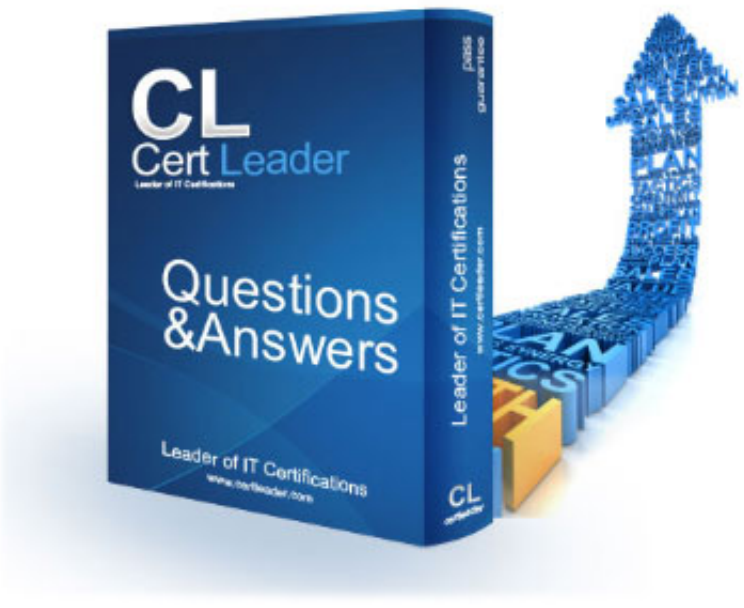
PCNSE Dumps

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

https://www.certleader.com/PCNSE-dumps.html



NEW QUESTION 1
A network-security engineer attempted to configure a bootstrap package on Microsoft Azure, but the virtual machine provisioning process failed. In reviewing the bootstrap package, the engineer only had the following directories: /config, /license and /software
Why did the bootstrap process fail for the VM-Series firewall in Azure?

A. All public cloud deployments require the /plugins folder to support proper firewall native integrations
B. The /content folder is missing from the bootstrap package
C. The VM-Series firewall was not pre-registered in Panorama and prevented the bootstrap process from successfully completing
D. The /config or /software folders were missing mandatory files to successfully bootstrap

Answer: B

NEW QUESTION 2
Which log type will help the engineer verify whether packet buffer protection was activated?

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

Answer: C

Explanation:
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.

NEW QUESTION 3
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

Answer: CD

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-exclusions/palo-alto-networ
The firewall provides a predefined SSL Decryption Exclusion list to exclude from decryption commonly used sites that break decryption because of technical reasons such as pinned certificates and mutual authentication.

NEW QUESTION 4
Where is Palo Alto Networks Device Telemetry data stored on a firewall with a device certificate installed?

A. Cortex Data Lake
B. Panorama
C. On Palo Alto Networks Update Servers
D. M600 Log Collectors

Answer: A

Explanation:
The Device Telemetry data is stored on Cortex Data Lak3e, which is a cloud-based service that collects and stores logs from your firewalls and other sources. Cortex Data Lake also enables you to analyze and visualize your data using various applications.
To use Device Telemetry, you need to install a device certificate on your firewall3. This certificate authenticates your firewall to Cortex Data Lake and encrypts the data in transit.

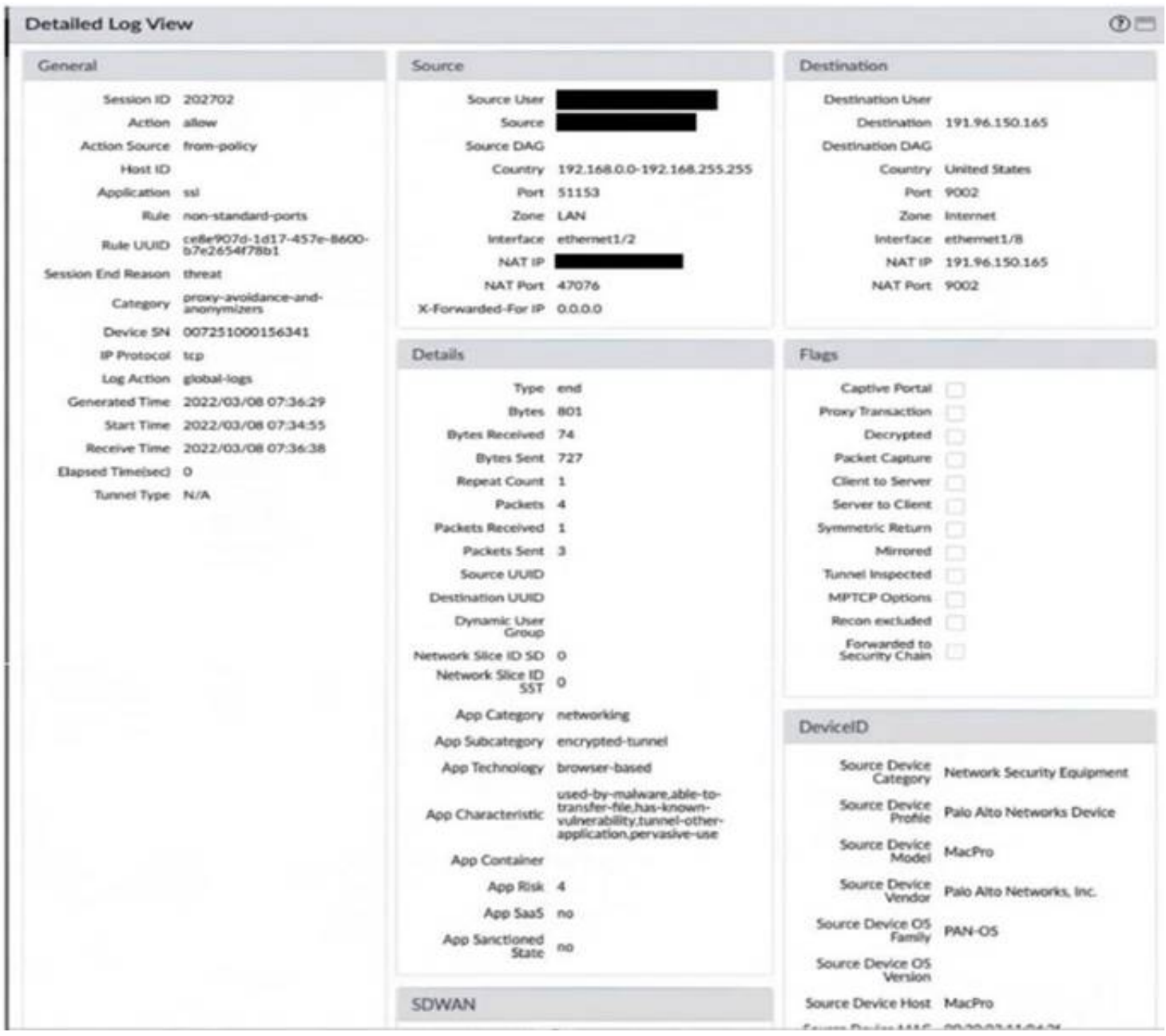
NEW QUESTION 5
What steps should a user take to increase the NAT oversubscription rate from the default platform setting?

