Paloalto-Networks

Exam Questions PCNSE

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

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

A. The IP-address and corresponding server type (Microsoft Active Directory or Microsoft Exchange) for each of the six servers
B. Network 192 168.28.32/28 with server type Microsoft Active Directory and network 192.168.28.48/28 with server type Microsoft Exchange
C. Network 192 168 28.32/27 with server type Microsoft
D. One IP address of a Microsoft Active Directory server and "Auto Discover" enabled to automatically obtain all five of the other servers

Answer: A

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

NEW QUESTION 4
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 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
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 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 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 9
A company with already deployed Palo Alto firewalls has purchased their first Panorama server. The security team has already configured all firewalls with the Panorama IP address and added all the firewall serial numbers in Panorama. What are the next steps to migrate configuration from the firewalls to Panorama?

A. Use API calls to retrieve the configuration directly from the managed devices
B. Export Named Configuration Snapshot on each firewall followed by Import Named Configuration Snapshot in Panorama
C. import Device Configuration to Panorama followed by Export or Push Device Config Bundle
D. Use the Firewall Migration plugin to retrieve the configuration directly from the managed devices

Answer: C

NEW QUESTION 10
When using SSH keys for CLI authentication for firewall administration, which method is used for authorization?

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

Answer: A

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

NEW QUESTION 10
An engineer is creating a template and wants to use variables to standardize the configuration across a large number of devices Which Mo variable types can be defined? (Choose two.)

A. Path group

B. Zone
C. IP netmask
D. FQDN

Answer: CD

NEW QUESTION 14
An engineer needs to permit XML API access to a firewall for automation on a network segment that is routed through a Layer 3 subinterface on a Palo Alto Networks firewall. However, this network segment cannot access the dedicated management interface due to the Security policy.
Without changing the existing access to the management interface, how can the engineer fulfill this request?

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

Answer: B

NEW QUESTION 18
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 22
A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours.
Which two steps are likely to mitigate the issue? (Choose TWO)

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

Answer: AC

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

NEW QUESTION 27
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 30
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 31
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 36
An engineer is tasked with configuring a Zone Protection profile on the untrust zone. Which three settings can be configured on a Zone Protection profile? (Choose three.)

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

Answer: BCD

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

NEW QUESTION 38
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 41
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 43
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 45
An organization is interested in migrating from their existing web proxy architecture to the Web Proxy feature of their PAN-OS 11.0 firewalls. Currently. HTTP and SSL requests contain the c IP address of the web server and the client browser is redirected to the proxy
Which PAN-OS proxy method should be configured to maintain this type of traffic flow?

