Exam Questions PCNSE

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

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

NEW QUESTION 1
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

Answer: B

NEW QUESTION 2
An engineer is tasked with enabling SSL decryption across the environment. What are three valid parameters of an SSL Decryption policy? (Choose three.)

A. URL categories
B. source users
C. source and destination IP addresses
D. App-ID
E. GlobalProtect HIP

Answer: ABC

NEW QUESTION 3
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 4
An administrator is building Security rules within a device group to block traffic to and from malicious locations
How should those rules be configured to ensure that they are evaluated with a high priority?

A. Create the appropriate rules with a Block action and apply them at the top of the Default Rules
B. Create the appropriate rules with a Block action and apply them at the top of the Security Post-Rules.
C. Create the appropriate rules with a Block action and apply them at the top of the local firewall Security rules.
D. Create the appropriate rules with a Block action and apply them at the top of the Security Pre-Rules

Answer: D

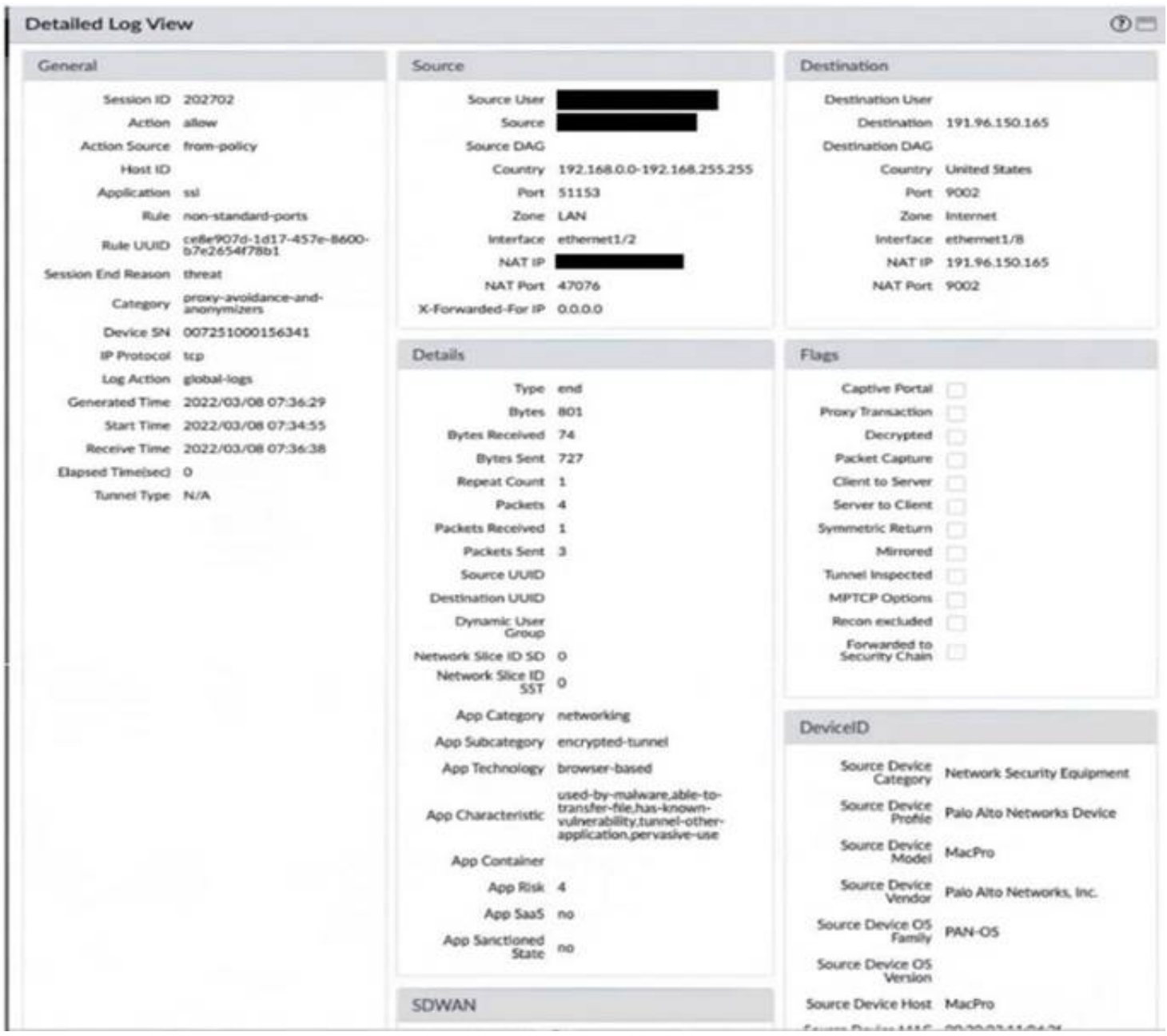
NEW QUESTION 5
A standalone firewall with local objects and policies needs to be migrated into Panorama. What procedure should you use so Panorama is fully managing the firewall?

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"

Answer: B

Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/transition-a-firewall-to-pan

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
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

Answer: BD

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-alto-networks-pcnse

NEW QUESTION 9
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 10
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 10
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.

Answer: A

NEW QUESTION 12
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 17
A network administrator is trying to prevent domain username and password submissions to phishing sites on some allowed URL categories
Which set of steps does the administrator need to take in the URL Filtering profile to prevent credential phishing on the firewall?

A. Choose the URL categories on Site Access column and set action to block Click the User credential Detection tab and select IP User Mapping Commit
B. Choose the URL categories in the User Credential Submission column and set action to block Select the User credential Detection tab and select use IP User Mapping Commit
C. Choose the URL categories in the User Credential Submission column and set action to block Select the URL filtering settings and enable Domain Credential Filter Commit
D. Choose the URL categories in the User Credential Submission column and set action to block Select the User credential Detection tab and select Use Domain Credential Filter Commit

Answer: D

Explanation:
credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions to known corporate credentials. You can configure solutions that detect and prevent credential phishing using URL filtering profiles and User-ID agents.