A. Navigate to Device > Setup > TCP Settings > NAT Oversubscription Rate
B. Navigate to Policies > NAT > Destination Address Translation > Dynamic IP (with session distribution)
C. Navigate to Policies > NAT > Source Address Translation > Dynamic IP (with session distribution)
D. Navigate to Device > Setup > Session Settings > NAT Oversubscription Rate

Answer: D

Explanation:
NAT oversubscription is a feature that allows you to reuse a translated IP address and port for multiple source devices. This can help you conserve public IP addresses and increase the number of sessions that can be translated by a NAT rule.

NEW QUESTION 6
Given the screenshot, how did the firewall handle the traffic?



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

Answer: D

NEW QUESTION 7
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

Answer: AB

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.

NEW QUESTION 8
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

Answer: D

NEW QUESTION 9
An enterprise information Security team has deployed policies based on AD groups to restrict user access to critical infrastructure systems However a recent phisning campaign against the organization has prompted Information Security to look for more controls that can secure access to critical assets For users that need to access these systems Information Security wants to use PAN-OS multi-factor authentication (MFA) integration to enforce MFA.
What should the enterprise do to use PAN-OS MFA1?

A. Configure a Captive Porta1 authentication policy that uses an authentication profile that references a RADIUS profile

B. Create an authentication profile and assign another authentication factor to be used by a Captive Portal authentication policy
C. Configure a Captive Portal authentication policy that uses an authentication sequence
D. Use a Credential Phishing agent to detect prevent and mitigate credential phishing campaigns

Answer: C

NEW QUESTION 10
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

Answer: A

NEW QUESTION 10
A firewall engineer creates a new App-ID report under Monitor > Reports > Application Reports > New Application to monitor new applications on the network and better assess any Security policy updates the engineer might want to make.
How does the firewall identify the New App-ID characteristic?

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

Answer: D

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

NEW QUESTION 12
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.

Answer: C

NEW QUESTION 15
Which statement is true regarding a Best Practice Assessment?

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

Answer: A

NEW QUESTION 20
An internal system is not functioning. The firewall administrator has determined that the incorrect egress interface is being used. After looking at the configuration, the administrator believes that the firewall is not using a static route.
What are two reasons why the firewall might not use a static route? (Choose two.)

A. no install on the route
B. duplicate static route
C. path monitoring on the static route
D. disabling of the static route

Answer: AC

NEW QUESTION 22
A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (Cas)

A. Enterprise-Trusted-CA; which is verified as Forward Trust Certificate (The CA is also installed in the trusted store of the end-user browser and system)i
B. Enterprise-Untrusted-CA, which is verified as Forward Untrust Certificateii
C. Enterprise-Intermediate-CAi
D. Enterprise-Root-CA which is verified only as Trusted Root CAAn end-user visits https //www example-website com/ with a server certificate Common Name (CN) www example-website com The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewallThe end-user's browser will show that the certificate for www.example-website.com was issued by which of the following?
E. Enterprise-Untrusted-CA which is a self-signed CA

F. Enterprise-Trusted-CA which is a self-signed CA
G. Enterprise-Intermediate-CA which wa
H. in turn, issued by Enterprise-Root-CA
I. Enterprise-Root-CA which is a self-signed CA

Answer: B

NEW QUESTION 26
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. SSUTLS Service
B. HTTP Server
C. Decryption
D. Interface Management

Answer: AD

NEW QUESTION 28
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

Answer: D

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-agg

NEW QUESTION 32
An organization wishes to roll out decryption but gets some resistance from engineering leadership regarding the guest network.
What is a common obstacle for decrypting traffic from guest devices?

A. Guest devices may not trust the CA certificate used for the forward untrust certificate.
B. Guests may use operating systems that can't be decrypted.
C. The organization has no legal authority to decrypt their traffic.
D. Guest devices may not trust the CA certificate used for the forward trust certificate.

Answer: D

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

NEW QUESTION 33
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 tocommit all Panorama changes.
D. Use the Scheduled Config Push taschedule Commit to Panorama and also Push to Devices.

Answer: D

NEW QUESTION 38
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

Answer: B

NEW QUESTION 43
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

Answer: BCE

Explanation:
The GlobalProtect Gateway supports three methods for split tunneling23:

- Access Route — 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 — 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 — 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.

NEW QUESTION 47
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.

Answer: ABC

NEW QUESTION 50
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

Answer: B

NEW QUESTION 53
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

Answer: AB

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-broker

NEW QUESTION 56
During the process of developing a decryption strategy and evaluating which websites are required for corporate users to access, several sites have been identified that cannot be decrypted due to technical reasons. In this case, the technical reason is unsupported ciphers. Traffic to these sites will therefore be blocked if decrypted
How should the engineer proceed?

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

Answer: A

NEW QUESTION 57
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.

Answer: D

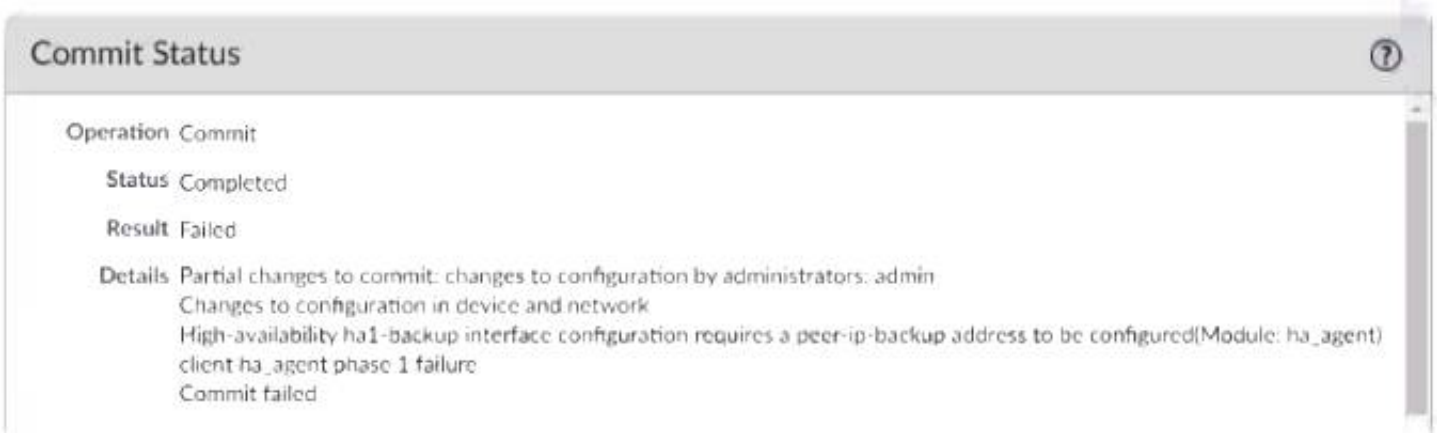
NEW QUESTION 61
A network administrator wants to use a certificate for the SSL/TLS Service Profile. Which type of certificate should the administrator use?