A. DNS proxy
B. Explicit proxy

C. SSL forward proxy
D. Transparent proxy

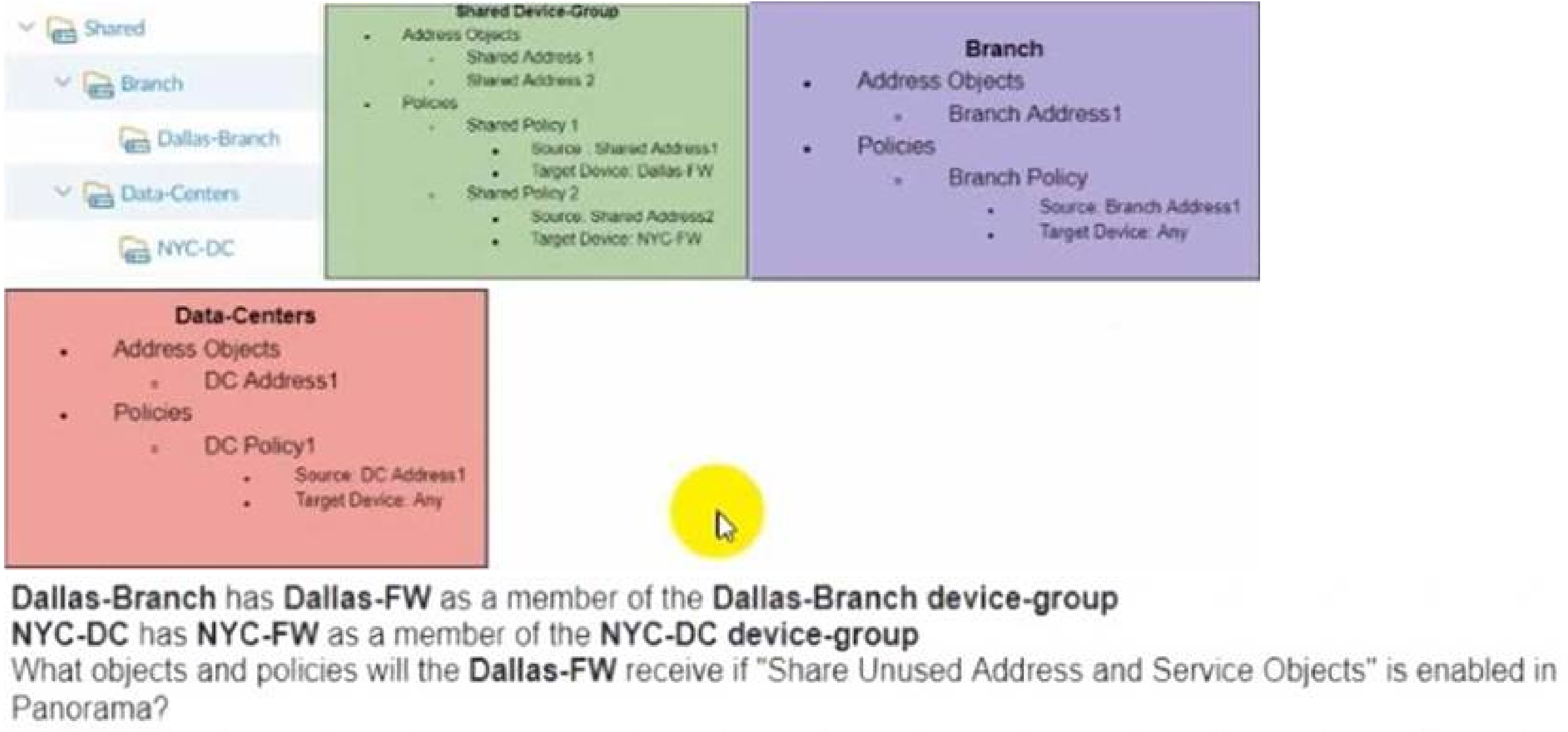
Answer: D

Explanation:
A transparent proxy is a type of web proxy that intercepts and redirects HTTP and HTTPS requests without requiring any configuration on the client browser1. The firewall acts as a gateway between the client and the web server, and performs security checks on the traffic.
A transparent proxy can be configured on PAN-OS 11.0 firewalls by performing the following steps1:

- Enable Web Proxy under Device > Setup > Services
- Select Transparent Proxy as the Proxy Type
- Configure a Service Route for Web Proxy
- Configure SSL/TLS Service Profile for Web Proxy
- Configure Security Policy Rules for Web Proxy Traffic

By configuring a transparent proxy on PAN-OS 11.0 firewalls, an organization can migrate from their existing web proxy architecture without changing their network topology or client settings2. The firewall will maintain the same type of traffic flow as before, where HTTP and HTTPS requests contain the IP address of the web server and the client browser is redirected to the proxy1.
Answer A is not correct because DNS proxy is a type of web proxy that intercepts DNS queries from clients and resolves them using an external DNS server3. This type of proxy does not redirect HTTP or HTTPS requests to the firewall.

NEW QUESTION 46
The following objects and policies are defined in a device group hierarchy



- Shared
  - Branch
    - Dallas-Branch
  - Data-Centers
    - NYC-DC

Shared Device-Group

- Address Objects
  - Shared Address 1
  - Shared Address 2
- Policies
  - Shared Policy 1
    - Source : Shared Address1
    - Target Device: Dallas-FW
  - Shared Policy 2
    - Source: Shared Address2
    - Target Device: NYC-FW

Branch

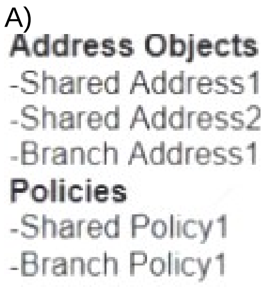
- Address Objects
  - Branch Address1
- Policies
  - Branch Policy
    - Source: Branch Address1
    - Target Device: Any

Data-Centers

- Address Objects
  - DC Address1
- Policies
  - DC Policy1
    - Source: DC Address1
    - Target Device: Any

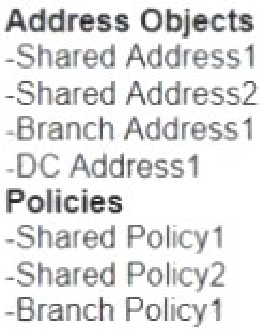
Dallas-Branch has **Dallas-FW** as a member of the **Dallas-Branch device-group**
NYC-DC has **NYC-FW** as a member of the **NYC-DC device-group**
What objects and policies will the **Dallas-FW** receive if "Share Unused Address and Service Objects" is enabled in Panorama?