NEW QUESTION 21
In the screenshot above which two pieces ot information can be determined from the ACC configuration shown? (Choose two)

A. The Network Activity tab will display all applications, including FTP.
B. Threats with a severity of "high" are always listed at the top of the Threat Name list
C. Insecure-credentials, brute-force and protocol-anomaly are all a part of the vulnerability Threat Type
D. The ACC has been filtered to only show the FTP application

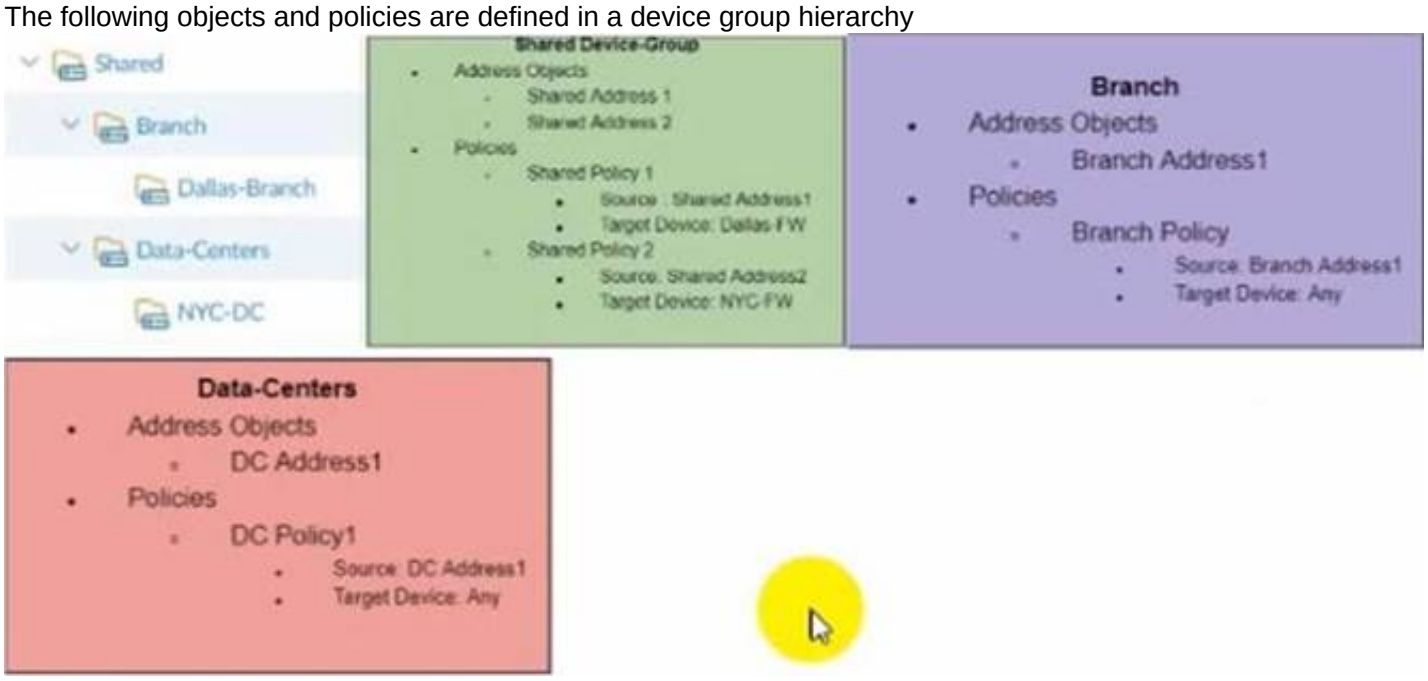
Answer: AC

NEW QUESTION 22
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
B. routes listed in the routing table with flags A?
C. under the BGP Summary tab
D. routes listed in the forwarding table with BGP in the Protocol column

Answer: C

NEW QUESTION 27
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 Policyl
D)
Address Objects -Shared Addressl -Shared Address2 -Branch Addressl Policies -Shared Policyl -Shared Policy2 -Branch Policyl

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

Answer: A

NEW QUESTION 29
What are two best practices for incorporating new and modified App-IDs? (Choose two.)

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

Answer: BD

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content

NEW QUESTION 32
An engineer is configuring Packet Buffer Protection on ingress zones to protect from single-session DoS attacks Which sessions does Packet Buffer Protection apply to?

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

Answer: D

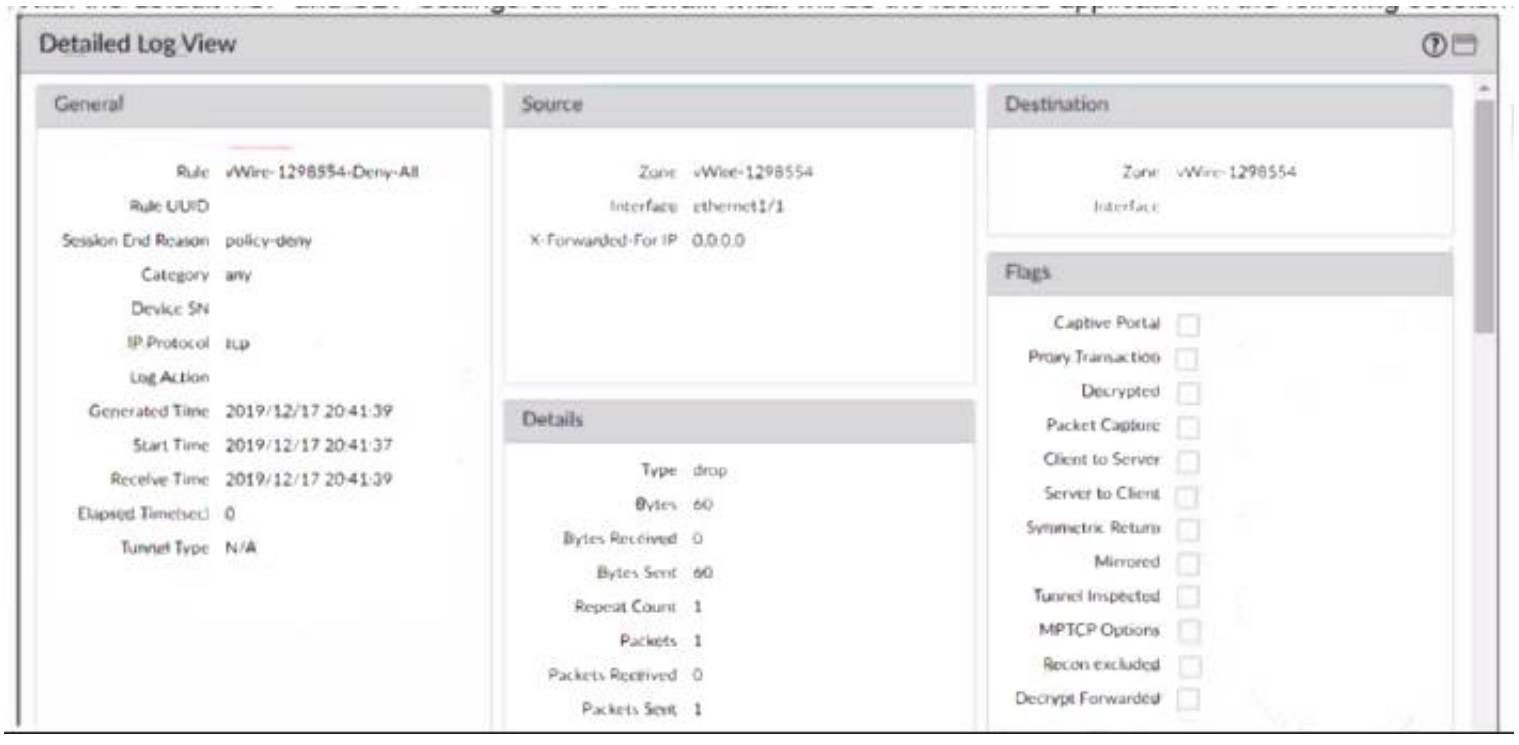
NEW QUESTION 35
What are two valid deployment options for Decryption Broker? (Choose two)