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

Answer: D

Explanation:
Use only signed certificates, not CA certificates, in SSL/TLS service profiles. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure-an-ssltls-service

NEW QUESTION 65
After configuring HA in Active/Passive mode on a pair of firewalls the administrator gets a failed commit with the following details.



What are two explanations for this type of issue? (Choose two)

A. The peer IP is not included in the permit list on Management Interface Settings
B. The Backup Peer HA1 IP Address was not configured when the commit was issued
C. Either management or a data-plane interface is used as HA1-backup
D. One of the firewalls has gone into the suspended state

Answer: BC

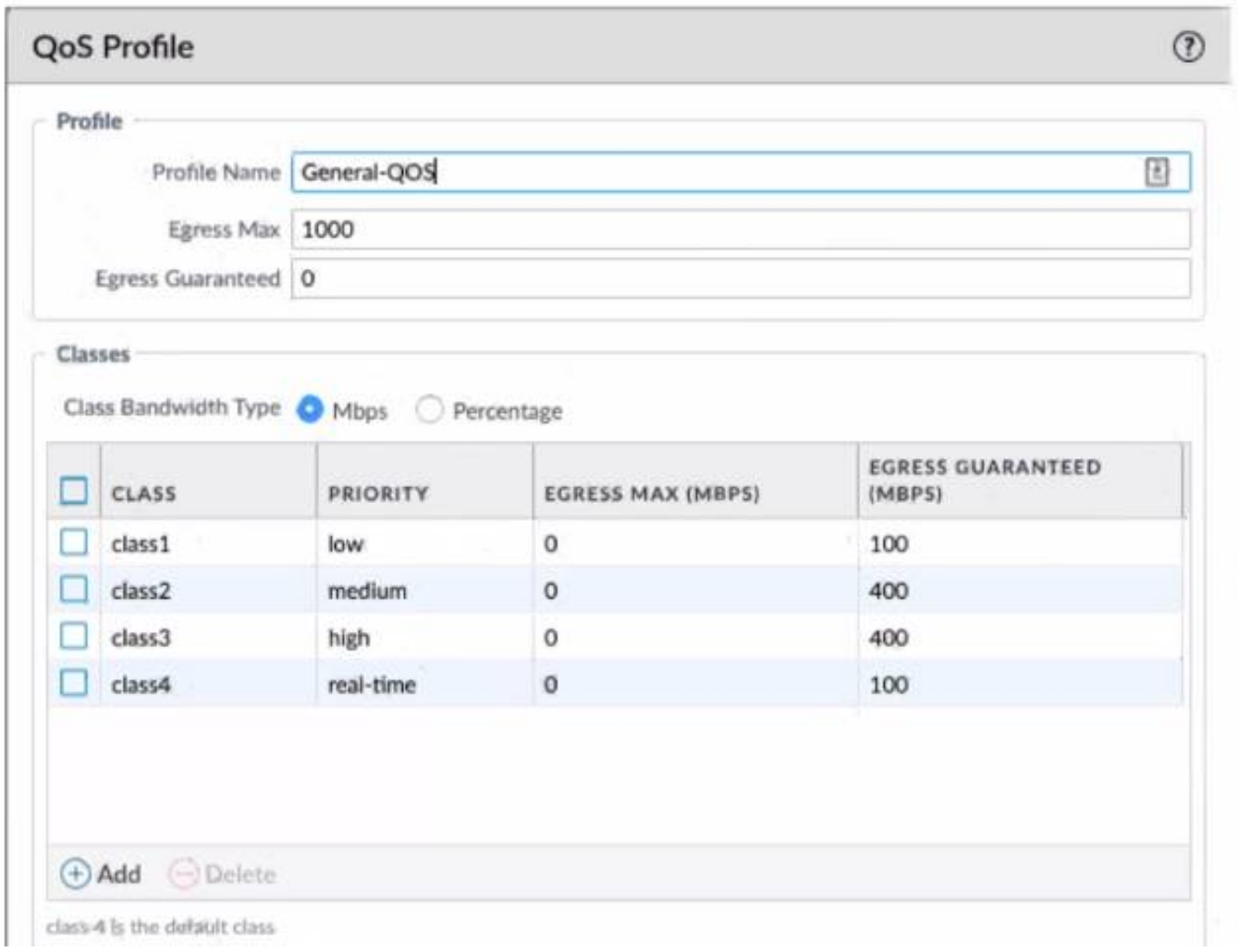
Explanation:
Cause The issue is seen when the HA1-backup is configured with either management (MGT) or an in-band interface. The "Backup Peer HA1 IP Address" is not configured : https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UmPCAU&lang=en_US%E

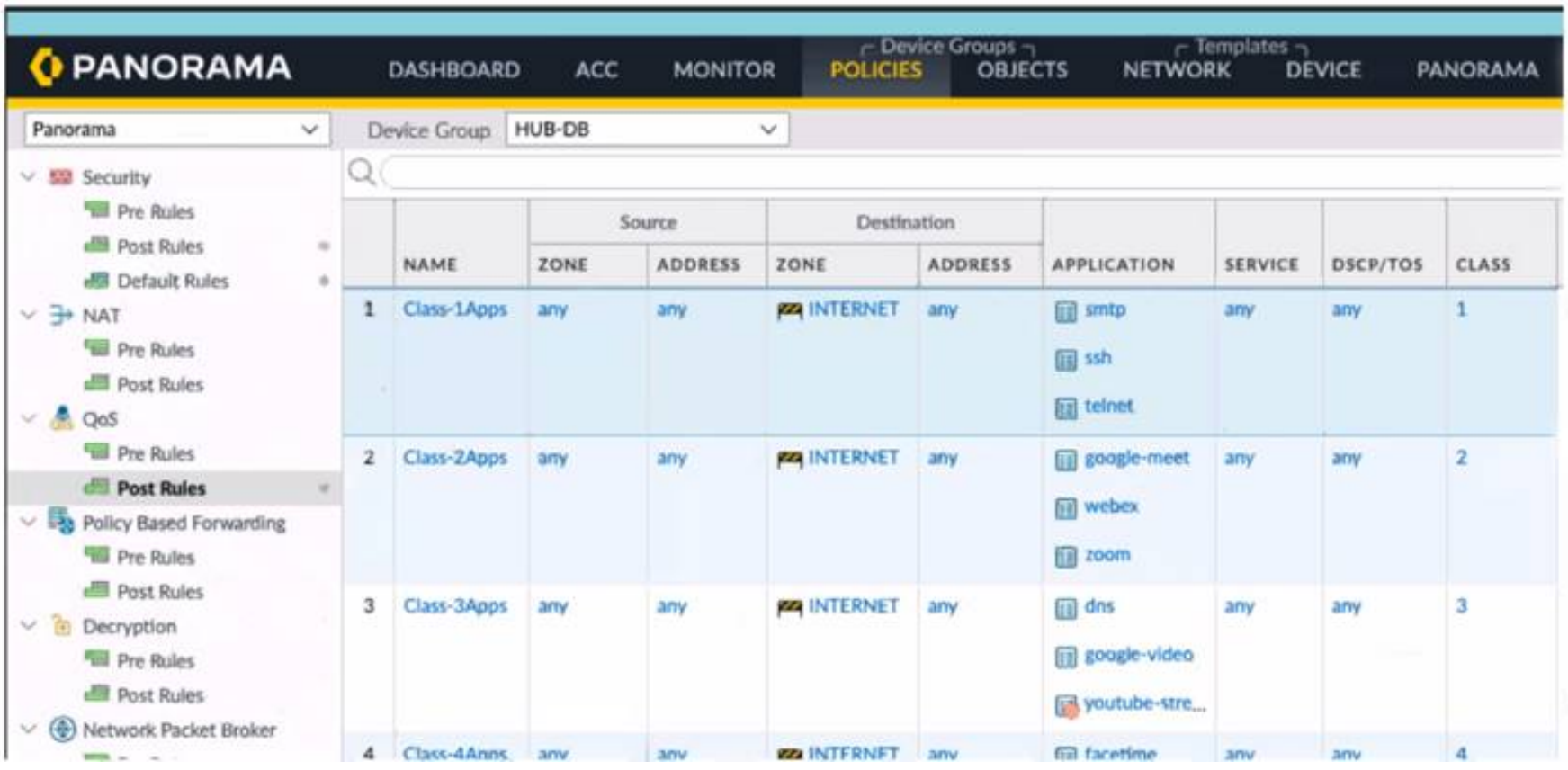
NEW QUESTION 67
An administrator has 750 firewalls. The administrator's central-management Panorama instance deploys dynamic updates to the firewalls. The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls.
If Panorama pushes the configuration of a dynamic 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.