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

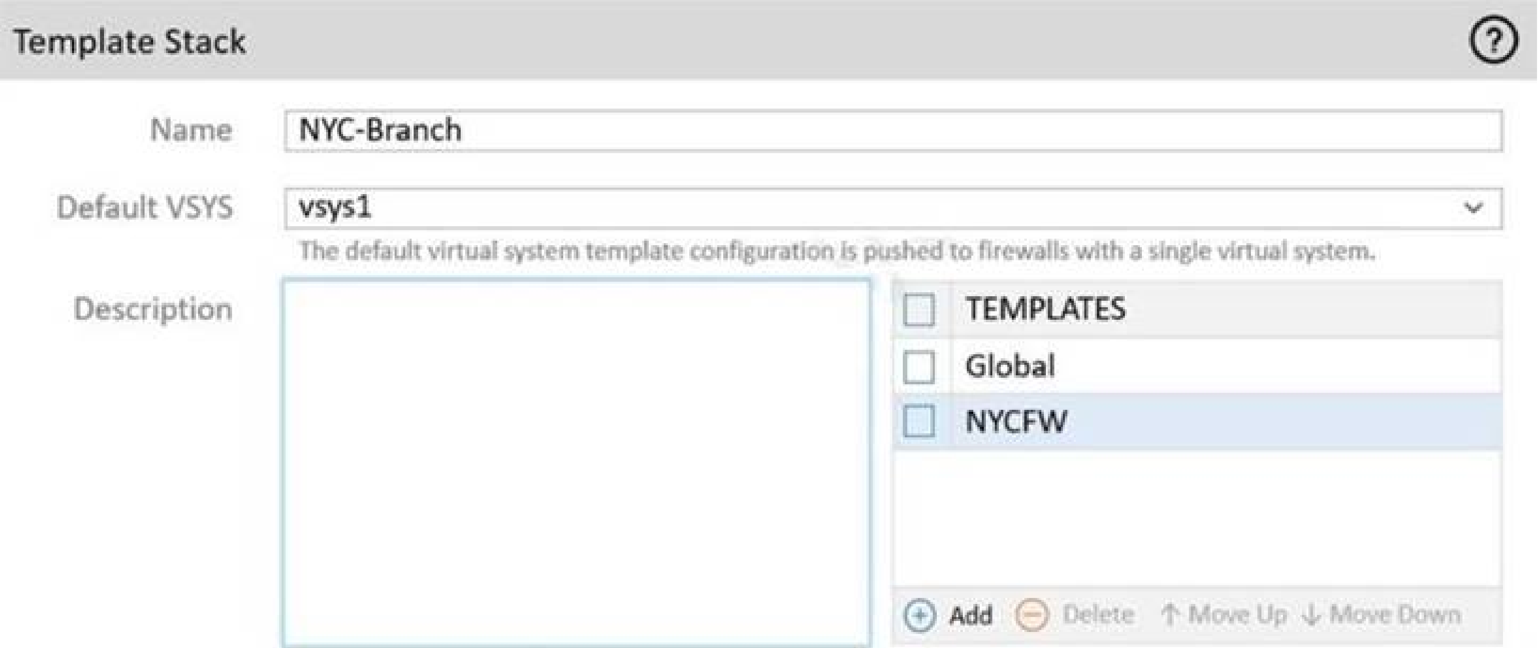
Answer: A

NEW QUESTION 49
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 51
Refer to the image.



Template Stack

Name: NYC-Branch

Default VSYS: vsys1

The default virtual system template configuration is pushed to firewalls with a single virtual system.

Description

□	TEMPLATES
□	Global
□	NYCFW

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

A. Override the value on the NYCFW template.
B. Override a template value using a template stack variable.
C. Override the value on the Global template.
D. Enable "objects defined in ancestors will take higher precedence" under Panorama settings.