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 40
With the default TCP and UDP settings on the firewall, what will be the identified application in the following session?



A. Incomplete
B. unknown-udp
C. Insufficient-data
D. not-applicable

Answer: B

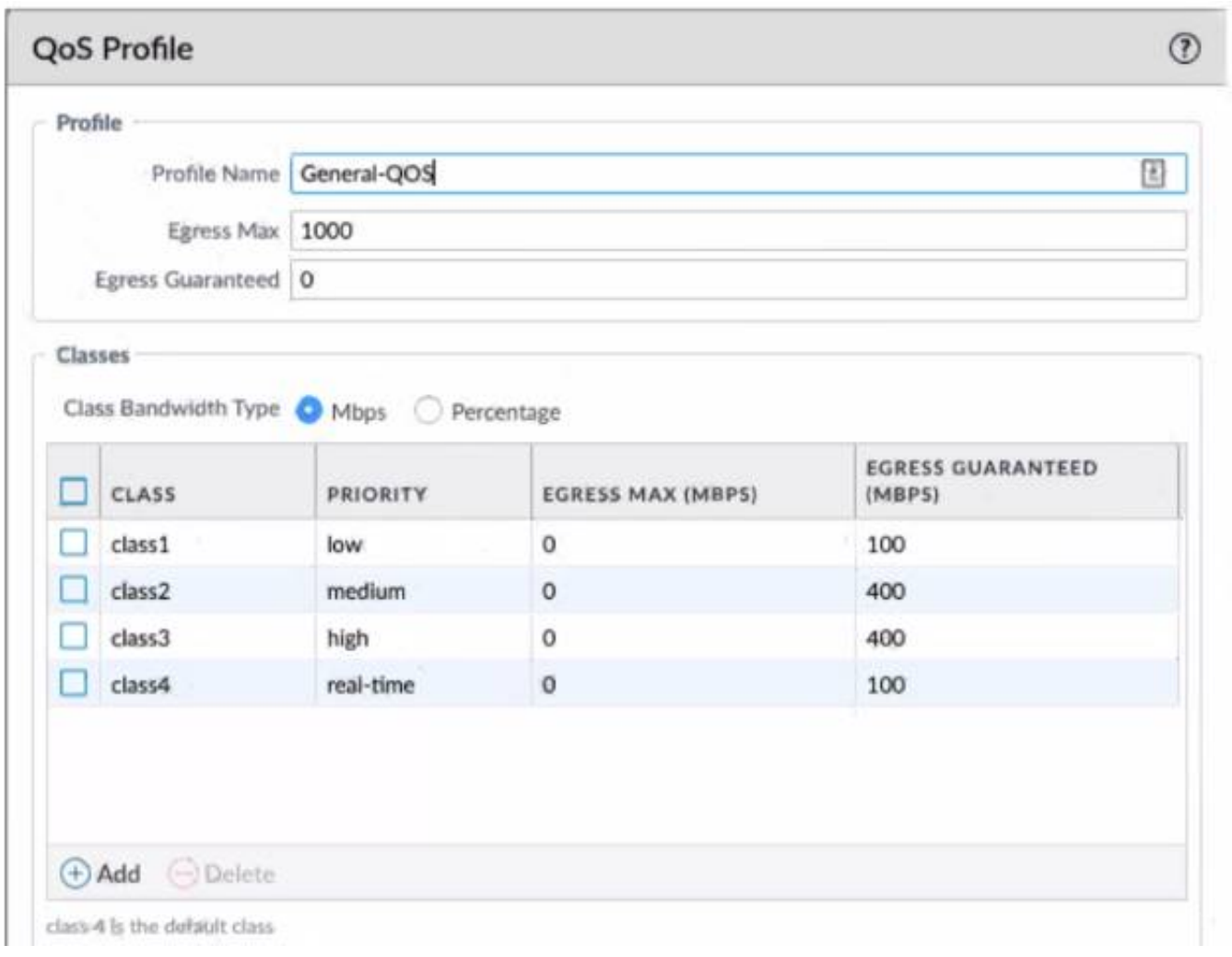
NEW QUESTION 44
A network administrator wants to use a certificate for the SSL/TLS Service Profile. Which type of certificate should the administrator use?