Answer: D

NEW QUESTION 71
View the screenshots.





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

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

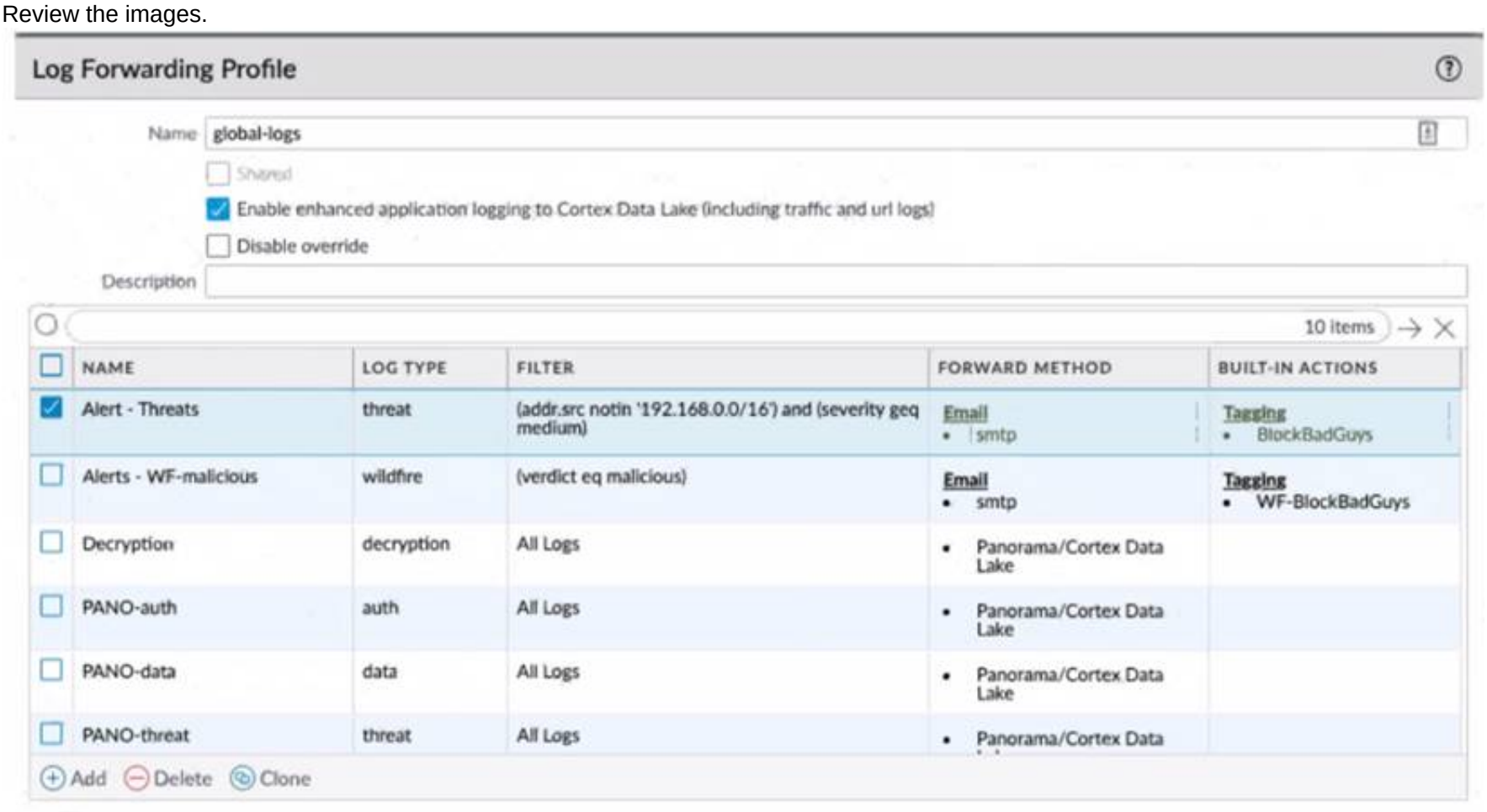
Answer: CD

NEW QUESTION 72
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

Answer: B

NEW QUESTION 77
Review the images.