Answer: B

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

NEW QUESTION 53
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 57
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 58
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 63
The decision to upgrade to PAN-OS 10.2 has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when trying to install.
When performing an upgrade on Panorama to PAN-OS 10.2, what is the potential cause of a failed install?

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

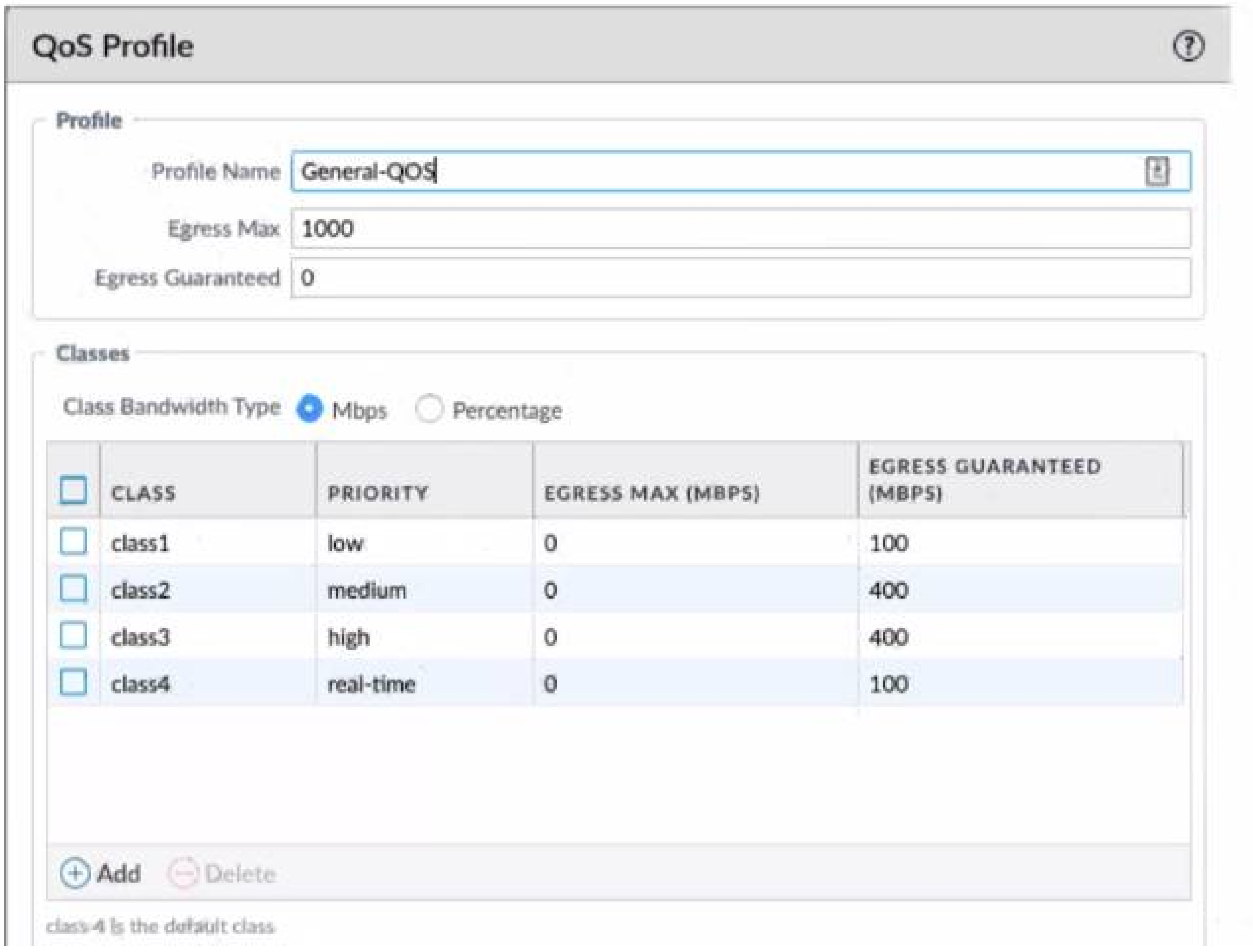
Answer: A

NEW QUESTION 68
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 69
View the screenshots.