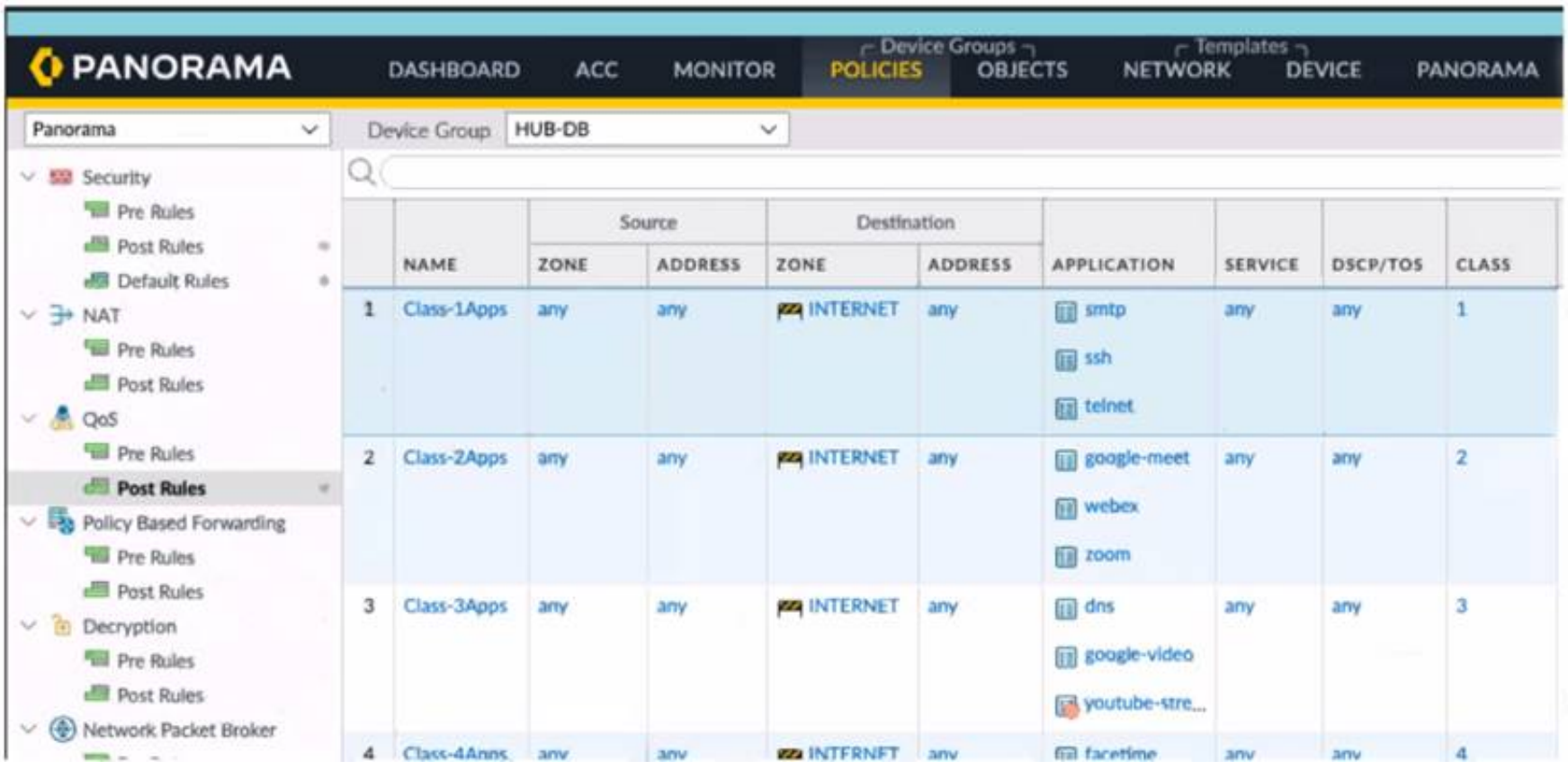
A. certificate authority (CA) certificate
B. client certificate
C. machine certificate
D. server certificate

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 47
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.

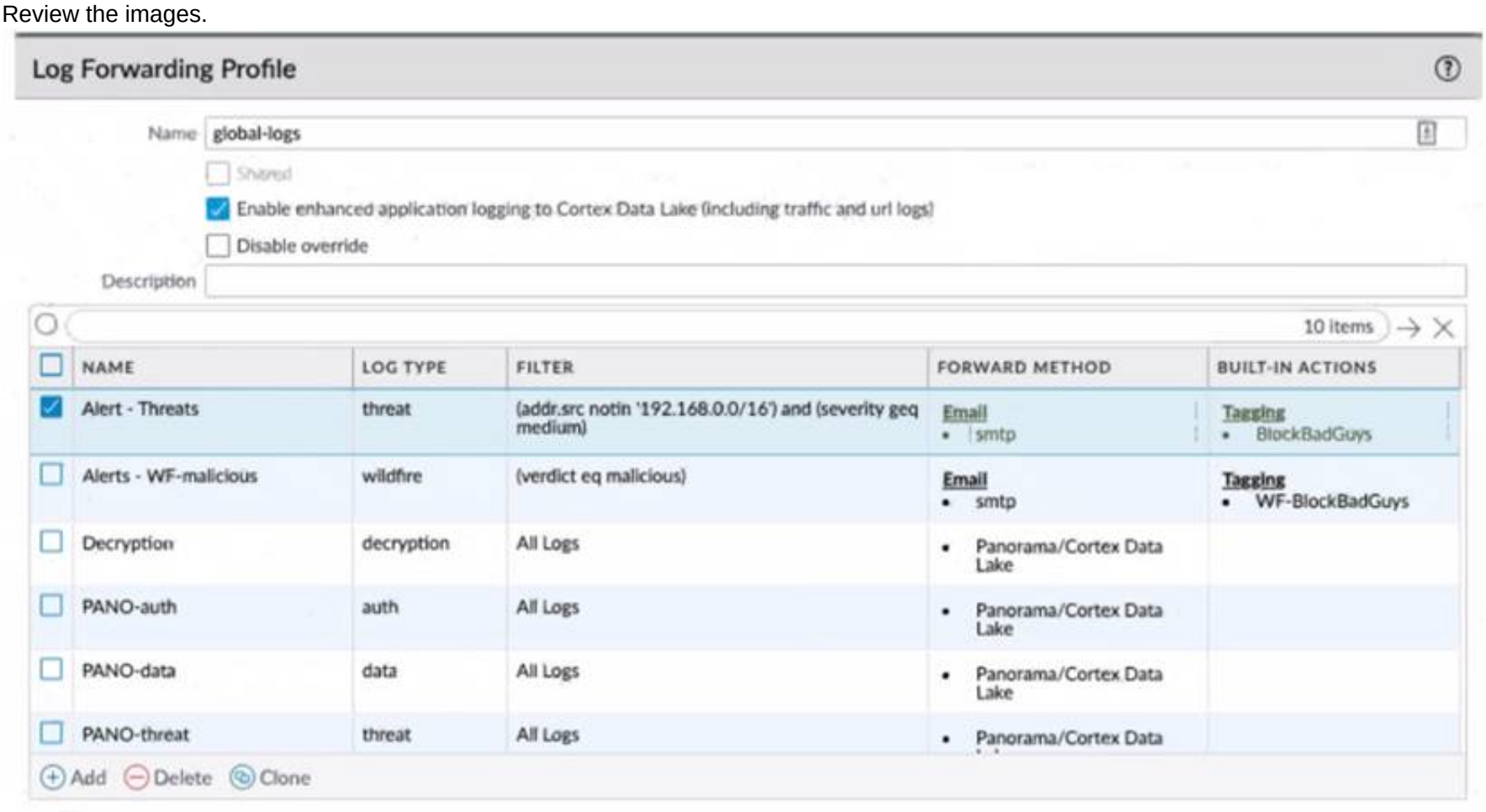
Answer: CD

NEW QUESTION 48
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 49
Review the images.