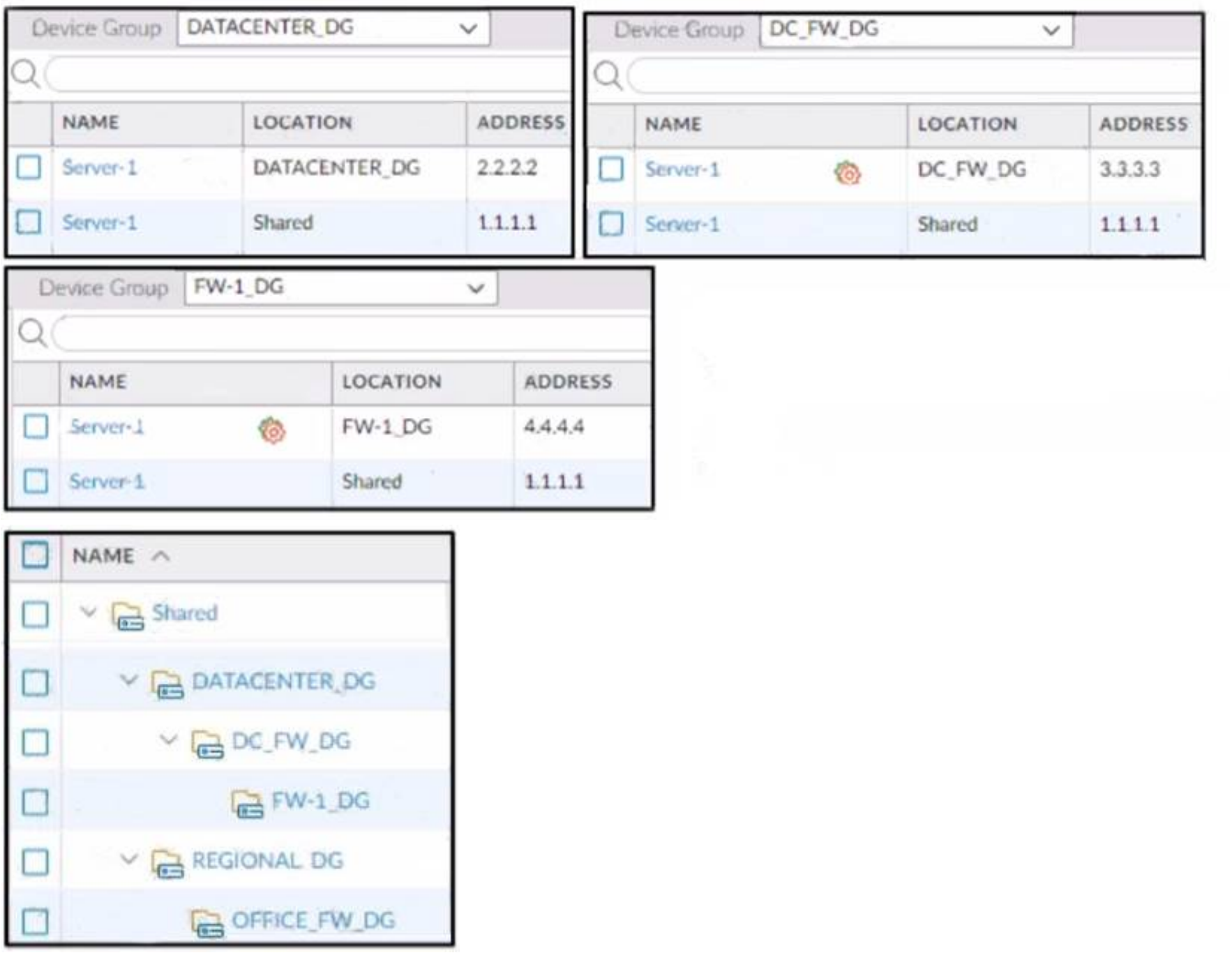
A firewall policy that permits web traffic includes the
What is the result of traffic that matches the "Alert - Threats" Profile Match List?

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.

Answer: D

NEW QUESTION 80
Refer to the exhibit.



Review the screenshots and consider the following information:
• FW-1 is assigned to the FW-1_DG device group, and FW-2 is assigned to OFFICE_FW_DG.
• 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 1.1.1.1. Server-1 will not be pushed to FW-2.
B. Server-1 on FW-1 will have IP 3.3.3.3. 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 4.4.4.4. Server-1 on FW-2 will have IP 1.1.1.1.

Answer: C

NEW QUESTION 82
An administrator analyzes the following portion of a VPN system log and notices the following issue "Received local id 10 10 1 4/24 type IPv4 address protocol 0 port 0, received remote id 10.1.10.4/24 type IPv4 address protocol 0 port 0."
What is the cause of the issue?

A. IPSec crypto profile mismatch
B. IPSec protocol mismatch
C. mismatched Proxy-IDs
D. bad local and peer identification IP addresses in the IKE gateway

Answer: C

NEW QUESTION 86
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

Answer: AC

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.

NEW QUESTION 89
A company is deploying User-ID in their network. The firewall learn needs to have the ability to see and choose from a list of usernames and user groups directly inside the Panorama policies when creating new security rules
How can this be achieved?

A. By configuring Data Redistribution Client in Panorama > Data Redistribution
B. By configuring User-ID source device in Panorama > Managed Devices
C. By configuring User-ID group mapping in Panorama > User Identification
D. By configuring Master Device in Panorama > Device Groups

Answer: C

Explanation:
User-ID group mapping is a feature that allows Panorama to retrieve user and group information from directory services such as LDAP or Active Directory1. This information can be used to enforce security policies based on user identity and group membership.
To configure User-ID group mapping on Panorama, you need to perform the following steps1:

- Select Panorama > User Identification > Group Mapping Settings
- Click Add and enter a name for the server profile
- Select a Server Type (LDAP or Active Directory)
- Click Add and enter the server details (IP address, port number, etc.)
- Click OK
- Select Group Include List and click Add
- Select the groups that you want to include in the group mapping
- Click OK
- Commit your changes

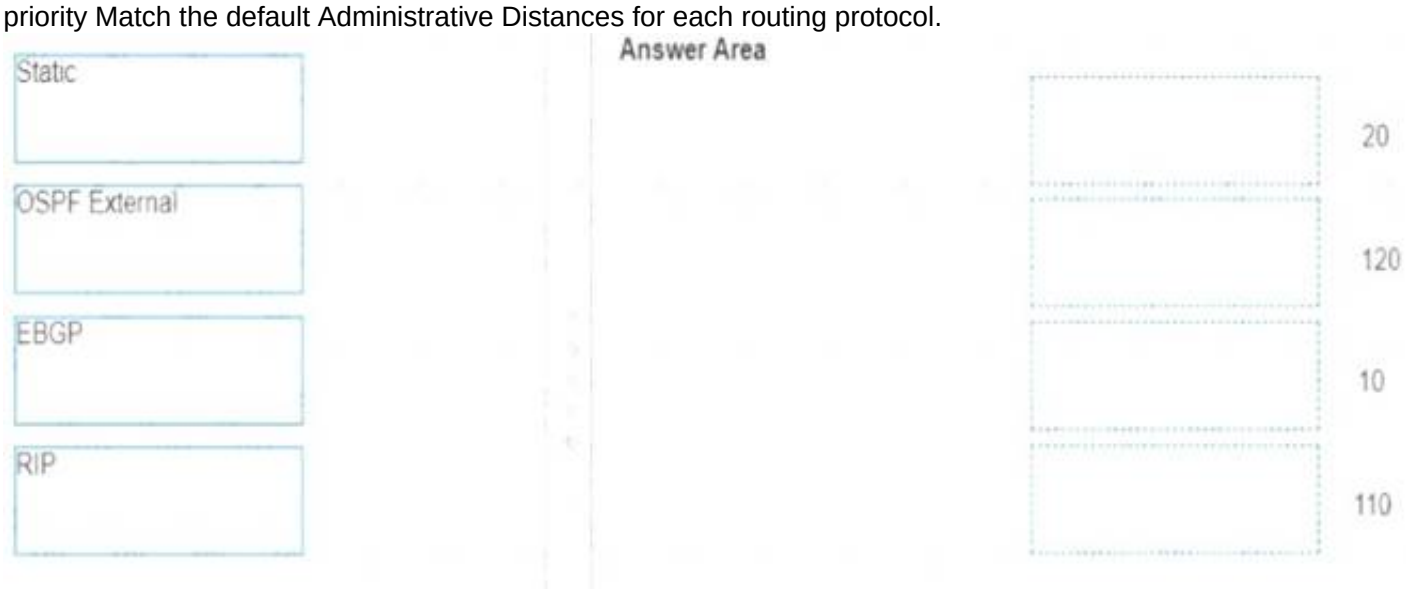
By configuring User-ID group mapping on Panorama, you can see and choose from a list of usernames and user groups directly inside the Panorama policies when creating new security rules2.

