Number: PCNSE
Passing Score: 800
Time Limit: 120
File Version: 31.1

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

Exam A

QUESTION 1
A firewall administrator is investigating high packet buffer utilization in the company firewall. After looking at the threat logs and seeing many flood attacks coming from a single source that are dropped a by the firewall, the administrator decides to enable packet butter protection to protect against similar attacks.
The administrator enables packet buffer protection globally in the firewall but still sees a high packet buffer utilization rate.
What else should the administrator do to stop packet buffers from being overflowed?

A. Add the default Vulnerability Protection profile to all security rules that allow traffic from outside.
B. Enable packet buffer protection for the affected zones.
C. Add a Zone Protection profile to the affected zones.
D. Apply DOS profile to security rules allow traffic from outside.

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

QUESTION 2
Which CLI command displays the physical media that are connected to ethernet1/8?

A. > show system state filter-pretty sys.si.p8.stats
B. > show system state filter-pretty sys.sl.p8.phy
C. > show interface ethernet1/8
D. > show system state filter-pretty sys.sl.p8.med

Correct Answer: B
Section:
Explanation:
Example output:
> show system state filter-pretty sys.s1.p1.phy
sys.s1.p1.phy: {
link-partner: { },
media: CAT5,
type: Ethernet,
}
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cld3CAC

QUESTION 3
During a laptop-replacement project, remote users must be able to establish a GlobalProtect VPN connection to the corporate network before logging in to their new Windows 10 endpoints.
The new laptops have the 5.2.10 GlobalProtect Agent installed, so the administrator chooses to use the Connect Before Logon feature to solve this issue.
What must be configured to enable the Connect Before Logon feature?

A. The GlobalProtect Portal Agent App Settings Connect Method to Pre-logon then On-demand.
B. Registry keys on the Windows system.

C. X-Auth Support in the GlobalProtect Gateway Tunnel Settings.
D. The Certificate profile in the GlobalProtect Portal Authentication Settings.

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/globalprotect/5-2/globalprotect-app-new-features/new- features-released-in-gp-app/connect-before-logon "To use Connect Before Logon, you must enable the settings in the Windows registry and choose the authentication method"

QUESTION 4
The decision to upgrade to PAN-OS 10.2 has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when trying to install.
When performing an upgrade on Panorama to PAN-OS 10.2, what is the potential cause of a failed install?

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

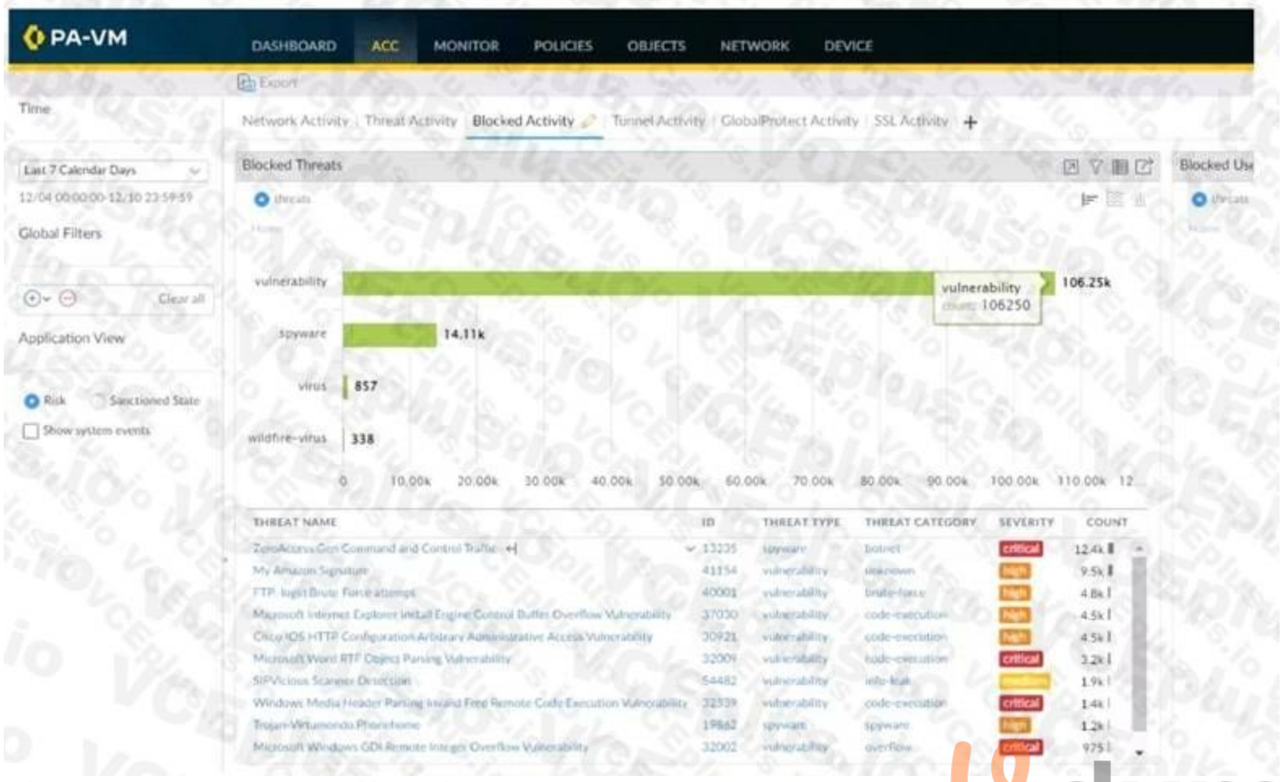
Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-upgrade/upgrade-panorama- plugins/panorama-plugins-upgrade-downgrade-considerations Before you upgrade to PAN-OS 11.0, you must download the Panorama plugin version supported on PAN-OS 11.0 for all plugins installed on Panorama. This is required to successfully upgrade to PAN-OS 11.0. See the Compatibility Matrixfor more information.

QUESTION 5
An engineer needs to collect User-ID mappings from the company's existing proxies.
What two methods can be used to pull this data from third party proxies? (Choose two.)

A. Syslog
B. XFF Headers
C. Client probing
D. Server Monitoring

Correct Answer: A, B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/user-id/user-id-concepts/user- mapping/xff-headers#idf60a278d-2285-4b19-9cc3-95a4b88d5c51 https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/user-id/user-id-concepts/user- mapping/syslog#idee459093-72c1-4ca5-9e44-2c4f359090bb

QUESTION 6
Refer to the exhibit.



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

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

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-the-application- command-center/interact-with-the-acc#id5cc39dae-04cf-4936-9916-1a4b0f3179b9

QUESTION 7
An administrator creates an application-based security policy rule and commits the change to the firewall. Which two methods should be used to identify the dependent applications for the respective rule? (Choose two.)

A. Use the show predefined xpath <value> command and review the output.
B. Review the App Dependency application list from the Commit Status view.
C. Open the security policy rule and review the Depends On application list.
D. Reference another application group containing similar applications.

Correct Answer: B, C
Section:
Explanation:
These two methods allow the administrator to see the dependent applications for a security policy rule that uses application-based criteria. The App Dependency application list shows the applications that are required for

the rule to function properly1. The Depends On application list shows the applications that are implicitly added to the rule based on the predefined dependencies2.Reference: 1: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/app-id-features/simplified-application-dependency-workflow 2: https://docs.paloaltonetworks.com/pan- os/10-1/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies

QUESTION 8
What happens when an A/P firewall cluster synchronizes IPsec tunnel security associations (SAs)?

A. Phase 1 and Phase 2 SAs are synchronized over HA3 links.
B. Phase 1 SAs are synchronized over HA1 links.
C. Phase 2 SAs are synchronized over HA2 links.
D. Phase 1 and Phase 2 SAs are synchronized over HA2 links.

Correct Answer: C
Section:
Explanation:
From the Palo Alto documentation below, "when a VPN is terminated on a Palo Alto firewall HA pair, not all IPSEC related information is synchronized between the firewalls... This is an expected behavior. IKE phase 1 SA information is NOT synchronized between the HA firewalls."And from the second link, "Data link (HA2) is used to sync sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in the HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive). It flows from the active firewall to the passive firewall."https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=e n_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetailhttps://help.aryaka.com/display/public/KNOW/Palo+Alto+Networks+NFV+Technical+Brief

QUESTION 9

Which time determines how long the passive firewall will wait before taking over as the active firewall alter losing communications with the HA peer?

A. Heartbeat Interval
B. Additional Master Hold Up Time
C. Promotion Hold Time
D. Monitor Fall Hold Up Time

Correct Answer: C

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

QUESTION 10
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 11
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 12
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 13
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 14
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 15
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 16
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 17
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 18
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 19
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 20
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 21
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 UI?
(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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29
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 scenarion 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 30
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 31
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 32
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 33
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 34
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 35
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

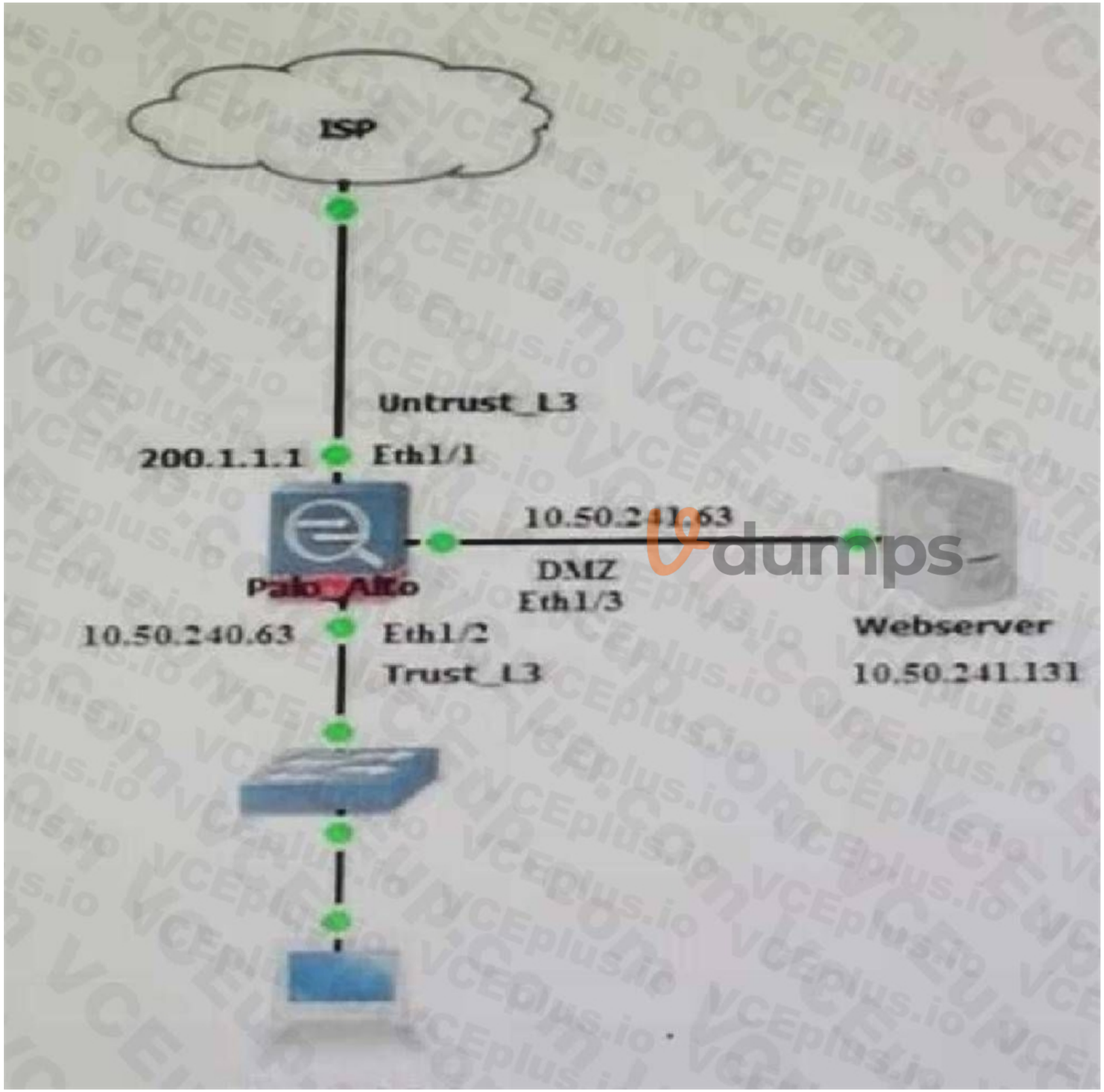
QUESTION 36
What are three reasons for excluding a site from SSL decryption? (Choose three.)

A. the website is not present in English

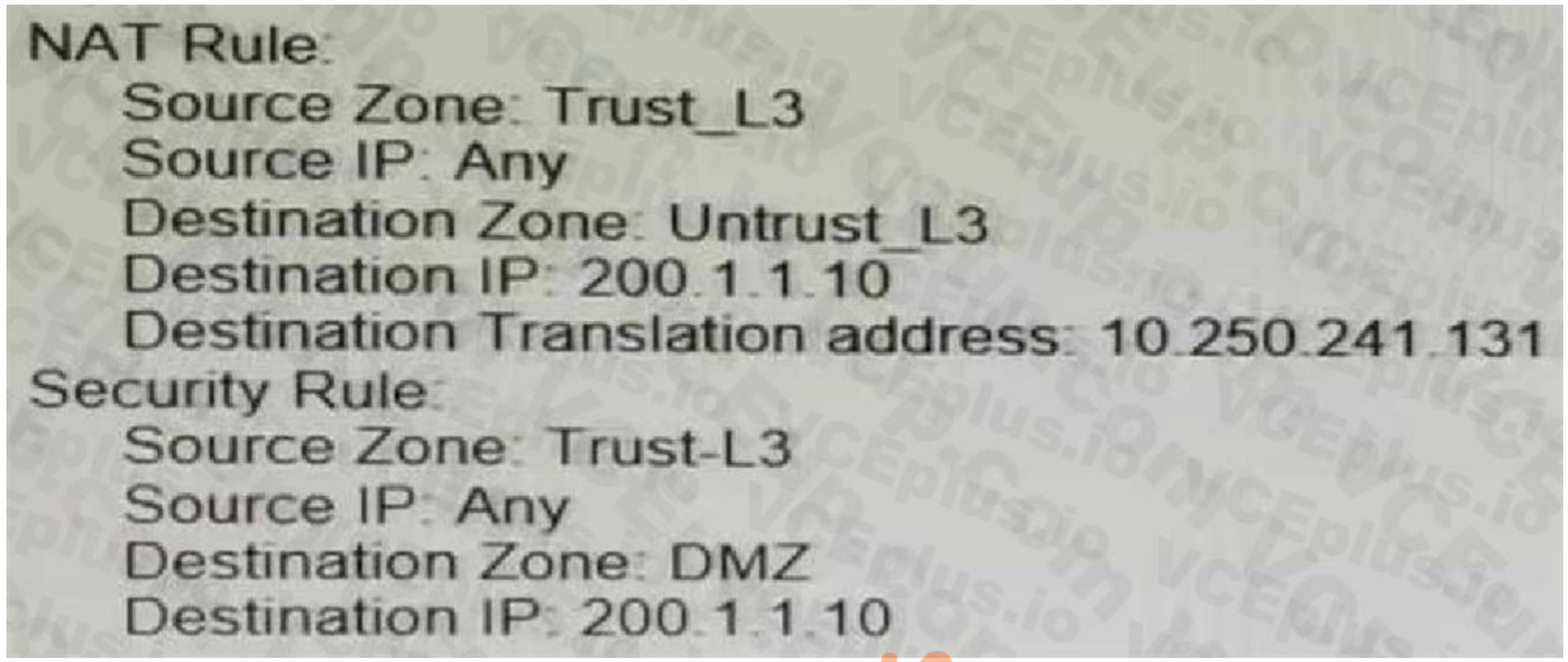
B. unsupported ciphers
C. certificate pinning
D. unsupported browser version
E. mutual authentication

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

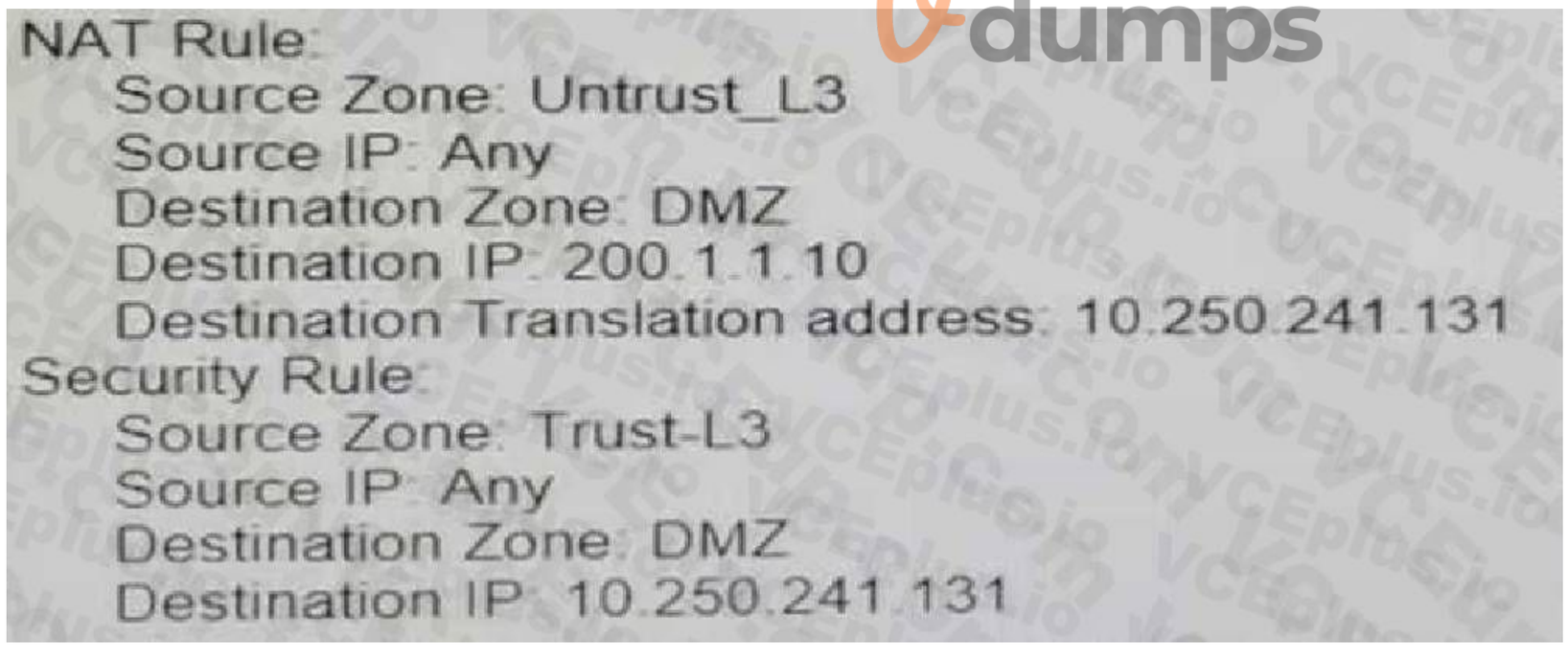
QUESTION 37
A user at an internal system queries the DNS server for their web server with a private IP of 10 250 241 131 in the. The DNS server returns an address of the web server's public address, 200.1.1.10.
In order to reach the web server, which security rule and U-Turn NAT rule must be configured on the firewall?


ISP
Untrust_L3
200.1.1.1
Eth1/1
10.50.241.63
DMZ
Eth1/3
Palo_Alto
10.50.240.63
Eth1/2
Trust_L3
Webserver
10.50.241.131

A.

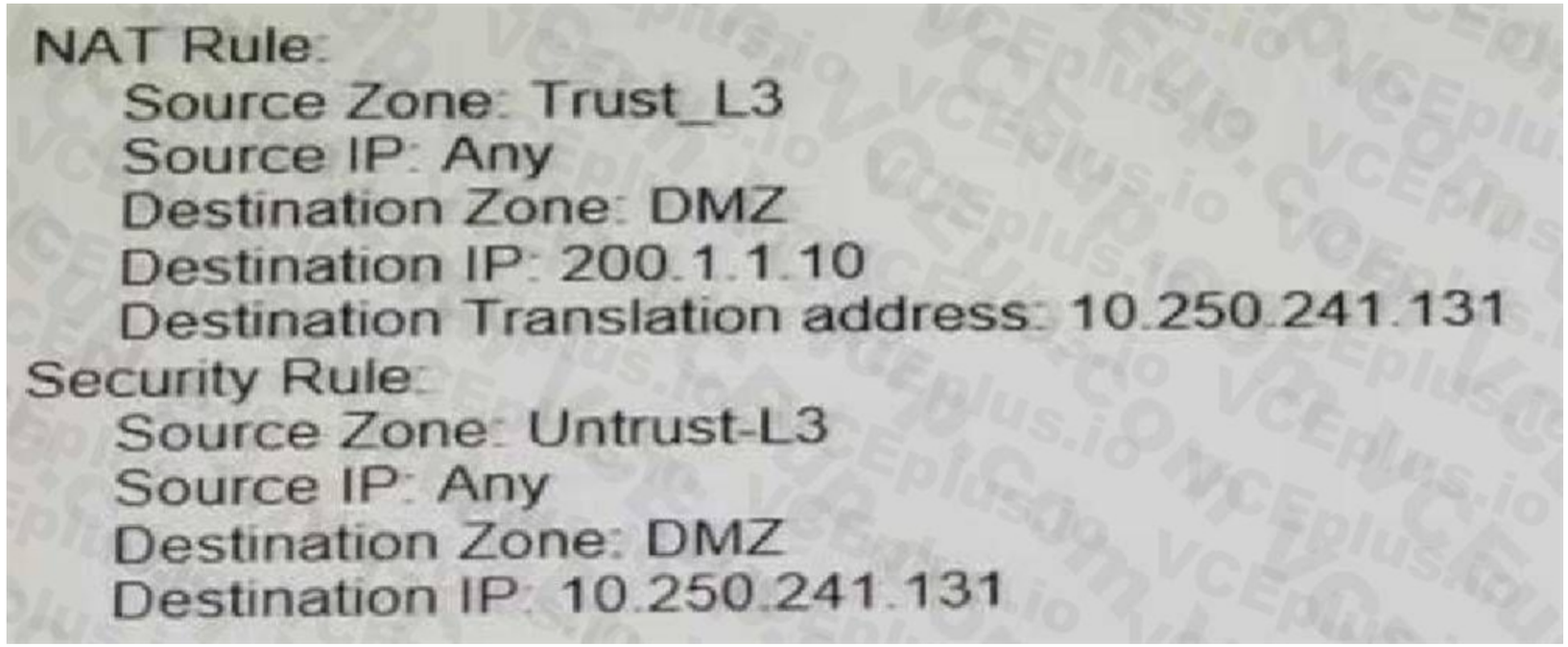

NAT Rule:
Source Zone: Trust_L3
Source IP: Any
Destination Zone: Untrust_L3
Destination IP: 200.1.1.10
Destination Translation address: 10.250.241.131
Security Rule:
Source Zone: Trust-L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 200.1.1.10

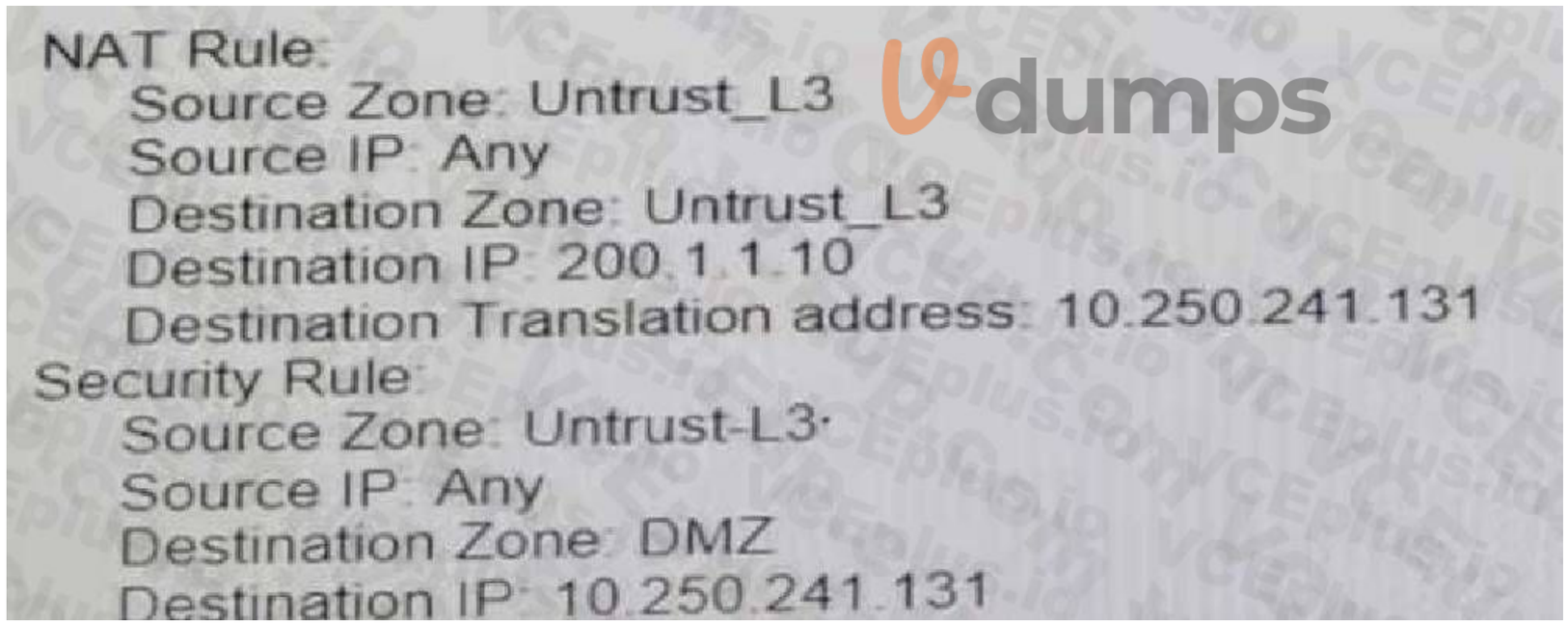
B.