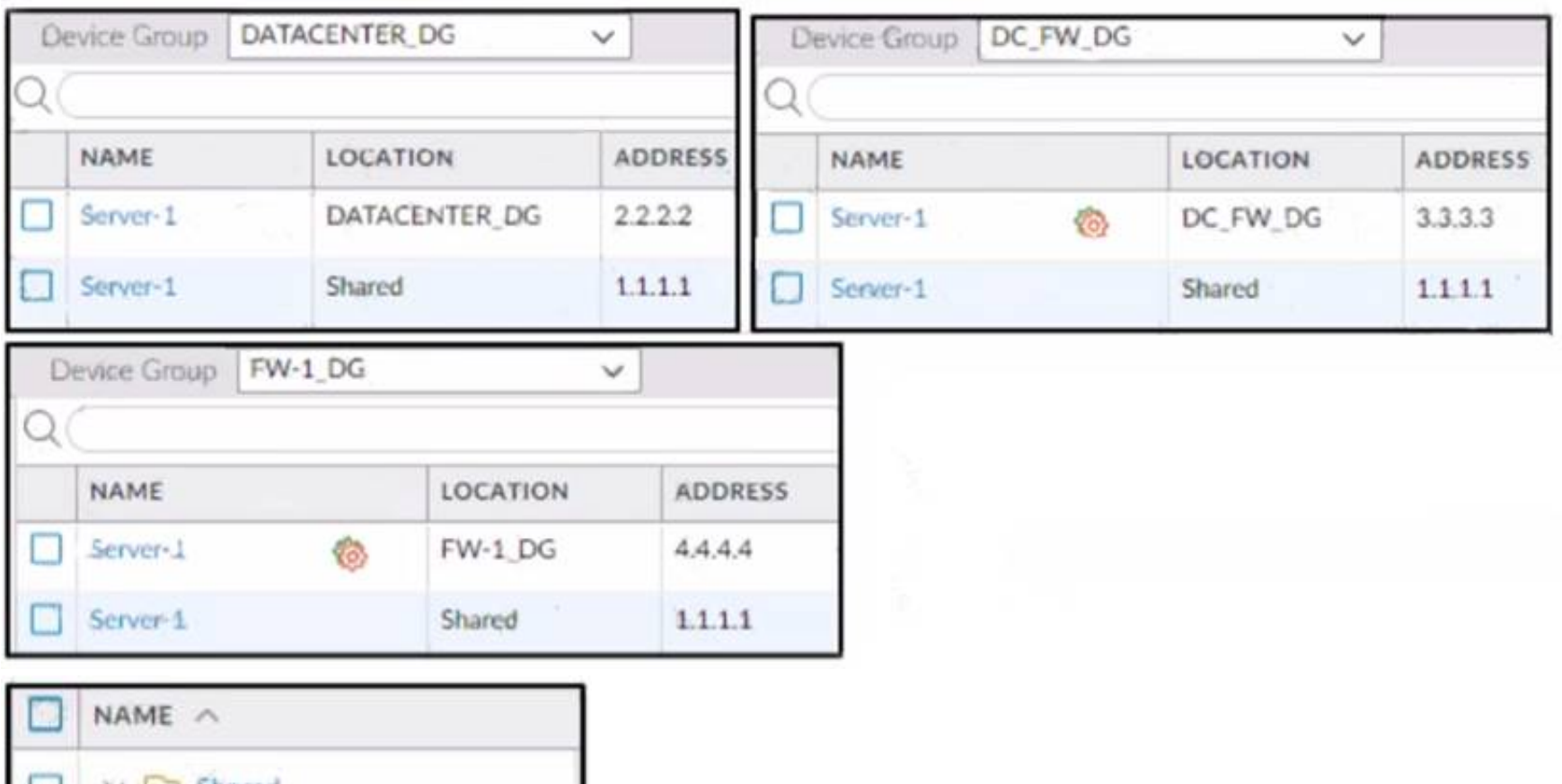
A firewall policy that permits web traffic includes the
What is the result of traffic that matches the "Alert - Threats" Profile Match List?

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 50
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 55
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

Answer: B

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

NEW QUESTION 57
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

Answer: D

NEW QUESTION 62
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 66
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 68
A firewall has Security policies from three sources
* 1. locally created policies
* 2. shared device group policies as pre-rules
* 3. the firewall's device group as post-rules
How will the rule order populate once pushed to the firewall?

A. shared device group policies, firewall device group policie
B. local policies.
C. firewall device group policies, local policie
D. shared device group policies
E. shared device group policie
F. local policies, firewall device group policies
G. local policies, firewall device group policies, shared device group policies

Answer: C

NEW QUESTION 71
An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications QoS natively integrates with which feature to provide service quality?

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

Answer: C

NEW QUESTION 73
An administrator discovers that a file blocked by the WildFire inline ML feature on the firewall is a false-positive action. How can the administrator create an exception for this particular file?

A. Add partial hash and filename in the file section of the WildFire inline ML tab of the Antivirus profile.
B. Set the WildFire inline ML action to allow for that protocol on the Antivirus profile.
C. Add the related Threat ID in the Signature exceptions tab of the Antivirus profile.
D. Disable the WildFire profile on the related Security policy.

Answer: A

NEW QUESTION 74
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 75
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

Answer: C

Explanation:
To allow the firewall to communicate with the User-ID agent, you need to configure a custom service route f 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 drop-down 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

NEW QUESTION 77
What can be used to create dynamic address groups?

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

Answer: C

NEW QUESTION 79
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. Add an authentication algorithm in the IPSec Crypto profile.
B. Enable PFS under the IPSec Tunnel advanced options.
C. Select the appropriate DH Group under the IPSec Crypto profile.
D. Enable PFS under the IKE gateway advanced options