NEW QUESTION 91
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

Answer: B

NEW QUESTION 92
An engineer is troubleshooting traffic routing through the virtual router. The firewall uses multiple routing protocols, and the engineer is trying to determine routing priority Match the default Administrative Distances for each routing protocol.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

- Static

—Range is 10-240; default is 10.

- OSPF Internal

—Range is 10-240; default is 30.

- OSPF External

—Range is 10-240; default is 110.

- IBGP

—Range is 10-240; default is 200.

- EBGP

—Range is 10-240; default is 20.

- RIP

—Range is 10-240; default is 120.

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/virtual-routers

NEW QUESTION 94
A network security administrator has been tasked with deploying User-ID in their organization. What are three valid methods of collecting User-ID information in a network? (Choose three.)

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

Answer: ABC

Explanation:
User-ID is a feature that 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.

NEW QUESTION 98
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)

Answer: A

NEW QUESTION 99
The administrator for a small company has recently enabled decryption on their Palo Alto Networks firewall using a self-signed root certificate. They have also created a Forward Trust and Forward Untrust certificate and set them as such
The admin has not yet installed the root certificate onto client systems What effect would this have on decryption functionality?

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

Answer: D

NEW QUESTION 100
Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

A. Create a no-decrypt Decryption Policy rule.
B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
C. Create a Dynamic Address Group for untrusted sites
D. Create a Security Policy rule with vulnerability Security Profile attached.
E. Enable the “Block sessions with untrusted issuers” setting.

Answer: AD

Explanation:
You can use the No Decryption tab to enable settings to block traffic that is matched to a decryption policy configured with the No Decrypt action (Policies > Decryption > Action). Use these options to control server certificates for the session, though the firewall does not decrypt and inspect the session traffic.
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-decryption-profile

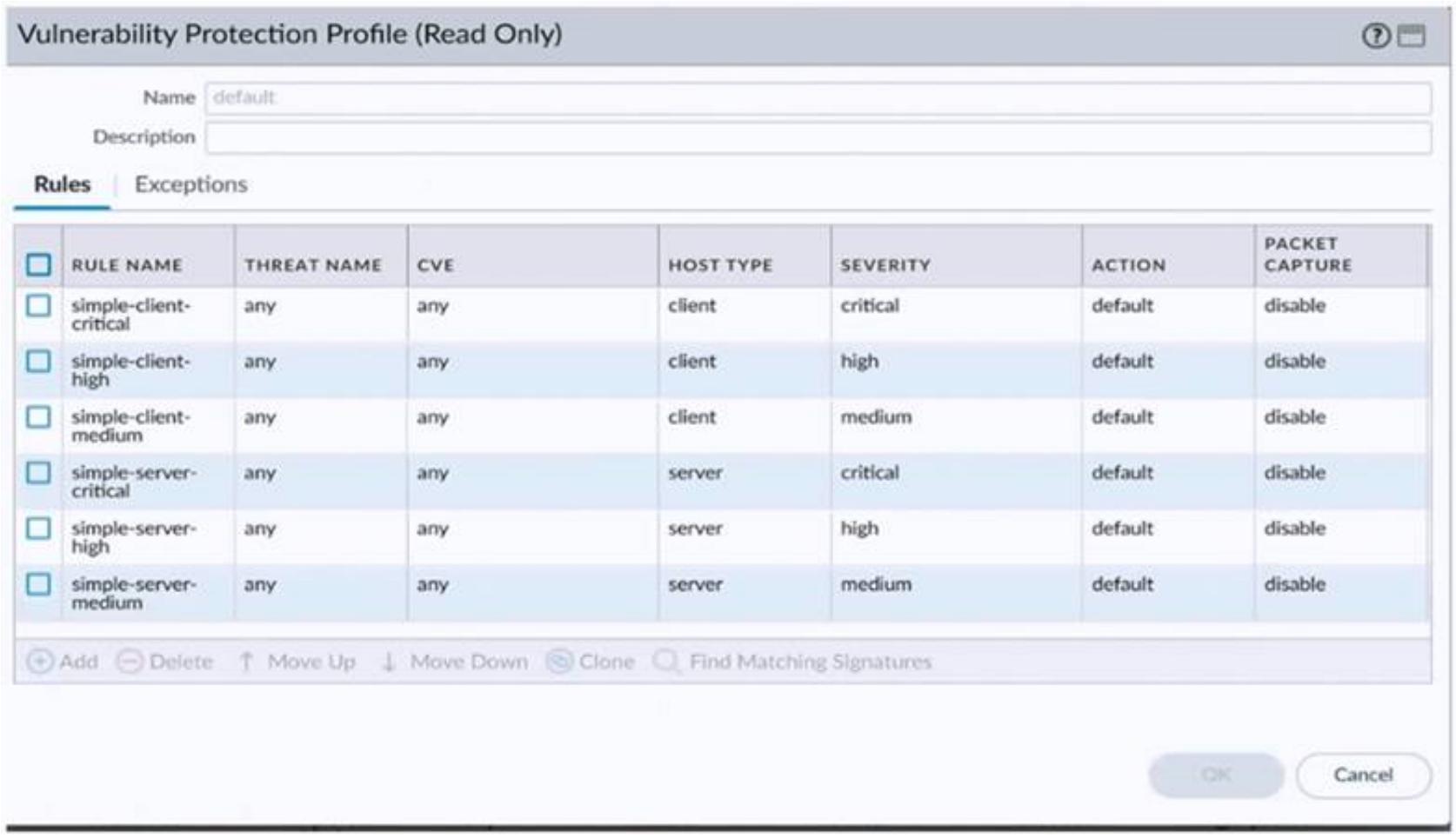
NEW QUESTION 102
An engineer needs to redistribute User-ID mappings from multiple data centers. Which data flow best describes redistribution of user mappings?

A. Domain Controller to User-ID agent

B. User-ID agent to Panorama
C. User-ID agent to firewall
D. firewall to firewall

Answer: D

NEW QUESTION 104
An administrator would like to determine which action the firewall will take for a specific CVE. Given the screenshot below, where should the administrator navigate to view this information?



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

Answer: A

NEW QUESTION 105
Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

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

Answer: ACD

Explanation:
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration

NEW QUESTION 108
What best describes the HA Promotion Hold Time?

A. the time that is recommended to avoid an HA failover due to the occasional flapping of neighboring devices
B. the time that is recommended to avoid a failover when both firewalls experience the same link/path monitor failure simultaneously
C. the time that the passive firewall will wait before taking over as the active firewall after communications with the HA peer have been lost
D. the time that a passive firewall with a low device priority will wait before taking over as the active firewall if the firewall is operational again

Answer: C

NEW QUESTION 113
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

Answer: C

Explanation:
Support for multiple instances per link—With 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/ospf-concepts/ospfv3

NEW QUESTION 115
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)

Answer: ABD

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."