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.

D.





Correct Answer: A
Section:

QUESTION 38
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 39
SAML SLO is supported for which two firewall features? (Choose two.)

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

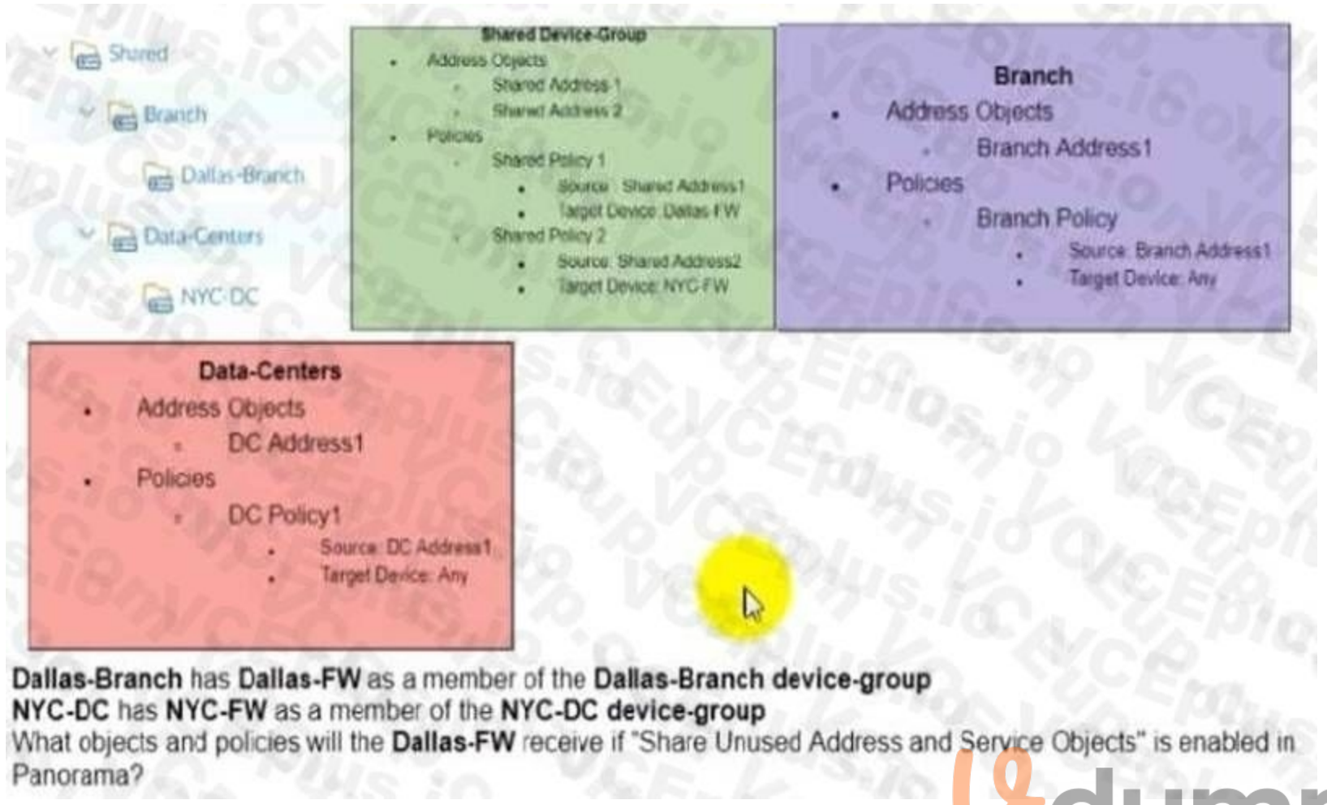
Correct Answer: A, B
Section:
Explanation:
SSO is available to administrators who access the web interface and to end users who access applications through GlobalProtect or Captive Portal. SLO is available to administrators and GlobalProtect end users, but not to Captive Portal end users.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/a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

QUESTION 40
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'

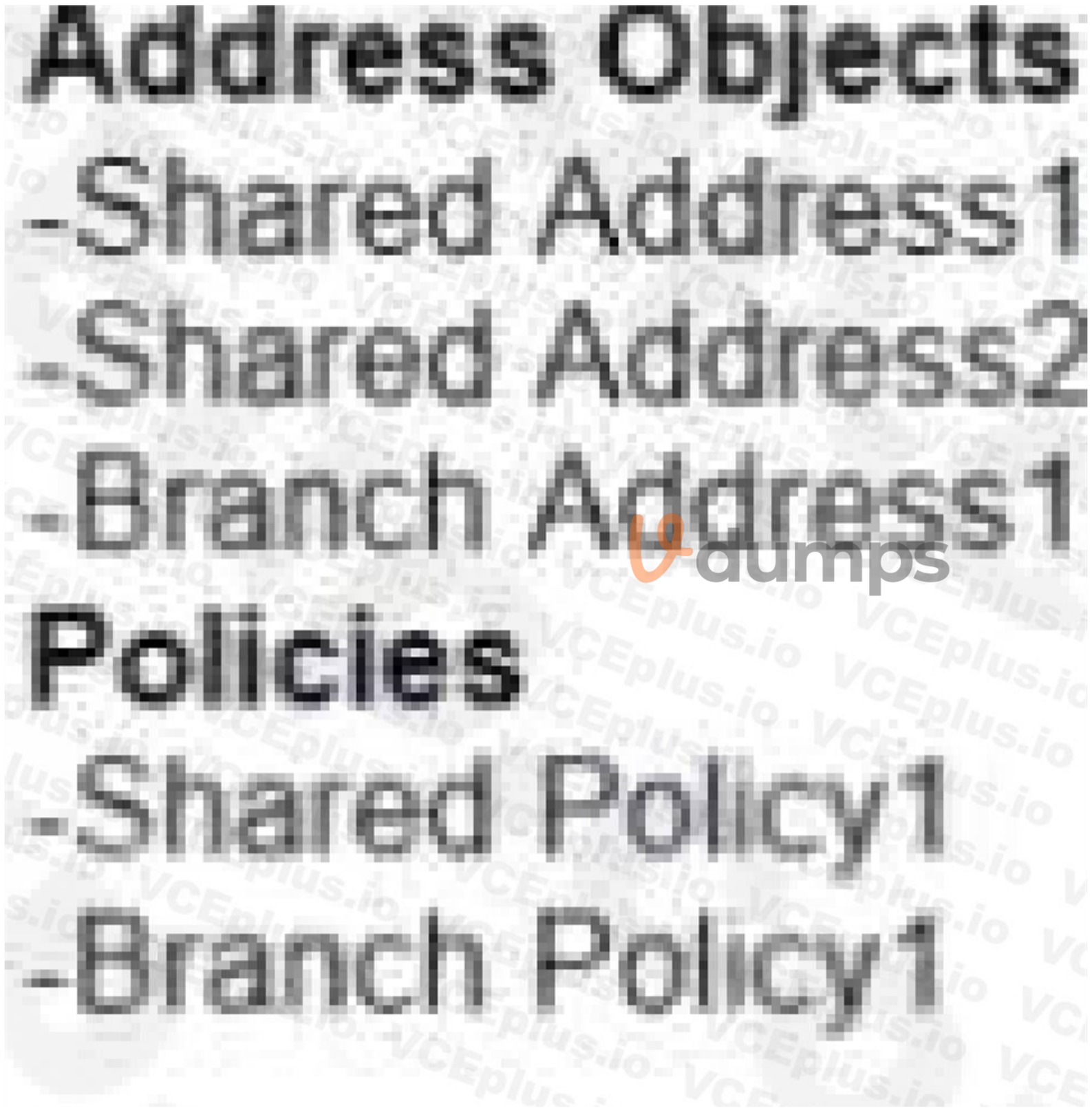
Correct Answer: C
Section:

QUESTION 41
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 42
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 43
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 44
An engineer needs to permit XML API access to a firewall for automation on a network segment that is routed through a Layer 3 subinterface on a Palo Alto Networks firewall. However, this network segment cannot access the dedicated management interface due to the Security policy.
Without changing the existing access to the management interface, how can the engineer fulfill this request?

A. Specify the subinterface as a management interface in Setup > Device > Interfaces.
B. Enable HTTPS in an Interface Management profile on the subinterface.
C. Add the network segment's IP range to the Permitted IP Addresses list
D. Configure a service route for HTTP to use the subinterface

Correct Answer: B
Section:
Explanation:
An interface management profile defines which services are available on an interface, such as HTTPS, SSH, ping, or SNMP. By enabling HTTPS in an interface management profile on the subinterface, the engineer can allow XML API access to the firewall for automation on the network segment that is routed through the subinterface. Specifying the subinterface as a management interface in Setup > Device > Interfaces is not possible, as only physical interfaces can be designated as management interfaces. Adding the network segment's IP range to the Permitted IP Addresses list will not help, as this list only applies to the dedicated management interface. Configuring a service route for HTTP to use the subinterface will not help, as this will only affect the outbound traffic from the firewall to external services, not the inbound traffic to the firewall for XML API access. Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/ networking/configure- interfaces/configure-interface-management-profiles https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/enable-api-access

QUESTION 45
An engineer needs to see how many existing SSL decryption sessions are traversing a firewall What command should be used?

A. show dataplane pool statistics I match proxy
B. debug dataplane pool statistics I match proxy
C. debug sessions I match proxy
D. show sessions all

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhdCAC

QUESTION 46
Which steps should an engineer take to forward system logs to email?

A. Create a new email profile under Device > server profiles; then navigate to Objects > Log Forwarding profile > set log type to system and the add email profile.
B. Enable log forwarding under the email profile in the Objects tab.
C. Create a new email profile under Device > server profiles: then navigate to Device > Log Settings > System and add the email profile under email.
D. Enable log forwarding under the email profile in the Device tab.

Correct Answer: C
Section:
Explanation:
An email profile defines the email server and sender address for sending email notifications from the firewall or Panorama. To forward system logs to email, the engineer needs to create a new email profile under Device > Server Profiles > Email and configure the required settings, such as SMTP server, sender email address, and recipient email address. Then, the engineer needs to navigate to Device > Log Settings > System and select the email profile under Email for each severity level of system logs that need to be forwarded. Enabling log forwarding under the email profile in the Objects tab or in the Device tab is not possible, as log forwarding profiles are configured under Objects > Log Forwarding. Log forwarding profiles are used for forwarding threat, traffic, URL filtering, data filtering, HIP match, configuration, and correlation logs, not system logs. Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-email-alerts https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-forwarding

QUESTION 47
A network security administrator has an environment with multiple forms of authentication. There is a network access control system in place that authenticates and restricts access for wireless users, multiple Windows domain controllers, and an MDM solution for company-provided smartphones. All of these devices have their authentication events logged.

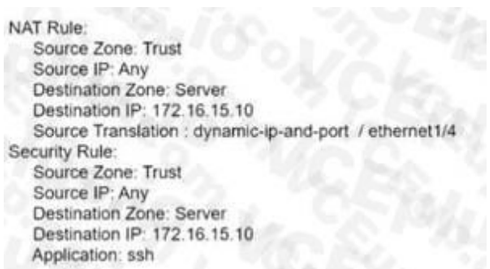
Given the information, what is the best choice for deploying User-ID to ensure maximum coverage?

A. Syslog listener
B. agentless User-ID with redistribution
C. standalone User-ID agent
D. captive portal

Correct Answer: C
Section:
Explanation:
A syslog listener is a User-ID agent that listens for syslog messages from network devices that contain user mapping information, such as network access control systems, domain controllers, or MDM solutions. By configuring a syslog listener on the firewall or Panorama and specifying the syslog format and filters, User-ID can parse the syslog messages and extract user mapping information from multiple sources. Agentless User-ID with redistribution is a method of using an existing firewall as a User-ID agent that redistributes user mappings to other firewalls or Panorama. This method does not involve syslog messages. A standalone User-ID agent is a software application that runs on a Windows server and collects user mappings from Active Directory servers or other sources. This method requires installing and managing a separate agent software. A captive portal is a web page that prompts users to authenticate before accessing certain network resources. This method does not involve syslog messages. Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to- users/syslog-monitoring.html https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to- users/user-id-agents.html

QUESTION 48
Refer to the diagram. Users at an internal system want to ssh to the SSH server The server is configured to respond only to the ssh requests coming from IP 172.16.16.1.
In order to reach the SSH server only from the Trust zone, which Security rule and NAT rule must be configured on the firewall?

A.



B.

C.

D.

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/source-nat-and- destination-nat/source-nat

QUESTION 49
Which Panorama feature protects logs against data loss if a Panorama server fails?

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

Correct Answer: B
Section:
Explanation:
A Panorama Collector Group is a group of dedicated log collectors that receive logs from firewalls and Panorama management servers. By enabling log redundancy in a collector group, Panorama can ensure that each log is written to two log collectors in the group, providing backup in case one log collector fails. Panorama HA does not automatically ensure that no logs are lost if a server fails inside the HA cluster, as HA only provides redundancy for configuration and device management, not for logging. Panorama HA with log redundancy is not a valid option, as log redundancy is configured at the collector group level, not at the HA level. Panorama Collector Group

does not automatically ensure that no logs are lost if a server fails inside the Collector Group, as log redundancy needs to be enabled explicitly in the collector group settings. Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-collection- and-forwarding/configure-log-collection-on-panorama https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-collection- and-forwarding/configure-log-redundancy

QUESTION 50
An administrator is seeing one of the firewalls in a HA active/passive pair moved to 'suspended" state due to Non-functional loop. Which three actions will help the administrator troubleshool this issue? (Choose three.)

A. Use the CLI command show high-availability flap-statistics
B. Check the HA Link Monitoring interface cables.
C. Check the High Availability > Link and Path Monitoring settings.
D. Check High Availability > Active/Passive Settings > Passive Link State
E. Check the High Availability > HA Communications > Packet Forwarding settings.

Correct Answer: A, B, C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhJCAS&lang=ja&r efURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail

QUESTION 51
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 52
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 53
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 54
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 55
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 56
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 57
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 58
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 59
A network security engineer has applied a File Blocking profile to a rule with the action of Block. The user of a Linux CLI operating system has opened a ticket. The ticket states that the user is being blocked by the firewall when trying to download a TAR file. The user is getting no error response on the system.
Where is the best place to validate if the firewall is blocking the user's TAR file?

A. URL Filtering log
B. Data Filtering log
C. Threat log
D. WildFire Submissions log

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClZ1CAK

QUESTION 60

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

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

Correct Answer: A, D
Section:
Explanation:
Option A is correct because setting "Reject Non-syn-TCP" to No and "Asymmetric Path" to Bypass in the Zone Protection profile disables the TCP checks that can cause the firewall to drop packets due to asymmetric routing. This allows the firewall to accept non-SYN TCP packets without a session match and packets that are out of sequence or out of window.Option D is correct because setting session tcp-reject-non-syn to no in the CLI also disables the TCP checks that can cause the firewall to drop packets due to asymmetric routing. This allows the firewall to accept non-SYN TCP packets without a session match and packets that are out of sequence or out of window.Option B is incorrect because setting session tcp-reject-non-syn to no in the CLI has the same effect as setting "Reject Non-syn-TCP" to No in the Zone Protection profile, so there is no need to do both.Also, setting "Asymmetric Path" to Global in the Zone Protection profile does not disable the TCP checks that can cause the firewall to drop packets due to asymmetric routing. It only allows the firewall to use a global timer for asymmetric path detection instead of a per-session timer.Option C is incorrect because setting "Reject Non-syn-TCP" to Global and "Asymmetric Path" to Global in the Zone Protection profile does not disable the TCP checks that can cause the firewall to drop packets due to asymmetric routing. It only allows the firewall to use a global timer for both non- SYN TCP rejection and asymmetric path detection instead of a per-session timer.Reference: 1 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClReCAK 2 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSHCA0

QUESTION 61
Which CLI command is used to determine how much disk space is allocated to logs?

A. show logging-status
B. show system info
C. debug log-receiver show
D. show system logdfo-quota

Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClgZCAS

QUESTION 62
An engineer has been tasked with reviewing traffic logs to find applications the firewall is unable to identify with App-ID. Why would the application field display as incomplete?

A. The client sent a TCP segment with the PUSH flag set.
B. The TCP connection was terminated without identifying any application data.
C. There is insufficient application data after the TCP connection was established.
D. The TCP connection did not fully establish.

Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC Incomplete in the application field: Incomplete means that either the three-way TCP handshake did not complete OR the three-way TCP handshake did complete but there was no enough data after the handshake to identify the application. In other words that traffic being seen is not really an application. One example is, if a client sends a server a SYN and the Palo Alto Networks

device creates a session for that SYN , but the server never sends a SYN ACK back to the client, then that session is incomplete.

QUESTION 63
In the New App Viewer under Policy Optimizer, what does the compare option for a specific rule allow an administrator to compare?

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

Correct Answer: C
Section:
Explanation:
The compare option for a specific rule in the New App Viewer under Policy Optimizer allows an administrator to compare the applications configured in the rule with the applications seen from traffic matching the same rule. This option helps the administrator to identify any discrepancies between the intended and actual applications allowed by the rule. The administrator can then optimize the rule by adding or removing applications as needed1. Option A is incorrect because the compare option does not compare the running configuration with the candidate configuration of the firewall. That is done by using the Commit > Commit and Push option2. Option B is incorrect because the compare option does not compare applications configured in the rule with their dependencies. That is done by using the App Dependencies tab under Policy Optimizer1. Option D is incorrect because the compare option does not compare the security rule with any other security rule selected. That is done by using the Compare Rules option under Policies > Security3.

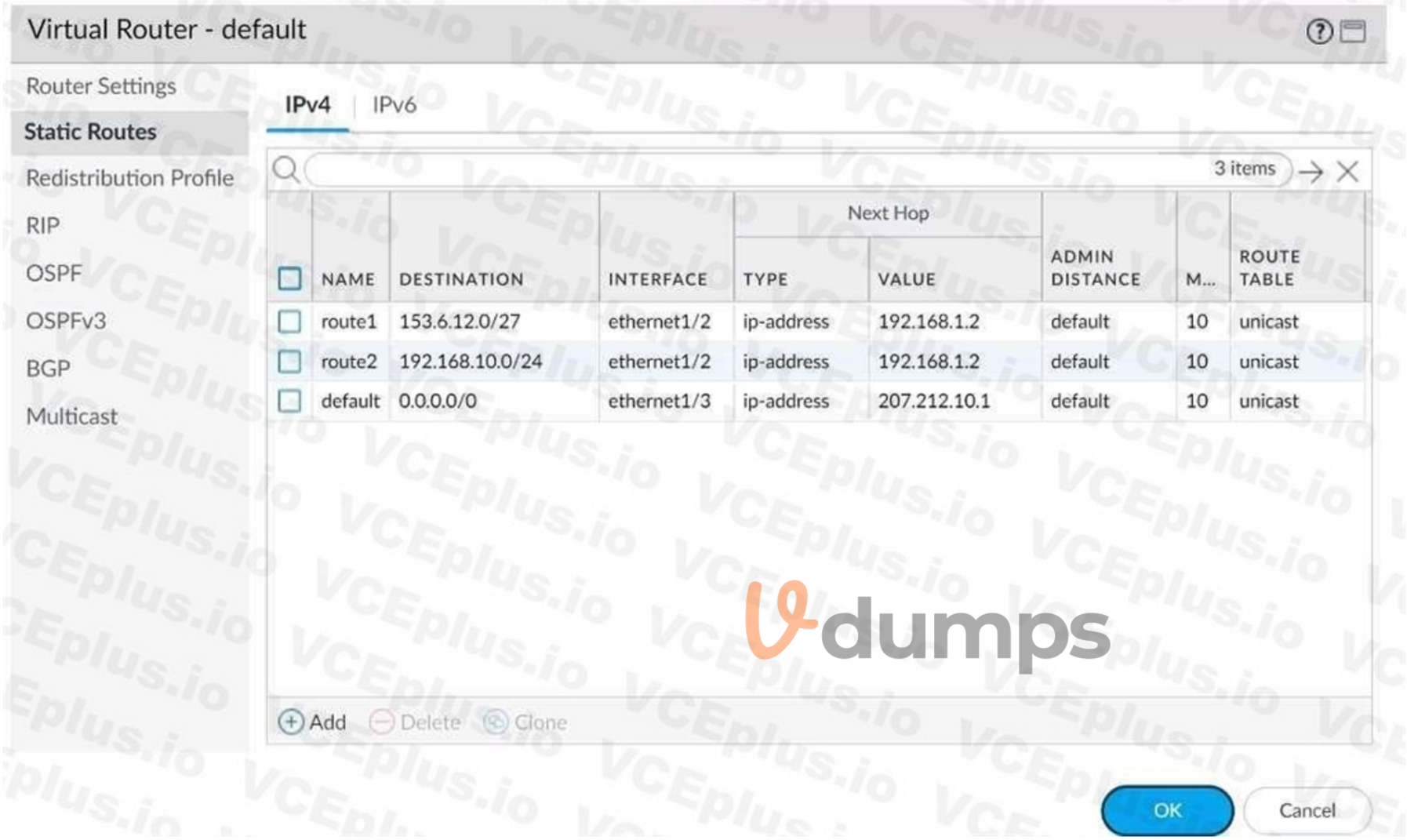
QUESTION 64
Which two profiles should be configured when sharing tags from threat logs with a remote User-ID agent? (Choose two.)