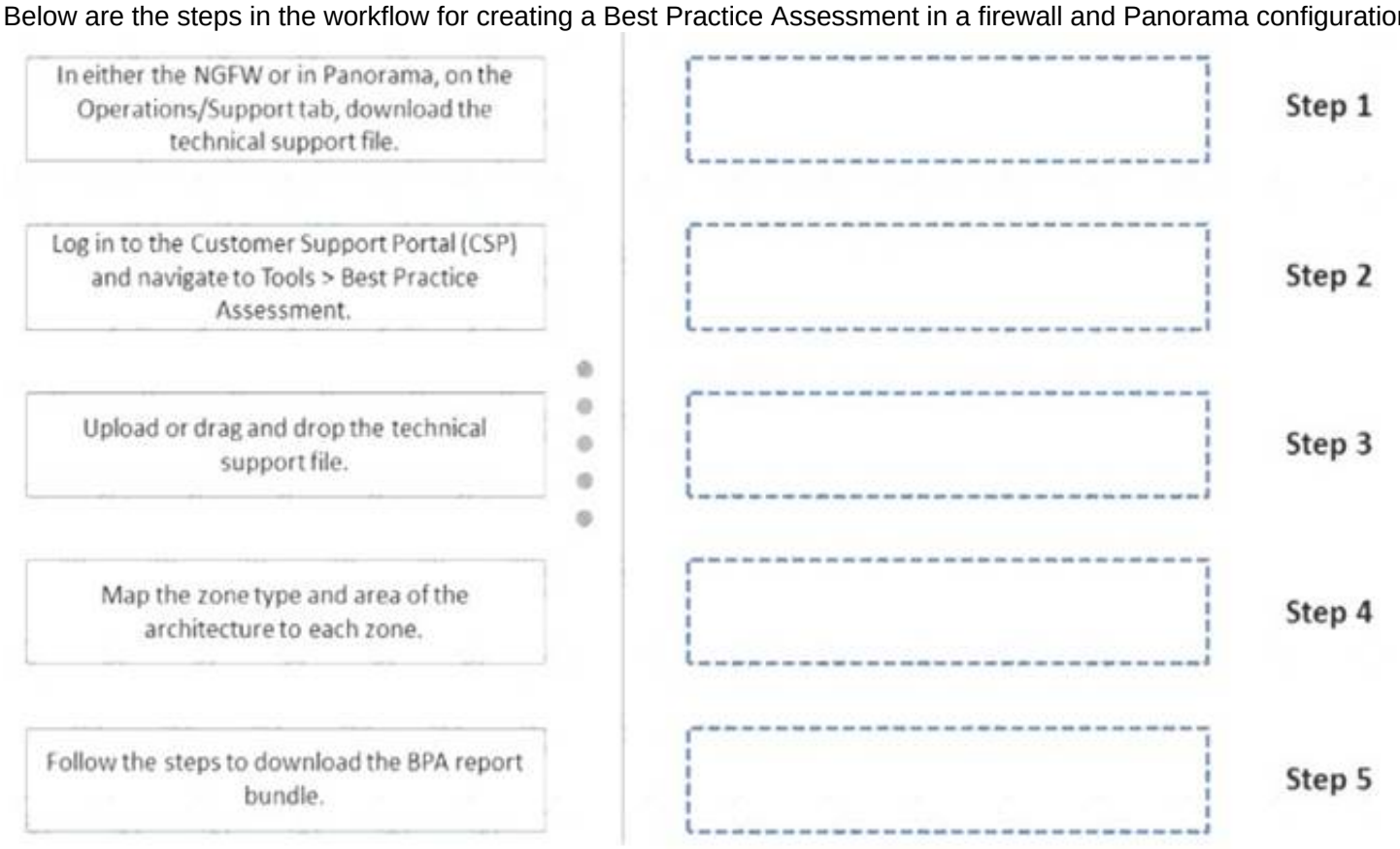
Answer: D

NEW QUESTION 84
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

Answer: B

NEW QUESTION 89
Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1. In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.
Step 2. Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment. Step 3. Upload or drag and drop the technical support file.
Step 4. Map the zone type and area of the architecture to each zone. Step 5.Follow the steps to download the BPA report bundle.

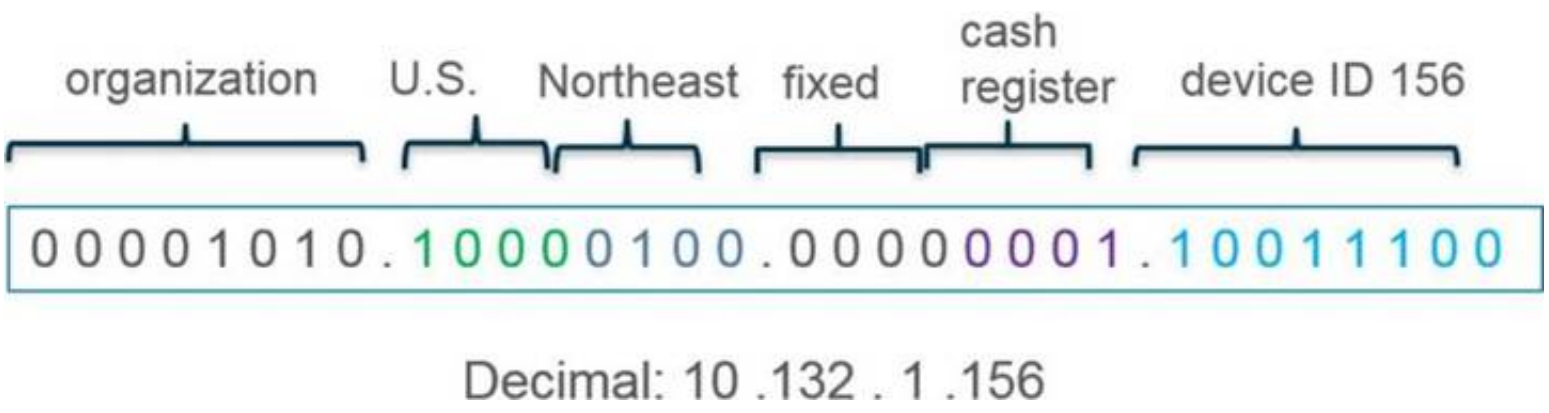
NEW QUESTION 94
The UDP-4501 protocol-port is used between which two GlobalProtect components?

A. GlobalProtect app and GlobalProtect gateway
B. GlobalProtect portal and GlobalProtect gateway
C. GlobalProtect app and GlobalProtect satellite
D. GlobalProtect app and GlobalProtect portal

Answer: A

Explanation:
UDP 4501 Used for IPSec tunnel connections between GlobalProtect apps and gateways. https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/reference-port-number-usag

NEW QUESTION 98
What type of address object would be useful for internal devices where the addressing structure assigns meaning to certain bits in the address, as illustrated in the diagram?



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

Answer: B

NEW QUESTION 101
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>

Answer: B

NEW QUESTION 105
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 108
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 112
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.)

