication in their environment

Which two pieces of information should the consultant provide regarding Web Proxy authentication? (Choose two.)

A. Kerberos or SAML authentication need to be configured
B. LDAP or TACACS+ authentication need to be configured
C. RADIUS is only supported for a transparent Web Proxy.
D. RADIUS is not supported for explicit or transparent Web Proxy

Correct Answer: A, D
Section:
Explanation:
For explicit Web Proxy deployment on PAN-OS, Palo Alto Networks currently supports Kerberos and SAML as authentication methods. RADIUS is not supported for explicit or transparent Web Proxy authentication on Palo Alto Networks appliances, which means that if the client is currently using RADIUS, they will need to configure an alternate supported authentication method. LDAP or TACACS+ authentication is not directly supported for Web Proxy authentication in PAN-OS. For more information on supported Web Proxy authentication methods, please refer to the latest Palo Alto Networks 'PAN-OS Web Interface Reference Guide'.

QUESTION 116
A root cause analysis investigation into a recent security incident reveals that several decryption rules have been disabled. The security team wants to generate email alerts when decryption rules are changed.
How should email log forwarding be configured to achieve this goal?

A. With the relevant configuration log filter inside Device > Log Settings
B. With the relevant system log filter inside Objects > Log Forwarding
C. With the relevant system log filter inside Device > Log Settings
D. With the relevant configuration log filter inside Objects > Log Forwarding

Correct Answer: C
Section:
Explanation:
To generate email alerts when decryption rules are changed in a Palo Alto Networks firewall, you would configure email log forwarding based on specific system logs that capture changes to decryption policies. This is done by setting up log forwarding profiles with filters that match events related to decryption rule modifications. These profiles are then applied to the relevant log types within the firewall's log settings.
To specifically monitor for changes to decryption rules, you would navigate to the Device > Log Settings section of the firewall's web interface. Here, you can configure log forwarding for system logs, which capture configuration changes among other system-level events. By creating a filter that looks for logs associated with decryption rule changes, and associating this filter with an email server profile, the firewall can automatically send out email alerts whenever a decryption rule is modified.
This setup ensures that the security team is promptly notified of any changes to the decryption policies, allowing for quick review and action if the changes were unauthorized or unintended. It is an essential part of maintaining the security posture of the network and ensuring compliance with organizational policies on encrypted traffic inspection.

QUESTION 117
An engineer needs to configure a standardized template for all Panorama-managed firewalls. These settings will be configured on a template named 'Global' and will be included in all template stacks.
Which three settings can be configured in this template? (Choose three.)

A. Log Forwarding profile
B. SSL decryption exclusion
C. Email scheduler
D. Login banner
E. Dynamic updates

Correct Answer: B, D, E
Section:
Explanation:
A template is a set of configuration options that can be applied to one or more firewalls or virtual systems managed by Panorama.A template can include settings from the Device and Network tabs on the firewall web

interface, such as login banner, SSL decryption exclusion, and dynamic updates4. These settings can be configured in a template named ''Global'' and included in all template stacks.A template stack is a group of templates that Panorama pushes to managed firewalls in an ordered hierarchy4.Reference:Manage Templates and Template Stacks, PCNSE Study Guide (page 50)

QUESTION 118
An engineer is monitoring an active/active high availability (HA) firewall pair.
Which HA firewall state describes the firewall that is currently processing traffic?

A. Initial

B. Passive

C. Active

D. Active-primary

Correct Answer: C
Section:
Explanation:
In an active/active high availability (HA) firewall pair, the firewall that is currently processing traffic is in the ''Active'' state. This state indicates that the firewall is fully functional and can own sessions and set up sessions. An active firewall can be either active-primary or active-secondary, depending on the Device ID and the HA configuration. An active-primary firewall connects to User-ID agents, runs DHCP server and DHCP relay, and matches NAT and PBF rules with the Device ID of the active-primary firewall. An active-secondary firewall connects to User-ID agents, runs DHCP server, and matches NAT and PBF rules with the Device ID of the active-secondary firewall.An active-secondary firewall does not support DHCP relay1.Reference:HA Firewall States, PCNSE Study Guide (page 53)