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

Correct Answer: B, C
Section:

QUESTION 65
A firewall engineer creates a destination static NAT rule to allow traffic from the internet to a webserver hosted behind the edge firewall. The pre-NAT IP address of the server is 153.6 12.10, and the post-NAT IP address is 192.168.10.10.
Refer to the routing and interfaces information below.

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



What should the NAT rule destination zone be set to?

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

Correct Answer: B
Section:
Explanation:
The destination zone in the NAT rule is determined after the route lookup of the destination IP address in the original packet (that is, the pre-NAT destination IP address).
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/nat-configurationexamples/destination-nat-exampleone-to-one-mapping
The NAT rule destination zone should be set to the zone where the traffic is destined before NAT. In this case, the traffic from the internet is destined to the pre-NAT IP address of the server, which is 153.6.12.10. This IP address belongs to the Outside zone, as shown in the routing and interfaces information. Therefore, the NAT rule destination zone should be set to Outside. The other options are not correct. None is not a valid option for the NAT rule destination zone. Inside and DMZ are the zones where the traffic is destined after NAT, which is 192.168.10.10. Reference: :
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/networking/nat/source-anddestination-nat/configure-destination-nat

QUESTION 66
The NAT rule destination zone should be set to Outside because that is the zone where the post-NAT IP address of the server (192.168.10.10) belongs. The destination zone of a NAT rule is the zone where the translated IP address resides.
Option A is incorrect because None is not a valid zone for a NAT rule. Option C is incorrect because DMZ is the zone where the pre-NAT IP address of the server (153.6 12.10) belongs, not the post-NAT IP address. Option D is incorrect because Inside is not a zone that is configured on the firewall.
An administrator is troubleshooting why video traffic is not being properly classified.
If this traffic does not match any QoS classes, what default class is assigned?

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

Correct Answer: D
Section:
Explanation:
The default class that is assigned to traffic that does not match any QoS classes is class 4. Class 4 is the default class for any session not matched to a QoS policy. QoS policy, like security policy, is processed top to bottom and the first policy match will be applied. If no policy match is found, the traffic is assigned to class 412. Option A is incorrect because class 1 is not the default class for unmatched traffic. Class 1 is a user-defined class that can be used to assign traffic based on QoS policy criteria. Option B is incorrect because class 2 is not the default class for unmatched traffic. Class 2 is a userdefined class that can be used to assign traffic based on QoS policy criteria. Option C is incorrect because class 3 is not the default class for unmatched traffic. Class 3 is a user-defined class that can be used to assign traffic based on QoS policy criteria3.

QUESTION 67
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 (Panorama).

QUESTION 68
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 69
Which statement about High Availability timer settings is true?

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

Correct Answer: B
Section:
Explanation:

QUESTION 70
What are two best practices for incorporating new and modified App-IDs? (Choose two)

A. Configure a security policy rule to allow new App-IDs that might have network-wide impact
B. Study the release notes and install new App-IDs if they are determined to have low impact
C. Perform a Best Practice Assessment to evaluate the impact or the new or modified App-IDs
D. Run the latest PAN-OS version in a supported release tree to have the best performance for the new App-IDs

Correct Answer: A, B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content- updates/best-practices-for-app-and-threat-content-updates/best-practices-security- first#id184AH00F06E

QUESTION 71
Which three firewall multi-factor authentication factors are supported by PAN-OS? (Choose three)

A. SSH key
B. User logon
C. Short message service
D. One-Time Password
E. Push

Correct Answer: B, D, E
Section:
Explanation:
According to Palo Alto Networks documentation123, multi-factor authentication (MFA) is a methodof verifying a user's identity using two or more factors, such as something they know, something they have, or something they are.The firewall supports MFA for administrative access, GlobalProtect VPN access, and Captive Portal access. The firewall can integrate with external MFA providers such as RSA SecurID, Duo Security, or Okta Verify.The three firewall MFA factors that are supported by PAN-OS are: User logon: This is something the user knows, such as a username and password.One-Time Password: This is something the user has, such as a code generated by an app or sent by email or
SMS.Push: This is something the user is, such as a biometric verification or a device approval.

QUESTION 72
An engineer has been given approval to upgrade their environment 10 PAN-OS 10 2 The environment consists of both physical and virtual firewalls a virtual Panorama HA pair, and virtual log collectors What is the

recommended order when upgrading to PAN-OS 10.2?

A. Upgrade Panorama, upgrade the log collectors, upgrade the firewalls
B. Upgrade the firewalls upgrade log collectors, upgrade Panorama
C. Upgrade the firewalls upgrade Panorama, upgrade the log collectors
D. Upgrade the log collectors, upgrade the firewalls, upgrade Panorama

Correct Answer: A
Section:
Explanation:
Make sure Panorama is running the same or a later PAN-OS version than you are upgrading to. You must upgrade Panorama and its Log Collectors to 10.2 before upgrading the managed firewalls to this version. In addition, when upgrading Log Collectors to 10.2, you must upgrade all Log Collectors at the same time due to changes in the logging infrastructure. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/upgrade-firewalls-using- panorama

QUESTION 73
Which benefit do policy rule UUIDs provide?

A. An audit trail across a policy's lifespan
B. Functionality for scheduling policy actions
C. The use of user IP mapping and groups in policies
D. Cloning of policies between device-groups

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/enumeration-of-rules-within- a-rulebase To keep track of rules within a rulebase, you can refer to the rule number, which changes depending on the order of a rule in the rulebase. The rule number determines the order in which the firewall applies the rule. The universally unique identifier (UUID) for a rule never changes even if you modify the rule, such as when you change the rule name. The UUID allows you to track the rule across rule bases even after you deleted the rule.

QUESTION 74
A network security administrator wants to begin inspecting bulk user HTTPS traffic flows egressingout of the internet edge firewall. Which certificate is the best choice to configure as an SSL ForwardTrust certificate?

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

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

QUESTION 75
An engineer is designing a deployment of multi-vsys firewalls.
What must be taken into consideration when designing the device group structure?

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

C. Multiple vsys and firewalls can be assigned to a device group, and a multi-vsys firewall can have each vsys in a different device group.
D. Only one vsys or one firewall can be assigned to a device group, and a multi-vsys firewall can have each vsys in a different device group.

Correct Answer: C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClETCA0

QUESTION 76
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same firewall. The update contains an application that matches the same traffic signatures as the custom application.
Which application will be used to identify traffic traversing the firewall?

A. Custom application
B. Unknown application
C. Incomplete application
D. Downloaded application

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/u-v/custom-app-id-and-threat-signatures/custom- application-and-threat-signatures/about-custom-application-signatures.html

QUESTION 77
What happens, by default, when the GlobalProtect app fails to establish an IPSec tunnel to the GlobalProtect gateway?

A. It stops the tunnel-establishment processing to the GlobalProtect gateway immediately.
B. It tries to establish a tunnel to the GlobalProtect gateway using SSL/TLS.
C. It keeps trying to establish an IPSec tunnel to the GlobalProtect gateway.
D. It tries to establish a tunnel to the GlobalProtect portal using SSL/TLS.

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClfoCAC "Should the IPSec connection fail, VPN will fall back to SSL protocol."

QUESTION 78
An engineer wants to configure aggregate interfaces to increase bandwidth and redundancy between the firewall and switch. Which statement is correct about the configuration of the interfaces assigned to an aggregate interface group?

A. They can have a different bandwidth.
B. They can have a different interface type such as Layer 3 or Layer 2.
C. They can have a different interface type from an aggregate interface group.
D. They can have different hardware media such as the ability to mix fiber optic and copper.

Correct Answer: D
Section:
Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure- interfaces/configure-an-aggregate-interface-group

QUESTION 79
What is a key step in implementing WildFire best practices?

A. In a mission-critical network, increase the WildFire size limits to the maximum value.
B. Configure the firewall to retrieve content updates every minute.
C. In a security-first network, set the WildFire size limits to the minimum value.
D. Ensure that a Threat Prevention subscription is active.

Correct Answer: D
Section:
Explanation:
In the WildFire best practices linked below, the first step is to "... make sure that you have an active Threat Prevention subscription. Together, WildFireÆ and Threat Prevention enable comprehensivethreat detection and prevention." https:// docs.paloaltonetworks.com/wildfire/10-1/wildfire- admin/wildfire-deployment-best-practices/wildfire-best-practices.html

QUESTION 80
An administrator is attempting to create policies for deployment of a device group and template stack. When creating the policies, the zone drop-down list does not include the required zone.
What can the administrator do to correct this issue?

A. Enable "Share Unused Address and Service Objects with Devices" in Panorama settings.
B. Add a firewall to both the device group and the template.
C. Specify the target device as the master device in the device group.
D. Add the template as a reference template in the device group.

Correct Answer: D
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 81
Review the images.

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

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

Correct Answer: C
Section:
Explanation:
The threat profile has the action set to "alert" which means that the traffic is allowed but logged. The profile also has the "Tag Source IP" option enabled with the tag name "BadGuys" and the timeout value of 180 minutes. This means that any source IP address that matches a threat signature will be tagged with "BadGuys" for 180 minutes. The tag can be used for dynamic address groups or external dynamic lists to enforce policy actions based on the tag. Reference: :https:// docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/set-up-antivirus- anti-spyware-and-vulnerability-protection/tag-source-ip-addresses-that-trigger-threat-signatures

QUESTION 82
A system administrator runs a port scan using the company tool as part of vulnerability check. The administrator finds that the scan is identified as a threat and is dropped by the firewall. After further investigating the logs, the administrator finds that the scan is dropped in the Threat Logs.
What should the administrator do to allow the tool to scan through the firewall?

A. Remove the Zone Protection profile from the zone setting.
B. Add the tool IP address to the reconnaissance protection source address exclusion in the Zone Protection profile.
C. Add the tool IP address to the reconnaissance protection source address exclusion in the DoS Protection profile.

D. Change the TCP port scan action from Block to Alert in the Zone Protection profile.

Correct Answer: B
Section:
Explanation:
The administrator should add the tool IP address to the reconnaissance protection source address exclusion in the Zone Protection profile to allow the tool to scan through the firewall. Reconnaissance protection is a feature of Zone Protection profiles that allows the firewall to detect and block network reconnaissance attempts, such as port scans. The source address exclusion list allows theadministrator to whitelist up to 20 IP addresses or netmask address objects that are exempt fromreconnaissance protection1. Option A is incorrect because removing the Zone Protection profile from the zone setting would disable all the zone protection features, not just reconnaissance protection.This would reduce the security of the zone and expose it to other types of attacks. Option C is incorrect because adding the tool IP address to the reconnaissance protection source address exclusion in the DoS Protection profile would not have any effect. DoS Protection profiles are used to protect against excessive traffic volume, not network reconnaissance attempts. Option D is incorrect because changing the TCP port scan action from Block to Alert in the Zone Protection profile would only affect TCP port scans, not other types of scans. It would also affect all TCP port scans, not just those from the tool IP address.https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos- protection/configure-zone-protection-to-increase-network-security/configure-reconnaissance- protection

QUESTION 83
An administrator has 750 firewalls. The administrator's central-management Panorama instance deploys dynamic updates to the firewalls. The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls.
If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the configuration does not appear, what is the root cause?

A. Panorama does not have valid licenses to push the dynamic updates.
B. Panorama has no connection to Palo Alto Networks update servers.
C. No service route is configured on the firewalls to Palo Alto Networks update servers.
D. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed.

Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKQCA0 "Locally defined dynamic updates setting on a managed Palo Alto Networks firewall take preference over the Panorama pushed setting."

QUESTION 84
An administrator wants to enable WildFire inline machine learning.
Which three file types does WildFire inline ML analyze? (Choose three.)

A. MS Office
B. ELF
C. APK
D. VBscripts
E. Powershell scripts

Correct Answer: A, B, E
Section:

QUESTION 85
An administrator wants to grant read-only access to all firewall settings, except administrator accounts, to a new-hire colleague in the IT department.
Which dynamic role does the administrator assign to the new-hire colleague?

A. Device administrator (read-only)
B. System administrator (read-only)
C. Firewall administrator (read-only)

D. Superuser (read-only)

Correct Answer: A
Section:
Explanation:
Read-only access to all firewall settings except password profiles (no access) and administratoraccounts (only the logged in account is visible). https://docs.paloaltonetworks.com/pan-os/10- 1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types

QUESTION 86
Which feature checks Panorama connectivity status after a commit?

A. Automated commit recovery
B. Scheduled config export
C. Device monitoring data under Panorama settings
D. HTTP Server profiles

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama- features/automatic-panorama-connection-recovery

QUESTION 87
What is the dependency for users to access services that require authentication?

A. An Authentication profile that includes those services
B. Disabling the authentication timeout
C. An authentication sequence that includes those services
D. A Security policy allowing users to access those services

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication- policy/configure-authentication-policy

QUESTION 88
A network engineer is troubleshooting a VPN and wants to verify whether the decapsulation/encapsulation counters are increasing. Which CLI command should the engineer run?

A. Show vpn tunnel name | match encap
B. Show vpn flow name <tunnel name>
C. Show running tunnel flow lookup
D. Show vpn ipsec-sa tunnel <tunnel name>

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClivCAC

QUESTION 89

A network administrator is troubleshooting an issue with Phase 2 of an IPSec VPN tunnel. The administrator determines that the lifetime needs to be changed to match the peer.
Where should this change be made?

A. IKE Gateway profile
B. IPSec Crypto profile
C. IPSec Tunnel settings
D. IKE Crypto profile

Correct Answer: B
Section:
Explanation:
The **IKE crypto profile** is used to set up the encryption and authentication algorithms used for the key exchange process in IKE Phase 1, and lifetime of the keys, which specifies how long the keys are valid. To invoke the profile, you must attach it to the IKE Gateway configuration. The **IPSec crypto profile** is invoked in IKE Phase 2. It specifies how the data is secured within the tunnel when Auto Key IKE is used to automatically generate keys for the IKE SAs.

QUESTION 90
How does Panorama prompt VMWare NSX to quarantine an infected VM?

A. Email Server Profile
B. Syslog Sewer Profile
C. SNMP Server Profile
D. HTTP Server Profile

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/vm-series/10-0/vm-series-deployment/set-up-the-vm-series- firewall-on-nsx/set-up-the-vm-series-firewall-on-vmware-nsx/dynamically-quarantine-infected- guests.html#id8e9a242e-e038-4ba2-b0ea-eaaf53690be0

QUESTION 91
Given the screenshot, how did the firewall handle the traffic?

A. Traffic was allowed by policy but denied by profile as encrypted.
B. Traffic was allowed by policy but denied by profile as a threat
C. Traffic was allowed by profile but denied by policy as a threat.
D. Traffic was allowed by policy but denied by profile as a nonstandard port.

Correct Answer: B
Section:
Explanation:
The screenshot shows the threat log which records the traffic that matches a threat signature or is blocked by a security profile. The log entry indicates that the traffic was allowed by the security policy rule "Allow-All" but was denied by the vulnerability protection profile "strict" as a threat. The threat name is "Microsoft Windows SMBv1 Multiple Vulnerabilities (MS17-010: EternalBlue)" and the action is "reset-both" which means that the firewall reset both the client and server connections.Reference: : https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-syslog- for-monitoring/syslog-field-descriptions/threat-log-fields

QUESTION 92
A user at an external system with the IP address 65.124.57.5 queries the DNS server at 4. 2.2.2 for the IP address of the web server, www,xyz.com. The DNS server returns an address of 172.16.15.1

In order to reach Ire web server, which Security rule and NAT rule must be configured on the firewall?

A.

NAT Rule:
Untrust-L3 (any) - Trust-L3 (172.16.15.1) Destination Translation : 192.168.15.47
Security Rule:
Untrust-L3 (any) - Trust-L3 (192.168.15.47) - Application : Web-browsing

B.

NAT Rule:
Untrust-L3 (any) - Trust-L3 (172.16.15.1) Destination Translation : 192.168.15.47
Security Rule:
Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application : Web-browsing

C.

NAT Rule:
Untrust-L3 (any) - Untrust-L3 (172.16.15.1) Destination Translation : 192.168.15.47
Security Rule:
Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application : Web-browsing

D.

NAT Rule:
Untrust-L3 (any) - Untrust-L3 (any) Destination Translati
Security Rule:
Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application :

Correct Answer: C
Section:
Explanation:
The addresses used in destination NAT rules always refer to the original IP address in the packet (that is, the pre-translated address). The destination zone in the NAT rule is determined after the route lookup of the destination IP address in the original packet (that is, the pre-NAT destination IP address). The addresses in the security policy also refer to the IP address in the original packet (that is, the pre-NAT address). However, the destination zone is the zone where the end host is physically connected. In other words, the destination zone in the security rule is determined after the routelookup of the post-NAT destination IP address.
https://docs.paloaltonetworks.com/pan-os/9-1/pan- os-admin/networking/nat/ nat-configuration-examples/destination-nat-exampleone-to-one-mapping

QUESTION 93
An administrator is receiving complaints about application performance degradation. After checking the ACC. the administrator observes that there Is an excessive amount of SSL traffic
Which three elements should the administrator configure to address this issue? (Choose three.)

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

Correct Answer: A, D, E
Section:
Explanation:
To address the issue of excessive SSL traffic, the administrator should configure QoS on both the ingress and egress interfaces for the traffic flows. This will allow the administrator to control the bandwidth allocation and priority of different applications based on their QoS classes. The administrator should also define a QoS profile that specifies the traffic classes and their guaranteed bandwidth percentages. The QoS profile can then be

applied to a QoS policy rule that matches the SSL traffic based on source and destination zones or other criteria. Reference: :https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/quality-of-service/configure-qos

QUESTION 94
A company has configured a URL Filtering profile with override action on their firewall. Which two profiles are needed to complete the configuration? (Choose two)

A. SSL/TLS Service
B. HTTP Server
C. Decryption
D. Interface Management

Correct Answer: A, D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/allow-password-access- to-certain-sites#id7e63ce07-8b30-4506-a1e3-5800303954e

QUESTION 95
An administrator accidentally closed the commit window/screen before the commit was finished.
Which two options could the administrator use to verify the progress or success of that commit task?
(Choose two.)

A. System Logs
B. Task Manager
C. Traffic Logs
D. Configuration Logs

Correct Answer: A, B
Section:
Explanation:
A. System Logs: The system logs contain information about various events that occur on the firewall, including the commit process. The administrator can review the system logs to verify whether the commit completed successfully or whether there were any errors or warnings during the commit process.
B. Task Manager: The task manager displays a list of all active tasks on the firewall, including the commit task. The administrator can use the task manager to check the status of the commit task, including whether it is in progress, completed successfully, or failed.

QUESTION 96
The same route appears in the routing table three times using three different protocols Which mechanism determines how the firewall chooses which route to use?

A. Administrative distance
B. Round Robin load balancing
C. Order in the routing table
D. Metric

Correct Answer: A
Section:
Explanation:
Administrative distance is the measure of trustworthiness of a routing protocol. It is used to determine the best path when multiple routes to the same destination exist. The route with the lowest administrative distance is chosen as the best route.
When the same route appears in the routing table three times using three different protocols, the mechanism that determines which route the firewall chooses to use is the administrative distance.
This is explained in the Palo Alto Networks PCNSE Study Guide in Chapter 6: Routing, under the section "Route Selection":

"Administrative distance is a value assigned to each protocol that the firewall uses to determine which route to use if multiple protocols provide routes to the same destination. The route with the lowest administrative distance is preferred."

QUESTION 97
An administrator is configuring SSL decryption and needs 10 ensure that all certificates for both SSL Inbound inspection and SSL Forward Proxy are installed properly on the firewall. When certificates are being imported to the firewall for these purposes, which three certificates require a private key?
(Choose three.)

A. Forward Untrust certificate
B. Forward Trust certificate
C. Enterprise Root CA certificate
D. End-entity (leaf) certificate
E. Intermediate certificate(s)

Correct Answer: A, B, D
Section:
Explanation:
This is discussed in the Palo Alto Networks PCNSE Study Guide in Chapter 9: Decryption, under the section "SSL Forward Proxy and Inbound Inspection Certificates":
"When importing SSL decryption certificates, you need to provide private keys for the forward trust, forward untrust, and end-entity (leaf) certificates. You do not need to provide private keys for the root CA and intermediate certificates."

QUESTION 98
A network administrator wants to deploy SSL Forward Proxy decryption. What two attributes should a forward trust certificate have? (Choose two.)

A. A subject alternative name
B. A private key
C. A server certificate
D. A certificate authority (CA) certificate

Correct Answer: A, C
Section:
Explanation:
When deploying SSL Forward Proxy decryption, a forward trust certificate must have a subject alternative name (SAN) and be a server certificate. SAN is an extension to the X.509 standard that allows multiple domain names to be protected by a single SSL/TLS certificate. It is used to identify the domain names or IP addresses that the certificate should be valid for. A private key is also required but it is not mentioned in the options. A certificate authority (CA) certificate is not required as the forward trust certificate itself is a CA certificate.

QUESTION 99
An engineer has been asked to limit which routes are shared by running two different areas within an OSPF implementation. However, the devices share a common link for communication. Which virtual router configuration supports running multiple instances of the OSPF protocol over a single link?

A. ASBR
B. ECMP
C. OSPFv3
D. OSPF

Correct Answer: C
Section:
Explanation:

Support for multiple instances per linkóWith OSPFv3, you can run multiple instances of the OSPF protocol over a single link. This is accomplished by assigning an OSPFv3 instance ID number. An interface that is assigned to an instance ID drops packets that contain a different ID.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/ospf/ospfconcepts/ospfv3

QUESTION 100
A Security policy rule is configured with a Vulnerability Protection Profile and an action of "Deny." Which action will this configuration cause on the matched traffic?

A. The Profile Settings section will be grayed out when the Action is set to "Deny"
B. It will cause the firewall to skip this Security policy rule. A warning will be displayed during a commit
C. The configuration will allow the matched session unless a vulnerability signature is detected.
D. The "Deny" action will supersede the per-severity defined actions defined in the associated Vulnerability Protection Profile It will cause the firewall to deny the matched sessions.
Any configured Security Profiles have no effect if the Security policy rule action is set to "Deny"

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/security-profiles.html
First note in above link states:
"Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy." The first thing the firewall checks per it's flow is the security policy match and action. The Security Profile never gets checked if a match happens on a policy set to deny that match.