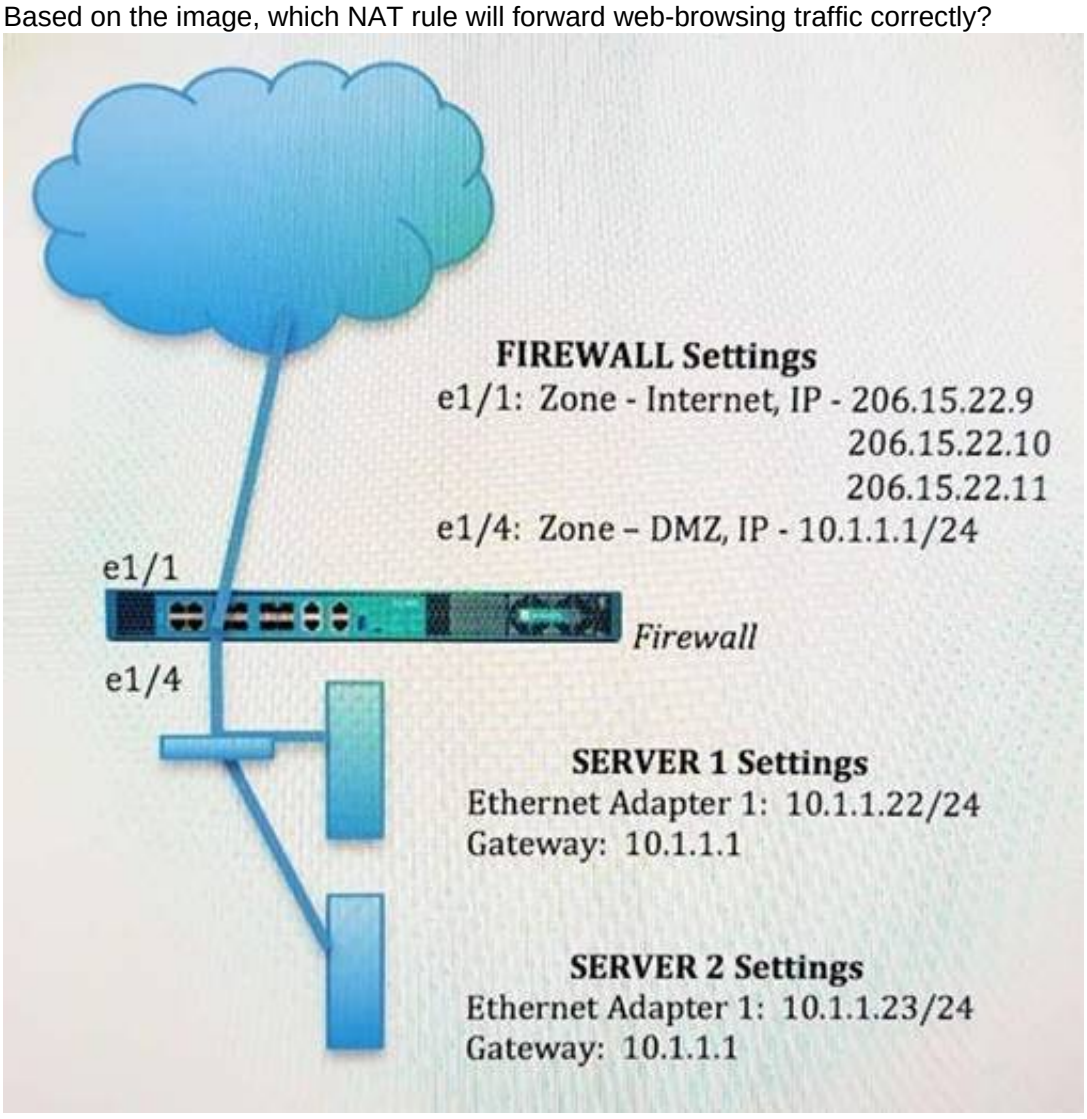
A. Forward Untrust certificate
B. Forward Trust certificate
C. Enterprise Root CA certificate
D. End-entity (leaf) certificate
E. Intermediate certificate(s)

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 116
An administrator wants multiple web servers In the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be

forwarded to the server at 10.1.1.22.
Based on the image, which NAT rule will forward web-browsing traffic correctly?



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

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

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

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

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

Answer: B

NEW QUESTION 119

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.

Answer: B

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."

NEW QUESTION 122
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 123
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 128
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 131
A security engineer received multiple reports of an IPSec VPN tunnel going down the night before. The engineer couldn't find any events related to VPN under system togs.
What is the likely cause?

A. Dead Peer Detection is not enabled.
B. Tunnel Inspection settings are misconfigured.
C. The Tunnel Monitor is not configured.
D. The log quota for GTP and Tunnel needs to be adjusted

Answer: C

Explanation:
This means that the firewall does not have a mechanism to monitor the status of the IPSec VPN tunnel and generate logs when it goes down or up. The Tunnel Monitor is an optional feature that can be enabled on each IPSec tunnel interface and it uses ICMP probes to check the connectivity of the tunnel peer. If the firewall does not receive a response from the peer after a specified number of retries, it marks the tunnel as down and logs an event1.

NEW QUESTION 135
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

Answer: ABE

Explanation:
The three multi-factor authentication methods that can be used to authenticate access to the firewall are One-time Password (OTP), User Certificate, and Fingerprint.
One-time Password (OTP) is a form of two-factor authentication in which a token or code is generated and sent to the user over a secure connection. The user then enters the code to authenticate their access.
User Certificate is a form of two-factor authentication in which the user is required to present a valid certificate in order to access the system. The certificate is usually stored on a physical device, such as a USB drive, and is usually issued by the authentication service provider.
Fingerprint is a form of two-factor authentication in which the user is required to present a valid fingerprint in order to access the system. The fingerprint is usually stored on a physical device, such as a fingerprint reader, and is usually issued by the authentication service provider.

NEW QUESTION 139
Which GlobalProtect component must be configured to enable Clientless VPN?

A. GlobalProtect satellite
B. GlobalProtect app
C. GlobalProtect portal
D. GlobalProtect gateway

Answer: C

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

NEW QUESTION 140
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 141
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.

Answer: D

NEW QUESTION 144
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

Answer: ABC

NEW QUESTION 145
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.