NEW QUESTION 120
A super user is tasked with creating administrator accounts for three contractors. For compliance purposes, all three contractors will be working with different device-groups m their hierarchy to deploy policies and objects.
Which type of role-based access is most appropriate for this project?

A. Create a Dynamic Admin with the Panorama Administrator role.
B. Create a Device Group and Template Admin.
C. Create a Custom Panorama Admin.
D. Create a Dynamic Read only superuser

Answer: C

Explanation:
A Custom Panorama Admin is a type of role-based access that allows a super user to create separate Panorama administrator accounts for each of the three contractors. This will allow each contractor to work with different device-groups in their hierarchy and deploy policies and objects in accordance with the organization's compliance requirements. The Custom Panorama Admin role also allows the super user to assign separate permissions to each contractor's account, granting them access to only the resources they are authorized to use. This type of role-based access is the most appropriate for this project as it will ensure that each contractor is only able to access the resources they need in order to do their job.

NEW QUESTION 121
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

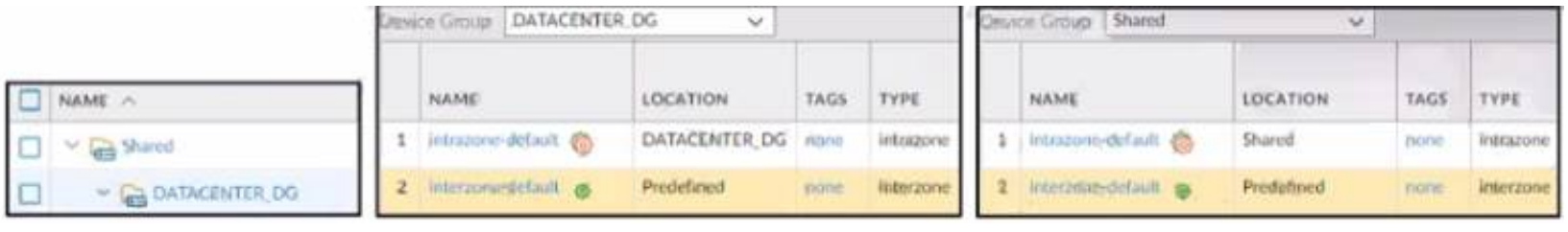
Answer: C

NEW QUESTION 122
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

Answer: D

NEW QUESTION 127
Refer to the exhibit.



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

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

default rules

Answer: A

NEW QUESTION 130
An organization conducts research on the benefits of leveraging the Web Proxy feature of PAN-OS 11.0. What are two benefits of using an explicit proxy method versus a transparent proxy method? (Choose two.)

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

Answer: BC

Explanation:
B. Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy12. This means that the client can see the proxy's IP address and port number, and can use tools like ping or traceroute to check connectivity and latency issues. Transparent proxies are invisible to the client browser, which makes it harder to diagnose problems.

C. Explicit proxy supports interception of traffic using non-standard HTTPS ports3. This means that the proxy can handle HTTPS requests that use ports other than 443, which may be required by some applications or websites. Transparent proxies can only intercept HTTPS traffic on port 443, which limits their functionality.

NEW QUESTION 133
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

Answer: A

NEW QUESTION 134
An administrator has two pairs of firewalls within the same subnet. Both pairs of firewalls have been configured to use High Availability mode with Active/Passive. The ARP tables for upstream routes display the same MAC address being shared for some of these firewalls.
What can be configured on one pair of firewalls to modify the MAC addresses so they are no longer in conflict?

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

Answer: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCAS
change 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.

NEW QUESTION 139
An engineer receives reports from users that applications are not working and that websites are only partially loading in an asymmetric environment. After investigating, the engineer observes the flow_tcp_non_syn_drop counter increasing in the show counters global output.
Which troubleshooting command should the engineer use to work around this issue?

A. set deviceconfig setting tcp asymmetric-path drop
B. set deviceconfig setting session tcp-reject-non-syn no
C. set session tcp-reject-non-syn yes
D. set deviceconfig setting tcp asymmetric-path bypass

Answer: B

Explanation:
To work around this issue, one possible troubleshooting command is set deviceconfig setting session tcp-reject-non-syn no which disables TCP reject non-SYN temporarily (until reboo4t). This command allows non-SYN first packet through without dropping it. The flow_tcp_non_syn_drop counter increases when the firewall receives packets with the ACK flag set, but not the SYN flag, which indicates asymmetric traffic flow. The tcp-reject-non-syn option enables or disables the firewall to drop non-SYN TCP packets. In this case, disabling the tcp-reject-non-syn option using the "set deviceconfig setting session tcp-reject-non-syn no" command can help work around the issue. This allows the firewall to accept non-SYN packets and create a session for the existing flow.

NEW QUESTION 141
When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?

A. The interface must be used for traffic to the required services
B. You must enable DoS and zone protection
C. You must set the interface to Layer 2 Layer 3. or virtual wire
D. You must use a static IP address

Answer: D

NEW QUESTION 143
An engineer needs to configure SSL Forward Proxy to decrypt traffic on a PA-5260. The engineer uses a forward trust certificate from the enterprise PKI that expires December 31, 2025. The validity date on the PA-generated certificate is taken from what?

A. The trusted certificate
B. The server certificate
C. The untrusted certificate
D. The root CA

Answer: B

NEW QUESTION 147
A firewall should be advertising the static route 10.2.0.0/24 Into OSPF. The configuration on the neighbor is correct, but the route is not in the neighbor's routing table.
Which two configurations should you check on the firewall? (Choose two.)

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

Answer: AB

NEW QUESTION 152
A network administrator plans a Prisma Access deployment with three service connections, each with a BGP peering to a CPE. The administrator needs to minimize the BGP configuration and management overhead on on-prem network devices.
What should the administrator implement?

A. target service connection for traffic steering
B. summarized BGP routes before advertising
C. hot potato routing
D. default routing

Answer: C

NEW QUESTION 157
A customer is replacing their legacy remote access VPN solution The current solution is in place to secure only internet egress for the connected clients Prisma Access has been selected to replace the current remote access VPN solution During onboarding the following options and licenses were selected and enabled
- Prisma Access for Remote Networks 300Mbps
- Prisma Access for Mobile Users 1500 Users
- Cortex Data Lake 2TB
- Trusted Zones trust
- Untrusted Zones untrust
- Parent Device Group shared
How can you configure Prisma Access to provide the same level of access as the current VPN solution?

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

Answer: D

NEW QUESTION 161
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)

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

Answer: CDE

NEW QUESTION 166
What can an engineer use with GlobalProtect to distribute user-specific client certificates to each GlobalProtect user?

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

Answer: D

NEW QUESTION 170
An administrator is using Panorama to manage me and suspects an IKE Crypto mismatch between peers, 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 ACC to consolidate the logs.
D. Use the scp logdb export command.