QUESTION 101
An engineer has discovered that certain real-time traffic is being treated as best effort due to it exceeding defined bandwidth Which QoS setting should the engineer adjust?

A. QoS profile: Egress Max
B. QoS interface: Egress Guaranteed
C. QoS profile: Egress Guaranteed
D. QoS interface: Egress Max

Correct Answer: C
Section:
Explanation:
When the egress guaranteed bandwidth is exceeded, the firewall passes traffic on a best-effort basis.
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/quality-of-service/qos-concepts/qos-bandwidth-management

QUESTION 102
A company is looking to increase redundancy in their network. Which interface type could help accomplish this?

A. Layer 2
B. Virtual wire
C. Tap
D. Aggregate ethernet

Correct Answer: D
Section:
Explanation:
An aggregate group increases the bandwidth between peers by load balancing traffic across the combined interfaces. It also provides redundancy https://docs.paloaltonetworks.com/pan-os/10- 1/pan-os-networking-admin/configure-interfaces/configure-an-aggregate-interfacegroup# id9c0f5a8b-0aad-4be5-821d-ef9d7c11a88d

QUESTION 103
An administrator has two pairs of firewalls within the same subnet. Both pairs of firewalls have been configured to use High Availability mode with Active/Passive. The ARP tables for upstream routes display the same MAC address being shared for some of these firewalls.
What can be configured on one pair of firewalls to modify the MAC addresses so they are no longer in conflict?

A. Configure a floating IP between the firewall pairs.
B. Change the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet.
C. Change the interface type on the interfaces that have conflicting MAC addresses from L3 to VLAN.
D. On one pair of firewalls, run the CLI command: set network interface vlan arp.

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCASchange the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet. This will prevent the MAC addresses from conflicting and allow the firewalls to properly route traffic. You can also configure a floating IP between the firewall pairs if necessary.

QUESTION 104
How can an administrator use the Panorama device-deployment option to update the apps and threat version of an HA pair of managed firewalls?

A. Configure the firewall's assigned template to download the content updates.
B. Choose the download and install action for both members of the HA pair in the Schedule object.
C. Switch context to the firewalls to start the download and install process.
D. Download the apps to the primary; no further action is required.

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/use-caseconfigure-firewalls-using-panorama/set-up-your-centralized-configuration-and-policies/add-themanaged-firewalls-and-deploy-updates

QUESTION 105
An engineer is tasked with configuring a Zone Protection profile on the untrust zone.
Which three settings can be configured on a Zone Protection profile? (Choose three.)

A. Ethernet SGT Protection
B. Protocol Protection
C. DoS Protection
D. Reconnaissance Protection
E. Resource Protection

Correct Answer: B, C, D
Section:
Explanation:
B. Protocol Protection: Protocol protection is used to limit or block traffic that uses certain protocols or application functions. For example, a Zone Protection profile can be configured to block traffic that uses non-standard protocols, such as IP-in-IP, or to limit the number of concurrent sessions for certain protocols, such as SIP.
C. DoS Protection: DoS protection is used to protect against various types of denial-of-service (DoS) attacks, such as SYN floods, UDP floods, ICMP floods, and others. A Zone Protection profile can be configured to limit the rate of traffic for certain protocols or to drop traffic that matches specific patterns, such as malformed packets or packets with invalid headers.
D. Reconnaissance Protection: Reconnaissance protection is used to prevent attackers from gathering information about the network, such as by using port scans or other techniques. A Zone Protection profile can be

configured to limit the rate of traffic for certain types of reconnaissance, such as port scans or OS fingerprinting, or to drop traffic that matches specific patterns, such as packets with invalid flags or payloads.

QUESTION 106
A firewall administrator requires an A/P HA pair to fail over more quickly due to critical business application uptime requirements.
What is the correct setting?

A. Change the HA timer profile to "aggressive" or customize the settings in advanced profile.
B. Change the HA timer profile to "fast".
C. Change the HA timer profile to "user-defined" and manually set the timers.
D. Change the HA timer profile to "quick" and customize in advanced profile.

Correct Answer: A
Section:
Explanation:
The HA timer profile determines the parameters for detecting failures and triggering failover in an A/P HA pair. The default timer profile is "recommended" which provides a balance between failover speed and stability. To achieve faster failover, the administrator can change the HA timer profile to "aggressive" which reduces the heartbeat intervals and timeouts. Alternatively, the administratorcan customize the settings in the advanced profile and manually adjust the timers according to their needs1. Reference: 1: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high- availability/ha-concepts/ha-timers

QUESTION 107
Where can an administrator see both the management-plane and data-plane CPU utilization in the WebUI?

A. System Resources widget
B. System Logs widget
C. Session Browser
D. General Information widget

Correct Answer: A
Section:
Explanation:
The System Resources widget of the Exadata WebUI, displays a real-time overview of the various resources like CPU, Memory, and I/O usage across the entire Exadata Database Machine. It shows the usage of both management-plane and data-plane CPU utilization.
System Resources Widget Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or Panorama).
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/dashboard/dashboardwidgets.html

QUESTION 108
An administrator would like to determine which action the firewall will take for a specific CVE. Given the screenshot below, where should the administrator navigate to view this information?

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

Correct Answer: C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClMnCAK

QUESTION 109
When using SSH keys for CLI authentication for firewall administration, which method is used for authorization?

A. Local
B. LDAP
C. Kerberos
D. Radius

Correct Answer: A
Section:
Explanation:
When using SSH keys for CLI authentication for firewall administration, the method used for authorization is local. This is described in the Palo Alto Networks PCNSE Study Guide in Chapter 4: Authentication and Authorization, under the section "CLI Authentication with SSH Keys":
"SSH keys use public key cryptography to authenticate users, but they do not provide a mechanism for authorization. Therefore, when using SSH keys for CLI authentication, authorization is always performed locally on the firewall."

QUESTION 110

An administrator Just enabled HA Heartbeat Backup on two devices However, the status on tie firewall's dashboard is showing as down High Availability.
What could an administrator do to troubleshoot the issue?

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

Correct Answer: B
Section:
Explanation:
If the HA status is showing as down after enabling HA Heartbeat Backup on two devices, an administrator could troubleshoot the issue by checking the peer IP address in the permit list in Device > Setup > Management > Interfaces > Management Interface Settings. This is described in the Palo Alto Networks PCNSE Study Guide in Chapter 7: High Availability, under the section "Configure Heartbeat Backup for Redundancy":
"Verify that the management interface's permitted IP addresses on each peer includes the IP address of the other peer's Heartbeat Backup interface."

QUESTION 111
A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours.
Which two steps are likely to mitigate the issue? (Choose TWO)

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

Correct Answer: A, C
Section:
Explanation:
This is because excluding video traffic from being sent over the VPN will reduce the amount of bandwidth being used during peak hours, allowing more bandwidth to be available for other types of traffic. Blocking non-work related traffic will also reduce the amount of bandwidth being used, further freeing up bandwidth for work-related traffic.
Enabling decryption and creating a Tunnel Inspection policy are not likely to mitigate the issue of decreased performance during peak-use hours, as they do not directly address the issue of limited bandwidth availability during these times.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PP3ICAW

QUESTION 112
An administrator is configuring a Panorama device group
Which two objects are configurable? (Choose two)

A. DNS Proxy
B. Address groups
C. SSL/TLS roles
D. URL Filtering profiles

Correct Answer: B, D
Section:
Explanation:
URL filtering is a feature in Palo Alto Networks firewalls that allows administrators to block access to specific URLs [1]. This feature can be configured via four different objects: Custom URL categories in URL Filtering profiles, PAN-DB URL categories in URL Filtering profiles, External Dynamic Lists (EDL) in URL Filtering profiles, and Custom URL categories in Security policy rules. The evaluation order for URL filtering is: Custom URL categories in URL Filtering profile, PAN-DB URL categories in URL Filtering profile, EDL in URL Filtering profile, and Custom URL category in Security policy rule. This information can be found in the Palo Alto Networks PCNSE Study Guide, which

can be accessed here:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/resource-library/palo-altonetworks-pcnse-study-guide.html.

QUESTION 113
A network security administrator wants to configure SSL inbound inspection.
Which three components are necessary for inspecting the HTTPS traffic as it enters the firewall?
(Choose three.)

A. An SSL/TLS Service profile
B. The web server's security certificate with the private key
C. A Decryption profile
D. A Decryption policy
E. The client's security certificate with the private key

Correct Answer: B, C, D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-inboundinspection

QUESTION 114
A network security administrator has been tasked with deploying User-ID in their organization.
What are three valid methods of collecting User-ID information in a network? (Choose three.)

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

Correct Answer: A, B, C
Section:
Explanation:
User-ID is a feature that enables the firewall to identify users and groups based on their IP addresses, usernames, or other attributes.
There are three valid methods of collecting User-ID information in a network:
Windows User-ID agent: This is a software agent that runs on a Windows server and collects user mapping information from Active Directory, Exchange servers, or other sources.
GlobalProtect: This is a VPN solution that provides secure remote access for users and devices. It also collects user mapping information from endpoints that connect to the firewall using GlobalProtect.
XMLAPI: This is an application programming interface that allows third-party applications or scripts to send user mapping information to the firewall using XML format.

QUESTION 115
After importing a pre-configured firewall configuration to Panorama, what step is required to ensure a commit/push is successful without duplicating local configurations?

A. Ensure Force Template Values is checked when pushing configuration.
B. Push the Template first, then push Device Group to the newly managed firewal.
C. Perform the Export or push Device Config Bundle to the newly managed firewall.
D. Push the Device Group first, then push Template to the newly managed firewall

Correct Answer: C

Section:
Explanation:
When importing a pre-configured firewall configuration to Panorama, you need to perform the following steps12:
Add the serial number of the firewall under Panorama > Managed Devices In Panorama, import the firewall's configuration bundle under Panorama > Setup > Operations > Import device configuration to Panorama Make changes to the imported firewall configuration within Panorama Commit the changes you made to Panorama Perform an Export or push Device Config Bundle operation under Panorama > Setup > Operations The Export or push Device Config Bundle operation allows you to push a complete configuration bundle from Panorama to a managed firewall without duplicating local configurations3. This operation ensures that any local settings on the firewall are preserved and merged with the settings from Panorama.

QUESTION 116
An engineer creates a set of rules in a Device Group (Panorama) to permit traffic to various services for a specific LDAP user group.
What needs to be configured to ensure Panorama can retrieve user and group information for use in these rules?

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

Correct Answer: A
Section:
Explanation:
To configure LDAP authentication on Panorama, you need to23:
Define an LDAP server profile that specifies the connection details and credentials for accessing the LDAP server.
Define an authentication profile that references the LDAP server profile and defines how users authenticate to Panorama (such as username format and password expiration).
Define an authentication sequence (optional) that allows users to authenticate using multiple methods (such as local database, LDAP, RADIUS, etc.).
Assign the authentication profile or sequence to a Panorama administrator role or a device group role.

QUESTION 117
An engineer is tasked with configuring SSL forward proxy for traffic going to external sites.
Which of the following statements is consistent with SSL decryption best practices?

A. The forward trust certificate should not be stored on an HSM.
B. The forward untrust certificate should be signed by a certificate authority that is trusted by the clients.
C. Check both the Forward Trust and Forward Untrust boxes when adding a certificate for use with SSL decryption
D. The forward untrust certificate should not be signed by a Trusted Root CA

Correct Answer: B
Section:
Explanation:
According to the PCNSE Study Guide1, SSL forward proxy is a feature that allows the firewall to decrypt and inspect SSL traffic going to external sites. The firewall acts as a proxy between the client and the server, generating a certificate on the fly for each site.
The best practices for configuring SSL forward proxy are23:
Use a forward trust certificate that is signed by a certificate authority (CA) that is trusted by the clients. This certificate is used to sign certificates for sites that have valid certificates from trusted CAs. The clients will not see any certificate errors if they trust the forward trust certificate.
Use a forward untrust certificate that is not signed by a trusted CA. This certificate is used to sign certificates for sites that have invalid or untrusted certificates. The clients will see certificate errors if they do not trust the forward untrust certificate. This helps alert users of potential risks and prevent man-in-the-middle attacks.
Do not store the forward trust or untrust certificates on an HSM (hardware security module). The HSM does not support on-the-fly signing of certificates, which is required for SSL forward proxy.

QUESTION 118
Which three methods are supported for split tunneling in the GlobalProtect Gateway? (Choose three.)

A. Video Streaming Application
B. Destination Domain
C. Client Application Process
D. Source Domain
E. URL Category

Correct Answer: B, C, E
Section:
Explanation:
The GlobalProtect Gateway supports three methods for split tunneling23:
Access Route ó You can define a list of IP addresses or subnets that are accessible through the VPN tunnel. All other traffic goes directly to the internet.
Domain and Application ó You can define a list of domains or applications that are accessible through the VPN tunnel. All other traffic goes directly to the internet. You can also use this method to exclude specific domains or applications from the VPN tunnel.
Video Traffic ó You can exclude video streaming traffic from the VPN tunnel based on predefined categories or custom URLs. This method reduces latency and jitter for video streaming applications.

QUESTION 119
An engineer discovers the management interface is not routable to the User-ID agent What configuration is needed to allow the firewall to communicate to the User-ID agent?

A. Create a NAT policy for the User-ID agent server
B. Add a Policy Based Forwarding (PBF) policy to the User-ID agent IP
C. Create a custom service route for the UID Agent
D. Add a static route to the virtual router

Correct Answer: C
Section:
Explanation:
To allow the firewall to communicate with the User-ID agent, you need to configure a custom service route for the UID Agent23. A custom service route allows you to specify which interface and source IP address the firewall uses to connect to a specific destination service. By default, the firewall uses its management interface for services such as User-ID, but you can override this behavior by creating a custom service route.
To configure a custom service route for the UID Agent, you need to do the following steps:
Go to Device > Setup > Services and click Service Route Configuration.
In the Service column, select User-ID Agent from the drop-down list.
In the Interface column, select an interface that can reach the User-ID agent server from the dropdown list.
In the Source Address column, select an IP address that belongs to that interface from the drop-down list.
Click OK and Commit your changes.
The correct answer is C. Create a custom service route for UID Agent

QUESTION 120
Which log type will help the engineer verify whether packet buffer protection was activated?

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

Correct Answer: C
Section:
Explanation:

The log type that will help the engineer verify whether packet buffer protection was activated is Threat Logs. Threat Logs are logs generated by the Palo Alto Networks firewall when it detects a malicious activity on the network. These logs contain information about the source, destination, and type of threat detected. They also contain information about the packet buffer protection that was activated in response to the detected threat. This information can help the engineer verify that packet buffer protection was activated and determine which actions were taken in response to the detected threat. Packet buffer protection is a feature that prevents packet buffer exhaustion by dropping packets, discarding sessions, or blocking source IP addresses when the packet buffer utilization exceeds a certain threshold. The firewall records these events in the threat log with different threat IDs andnames1. The system log also records an alert event when the packet buffer congestion reaches thealert threshold2. The other types of logs do not show packet buffer protection events. Reference: 1:https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection 2: https://docs.paloaltonetworks.com/pan-os/10- 2/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/system-log-fields

QUESTION 121
Which GlobalProtect gateway selling is required to enable split-tunneling by access route, destination domain, and application?

A. No Direct Access to local networks
B. Tunnel mode
C. iPSec mode
D. Satellite mode

Correct Answer: B
Section:
Explanation:
To enable split-tunneling by access route, destination domain, and application, you need to configure a split tunnel based on the domain and application on your GlobalProtect gateway2. This allows you to specify which domains and applications are included or excluded from the VPN tunnel.

QUESTION 122
Which three multi-factor authentication methods can be used to authenticate access to the firewall?
(Choose three.)

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

Correct Answer: A, B, D
Section:
Explanation:
These three methods are examples of multi-factor authentication that can be used to authenticate access to the firewall. A one-time password is a code that is generated by an authentication app or sent by email or SMS and expires after a single use. A user certificate is a digital credential that is issued by a trusted authority and stored on the user's device. SMS is a text message that is sent tothe user's phone number with a code or a link to verify their identity1. The other methods are notsupported by the firewall for multi-factor authentication. Voice and fingerprint are biometric factorsthat require special hardware and software to capture and analyze. Reference: 1: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/configure-multi- factor-authentication

QUESTION 123
An engineer must configure the Decryption Broker feature. To which router must the engineer assign the decryption forwarding interfaces that are used in Decryption Broker security chain?

A. A virtual router that has no additional interfaces for passing data-type traffic and no other configured routes than those used for the security chain.
B. The default virtual router. If there is no default virtual router , the engineer must create one during setup.
C. A virtual router that is configured with at least one dynamic routing protocol and has at least one entry in the RIB
D. The virtual router that routes the traffic that the Decryption Broker security chain inspects.

Correct Answer: D
Section:
Explanation:
Decryption Broker is a feature that allows you to use a Palo Alto Networks firewall as a decryption broker for other security devices in your network1. It works by decrypting traffic on one interface and forwarding it to another interface where it can be inspected by other devices before being reencrypted and sent to its destination2. The firewall acts as a transparent bridge between the two interfaces and does not change the source or destination IP addresses of the traffic2.
To configure Decryption Broker, you need to assign decryption forwarding interfaces (DFIs) to the virtual router that routes the traffic that you want to inspect. The DFIs are used to forward decrypted traffic from one interface to another in a security chain3. A security chain is a set of devices that perform different security functions on the same traffic flow3. You can have multiple security chains for different types of traffic or different segments of your network3.
The reason why you need to assign DFIs to the virtual router that routes the traffic is because Decryption Broker uses routing tables to determine which DFI belongs to which security chain and how to forward traffic between them2. If you assign DFIs to a different virtual router than the one that routes the traffic, Decryption Broker will not be able to find them or forward traffic correctly2.

QUESTION 124
An administrator wants to enable WildFire inline machine learning. Which three file types does WildFire inline ML analyze?
(Choose three.)

A. MS Office
B. ELF
C. Powershell scripts
D. VBscripts
E. APK

Correct Answer: A, B, C
Section:

QUESTION 125
A network security administrator wants to enable Packet-Based Attack Protection in a Zone Protection profile.
What are two valid ways to enable Packet-Based Attack Protection? (Choose two.)

A. ICMP Drop
B. TCP Drop
C. TCP Port Scan Block
D. SYN Random Early Drop

Correct Answer: B, D
Section:
Explanation:
Packet-Based Attack Protection is a feature of Zone Protection Profiles that allows the firewall to drop packets that are malformed, spoofed, or part of a port scan. TCP Drop and SYN Random Early Drop are two options under Packet-Based
Attack Protection that can be enabled to protect against TCPbased attacks. TCP Drop enables the firewall to check for spoofed IP addresses, mismatched overlapping TCP segments, and invalid IP options. SYN Random Early Drop enables the firewall to drop SYN packets randomly when the SYN queue is full, preventing SYN flood attacks. ICMP Drop and TCP Port Scan Block are not valid options under Packet-Based Attack Protection

QUESTION 126
Where can a service route be configured for a specific destination IP?

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

D. Use Device > Setup > Services > Service Route Configuration > Customize > IPv4

Correct Answer: C
Section:
Explanation:
A service route is the path from the interface to the service on a server. By default, the firewall uses the management interface to communicate to various servers, including DNS, Email, Palo Alto Updates, User-ID agent, Syslog, Panorama, dynamic updates, URL updates, licenses, and AutoFocus.
etc. Sometimes, it is necessary to use an alternative path other than Firewall management IP due to many restrictions. To configure service routes for non-predefined services, the destination addresses can be manually entered in the Destination section under Device > Setup > Services > Service Route Configuration > Customize1. Option A is incorrect because it is used to configure static routes for network traffic, not service routes for firewall services. Option B is incorrect because it is used to configure general service settings such as NTP server and proxy server, not service routes for specific destinations. Option D is incorrect because it is used to configure service routes for predefined services such as DNS and Syslog, not service routes for non-predefined services2.

QUESTION 127
Which feature of Panorama allows an administrator to create a single network configuration that can be reused repeatedly for large-scale deployments even if values of configured objects, such as routes and interface addresses, change?

A. Template stacks
B. Template variables
C. The Shared device group
D. A device group

Correct Answer: B
Section:
Explanation:
Template variables are placeholders that you can use in a template or a template stack to represent values that differ across firewalls, such as IP addresses, hostnames, or interface names. Template variables allow you to create a single network configuration that can be reused repeatedly for largescale deployments even if values of configured objects change1. Option A is incorrect because template stacks are used to group multiple templates together and apply them to firewalls or device groups. Template stacks do not allow you to use variables for different values2. Option C is incorrect because the Shared device group is used to push policies and objects that are common across all firewalls managed by Panoram a. The Shared device group does not allow you to use variables for different values3. Option D is incorrect because a device group is used to group firewalls that require similar policies and objects. A device group does not allow you to use variables for different values3.

QUESTION 128
A firewall administrator wants to have visibility on one segment of the company network. The traffic on the segment is routed on the Backbone switch. The administrator is planning to apply Security rules on segment X after getting the visibility.
There is already a PAN-OS firewall used in L3 mode as an internet gateway, and there are enough system resources to get extra traffic on the firewall. The administrator needs to complete this operation with minimum service interruptions and without making any IP changes.
What is the best option for the administrator to take?

A. Configure the TAP interface for segment X on the firewall.
B. Configure vwire interfaces for segment X on the firewall.
C. Configure a Layer 3 interface for segment X on the firewall.
D. Configure a new vsys for segment X on the firewall.

Correct Answer: A
Section:
Explanation:
A TAP interface is a dedicated interface on the firewall that can be connected to a switch SPAN or mirror port to passively monitor traffic flows across a network. A TAP interface provides application visibility and threat detection without being in the flow of network traffic. A TAP interface does not require any IP changes or service interruptions on the network segment1. Option B is incorrect because vwire interfaces are used to create virtual wires that transparently connect two network segments. Vwire interfaces require physical cabling changes and may cause service interruptions on the network segment2. Option C is incorrect because a Layer 3 interface is used to route traffic between different subnets. A Layer 3 interface requires IP changes and may cause service interruptions on the network segment2. Option D is incorrect because a new vsys is used to create a

virtual system that can have its own set of policies and objects. A new vsys does not provide visibility or security for a specific network segment3.

QUESTION 129
Refer to the exhibit.

An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.
How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all the existing monitoring/security platforms?

A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services
B. Configure log compression and optimization features on all remote firewalls
C. Any configuration on an M-500 would address the insufficient bandwidth concerns
D. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW

Correct Answer: A
Section:
Explanation:
Forwarding logs from firewalls only to Panorama and having Panorama forward logs to other external services is the best option for the administrator to reduce WAN traffic while maintaining support for all the existing monitoring/security platforms. This option minimizes the number of log forwarding destinations on each firewall and consolidates log forwarding on Panoram a. Panorama can forward logs to external destinations such as syslog servers, email servers, SNMP trap receivers, HTTP servers, or AutoFocus1. Option B is incorrect because configuring log compression and optimization features on all remote firewalls may reduce the size of log files but does not reduce the number of log forwarding destinations. Option C is incorrect because any configuration on an M-500 would not address the insufficient bandwidth concerns. An M-500 is a dedicated log collector that can store logs from multiple firewalls and Panorama appliances. However, it does not reduce the WAN traffic generated by log forwarding2. Option D is incorrect because forwarding logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW does not reduce WAN traffic while maintaining support for all the existing monitoring/security platforms. This option would increase the WAN traffic by sending logs back and forth between Panorama and the NGFW1.