Answer: A

NEW QUESTION 148
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 150
Which two statements correctly describe Session 380280? (Choose two.)

```
> show session id 380280

Session          380280

        c2s flow:
                source:      172.17.149.129 [L3-Trust]
                dst:         104.154.89.105
                proto:       6
                sport:       60997           dport:       443
                state:       ACTIVE          type:        FLOW
                src user:    unknown
                dst user:    unknown

        s2c flow:
                source:      104.154.89.105 [L3-Untrust]
                dst:         10.46.42.149
                proto:       6
                sport:       443             dport:       7260
                state:       ACTIVE          type:        FLOW
                src user:    unknown
                dst user:    unknown

        start time                          : Tue Feb  9 20:38:42 2021
        timeout                             : 15 sec
        time to live                        : 2 sec
        total byte count(c2s)               : 3330
        total byte count(s2c)               : 12698
        layer7 packet count(c2s)            : 14
        layer7 packet count(s2c)            : 19
        vsys                                : vsys1
        application                         : web-browsing
        rule                                : Trust-to-Untrust
        service timeout override(index)     : False
        session to be logged at end         : True
        session in session ager             : True
        session updated by HA peer          : False
        session proxied                     : True
        address/port translation            : source
        nat-rule                            : Trust-NAT(vsys1)
        layer7 processing                   : completed
        URL filtering enabled               : True
        URL category                        : computer-and-internet-info, low-risk
        session via syn-cookies             : False
        session terminated on host          : False
        session traverses tunnel            : False
        session terminate tunnel            : False
        captive portal session              : False
        ingress interface                   : ethernet1/6
        egress interface                    : ethernet1/3
        session QoS rule                    : N/A (class 4)
        tracker stage l7proc                : proxy timer expired
        end-reason                          : unknown
```

A. The session went through SSL decryption processing.
B. The session has ended with the end-reason unknown.
C. The application has been identified as web-browsing.
D. The session did not go through SSL decryption processing.

Answer: AC

NEW QUESTION 153
Which GlobalProtect component must be configured to enable Clientless VPN?

A. GlobalProtect satellite
B. GlobalProtect app
C. GlobalProtect portal
D. GlobalProtect gateway

Answer: C

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

NEW QUESTION 155
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.

Answer: C

NEW QUESTION 157
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

Answer: B

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 gatewa2y. This allows you to specify which domains and applications are included or excluded from the VPN tunnel.

NEW QUESTION 160
What is a correct statement regarding administrative authentication using external services with a local authorization method?

A. Prior to PAN-OS 10.2. an administrator used the firewall to manage role assignments, but access domains have not been supported by this method.
B. Starting with PAN-OS 10.2. an administrator needs to configure Cloud Identity Engine to use external authentication services for administrative authentication.
C. The administrative accounts you define locally on the firewall serve as references to the accounts defined on an external authentication server.
D. The administrative accounts you define on an external authentication server serve as references to the accounts defined locally on the firewall.

Answer: B

NEW QUESTION 165
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 169
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'

Answer: C

Explanation:
https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices/best-practice-internet-gate "Enable extended-capture for critical, high, and medium severity events and single-packet capture for low severity events. "
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-vulner

NEW QUESTION 173
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.

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/

NEW QUESTION 176
A client wants to detect the use of weak and manufacturer-default passwords for IoT devices. Which option will help the customer?

A. Configure a Data Filtering profile with alert mode.
B. Configure an Antivirus profile with alert mode.
C. Configure a Vulnerability Protection profile with alert mode
D. Configure an Anti-Spyware profile with alert mode.

Answer: C

NEW QUESTION 177
Which profile generates a packet threat type found in threat logs?

A. Zone Protection
B. WildFire
C. Anti-Spyware
D. Antivirus

Answer: A

NEW QUESTION 179
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 182
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

Answer: B

Explanation:
https://docs.paloaltonetworks.com/compatibility-matrix/user-id-agent/which-servers-can-the-user-id-agent-moni

NEW QUESTION 187
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 190
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 191
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

Answer: D

NEW QUESTION 194
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 198
Which three use cases are valid reasons for requiring an Active/Active high availability deployment? (Choose three.)

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

Answer: BCD

NEW QUESTION 200
A firewall administrator wants to avoid overflowing the company syslog server with traffic logs. What should the administrator do to prevent the forwarding of DNS traffic logs to syslog?

A. Disable logging on security rules allowing DNS.
B. Go to the Log Forwarding profile used to forward traffic logs to syslo
C. Then, under traffic logs match list, create a new filter with application not equal to DNS.
D. Create a security rule to deny DNS traffic with the syslog server in the destination
E. Go to the Log Forwarding profile used to forward traffic logs to syslo
F. Then, under traffic logs match list, create a new filter with application equal to DNS.

Answer: D

NEW QUESTION 201
A network security administrator wants to begin inspecting bulk user HTTPS traffic flows egressing out of the internet edge firewall. Which certificate is the best choice to configure as an SSL Forward Trust 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

Answer: A

NEW QUESTION 202
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 processor-intensive decryption methods for lower-risk traffic
B. Use PFS in a Decryption profile for higher-priority and higher-risk traffic, and use lessprocessor-intensive 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

Answer: B

NEW QUESTION 206
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 209
A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?

A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096 in the "Tag Allowed" field of the V-Wire object.
B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the Tag Allowed" field of the V-Wire objec
C. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffi
D. Assign each interface/sub interface to a unique zone.
E. Create Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router.The physical Layer 3 interface would handle untagged traffi
F. Assign each interface/subinterface t
G. unique zon
H. Do not assign any interface an IP address.
I. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN I
J. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffi
K. Assign each interface/sub interface to a unique zone.

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfa Virtual wire interfaces by default allow all untagged traffic. You can, however, use a virtual wire to connect two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags. VLAN tag 0 indicates untagged traffic.You can also create multiple subinterfaces, add them into different zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.

NEW QUESTION 212
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 216
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 218
In a Panorama template which three types of objects are configurable? (Choose three)

A. certificate profiles
B. HIP objects
C. QoS profiles
D. security profiles
E. interface management profiles

Answer: ACE

Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewall

NEW QUESTION 220
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.

Answer: B

Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/use-case-configure-firewa

NEW QUESTION 224
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 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 229
WildFire will submit for analysis blocked files that match which profile settings?

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

Answer: C

NEW QUESTION 230
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 232
An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Path Monitoring has been enabled with a Failure Condition of "any." A path group is configured with Failure Condition of "all" and contains a destination IP of 8.8.8.8 and 4.2.2.2 with a Ping Interval of 500ms and a Ping count of 3.
Which scenario will cause the Active firewall to fail over?

A. IP address 8.8.8.8 is unreachable for 1 second.
B. IP addresses 8.8.8.8 and 4.2.2.2 are unreachable for 1 second.
C. IP addresses 8.8.8.8 and 4.2.2.2 are unreachable for 2 seconds
D. IP address 4.2.2.2 is unreachable for 2 seconds.

Answer: C

NEW QUESTION 235
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

Answer: BC

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administra

NEW QUESTION 237
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 241
The firewall identifies a popular application as an unKnown-tcp.
Which two options are available to identify the application? (Choose two.)

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

Answer: AB

NEW QUESTION 243
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
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

PCNSE Practice Exam Features:

* PCNSE Questions and Answers Updated Frequently

* PCNSE Practice Questions Verified by Expert Senior Certified Staff

* PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year