Answer: D

NEW QUESTION 171
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.

Answer: A

NEW QUESTION 176
Which function is handled by the management plane (control plane) of a Palo Alto Networks firewall?

A. signature matching for content inspection
B. IPSec tunnel standup
C. Quality of Service
D. logging

Answer: D

NEW QUESTION 179
An administrator is required to create an application-based Security policy rule to allow Evernote. The Evernote application implicitly uses SSL and web browsing.
What is the minimum the administrator needs to configure in the Security rule to allow only Evernote?

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

Answer: C

NEW QUESTION 183
Which data flow describes redistribution of user mappings?

A. User-ID agent to firewall

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

Answer: B

Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-firewalls-to-redistribute- https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/red

NEW QUESTION 185
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.

Answer: D

NEW QUESTION 187
Which configuration task is best for reducing load on the management plane?

A. Disable logging on the default deny rule
B. Enable session logging at start
C. Disable pre-defined reports
D. Set the URL filtering action to send alerts

Answer: C

NEW QUESTION 190
Before an administrator of a VM-500 can enable DoS and zone protection, what actions need to be taken?

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

Answer: A

Explanation:
* 1 https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone-protection-best-practices/dos-and-zone-prote
* 2 https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/ta
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection.html

NEW QUESTION 194
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

Answer: AB

NEW QUESTION 198
An engineer configures SSL decryption in order to have more visibility to the internal users' traffic when it is regressing the firewall.
Which three types of interfaces support SSL Forward Proxy? (Choose three.)

A. High availability (HA)
B. Layer
C. Virtual Wire
D. Tap
E. Layer 3

Answer: BCE

Explanation:
SSL Forward Proxy is a feature that allows the firewall to decrypt and inspect outbound SSL traffic from internal users to external servers1. The firewall acts as a proxy (MITM) generating a new certificate for the accessed URL and presenting it to the client during SSL handshake2.
SSL Forward Proxy can be configured on any interface type that supports security policies, which are Layer 2, Virtual Wire, and Layer 3 interfaces1. These interface types allow the firewall to apply security profiles and URL filtering on the decrypted SSL traffic.

NEW QUESTION 202

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

Answer: B

NEW QUESTION 205
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

Answer: A

NEW QUESTION 206
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

Answer: C

Explanation:
When importing a pre-configured firewall configuration to Panorama, you need to perform the following steps 12:
- 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
- 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.

NEW QUESTION 210
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.

Answer: C

NEW QUESTION 211
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

Answer: ACD

NEW QUESTION 214
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.

Answer: D

Explanation:
In order to see what is in a template, the device-group needs the template referenced. Even if you add the firewall to both the template and device-group, the device-group will not see what is in the template.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNfeCAG

NEW QUESTION 217
Which source is the most reliable for collecting User-ID user mapping?

A. GlobalProtect
B. Microsoft Active Directory
C. Microsoft Exchange
D. Syslog Listener

Answer: A

Explanation:
User-ID is a feature that enables you to identify and control users on your network based on their usernames instead of their IP addresses1. User mapping is the process of mapping IP addresses to usernames using various sources of information1.
The most reliable source for collecting User-ID user mapping is GlobalProte2ct. GlobalProtect is a solution that provides secure access to your network and resources from anywhere. GlobalProtect agents on endpoints send user mapping information directly to the firewall or Panorama, which eliminates the need for probing other sources2. GlobalProtect also supports dynamic IP address changes and roaming use2rs.

NEW QUESTION 220
Four configuration choices are listed, and each could be used to block access to a specific URL
II you configured each choice to block the same URL, then which choice would be evaluated last in the processing order to block access to the URL1?

A. PAN-DB URL category in URL Filtering profile
B. Custom URL category in Security policy rule
C. Custom URL category in URL Filtering profile
D. EDL in URL Filtering profile

Answer: A

NEW QUESTION 221
A network security engineer configured IP multicast in the virtual router to support a new application. Users in different network segments are reporting that they are unable to access the application.
What must be enabled to allow an interface to forward multicast traffic?

A. IGMP
B. PIM
C. BFD
D. SSM

Answer: B

Explanation:
A protocol that enables routers to forward multicast traffic efficiently based on the source and destination addresses. PIM can operate in two modes: sparse mode (PIM-SM) or dense mode (PIM-DM). PIM-SM uses a rendezvous point (RP) as a central point for distributing multicast traffic, while PIM-DM uses flooding and pruning techniques2.
to enable PIM on the interface which allows routers to forward multicast traffic using either sparse mode o dense mode depending on your network topology and requirements.

NEW QUESTION 222
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.

Answer: AB

NEW QUESTION 225
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

Answer: A

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=en_US%E

NEW QUESTION 230
An administrator has configured the Palo Alto Networks NGFW's management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.
Which configuration setting or step will allow the firewall to get automatic application signature updates?

A. A scheduler will need to be configured for application signatures.
B. A Security policy rule will need to be configured to allow the update requests from the firewall to the update servers.
C. A Threat Prevention license will need to be installed.
D. A service route will need to be configured.

Answer: A

NEW QUESTION 234
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

Answer: B

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.

NEW QUESTION 238
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 init-cfg 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

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/boots

NEW QUESTION 241
The Aggregate Ethernet interface is showing down on a passive PA-7050 firewall of an active/passive HA pair. The HA Passive Link State is set to "Auto" under Device > High Availability > General > Active/Passive Settings. The AE interface is configured with LACP enabled and is up only on the active firewall.
Why is the AE interface showing down on the passive firewall?

A. It does not perform pre-negotiation LACP unless "Enable in HA Passive State" is selected under the High Availability Options on the LACP tab of the AE Interface.
B. It does not participate in LACP negotiation unless Fast Failover is selected under the Enable LACP selection on the LACP tab of the AE Interface.
C. It participates in LACP negotiation when Fast is selected for Transmission Rate under the Enable LACP selection on the LACP tab of the AE Interface.
D. It performs pre-negotiation of LACP when the mode Passive is selected under the Enable LACP selection on the LACP tab of the AE Interface.

Answer: A

NEW QUESTION 244
During the implementation of SSL Forward Proxy decryption, an administrator imports the company's Enterprise Root CA and Intermediate CA certificates onto the firewall. The company's Root and Intermediate CA certificates are also distributed to trusted devices using Group Policy and GlobalProtect. Additional device certificates and/or Subordinate certificates requiring an Enterprise CA chain of trust are signed by the company's Intermediate CA.
Which method should the administrator use when creating Forward Trust and Forward Untrust certificates on the firewall for use with decryption?

A. Generate a single subordinate CA certificate for both Forward Trust and Forward Untrust.
B. Generate a CA certificate for Forward Trust and a self-signed CA for Forward Untrust.
C. Generate a single self-signed CA certificate for Forward Trust and another for Forward Untrust
D. Generate two subordinate CA certificates, one for Forward Trust and one for Forward Untrust.

Answer: B

NEW QUESTION 246
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

Answer: CDE

NEW QUESTION 251
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PCNSE Exam with Our Prep Materials Via below:

https://www.certleader.com/PCNSE-dumps.html