QUESTION 130
An ISP manages a Palo Alto Networks firewall with multiple virtual systems for its tenants.
Where on this firewall can the ISP configure unique service routes for different tenants?

A. Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Inherit Global Service Route Configuration
B. Setup > Services > Global > Service Route Configuration > Customize

C. Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Customize
D. Setup > Services > Global > Service Route Configuration > Use Management Interface for all

Correct Answer: C
Section:
Explanation:
The best option for the ISP to configure unique service routes for different tenants is to use the Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Customize option on the firewall. This option allows the ISP to customize the service routes for each virtual system that represents a tenant. A service route is the path from the interface to the service on a server, such as DNS, email, or Panorama. By customizing the service routes for each virtual system, the ISP can ensure that each tenant uses a different interface or IP address to access these services1. Option A is incorrect because it is used to inherit the global service route configuration for a virtual system, not to customize it.
Option B is incorrect because it is used to customize the global service route configuration for all virtual systems, not for a specific one. Option D is incorrect because it is used to use the management interface for all service routes, not to customize them1.

QUESTION 131
An engineer is tasked with deploying SSL Forward Proxy decryption for their organization.
What should they review with their leadership before implementation?

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

Correct Answer: D
Section:
Explanation:
The engineer should review the legal compliance regulations and acceptable usage policies with their leadership before implementing SSL Forward Proxy decryption for their organization. SSL Forward Proxy decryption allows the firewall to decrypt and inspect the traffic from internal users to external servers. This can raise privacy and legal concerns for the users and the organization.
Therefore, the engineer should ensure that the leadership is aware of the implications and benefits of SSL Forward Proxy decryption and that they have a clear policy for informing and obtaining consent from the users.
Option A is incorrect because browser-supported cipher documentation is not relevant for SSL Forward Proxy decryption. The firewall uses its own cipher suite to negotiate encryption with the external server, regardless of the browser settings. Option B is incorrect because cipher documentation supported by the endpoint operating system is not relevant for SSL Forward Proxy decryption. The firewall uses its own cipher suite to negotiate encryption with the external server, regardless of the endpoint operating system. Option C is incorrect because URL risk-based category distinctions are not relevant for
SSL Forward Proxy decryption. The firewall can decrypt and inspect traffic based on any URL category, not just risk-based ones.

QUESTION 132
What can be used as an Action when creating a Policy-Based Forwarding (PBF) policy?

A. Deny
B. Discard
C. Allow
D. Next VR

Correct Answer: D
Section:
Explanation:
Next VR can be used as an Action when creating a Policy-Based Forwarding (PBF) policy. A PBF policy allows the firewall to forward traffic based on criteria such as source and destination IP addresses, application, user, and service. The Action of a PBF policy defines how the firewall forwards the matching traffic. Next VR specifies the virtual router to which the firewall forwards the traffic. Option A is incorrect because Deny is not a valid Action for a PBF policy. Deny is an Action for a security policy that blocks the matching traffic. Option B is incorrect because Discard is not a valid Action for a PBF policy. Discard is an Action for a DoS protection policy that drops the matching traffic. Option C is incorrect because Allow is not a valid Action for a PBF policy. Allow is an Action for a security policy that permits the matching traffic.

QUESTION 133
An engineer reviews high availability (HA) settings to understand a recent HA failover event. Review the screenshot below.


Election Settings
Device Priority
100
Preemptive
Heartbeat Backup
HA Timer Settings
Advanced
Promotion Hold Time (ms)
2000
Hello Interval (ms)
8000
Heartbeat Interval (ms)
2000
Flap Max
3
Preemption Hold Time (min)
1
Monitor Fail Hold Up Time (ms)
0
Additional Master Hold Up Time (ms)
500
Load Recommended
Load Aggressive
OK
Cancel

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

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

Correct Answer: C
Section:
Explanation:
The heartbeat interval determines the frequency at which the HA peers exchange messages in the form of an ICMP (ping). The default value is 1000 milliseconds (1 second). The heartbeat interval is used to detect failures and trigger failover in an HA pair1. The other options are not correct. The hello interval determines the frequency at which the HA peers exchange messages in the form of an HA packet. The default value is 3000 milliseconds (3 seconds). The hello interval is used to establish and maintain HA connectivity2. The promotion hold time determines the amount of time that a passive firewall waits before it becomes active after detecting a failure on the active firewall. The default value is 5000 milliseconds (5 seconds)3. The monitor fail hold up time determines the amount of time that a firewall waits before it declares a monitor failure after detecting a link down event on an interface. The default value is 2000 milliseconds (2 seconds)4. Reference: 1:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/hatimers 2:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/haconcepts/ha-timers 3:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/highavailability/ha-concepts/ha-timers 4:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-osadmin/high-availability/ha-concepts/ha-timers

QUESTION 134
Which three options does Panorama offer for deploying dynamic updates to its managed devices? (Choose three.)

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

Correct Answer: B, C, E
Section:
Explanation:
Panorama offers three options for deploying dynamic updates to its managed devices: Schedules, Install from file, and Revert content. Schedules allows the administrator to configure a recurring schedule for downloading and installing dynamic updates from the Palo Alto Networks update server. Install from file allows the administrator to manually upload and install a dynamic update file from a local system. Revert content allows the administrator to revert to a previous version of a dynamic update in case of any issues with the current version. Option A is incorrect because Verify is not an option for deploying dynamic updates on Panoram a. Verify is an option for validating the configuration on Panorama or a managed device. Option D is incorrect because Check dependencies is not an option for deploying dynamic updates on Panorama. Check dependencies is an option for checking if a configuration change affects other settings on Panorama or a managed device.

QUESTION 135
An engineer troubleshooting a VPN issue needs to manually initiate a VPN tunnel from the CLI.
Which CLI command can the engineer use?

A. test vpn flow
B. test vpn Ikeósa
C. test vpn tunnel
D. test vpn gateway

Correct Answer: D

Section:
Explanation:
The engineer can use the test vpn gateway CLI command to manually initiate a VPN tunnel from the CLI. This command allows the engineer to specify the name of the VPN gateway and the IP address of the peer to initiate an IKE negotiation and establish a VPN tunnel. Option A is incorrect because test vpn flow is not a valid CLI command. Option B is incorrect because test vpn ike-sa is a CLI command that displays information about the IKE security associations, not initiates a VPN tunnel. Option C is incorrect because test vpn tunnel is a CLI command that displays information about the IPSec security associations, not initiates a VPN tunnel.

QUESTION 136
As a best practice, logging at session start should be used in which case?

A. On all Allow rules
B. While troubleshooting
C. Only when log at session end is enabled
D. Only on Deny rules

Correct Answer: B
Section:
Explanation:
Logging at session start should be used as a best practice while troubleshooting. Logging at session start allows the administrator to see the logs for sessions that are initiated but not completed, such as sessions that are dropped or blocked by the firewall. This can help the administrator to identify and resolve issues with network connectivity or firewall configuration. Logging at session start should not be used for normal operations because it generates more logs and consumes more resources on the firewall. Option A is incorrect because logging at session start should not be used on all Allow rules. Logging at session end is sufficient for Allow rules because it provides information about the completed sessions, such as bytes and packets transferred, application, user, and threat information.
Option C is incorrect because logging at session start can be used independently of logging at session end. Logging at session start and logging at session end are not mutually exclusive options. Option D is incorrect because logging at session start should not be used only on Deny rules. Logging at session end is sufficient for Deny rules because it provides information about the denied sessions, such as source and destination IP addresses, ports, and protocol.

QUESTION 137
An auditor is evaluating the configuration of Panorama and notices a discrep-ancy between the Panorama template and the local firewall configuration.
When overriding the firewall configuration pushed from Panorama, what should you consider?

A. The modification will not be visible in Panorama.
B. The firewall template will show that it is out of sync within Panorama.
C. Panorama will update the template with the overridden value.
D. Only Panorama can revert the override.

Correct Answer: A
Section:
Explanation:
When overriding the firewall configuration pushed from Panorama, the modification will not be visible in Panoram a. The firewall will show an override icon next to the modified setting and will display a warning message that the local configuration differs from Panorama. The override icon will also appear on Panorama next to the firewall name in the Device Groups and Templates tabs1. The other options are not correct. The firewall template will not show that it is out of sync within Panorama, because the template itself is not modified. Panorama will not update the template with the overridden value, because the template is read-only on the firewall. The override can be reverted either from Panorama or from the firewall2. Reference: 1: https://docs.paloaltonetworks.com/pan-os/10-2/panos-admin/firewall-administration/manage-configuration/override-a-template-setting 2: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manageconfiguration/revert-an-overridden-template-setting

QUESTION 138
Which type of zone will allow different virtual systems to communicate with each other?

A. Tap
B. External

C. Virtual Wire
D. Tunnel

Correct Answer: B
Section:
Explanation:
An external zone is a type of zone that will allow different virtual systems to communicate with each other. An external zone is a special zone that is shared by all virtual systems on the firewall and can be used to route traffic between virtual systems without leaving the firewall. The external zone can also be used to route traffic to other zones within the same virtual system1. The other options are not correct. A tap zone is a type of zone that is used to passively monitor traffic without affecting the flow of packets2. A virtual wire zone is a type of zone that is used to create a transparent bridge between two network segments without changing the original IP addressing or routing3. A tunnel zone is a type of zone that is used to terminate VPN tunnels or other types of encapsulated traffic4.
Reference: 1: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/virtualsystems/communication-between-virtual-systems/inter-vsys-traffic-that-remains-within-thefirewall/external-zone 2: https://docs.paloaltonetworks.com/pan-os/10-2/pan-osadmin/networking/configure-interfaces/configure-a-tap-interface 3: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/networking/configureinterfaces/configure-a-virtual-wire 4: https://docs.paloaltonetworks.com/pan-os/10-2/pan-osadmin/networking/configure-interfaces/configure-a-tunnel-interface

QUESTION 139
What must be configured to apply tags automatically based on User-ID logs?

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

Correct Answer: C
Section:
Explanation:
Depending on the type of log you want to use for tagging, create a log forwarding profile or configure the log settings to define how you want the firewall or Panorama to handle logs. For Authentication, Data, Threat, Traffic, Tunnel Inspection, URL, and WildFire logs, create a log forwarding profile. For User-ID, GlobalProtect, and IP-Tag logs, configure the log settings.
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-auto-tagging-toautomate-security-actions

QUESTION 140
An administrator needs to gather information about the firewall CPU utiliza-tion on both the management plane and the data plane.
Where does the administrator view the desired data?

A. Application Command and Control Center
B. Monitor > Utilization
C. Support > Resources
D. System Resources Widget on the Dashboard

Correct Answer: D
Section:
Explanation:
The System Resources widget on the Dashboard in the WebUI shows both the management plane and data plane CPU utilization as well as other system resources such as memory, disk, and session1.
The other options do not show both the management plane and data plane CPU utilization. The Application Command and Control Center (ACC) shows the network activity and application usage based on traffic logs2. The Monitor >
Utilization page shows the interface utilization and packet buffer utilization3. The Support > Resources page shows the system resources for Panorama only4.
Reference: 1: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interfacehelp/dashboard/dashboard-widgets 2: https://docs.paloaltonetworks.com/pan-os/10-2/pan-osweb-interface-help/acc/acc-overview 3: https://docs.paloaltonetworks.com/pan-os/10-2/pan-osweb-interface-help/monitor/monitor-utilization 4:

https://docs.paloaltonetworks.com/panorama/10-2/panorama-web-interfacehelp/support/support-resources

QUESTION 141
An administrator has purchased WildFire subscriptions for 90 firewalls globally.
What should the administrator consider with regards to the WildFire infra-structure?

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

Correct Answer: B
Section:
Explanation:
According to the Palo Alto Networks website1, there are five WildFire public clouds that customers can choose from based on their location and data privacy requirements: WildFire Global Cloud (U.S.), WildFire Europe Cloud, WildFire Japan Cloud, WildFire Singapore Cloud, and WildFire United Kingdom Cloud. Additionally, there are three more regional public clouds that are available as of PAN-OS 10.0: WildFire Canada Cloud, WildFire Australia Cloud, and WildFire Germany
Cloud2. Therefore, the correct answer is B. Reference: 1:
https://www.paloaltonetworks.com/network-security/wildfire 2:
https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfiredeployments/wildfire-global-cloud

QUESTION 142
An administrator connected a new fiber cable and transceiver to interface Ethernetl/l on a Palo Alto Networks firewall. However, the link does not seem to be coming up.
If an administrator were to troubleshoot, how would they confirm the transceiver type, tx-power, rxpower, vendor name, and part number via the CLI?

A. show system state filter sw.dev.interface.config
B. show chassis status slot s1
C. show system state filter-pretty sys.s1.*
D. show system state filter ethernet1/1

Correct Answer: D
Section:
Explanation:
According to the Palo Alto Networks documentation1, the command show system state filter displays the current state of the system and allows you to filter the output by a specific keyword. The keyword ethernet1/1 matches the interface name that the administrator wants to troubleshoot. The output of this command will show information about the transceiver type, tx-power, rx-power, vendor name, and part number for that interface2. Therefore, the correct answer is D. Reference: 1:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-cli-quick-start/use-the-cli/find-a-command 2:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFmCAK

QUESTION 143
A remote administrator needs access to the firewall on an untrust interface. Which three options would you configure on an Interface Management profile to secure management access? (Choose three.)

A. Permitted IP Addresses
B. SSH
C. https
D. User-ID
E. HTTP

Correct Answer: A, B, C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/getting-started/best-practices-forsecuring-administrative-access

QUESTION 144
Which two factors should be considered when sizing a decryption firewall de-ployment? (Choose two.)

A. Number of blocked sessions
B. TLS protocol version
C. Encryption algorithm
D. Number of security zones in decryption policies

Correct Answer: B, C
Section:
Explanation:
According to the Palo Alto Networks documentation1, decryption consumes firewall CPU resources, so it is important to evaluate the amount of SSL decryption that the firewall deployment can support. Two factors that affect the CPU consumption are the TLS protocol version and the encryption algorithm used by the encrypted traffic. The newer versions of TLS (such as TLS 1.3) and the stronger encryption algorithms (such as AES-256-GCM) require more CPU resources to decrypt than the older versions and weaker algorithms. Therefore, the correct answer is B and C.
The other options are not relevant or important for sizing a decryption firewall deployment: Number of blocked sessions: This option refers to the number of sessions that the firewall blocks based on Security policy rules. It does not affect the decryption performance or resource consumption.
Number of security zones in decryption policies: This option refers to the number of security zones that are used to define the source and destination of the traffic to be decrypted. It does not affect the decryption performance or resource consumption.
Reference: 1: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/prepare-todeploy-decryption/size-the-decryption-firewall-deployment

QUESTION 145
Which operation will impact the performance of the management plane?

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

Correct Answer: B
Section:
Explanation:
According to the Palo Alto Networks documentation1, generating a SaaS Application report can impact the performance of the management plane because it requires querying and processing a large amount of log data. Therefore, the correct answer is B.
The other options are not related to the management plane performance:
Decrypting SSL sessions: This option affects the data plane performance, not the management plane performance. Decrypting SSL sessions consumes CPU resources on the data plane, which handles traffic processing and security enforcement2.
Enabling DoS protection: This option also affects the data plane performance, not the management plane performance. Enabling DoS protection allows the firewall to detect and prevent denial-ofservice (DoS) attacks by monitoring and limiting the rate of sessions and packets3.
Enabling packet buffer protection: This option also affects the data plane performance, not the management plane performance. Enabling packet buffer protection allows the firewall to monitor and control the packet buffer usage on each interface to prevent buffer exhaustion and packet drops4.
Reference: 1: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-theapplication-command-center-acc/acc-saas-applications 2:
https://docs.paloaltonetworks.com/panos/9-1/pan-os-admin/decryption/decryption-concepts/how-decryption-works 3:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-denial-ofservice-dos-attacks 4:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-osadmin/networking/configure-packet-buffer-protection

QUESTION 146
Which three items must be configured to implement application override? (Choose three)

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

Correct Answer: A, B, C
Section:
Explanation:
According to the Palo Alto Networks documentation1, application override is where the firewall is configured to override the normal application identification (App-ID) of specific traffic passing through the firewall. To implement application override, the following items must be configured: Custom app: This is a user-defined application that is used to identify the traffic that needs to be overridden. It is recommended to create a custom app for the application override policy, rather than using a predefined app that may have different default ports and threat inspection capabilities2.
Security policy rule: This is a rule that allows the traffic that matches the custom app through the firewall. The security policy rule must use the custom app as the application filter and specify the source and destination zones, addresses, and users as needed2.
Application override policy rule: This is a rule that defines the criteria for overriding the App-ID of the traffic. The application override policy rule must use the custom app as the application filter and specify the source and destination zones, addresses, ports, and protocols as needed2. The other options are not required or relevant for implementing application override:
Decryption policy rule: This is a rule that defines the criteria for decrypting encrypted traffic. It is not related to application override, although decryption may be needed to identify some applications that use encryption.
Application filter: This is an object that groups applications based on various criteria, such as category, subcategory, technology, or risk. It is not an item that must be configured for application override, although it can be used as a reference in security policy rules or custom apps.
Reference: 1: https://live.paloaltonetworks.com/t5/blogs/tips-amp-tricks-how-to-create-anapplication-override/ba-p/451872 2: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0 : https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryptionconcepts/how-decryption-works : https://docs.paloaltonetworks.com/pan-os/9-1/pan-osadmin/app-id/manage-custom-or-unknown-applications/create-an-application-filter

QUESTION 147
After implementing a new NGFW, a firewall engineer sees a VoIP traffic issue going through the firewall After troubleshooting the engineer finds that the firewall performs NAT on the voice packets payload and opens dynamic pinholes for media ports
What can the engineer do to solve the VoIP traffic issue?

A. Disable ALG under H.323 application
B. Increase the TCP timeout under H.323 application
C. Increase the TCP timeout under SIP application
D. Disable ALG under SIP application

Correct Answer: D
Section:
Explanation:
According to the Palo Alto Networks documentation1, application-level gateway (ALG) is a feature that allows the firewall to inspect and modify the payload of some protocols, such as SIP, to enable NAT traversal and firewall policy enforcement. However, ALG can also cause issues with some VoIP implementations, such as modifying the SIP headers incorrectly or opening unnecessary pinholes for media ports. Therefore, disabling ALG under SIP application can help solve the VoIP traffic issue by preventing the firewall from altering the voice packets payload and opening dynamic pinholes2.
Therefore, the correct answer is D.
The other options are not relevant or helpful for solving the VoIP traffic issue:
Disable ALG under H.323 application: This option would disable ALG for H.323 protocol, which is another VoIP protocol, but not the one used in this scenario. The scenario mentions SIP as the signaling protocol, so disabling ALG under
H.323 application would have no effect on the VoIP traffic issue.
Increase the TCP timeout under H.323 application: This option would increase the TCP timeout for H.323 protocol, which is another VoIP protocol, but not the one used in this scenario. The scenario mentions SIP as the

signaling protocol, which uses UDP by default, so increasing the TCP timeout under H.323 application would have no effect on the VoIP traffic issue.
Increase the TCP timeout under SIP application: This option would increase the TCP timeout for SIP protocol, which is the signaling protocol used in this scenario. However, SIP uses UDP by default, so increasing the TCP timeout would have no effect on the VoIP traffic issue. Moreover, increasing the TCP timeout would not address the problem of NAT on the voice packets payload and dynamic pinholes for media ports.
Reference: 1: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/disable-the-sipapplication-level-gateway-alg 2:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEsCAK

QUESTION 148
An administrator receives the following error message:
"IKE phase-2 negotiation failed when processing Proxy ID. Received local id 192.168 33 33/24 type IPv4 address protocol 0 port 0, received remote id 172.16 33.33/24 type IPv4 address protocol 0 port 0."
How should the administrator identify the root cause of this error message?

A. In the IKE Gateway configuration, verify that the IP address for each VPN peer is accurate
B. Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure
C. Check whether the VPN peer on one end is set up correctly using policy-based VPN
D. In the IPSec Crypto profile configuration, verify that PFS is either enabled on both VPN peers or disabled on both VPN peers.

Correct Answer: C
Section:
Explanation:
According to the Palo Alto Networks documentation1, the error message "IKE phase-2 negotiation failed when processing Proxy ID" indicates that there is a mismatch between the Proxy ID settings on the two VPN peers. Proxy ID is used to identify the traffic that needs to be encrypted and tunneled. It consists of the local and remote IP addresses, protocols, and ports. If the Proxy ID settings do not match on both VPN peers, the phase-2 negotiation will fail. Therefore, the administrator should check whether the VPN peer on one end is set up correctly using policy-based VPN, which allows specifying the Proxy ID settings manually2. Therefore, the correct answer is C.
The other options are not relevant or helpful for identifying the root cause of this error message:
In the IKE Gateway configuration, verify that the IP address for each VPN peer is accurate: This option would help to identify the root cause of a phase-1 negotiation failure, not a phase-2 negotiation failure. The IP address for each VPN peer is used to establish the IKE gateway, which is part of the phase-1 negotiation. If the IP address is inaccurate, the phase-1 negotiation will fail and the error message will be different.
Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure: This option would also help to identify the root cause of a phase-1 negotiation failure, not a phase-2 negotiation failure. The ability to ping and route between the IP addresses of the VPN peers is a prerequisite for establishing the IKE gateway, which is part of the phase-1 negotiation. If there are routing issues or connectivity problems, the phase-1 negotiation will fail and the error message will be different.
In the IPSec Crypto profile configuration, verify that PFS is either enabled on both VPN peers or disabled on both VPN peers: This option would help to identify the root cause of a different phase-2 negotiation failure, not the one related to Proxy ID mismatch. PFS stands for Perfect Forward Secrecy, which is an option to generate a new encryption key for each IPSec session. If PFS is enabled on one
VPN peer but disabled on another, the phase-2 negotiation will fail and the error message will be "IKEv2 IPSec SA negotiation failed. Invalid syntax."3.
Reference: 1:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClbXCAS 2:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/vpn/site-to-site-vpn/set-up-a-site-tosite-vpn-between-two-firewalls/policy-based-vpn 3:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClZSCA0

QUESTION 149
An administrator needs to identify which NAT policy is being used for internet traffic.
From the Monitor tab of the firewall GUI, how can the administrator identify which NAT policy is in use for a traffic flow?

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

Correct Answer: C
Section:

QUESTION 150
An administrator troubleshoots an issue that causes packet drops.
Which log type will help the engineer verify whether packet buffer protection was activated?

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

Correct Answer: B
Section:
Explanation:
The firewall records alert events in the System log and events for dropped traffic, discarded sessions, and blocked IP address in the Threat log when packet buffer protection is activated12.Packet buffer protection is a feature that helps prevent packet buffer exhaustion by identifying and dropping traffic from sources that consume excessive packet buffers3. Reference:3: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection1: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oNB7CAM&lang=en_US2: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNGFCA4

QUESTION 151
Which two policy components are required to block traffic in real time using a dynamic user group (DUG)? (Choose two.)

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

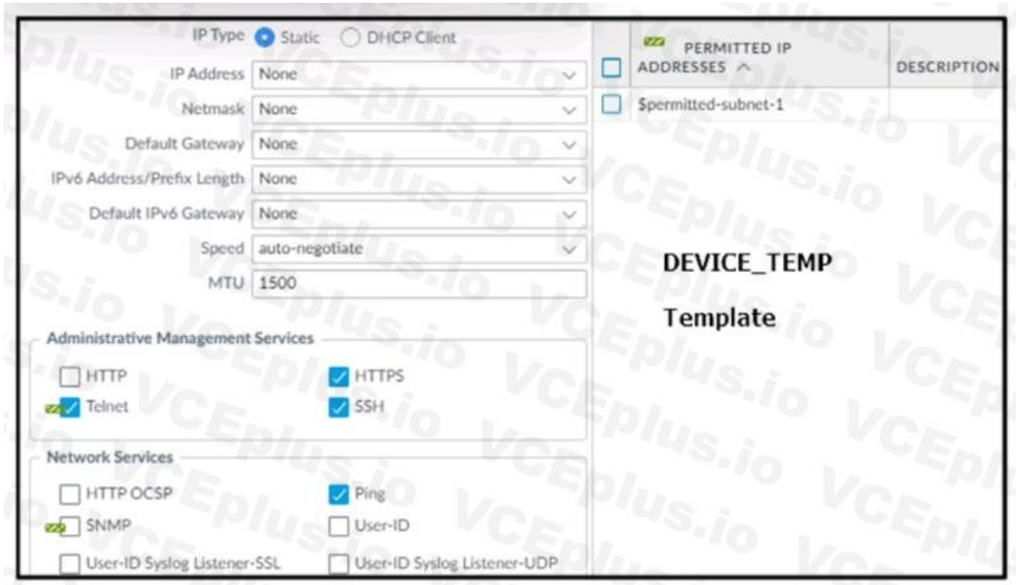
Correct Answer: A, B
Section:

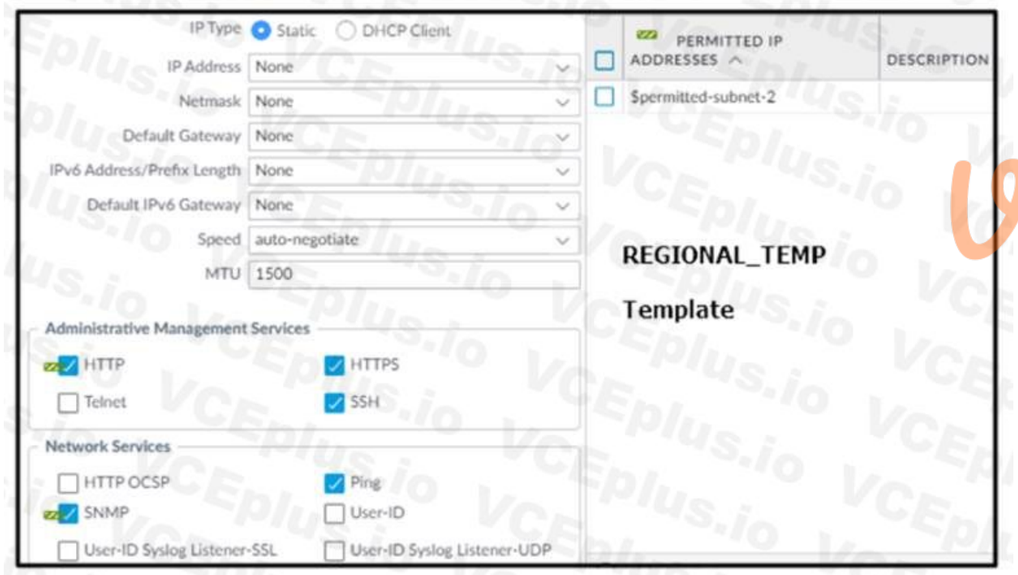
QUESTION 152
A network security administrator wants to inspect HTTPS traffic from users as it egresses through a firewall to the Internet/Untrust zone from trusted network zones.
The security admin wishes to ensure that if users are presented with invalid or untrusted security certificates, the user will see an untrusted certificate warning.
What is the best choice for an SSL Forward Untrust certificate?

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

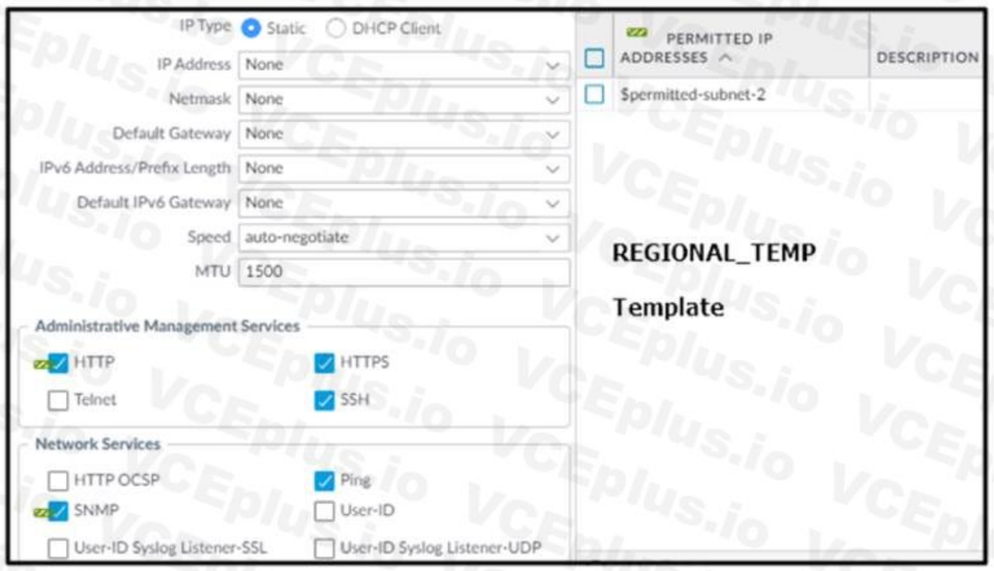
Correct Answer: B
Section:

QUESTION 153
Based on the screenshots above, and with no configuration inside the Template Stack itself, what access will the device permit on its Management port?





NAME	TYPE	STACK
TEMP_STACK	template-stack	DEVICE_TEMP REGIONAL_TEMP



NAME	TYPE	STACK
TEMP_STACK	template-stack	DEVICE_TEMP REGIONAL_TEMP

A. The firewall will allow HTTP, Telnet, HTTPS, SSH, and Ping from IP addresses defined as $permitted-subnet-2.
B. The firewall will allow HTTP, Telnet, HTTPS, SSH, and Ping from IP addresses defined as $permitted-subnet-l and Spermitted-subnet-2.
C. The firewall will allow HTTP, Telnet, HTTPS, SSH, and Ping from IP addresses defined as $permitted-subnet-l.
D. The firewall will allow HTTP, Telnet, SNMP, HTTPS, SSH, and Ping from IP addresses defined as $permitted-subnet-l and $permitted-subnet-2.

Correct Answer: C
Section:

QUESTION 154
An engineer is configuring a firewall with three interfaces:
* MGT connects to a switch with internet access.
* Ethernet1/1 connects to an edge router.
* Ethernet1/2 connects to a visualization network.
The engineer needs to configure dynamic updates to use a dataplane interface for internet traffic. What should be configured in Setup > Services > Service Route Configuration to allow this traffic?

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

Correct Answer: A
Section:

QUESTION 155
Which type of policy in Palo Alto Networks firewalls can use Device-ID as a match condition?

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

Correct Answer: B
Section:

QUESTION 156
A company wants to add threat prevention to the network without redesigning the network routing.
What are two best practice deployment modes for the firewall? (Choose two.)

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

Correct Answer: A, D
Section:
Explanation:
VirtualWire and Layer2 deployment modes allow the firewall to act as a bump in the wire without changing the existing network routing. In VirtualWire mode, the firewall bridges two interfaces and passes traffic between them without any IP-layer processing. In Layer2 mode, the firewall acts as a transparent switch and processes traffic at Layer2 of the OSI model. Reference:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/networking/configure-interfaces/virtual-wire-deployments.html

QUESTION 157
An administrator is using Panorama to manage multiple firewalls. After upgrading all devices to the latest PAN-OS software, the administrator enables log forwarding from the firewalls to Panorama. However, pre-existing logs from the firewalls are not appearing in Panorama.
Which action should be taken to enable the firewalls to send their pre-existing logs to Panorama?

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

Correct Answer: B
Section:
Explanation:
The import option allows the administrator to pull logs from the firewalls to Panorama. This option is useful when the firewalls have pre-existing logs that were not forwarded to Panorama before. The import option can be configured on Panorama by selecting Device > Log Collection > Import Logs. Reference:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama/import-logs-from-firewallsto-panorama.html

QUESTION 158
An engineer configures a specific service route in an environment with multiple virtual systems instead of using the inherited global service route configuration.
What type of service route can be used for this configuration?

A. IPv6 Source or Destination Address
B. Destination-Based Service Route
C. IPv4 Source Interface

D. Inherit Global Setting

Correct Answer: C
Section:
Explanation:
The IPv4 Source Interface service route allows the administrator to specify a source interface for a service based on the virtual system. This option overrides the inherited global service route configuration and provides more granular control over the service routes for each virtual system. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/virtual-systems/customize-service-routes-for-a-virtual-system.html

QUESTION 159
A firewall engineer creates a NAT rule to translate IP address 1.1.1.10 to 192.168.1.10. The engineer also plans to enable DNS rewrite so that the firewall rewrites the IPv4 address in a DNS response based on the original destination IP address and translated destination IP address configured for the rule. The engineer wants the firewall to rewrite a DNS response of 1.1.1.10 to 192.168.1.10.
What should the engineer do to complete the configuration?

A. Create a U-Turn NAT to translate the destination IP address 192.168.1.10 to 1.1.1.10 with the destination port equal to UDP/53.
B. Enable DNS rewrite under the destination address translation in the Translated Packet section of the NAT rule with the direction Forward.
C. Enable DNS rewrite under the destination address translation in the Translated Packet section of the NAT rule with the direction Reverse.
D. Create a U-Turn NAT to translate the destination IP address 1.1.1.10 to 192.168.1.10 with the destination port equal to UDP/53.

Correct Answer: B
Section:
Explanation:
If the DNS response matches the Original Destination Address in the rule, translate the DNS response using the same translation the rule uses. For example, if the rule translates IP address 1.1.1.10 to 192.168.1.10, the firewall rewrites a DNS response of 1.1.1.10 to 192.168.1.10. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/source-nat-and-destination-nat/destination-nat-dns-rewrite-use-cases#id0d85db1b-05b9-4956-a467-f71d558263bb

QUESTION 160
An organization wants to begin decrypting guest and BYOD traffic.
Which NGFW feature can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted?

A. Authentication Portal
B. SSL Decryption profile
C. SSL decryption policy
D. comfort pages

Correct Answer: A
Section:
Explanation:
An authentication portal is a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An authentication portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The authentication portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button.The authentication portal can also be configured to use different authentication methods, such as local database, RADIUS, LDAP, Kerberos, or SAML1.By using an authentication portal, the firewall can redirect BYOD users to a web page where they can learn about the decryption policy, download and install the CA certificate, and agree to the terms of use before accessing the network or the internet2.
An SSL decryption profile is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption profile is a set of options that define how the firewall handles SSL/TLS traffic that it decrypts.An SSL decryption profile can include settings such as certificate verification, unsupported protocol handling, session caching, session resumption, algorithm selection, etc3. An SSL decryption profile does not provide any user identification or notification functions.
An SSL decryption policy is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption policy is a set of rules that determine which traffic the firewall decrypts based on various criteria, such as source and destination zones, addresses, users, applications, services, etc.An SSL decryption policy can also

specify which type of decryption to apply to the traffic, such as SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy4. An SSL decryption policy does not provide any user identification or notification functions.
Comfort pages are not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. Comfort pages are web pages that the firewall displays to users when it blocks or fails to decrypt certain traffic due to security policy or technical reasons.Comfort pages can include information such as the reason for blocking or failing to decrypt the traffic, the URL of the original site, the firewall serial number, etc5. Comfort pages do not provide any user identification or notification functions before decrypting the traffic.

QUESTION 161
After switching to a different WAN connection, users have reported that various websites will not load, and timeouts are occurring. The web servers work fine from other locations.
The firewall engineer discovers that some return traffic from these web servers is not reaching the users behind the firewall. The engineer later concludes that the maximum transmission unit (MTU) on an upstream router interface is set to 1400 bytes.
The engineer reviews the following CLI output for ethernet1/1.

```
> show interface ethernet1/1

---------------------------------------------------------------------------
Name: ethernet1/1, ID: 16
Operation mode: layer3
Untagged sub-interface support: no
---------------------------------------------------------------------------
Name: ethernet1/1, ID: 16
Operation mode: layer3
Virtual router default
Interface MTU 1500
Interface IP address: 99.166.70.146/23
Interface management profile: ping
  ping: yes  telnet: no  ssh: no  http: no  https: no
  snmp: no  response-pages: no  userid-service: no
Service configured: SSL-VPN
Zone: L3-WAN, virtual system: vsys1
Adjust TCP MSS: no
Ignore IPv4 DF: no
Policing: no
---------------------------------------------------------------------------
```

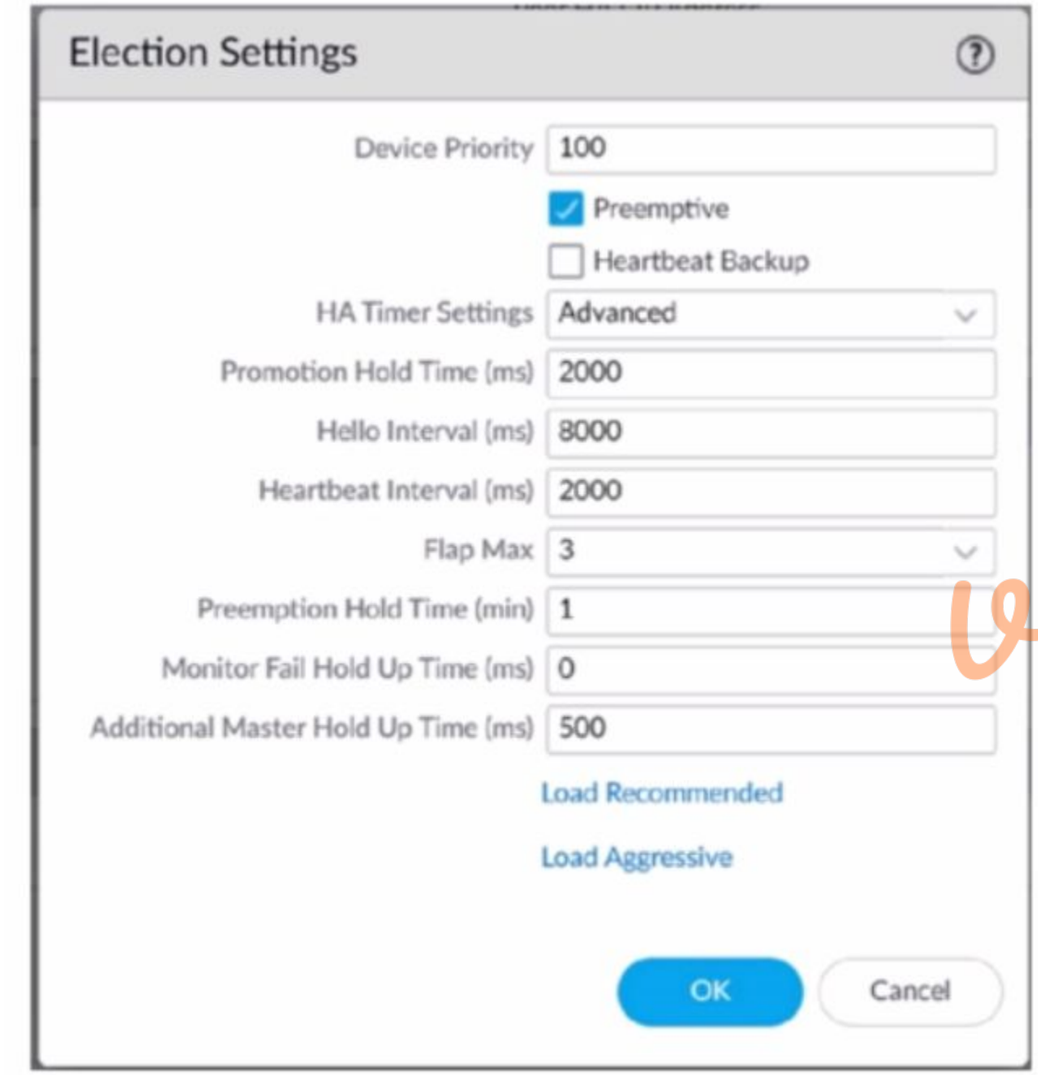
Which setting should be modified on ethernet1/1 to remedy this problem?

A. Lower the interface MTU value below 1500.
B. Enable the Ignore IPv4 Don't Fragment (DF) setting.
C. Change the subnet mask from /23 to /24.
D. Adjust the TCP maximum segment size (MSS) value. *

Correct Answer: D
Section:

Explanation:

QUESTION 162
An engineer is reviewing the following high availability (HA) settings to understand a recent HAfailover event.

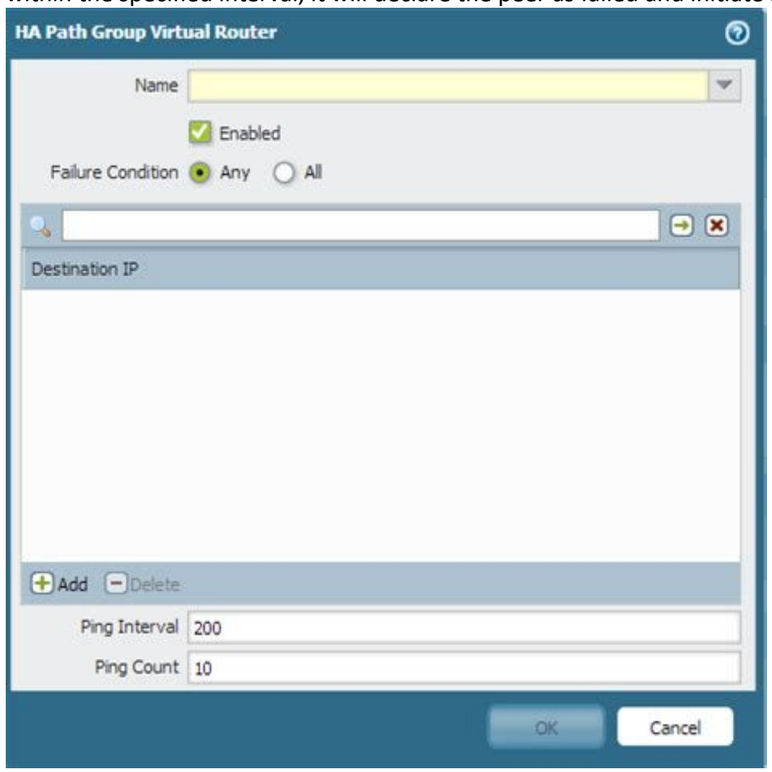


Which timer determines the frequency between packets sent to verify that the HA functionality on the other HA firewall is operational?

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

Correct Answer: D
Section:
Explanation:

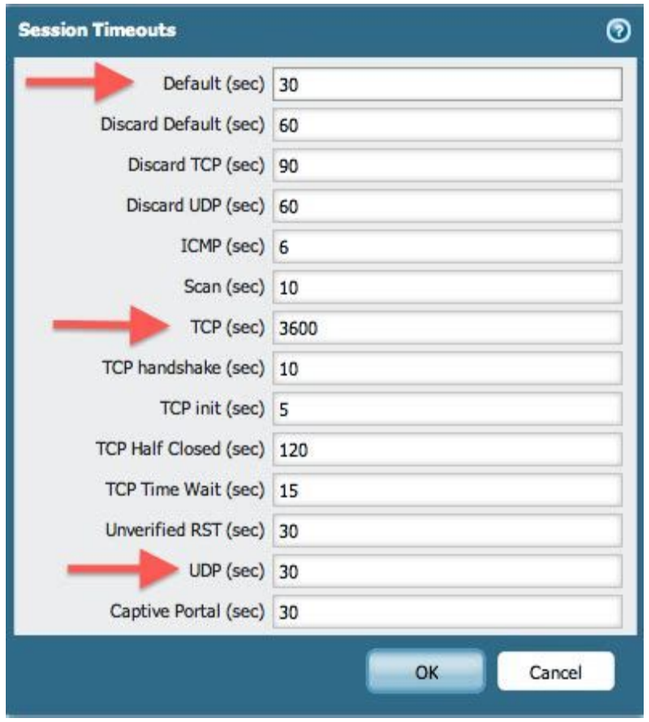
The timer that determines the frequency between packets sent to verify that the HA functionality on the other HA firewall is operational is the Hello Interval. The Hello Interval is the interval in milliseconds between hello packets that are sent to check the HA status of the peer firewall. The default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



QUESTION 163
What is the best description of the Cluster Synchronization Timeout (min)?

A. The maximum time that the local firewall waits before going to Active state when another cluster member is preventing the cluster from fully synchronizing
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 maximum interval between hello packets that are sent to verify that the HA functionality on the other firewall is operational

Correct Answer: A
Section:
Explanation:
The best description of the Cluster Synchronization Timeout (min) is the maximum time that the local firewall waits before going to Active state when another cluster member is preventing the cluster from fully synchronizing. This is a parameter that can be configured in an HA cluster, which is a group of firewalls that share session state and provide high availability and scalability. The Cluster Synchronization Timeout (min) determines how long the local firewall will wait for the cluster to reach a stable state before it decides to become Active and process traffic. A stable state means that all cluster members are either Active or Passive, and have synchronized their sessions with each other. If there is another cluster member that is in an unknown or unstable state, such as Initializing, Non-functional, or Suspended, then it may prevent the cluster from fully synchronizing and cause a delay in traffic processing. The Cluster Synchronization Timeout (min) can be set to a value between 0 and 30 minutes, with a default of 0. If it is set to 0, then the local firewall will not wait for any other cluster member and will immediately go to Active state.If it is set to a positive value, then the local firewall will wait for that amount of time before going to Active state, unless the cluster reaches a stable state earlier12.Reference:Configure HA Clustering, PCNSE Study Guide (page 53)



QUESTION 164

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

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

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

Correct Answer: D
Section:
Explanation:

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

QUESTION 165
An administrator configures a site-to-site IPsec VPN tunnel between a PA-850 and an external customer on their policy-based VPN devices.
What should an administrator configure to route interesting traffic through the VPN tunnel?

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

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

QUESTION 166
Given the following configuration, which route is used for destination 10 10 0 4?

```
network virtual-router 2 routing-table ip static-route "Route 1" nexthop ip-address 192.168.1.2
network virtual-router 2 routing-table ip static-route "Route 1" metric 30
network virtual-router 2 routing-table ip static-route "Route 1" destination 10.10.0.0/24
network virtual-router 2 routing-table ip static-route "Route 1" route-table unicast
network virtual-router 2 routing-table ip static-route "Route 2" nexthop ip-address 192.168.1.2
network virtual-router 2 routing-table ip static-route "Route 2" metric 20
network virtual-router 2 routing-table ip static-route "Route 2" destination 10.10.0.0/24
network virtual-router 2 routing-table ip static-route "Route 2" route-table unicast
network virtual-router 2 routing-table ip static-route "Route 3" nexthop ip-address 10.10.20.1
network virtual-router 2 routing-table ip static-route "Route 3" metric 5
network virtual-router 2 routing-table ip static-route "Route 3" destination 0.0.0.0/0
network virtual-router 2 routing-table ip static-route "Route 3" route-table unicast
network virtual-router 2 routing-table ip static-route "Route 4" nexthop ip-address 192.168.1.2
network virtual-router 2 routing-table ip static-route "Route 4" metric 10
network virtual-router 2 routing-table ip static-route "Route 4" destination 10.10.1.0/25
network virtual-router 2 routing-table ip static-route "Route 4" route-table unicast
```

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

Correct Answer: A
Section:

QUESTION 167
An engineer configures a new template stack for a firewall that needs to be deployed. The template stack should consist of four templates arranged according to the diagram

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

A. Values in Chicago
B. Values in efw01lab.chi
C. Values in Datacenter
D. Values in Global Settings

Correct Answer: B
Section:

QUESTION 168
What can the Log Forwarding built-in action with tagging be used to accomplish?

A. Block the source zones of selected unwanted traffic.
B. Block the destination IP addresses of selected unwanted traffic.
C. Forward selected logs to the Azure Security Center.
D. Block the destination zones of selected unwanted traffic.

Correct Answer: B
Section:
Explanation:
The Log Forwarding feature in Palo Alto Networks firewalls allows administrators to perform automated actions based on logs. One of the actions that can be configured is to tag an IP address, which can then be used in conjunction with Dynamic Address Groups (DAG) to enforce security policies. By tagging the destination IP addresses of unwanted traffic, an administrator can dynamically update policies to block traffic to those destinations. This method is particularly useful for responding quickly to detected threats by creating and enforcing a policy that blocks traffic to tagged destinations without the need for manual intervention or policy changes. For a detailed explanation, the Palo Alto Networks' 'PAN-OS Administrator's Guide' provides information on log forwarding and automated actions.

QUESTION 169
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 170
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 171
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 172
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 173
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 174
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 175
When creating a Policy-Based Forwarding (PBF) policy, which two components can be used? (Choose two.)

A. Schedule
B. Source Device
C. Custom Application
D. Source Interface

Correct Answer: A, D
Section:

QUESTION 176
An administrator configures HA on a customer's Palo Alto Networks firewalls with path monitoring by using the default configuration values.
What are the default values for ping interval and ping count before a failover is triggered?

A. Ping interval of 200 ms and ping count of three failed pings
B. Ping interval of 5000 ms and ping count of 10 failed pings
C. Ping interval of 200 ms and ping count of 10 failed pings
D. Ping interval of 5000 ms and ping count of three failed pings

Correct Answer: C
Section:
Explanation:
Ping Interval---Specify the interval between pings that are sent to the destination IP address (range is 200 to 60,000ms; default is 200ms). Ping Count---Specify the number of failed pings before declaring a failure (range is 3 to 10; default is 10).

QUESTION 177
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: D
Section:
Explanation:

QUESTION 178
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 179
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 180
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 181
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 182
A network administrator notices a false-positive state after enabling Security profiles. When the administrator checks the threat prevention logs, the related signature displays the following:
threat type: spyware category: dns-c2 threat ID: 1000011111
Which set of steps should the administrator take to configure an exception for this signature?

A. Navigate to Objects > Security Profiles > Anti-Spyware Select related profile Select DNS exceptions tabs Search related threat ID and click enable Commit
B. Navigate to Objects > Security Profiles > Vulnerability Protection Select related profile Select the signature exceptions tab and then click show all signatures Search related threat ID and click enable Change the default action Commit
C. Navigate to Objects > Security Profiles > Vulnerability Protection Select related profile Select the Exceptions lab and then click show all signatures Search related threat ID and click enable Commit
D. Navigate to Objects > Security Profiles > Anti-Spyware Select related profile Select the Exceptions lab and then click show all signatures Search related threat ID and click enable Commit

Correct Answer: A
Section:
Explanation:
When dealing with a false positive, particularly for a spyware threat detected through DNS queries (as indicated by the category 'dns-c2'), the correct course of action involves creating an exception in the Anti-Spyware profile, not the Vulnerability Protection profile. This is because the Anti-Spyware profile in Palo Alto Networks firewalls is designed to detect and block spyware threats, which can include command and control (C2) activities often signaled by DNS queries.
The steps to configure an exception for this specific spyware signature (threat ID: 1000011111) are as follows:
Navigate to Objects > Security Profiles > Anti-Spyware. This is where all the Anti-Spyware profiles are listed.
Select the related Anti-Spyware profile that is currently applied to the security policy which is generating the false positive.
Within the profile, go to the DNS Exceptions tab. This tab allows you to specify exceptions based on DNS signatures.
Search for the related threat ID (in this case, 1000011111) and click enable to create an exception for it. By doing this, you instruct the firewall to bypass the detection for this specific signature, effectively treating it as a false positive.
Commit the changes to make the exception active.
By following these steps, the administrator can effectively address the false positive without disabling the overall spyware protection capabilities of the firewall.

QUESTION 183
A firewall engineer is configuring quality of service (OoS) policy for the IP address of a specific server in an effort to limit the bandwidth consumed by frequent downloads of large files from the internet.
Which combination of pre-NAT and / or post-NAT information should be used in the QoS rule?

A. Post-NAT source IP address Pre-NAT source zone
B. Post-NAT source IP address Post-NAT source zone
C. Pre-NAT source IP address Post-NAT source zone
D. Pre-NAT source IP address Pre-NAT source zone

Correct Answer: D
Section:
Explanation:

When configuring Quality of Service (QoS) policies, particularly for traffic going to or from specific IP addresses and involving NAT, it's important to base the rule on how the firewall processes the traffic. For QoS, the firewall evaluates traffic using pre-NAT IP addresses and zones because QoS policies typically need to be applied before the NAT action occurs. This is especially true for inbound traffic, where the goal is to limit bandwidth before the destination IP is translated.
The correct combination for a QoS rule in this scenario, where the aim is to limit bandwidth for downloads from a specific server (implying inbound traffic to the server), would be:
D. Pre-NAT source IP address Pre-NAT source zone: Pre-NAT source IP address: This refers to the original IP address of the client or source device before any NAT rules are applied. Since QoS policies are evaluated before NAT, using the pre-NAT IP address ensures that the policy applies to the correct traffic. Pre-NAT source zone: This is the zone associated with the source interface before NAT takes place. Using the pre-NAT zone ensures that the QoS policy is applied to traffic as it enters the firewall, before any translations or routing decisions are made. By configuring the QoS rule with pre-NAT information, the firewall can accurately apply bandwidth limitations to the intended traffic, ensuring efficient use of network resources and mitigating the impact of large file downloads from the specified server. For detailed guidelines on configuring QoS policies, refer to the Palo Alto Networks documentation, which provides comprehensive instructions and best practices for managing bandwidth and traffic priorities on the network.

QUESTION 184
A firewall engineer creates a source NAT rule to allow the company's internal private network 10.0.0.0/23 to access the internet. However, for security reasons, one server in that subnet (10.0.0.10/32) should not be allowed to access the internet, and therefore should not be translated with the NAT rule.
Which set of steps should the engineer take to accomplish this objective?

A. 1. Create a source NAT rule (NAT-Rule-1) to translate 10.0.0/23 with source address translation set to dynamic IP and port. 2. Create another NAT rule (NAT-Rule-2) with source IP address in the original packet set to 10.0.0.10/32 and source translation set to none. 3. Place (NAT-Rule-1) above (NAT-Rule-2).
B. 1- Create a NAT rule (NAT-Rule-1) and set the source address in the original packet to 10.0.0.0/23. 2. Check the box for negate option to negate this IP subnet from NAT translation.
C. 1. Create a source NAT rule (NAT-Rule-1) to translate 10.0.0/23 with source address translation set to dynamic IP and port. 2. Create another NAT rule (NAT-Rule-2) with source IP address in the original packet set to 10.0.0.10/32 and source translation set to none. 3. Place (NAT-Rule-2) above (NAT-Rule-1).
D. 1. Create a NAT rule (NAT-Rule-1) and set the source address in the original packet to 10.0.0.10/32. 2. Check the box for negate option to negate this IP from the NAT translation.

Correct Answer: C
Section:
Explanation:
In Palo Alto Networks firewalls, the processing of NAT rules occurs in a top-down fashion, similar to security policies. To exclude a specific IP address from a broader source NAT rule, a more specific NAT rule must be placed above the broader rule.
C) Place a more specific NAT rule above the broader one:
Create a source NAT rule (NAT-Rule-1) to translate the broader network range (10.0.0.0/23) with dynamic IP and port translation. This rule allows the majority of the subnet to access the internet through NAT.
Create another NAT rule (NAT-Rule-2) with the source IP address in the original packet set specifically to the IP address that should not be translated (10.0.0.10/32). In this rule, set the source translation to none, indicating that this traffic should not be translated and thus not allowed to access the internet.
Place NAT-Rule-2 above NAT-Rule-1 in the NAT policy list. This ensures that the more specific rule (NAT-Rule-2) is evaluated first. If traffic matches NAT-Rule-2, it will not be translated or allowed to the internet, effectively excluding the specific server from internet access.
This configuration leverages the principle of specificity and the order of operation in NAT policies to exclude a specific IP address from source NAT translation, thereby preventing it from accessing the internet.

QUESTION 185
Which rule type controls end user SSL traffic to external websites?

A. SSL Outbound Proxyless Inspection
B. SSL Forward Proxy
C. SSH Proxy
D. SSL Inbound Inspection

Correct Answer: B
Section:
Explanation:
The SSL Forward Proxy rule type is designed to control and inspect SSL traffic from internal users to external websites. When an internal user attempts to access an HTTPS site, the Palo Alto Networks firewall, acting as an SSL Forward Proxy, intercepts the SSL request. It then establishes an SSL connection with the requested website on behalf of the user. Simultaneously, the firewall establishes a separate SSL connection with the user. This setup allows the firewall to decrypt and inspect the traffic for threats and compliance with security policies before re-encrypting and forwarding the traffic to its destination.

This process is transparent to the end user and ensures that potentially harmful content delivered over encrypted SSL connections can be identified and blocked. SSL Forward Proxy is a critical component of a comprehensive security strategy, allowing organizations to enforce security policies and protect against threats in encrypted traffic.

QUESTION 186
Forwarding of which two log types is configured in Device > Log Settings? (Choose two.)

A. Threat
B. HIP Match
C. Traffic
D. Configuration

Correct Answer: A, C
Section:

QUESTION 187
A security team has enabled real-time WildFire signature lookup on all its firewalls. Which additional action will further reduce the likelihood of newly discovered malware being allowed through the firewalls?

A. increase the frequency of the applications and threats dynamic updates.
B. Increase the frequency of the antivirus dynamic updates
C. Enable the 'Hold Mode' option in Objects > Security Profiles > Antivirus.
D. Enable the 'Report Grayware Files' option in Device > Setup > WildFire.

Correct Answer: B
Section:

QUESTION 188
A company is expanding its existing log storage and alerting solutions All company Palo Alto Networks firewalls currently forward logs to Panorama. Which two additional log forwarding methods will PAN-OS support? (Choose two)

A. SSL
B. TLS
C. HTTP
D. Email

Correct Answer: C, D
Section:

QUESTION 189
A firewall administrator manages sets of firewalls which have two unique idle timeout values. Datacenter firewalls needs to be set to 20 minutes and BranchOffice firewalls need to be set to 30 minutes. How can the administrator assign these settings through the use of template stacks?

A. Create one template stack and place the BranchOffice_Template in higher priority than Datacenter_Template.
B. Create one template stack and place the Datanceter_Template in higher priority than BranchOffice_template.
C. Create two separate template stacks one each for Datacenter and BranchOffice, and verify that Datacenter_Template and BranchOffice_template are at the bottom of their stack.
D. Create two separate template stacks one each for Datacenter and BranchOffice, and verify that Datacenter_template are at the top of their stack

Correct Answer: D

Section:

QUESTION 190
Exhibit.

Device Group: DATACENTER_DG

NAME	LOCATION	ADDRESS
Server-1	DATACENTER_DG	2.2.2.2
Server-1	Shared	1.1.1.1

Device Group: DC_FW_DG

NAME	LOCATION	ADDRESS
Server-1	DC_FW_DG	3.3.3.3
Server-1	Shared	1.1.1.1

Device Group: FW-1_DG

NAME	LOCATION	ADDRESS
Server-1	FW-1_DG	4.4.4.4
Server-1	Shared	1.1.1.1

Review the screenshots and consider the following information
1. FW-1is assigned to the FW-1_DG device group, and FW-2 is assigned to OFFICE_FW_DC
2. There are no objects configured in REGIONAL_DG and OFFICE_FW_DG device groups
Which IP address will be pushed to the firewalls inside Address Object Server-1?

A. Server-1 on FW-1 will have IP 4.4.4.4. Server-1 on FW-2 will have IP 1.1.1.1
B. Server-1 on FW-1 will have IR 111.1. Server-1 will not be pushed to FW-2.
C. Server-1 on FW-1 will have IP 2.2.2.2. Server-1 will not be pushed to FW-2.
D. Server-1 on FW-1 will have IP 3.3.3.3. Server-1 will not be pushed to FW-2.

Correct Answer: A
Section:
Explanation:
Device Group Hierarchy
Shared
DATACENTER_DG
DC_FW_DG
REGIONAL_DG
OFFICE_FW_DG
FW-1_DG
Analysis
Considerations:
FW-1 is assigned to the FW-1_DG device group.
FW-2 is assigned to the OFFICE_FW_DG device group.
There are no objects configured in REGIONAL_DG and OFFICE_FW_DG device groups.

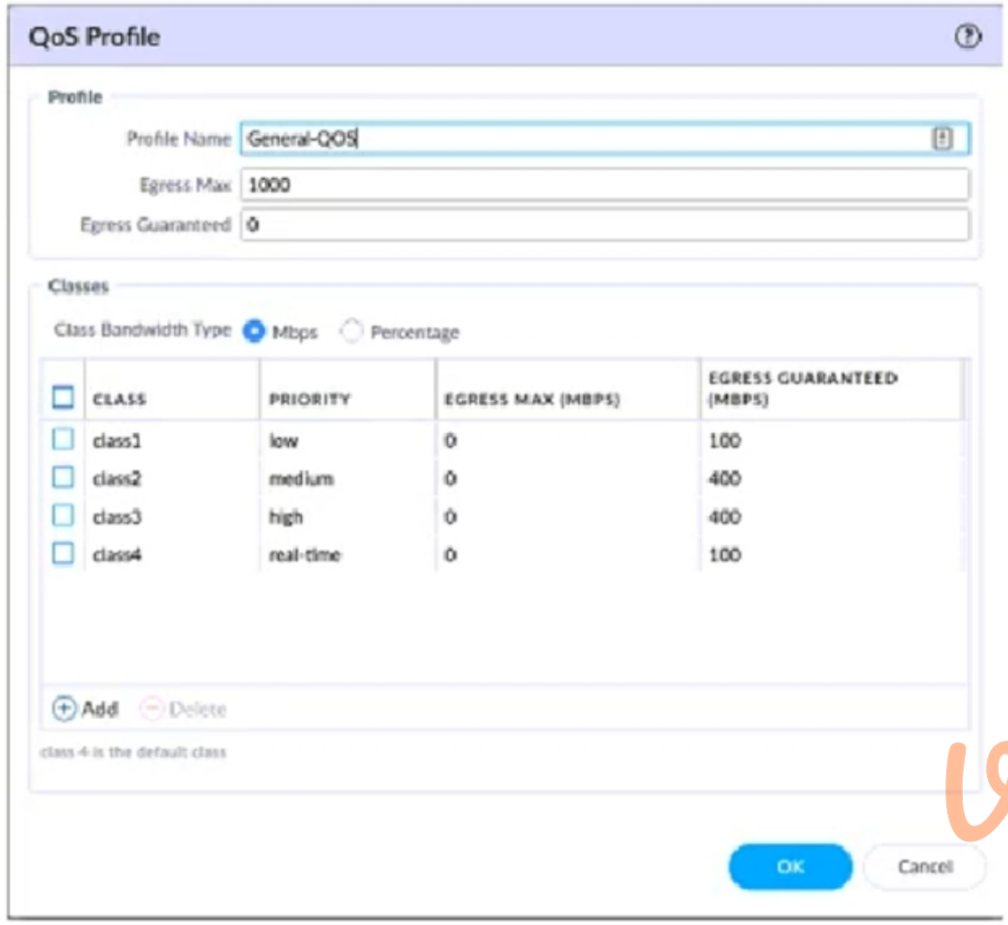
The address object Server-1 appears in multiple device groups with different IP addresses. The device groups have a hierarchy, which means objects can be inherited from parent groups unless overridden in the child group.
FW-1_DG:
Server-1 has IP 4.4.4.4, which will be pushed to FW-1 because it is in the FW-1_DG device group.
OFFICE_FW_DG (for FW-2):
Since there are no objects in OFFICE_FW_DG and REGIONAL_DG, FW-2 will inherit from Shared.
In the Shared group, Server-1 has IP 1.1.1.1.

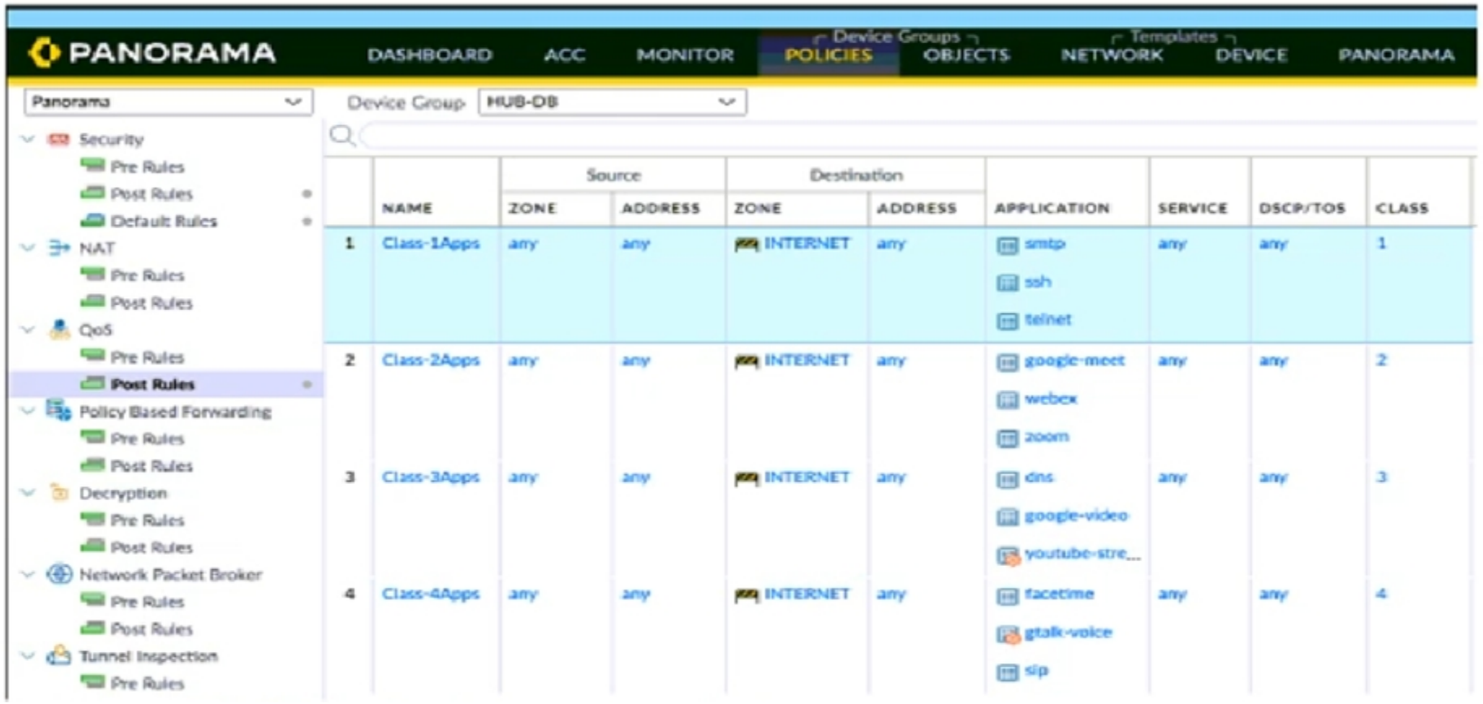
QUESTION 191
An administrator is configuring a Panorama device group. Which two objects are configurable? (Choose two.)

A. DNS Proxy
B. SSL/TLS profiles
C. address groups
D. URL Filtering profiles

Correct Answer: C, D
Section:

QUESTION 192
Refer to the exhibit.
View the screenshots


QoS Profile
Profile
Profile Name
General-QOS
Egress Max
1000
Egress Guaranteed
0
Classes
Class Bandwidth Type
Mbps
Percentage
CLASS
PRIORITY
EGRESS MAX (MBPS)
EGRESS GUARANTEED (MBPS)
class1
low
0
100
class2
medium
0
400
class3
high
0
400
class4
real-time
0
100
Add
Delete
class 4 is the default class
OK
Cancel



A QoS profile and policy rules are configured as shown. Based on this information which two statements are correct?

A. SMTP has a higher priority but lower bandwidth than Zoom.
B. DNS has a higher priority and more bandwidth than SSH.
C. google-video has a higher priority and more bandwidth than WebEx.
D. Facetime has a higher priority but lower bandwidth than Zoom.

Correct Answer: B, D
Section:

QUESTION 193
An administrator wants to use LDAP, TACACS+, and Kerberos as external authentication services for authenticating users. What should the administrator be aware of regarding the authentication sequence, based on the Authentication profile in the order Kerberos LDAP, and TACACS+?

A. The firewall evaluates the profiles in the alphabetical order the Authentication profiles have been named until one profile successfully authenticates the user.
B. The firewall evaluates the profiles in top-to-bottom order until one Authentication profile successfully authenticates the user.
C. The priority assigned to the Authentication profile defines the order of the sequence.
D. If the authentication times cut for the firs: Authentication profile in the authentication sequence, no further authentication attempts will be made.

Correct Answer: B
Section:

QUESTION 194
A company wants to use GlobalProtect as its remote access VPN solution.
Which GlobalProtect features require a Gateway license?

A. Multiple external gateways
B. Single or multiple internal gateways
C. Split DNS and HIP checks
D. IPv6 for internal gateways

Correct Answer: C
Section:

QUESTION 195
An administrator is troubleshooting application traffic that has a valid business use case, and observes the following decryption log message: 'Received fatal alert UnknownCA from client.'
How should the administrator remediate this issue?

A. Contact the site administrator with the expired certificate to request updates or renewal.
B. Enable certificate revocation checking to deny access to sites with revoked certificates.
C. Add the server's hostname to the SSL Decryption Exclusion List to allow traffic without decryption.
D. Check for expired certificates and take appropriate actions to block or allow access based on business needs.

Correct Answer: C
Section:

QUESTION 196
After configuring an IPSec tunnel, how should a firewall administrator initiate the IKE phase 1 to see if it will come up?

A. debug ike stat
B. test vpn ipsec-sa tunnel <tunnel_name>
C. show vpn ipsec-sa tunnel <tunnel_name>
D. test vpn ike-sa gateway <gateway_name>

Correct Answer: D
Section:

QUESTION 197
While troubleshooting an issue, a firewall administrator performs a packet capture with a specific filter. The administrator sees drops for packets with a source IP address of 10.1.1.1.
How can the administrator further investigate these packet drops by looking at the global counters for this packet capture filter?

A. > show counter global filter packet-filter yes delta yes
B. > show counter global filter severity drop
C. > debug dataplane packet-diag set capture stage drop
D. > show counter global filter delta yes I match 10.1.1.1

Correct Answer: A
Section:

QUESTION 198
What does the User-ID agent use to find login and logout events in syslog messages?

A. Syslog Server profile

B. Authentication log
C. Syslog Parse profile
D. Log Forwarding profile

Correct Answer: C
Section:

QUESTION 199
An engineer configures a destination NAT policy to allow inbound access to an internal server in the DMZ. The NAT policy is configured with the following values:
- Source zone: Outside and source IP address 1.2.2.2
- Destination zone: Outside and destination IP address 2.2.2.1
The destination NAT policy translates IP address 2.2.2.1 to the real IP address 10.10.10.1 in the DMZ zone.
Which destination IP address and zone should the engineer use to configure the security policy?

A. Destination Zone Outside. Destination IP address 2.2.2.1
B. Destination Zone DMZ, Destination IP address 10.10.10.1
C. Destination Zone DMZ, Destination IP address 2.2.2.1
D. Destination Zone Outside. Destination IP address 10.10.10.1

Correct Answer: C
Section:

QUESTION 200
When configuring explicit proxy on a firewall, which interface should be selected under the Listening interface option?

A. ingress for the outgoing traffic to the internet
B. Loopback for the proxy
C. Firewall management
D. ingress for the client traffic

Correct Answer: D
Section:

QUESTION 201
Which three sessions are created by a NGFW for web proxy? (Choose three.)

A. A session for DNS proxy to DNS servers
B. A session for proxy to web server
C. A session for client to proxy
D. A session for proxy to authentication server
E. A session for web server to client

Correct Answer: A, B, C
Section:

QUESTION 202
A firewall engineer at a company is researching the Device Telemetry feature of PAN-OS. Which two aspects of the feature require further action for the company to remain compliant with local laws regarding privacy and

data storage? (Choose two.)

A. Telemetry feature is automatically enabled during PAN-OS installation.
B. Telemetry data is uploaded into Strata Logging Service.
C. Telemetry feature is using Traffic logs and packet captures to collect data.
D. Telemetry data is shared in real time with Palo Alto Networks.

Correct Answer: A, C
Section:
Explanation:
To address the question about the Device Telemetry feature in PAN-OS and its compliance with privacy and data storage laws, let's examine the details thoroughly.
Understanding Device Telemetry in PAN-OS
Device Telemetry is a feature in Palo Alto Networks' PAN-OS that collects data from the firewall to provide insights for:
Product usage trends.
Threat analysis.
Operational optimizations.
Telemetry may include:
Configuration data.
Threat logs.
Performance metrics.
However, specific aspects of this feature require attention to ensure compliance with local privacy laws.
Explanation of Options
A . Telemetry feature is automatically enabled during PAN-OS installation
Why It Requires Action:
Telemetry may be enabled by default when upgrading or installing PAN-OS. Local privacy laws (e.g., GDPR in Europe, CCPA in California) often require explicit user consent before enabling data collection.
Relevant Action:
Administrators must review and disable telemetry if required or configure it to align with local compliance laws.
PAN-OS 11.0 Admin Guide: Telemetry configuration is detailed under the 'Device Telemetry' section.
PCNSA Study Guide (Domain 1: Device Management): Covers the importance of managing device settings, including Telemetry.
B . Telemetry data is uploaded into Strata Logging Service
Why It Does Not Require Immediate Action:
Data sent to the Strata Logging Service is anonymized and typically adheres to Palo Alto Networks' privacy guidelines. Administrators can disable Strata Logging uploads if necessary.
Optional Action:
Ensure the data is anonymized or disable the service if the organization does not agree with external data storage.
PAN-OS 11.0 Admin Guide: Details on Strata Logging and its integration with telemetry.
C . Telemetry feature is using Traffic logs and packet captures to collect data
Why It Requires Action:
If the telemetry feature collects detailed Traffic Logs or Packet Captures, it could include sensitive user data (e.g., IP addresses, URLs). Many privacy laws prohibit sharing this type of identifiable information unless anonymized.
Relevant Action:
Administrators should ensure traffic logs are anonymized or exclude sensitive data fields to meet privacy requirements.
PAN-OS 11.0 Admin Guide: Outlines telemetry data collection and traffic log inclusion.
PNSE Study Guide (Domain 3: Logging and Reporting): Emphasizes securing and managing logs in compliance with privacy standards.
D . Telemetry data is shared in real time with Palo Alto Networks
Why It Does Not Require Immediate Action:
While data is shared in real time, this process is often anonymized and only includes operational and diagnostic data. Administrators can configure or disable real-time sharing if deemed non-compliant.
PAN-OS 11.0 Admin Guide: Covers real-time telemetry sharing configuration.
Key Objectives in PCNSA and PCNSE Study Guides
PCNSA Study Guide:

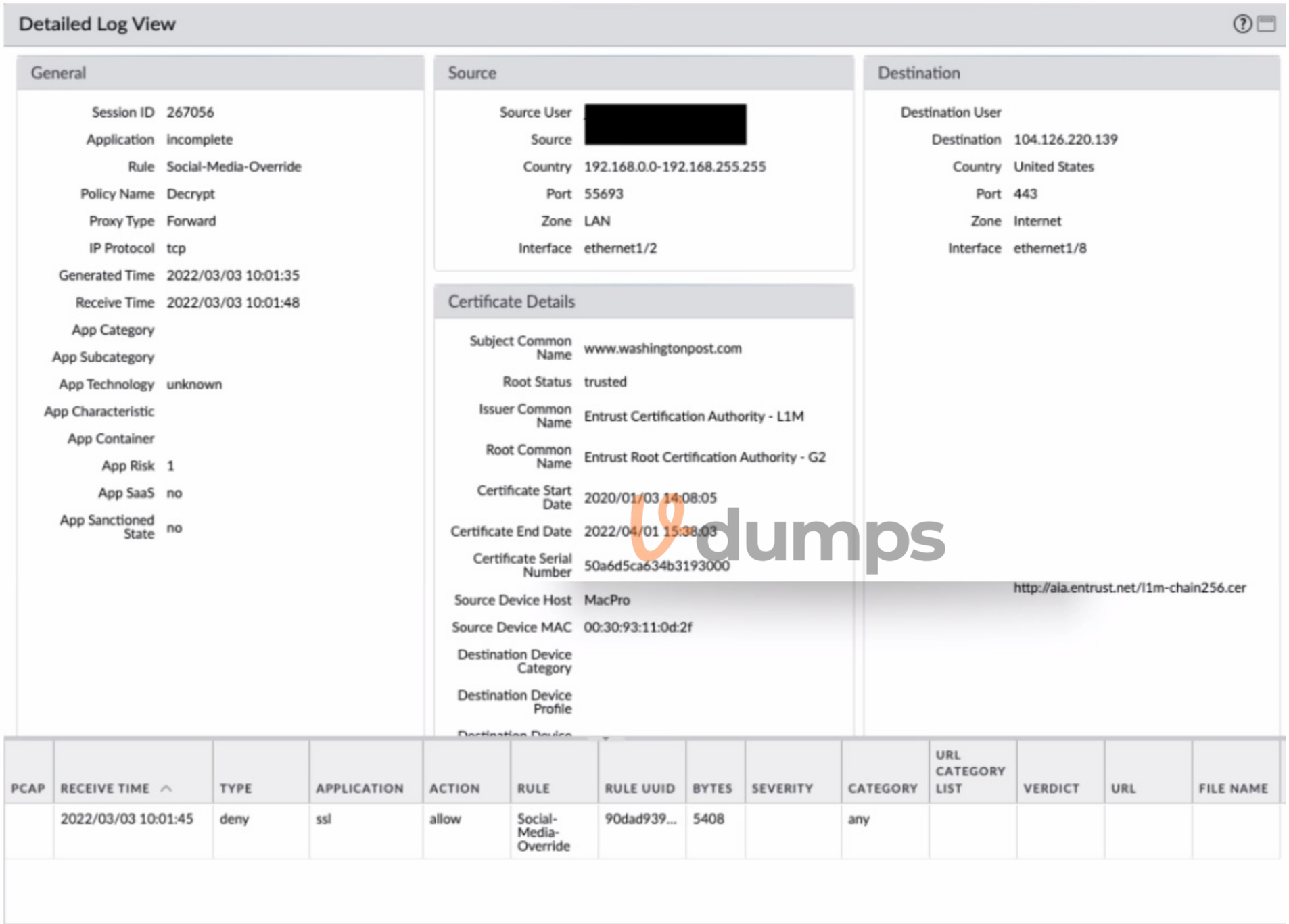
Domain 1: Device Management:
Emphasizes understanding and configuring administrative functions such as telemetry and privacy settings.
Domain 4: Securing Traffic:
Stresses compliance with local laws when collecting and forwarding logs.
PCNSE Study Guide:
Domain 2: Logging and Reporting:
Highlights secure log collection and forwarding to external services.
Domain 5: Security Operations:
Focuses on privacy and regulatory compliance in operational activities.
Actions to Ensure Compliance
Review Privacy Regulations:
Check local laws like GDPR (Europe) or CCPA (California) to identify restrictions on data collection and sharing.
Disable Default Telemetry:
During installation or upgrade, explicitly review telemetry settings in Device > Setup > Telemetry.
Customize Data Collection:
Use the PAN-OS telemetry interface to include/exclude sensitive data like packet captures or detailed traffic logs.
Educate Administrators:
Ensure staff managing firewalls are familiar with compliance requirements through PCNSA and PCNSE training.
PAN-OS 11.0 Documentation Reference
Device Telemetry Overview:
PAN-OS 11.0 Admin Guide - Device Telemetry
Telemetry Configuration Settings: PAN-OS 11.0 Admin Guide - Telemetry Configuration

QUESTION 203
In which two scenarios would it be necessary to use Proxy IDs when configuring site-to-site VPN Tunnels? (Choose two.)

A. Firewalls which support policy-based VPNs.
B. The remote device is a non-Palo Alto Networks firewall.
C. Firewalls which support route-based VPNs.
D. The remote device is a Palo Alto Networks firewall.

Correct Answer: A, B
Section:

QUESTION 204
Review the screenshots.



Detailed Log View

General

Session ID	267056
Application	incomplete
Rule	Social-Media-Override
Policy Name	Decrypt
Proxy Type	Forward
IP Protocol	tcp
Generated Time	2022/03/03 10:01:35
Receive Time	2022/03/03 10:01:48
App Category	
App Subcategory	
App Technology	unknown
App Characteristic	
App Container	
App Risk	1
App SaaS	no
App Sanctioned State	no

Source

Source User	[redacted]
Source	192.168.0.0-192.168.255.255
Country	
Port	55693
Zone	LAN
Interface	ethernet1/2
Source Device Host	MacPro
Source Device MAC	00:30:93:11:0d:2f
Destination Device Category	
Destination Device Profile	

Destination

Destination User	
Destination	104.126.220.139
Country	United States
Port	443
Zone	Internet
Interface	ethernet1/8

Certificate Details

Subject Common Name	www.washingtonpost.com
Root Status	trusted
Issuer Common Name	Entrust Certification Authority - L1M
Root Common Name	Entrust Root Certification Authority - G2
Certificate Start Date	2020/01/03 14:08:05
Certificate End Date	2022/04/01 15:38:03
Certificate Serial Number	50a6d5ca634b3193000
	http://aia.entrust.net/l1m-chain256.cer

PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT	URL	FILE NAME
	2022/03/03 10:01:45	deny	ssl	allow	Social-Media-Override	90dad939...	5408		any				

What is the most likely reason for this decryption error log?

A. The Certificate fingerprint could not be found.
B. The client expected a certificate from a different CA than the one provided.
C. The client received a CA certificate that has expired or is not valid.

D. Entrust is not a trusted root certificate authority (CA).

Correct Answer: D
Section:

QUESTION 205
A network engineer troubleshoots a VPN Phase 2 mismatch and decides that PFS (Perfect Forward Secrecy) needs to be enabled. What action should the engineer take?

A. Enable PFS under the IKE gateway advanced options.
B. Enable PFS under the IPSec Tunnel advanced options.
C. Add an authentication algorithm in the IPSec Crypto profile.
D. Select the appropriate DH Group under the IPSec Crypto profile.

Correct Answer: B
Section:

QUESTION 206
A security engineer is informed that the vulnerability protection profile of their on-premises Palo Alto Networks firewall is triggering on a common Threat ID, and which has been determined to be a false positive. The engineer is asked to resolve the issue as soon as possible because it is causing an outage for a critical service The engineer opens the vulnerability protection profile to add the exception, but the Threat ID is missing.
Which action is the most operationally efficient for the security engineer to find and implement the exception?

A. Review high severity system logs to identify why the threat is missing in Vulnerability Profile Exceptions.
B. Open a support case.
C. Review traffic logs to add the exception from there.
D. Select 'Show all signatures' within the Vulnerability Protection Profile under 'Exceptions'.

Correct Answer: D
Section:

QUESTION 207
A company has a PA-3220 NGFW at the edge of its network and wants to use active directory groups in its Security policy rules. There are 1500 groups in its active directory. An engineer has been provided 800 active directory groups to be used in the Security policy rules.
What is the engineer's next step?

A. Create a Group Mapping with 800 groups in the Group Include List.
B. Create two Group Include Lists, each with 400 Active Directory groups.
C. Create a Group Include List with the 800 Active Directory groups.
D. Create two Group Mappings, each with 400 groups in the Group Include List.

Correct Answer: B
Section:

QUESTION 208
An engineer is configuring secure web access (HTTPS) to a Palo Alto Networks firewall for management.
Which profile should be configured to ensure that management access via web browsers is encrypted with a trusted certificate?

A. An SSL/TLS Service profile with a certificate assigned.

B. An Interface Management profile with HTTP and HTTPS enabled.
C. A Certificate profile with a trusted root CA.
D. An Authentication profile with the allow list of users.

Correct Answer: A
Section:

QUESTION 209
An organization has recently migrated its infrastructure and configuration to NGFWs, for which Panorama manages the devices. The organization is coming from a L2-L4 firewall vendor, but wants to use App-ID while identifying policies that are no longer needed.
Which Panorama tool can provide a solution?

A. Application Groups
B. Policy Optimizer
C. Test Policy Match
D. Config Audit

Correct Answer: B
Section:

QUESTION 210
A new firewall has the Threat Prevention subscription, but the Antivirus does not appear in Dynamic Updates.
What must occur to have Antivirus signatures update?

A. An Antivirus license is needed first, then a Security profile for Antivirus needs to be created.
B. An Antivirus license must be obtained before Dynamic Updates can be downloaded or installed.
C. An Advanced Threat Prevention license is required to see the Dynamic Updates for Antivirus.
D. Install the Application and Threats updates first, then refresh the Dynamic Updates.

Correct Answer: D
Section:

QUESTION 211
An existing log forwarding profile is currently configured to forward all threat logs to Panorama. The firewall engineer wants to add syslog as an additional log forwarding method. The requirement is to forward only medium or higher severity threat logs to syslog. Forwarding to Panorama must not be changed.
Which set of actions should the engineer take to achieve this goal?

A. 1- Open the current log forwarding profile. 2. Open the existing match list for threat log type. 3. Define the filter. 4. Select the syslog forward method.
B. 1. Create a new log forwarding profile. 2. Add a new match list for threat log type. 3. Define the filter. 4. Select the Panorama and syslog forward methods.
C. 1. Open the current log forwarding profile. 2. Add a new match list for threat log type. 3. Define the filter. 4. Select the syslog forward method.
D. 1. Create a new log forwarding profile. 2. Add a new match list for threat log type. 3. Define the filter. 4. Select the syslog forward method.

Correct Answer: C
Section:

QUESTION 212
An administrator plans to install the Windows-Based User-ID Agent to prevent credential phishing.

Which installer package file should the administrator download from the support site?

A. UaCredInstall64-11.0.0.msi
B. GlobalProtect64-6.2.1.msi
C. TaInstall-11.0.0.msi
D. UaInstall-11.0.0msi

Correct Answer: A
Section:

QUESTION 213
An administrator is tasked to provide secure access to applications running on a server in the company's on-premises datacenter.
What must the administrator consider as they prepare to configure the decryption policy?

A. Ensure HA3 interfaces are configured in a HA pair environment to sync decrypted sessions.
B. Obtain or generate the server certificate and private key from the datacenter server.
C. Obtain or generate the self-signed certificate with private key in the firewall
D. Obtain or generate the forward trust and forward untrust certificate from the datacenter server.

Correct Answer: B
Section:

QUESTION 214
An administrator needs to validate that policies that will be deployed will match the appropriate rules in the device-group hierarchy. Which tool can the administrator use to review the policy creation logic and verify that unwanted traffic is not allowed?

A. Preview Changes
B. Managed Devices Health
C. Test Policy Match
D. Policy Optimizer

Correct Answer: C
Section:
Explanation:
The Test Policy Match tool in Palo Alto Networks' management systems (such as Panorama or the firewall interface) allows administrators to simulate traffic against configured security policies. This tool is critical for ensuring that the correct policies are applied to specific traffic patterns and that no unintended access is granted.
Key Points:
Test Policy Match enables you to input parameters like source IP, destination IP, application, user, and more, and the system will determine which policy would apply.
It is especially useful for verifying the device-group hierarchy in multi-tenant or Panorama-managed environments, ensuring that inherited or overridden rules are correctly applied.
The tool also helps to proactively check that traffic will be blocked or allowed as intended, reducing misconfigurations and preventing unwanted traffic.
Why not the other options?
A . Preview Changes: This feature is used to review configuration changes before committing them but does not simulate or validate policy matches.
B . Managed Devices Health: This option is related to checking the health and connectivity status of managed devices, not policies.
D . Policy Optimizer: This tool is used to refine existing security policies by identifying overly permissive rules or unused objects, not for testing specific traffic matches.
The Test Policy Match tool is the most appropriate choice for the scenario described.

QUESTION 215
A customer would like to support Apple Bonjour in their environment for ease of configuration.

Which type of interface in needed on their PA-3200 Series firewall to enable Bonjour Reflector in a segmented network?

A. Virtual Wire interface
B. Loopback interface
C. Layer 3 interface
D. Layer 2 interface

Correct Answer: D
Section:

QUESTION 216
An internal audit team has requested additional information to be included inside traffic logs forwarded from Palo Alto Networks firewalls to an internal syslog server.
Where can the firewall engineer define the data to be added into each forwarded log?

A. Custom Log Format within Device > Server Profiles > Syslog
B. Built-in Actions within Objects > Log Forwarding Profile
C. Logging and Reporting Settings within Device > Setup > Management
D. Data Patterns within Objects > Custom Objects

Correct Answer: A
Section:
Explanation:
To facilitate the integration with external log parsing systems, the firewall allows you to customize the log format; it also allows you to add custom Key: Value attribute pairs. Custom message formats can be configured under DeviceServer ProfilesSyslogSyslog Server ProfileCustom Log Format. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/custom-logevent-format
Step-by-Step Explanation:
Understanding Log Forwarding in PAN-OS:
Palo Alto Networks firewalls allow forwarding logs to external systems like syslog servers, SNMP servers, or email systems for external analysis or compliance.
Traffic logs can be customized to include additional information that meets the audit or operational requirements.
Syslog Server Profiles:
Syslog Server Profiles specify the format and destination of the log data sent to the syslog server.
These profiles allow customization through the Custom Log Format option, where the firewall engineer can add or modify log fields (e.g., source address, destination address, URL category).
Custom Log Format:
Navigate to Device > Server Profiles > Syslog.
Within the Syslog Server Profile, define a Custom Log Format for traffic logs.
Using this feature, the engineer can include additional fields requested by the internal audit team, such as threat severity, application details, or user ID.
Field Specification:
In the Custom Log Format, fields are defined using variables corresponding to the log fields in PAN-OS.
Example:
$receive_time,$src,$dst,$app,$action,$rule
The engineer can include specific details as requested by the audit team.
Comparison of Other Options:
Option B: Built-in Actions within Objects > Log Forwarding Profile
Log Forwarding Profiles are used to specify what logs are forwarded based on security policy matches. However, they do not control the format of logs.
Log Forwarding Profiles define actions (e.g., forwarding to syslog, SNMP), but customization of log data happens within Syslog Server Profiles.
Option C: Logging and Reporting Settings within Device > Setup > Management
These settings control general logging behavior and settings but do not allow customization of log data for syslog forwarding.
Option D: Data Patterns within Objects > Custom Objects
Data Patterns are used for identifying sensitive data or patterns in data filtering. They are unrelated to log customization.
Why A is Correct?

The Custom Log Format under Device > Server Profiles > Syslog is the only place where additional information can be defined and added to forwarded traffic logs.
This flexibility allows the firewall engineer to meet specific compliance or audit requirements.
Documentation
Reference:
PCNSA Study Guide: Logging and Monitoring section discusses Syslog Server Profiles and log forwarding configurations.
PAN-OS Admin Guide: Covers Custom Log Format configuration under the Syslog Server Profile.
When troubleshooting Palo Alto Networks services, such as dynamic updates, verifying the status of service routes is critical. Service routes determine how the firewall communicates with external services (e.g., Palo Alto Networks update servers, WildFire, DNS, etc.) from the Management Plane or data plane interfaces.
Why 'debug dataplane internal vif route 250' is Correct
Purpose of the Command:
This command allows administrators to view the service routes configured on the firewall and verify if they are installed correctly and actively working.
The number 250 specifically refers to service routes in the Management Plane.
Output:
The command displays detailed information about service routes, including routing decisions, source interfaces, and next-hop IPs.
Helps identify issues such as:
Incorrect interface configuration.
Invalid next-hop IPs.
Missing routes for specific services.
Analysis of Other Options
debug dataplane internal vif route 255
Incorrect:
The number 255 does not correspond to service routes but is used for internal route debugging unrelated to management plane service routes.
show routing route type management
Incorrect:
This command does not exist in PAN-OS CLI. It might be a misrepresentation of another command.
debug dataplane internal vif route 250
Correct:
As explained above, this is the correct command for verifying service routes in the Management Plane.
show routing route type service-route
Incorrect:
This is not a valid PAN-OS CLI command.
PAN-OS Documentation Reference
Service Routes in PAN-OS 11.0:
The configuration and verification of service routes are covered under the Device > Setup > Services section of the GUI.
For CLI, the debug dataplane internal vif route 250 command is specifically used for troubleshooting service routes in the Management Plane.
For more details, refer to:
PAN-OS 11.0 CLI Guide: Covers debugging tools and service route verification.
PCNSA Study Guide: Domain 1 includes service route configurations and their importance in maintaining connectivity for management services.