QoS Profile

Profile

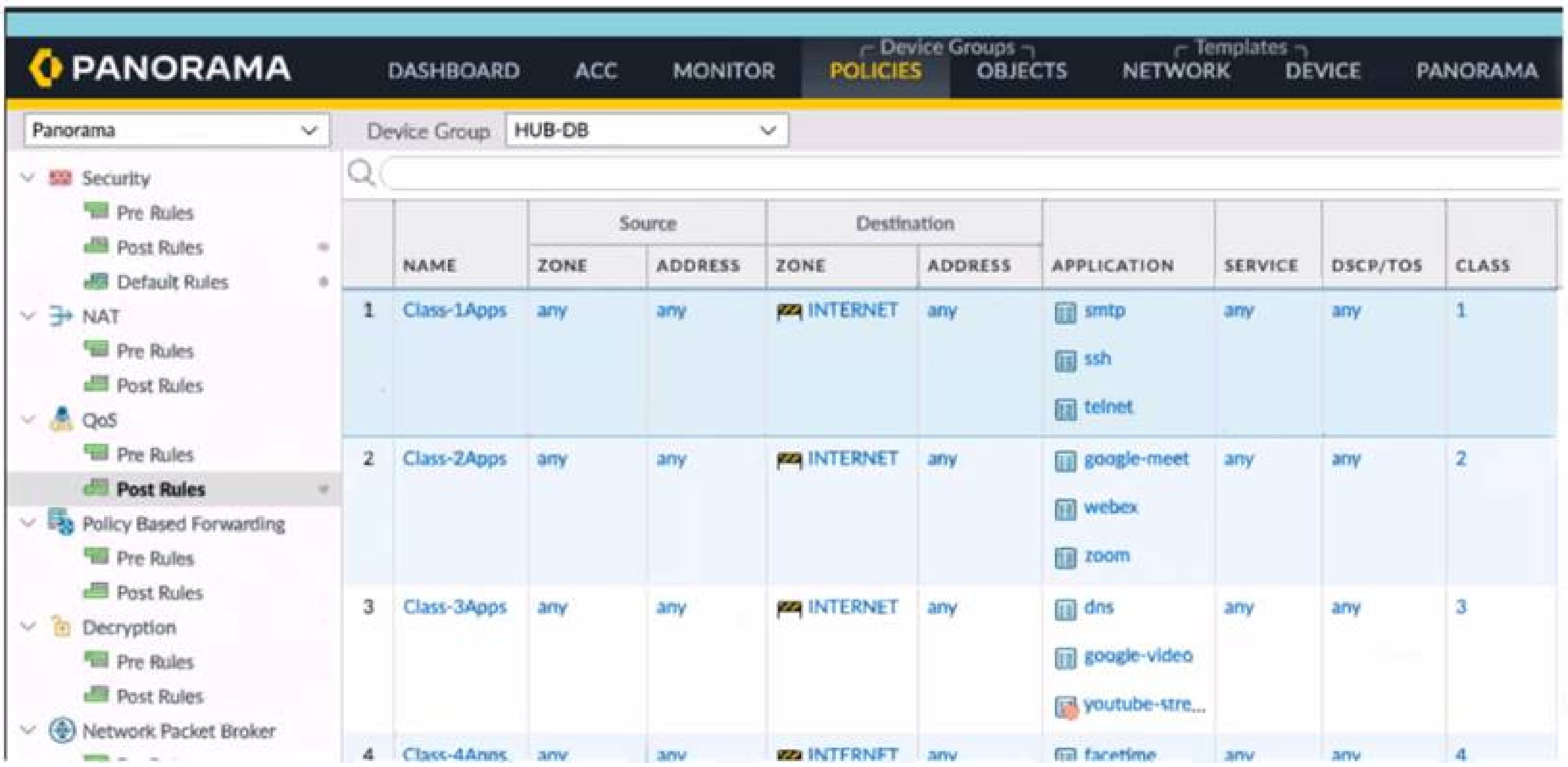
Profile Name: General-QOS
Egress Max: 1000
Egress Guaranteed: 0

Classes

Class Bandwidth Type ● Mbps ○ Percentage

□	CLASS	PRIORITY	EGRESS MAX (MBPS)	EGRESS GUARANTEED (MBPS)
□	class1	low	0	100
□	class2	medium	0	400
□	class3	high	0	400
□	class4	real-time	0	100

class 4 is the default class



		Source		Destination					
	NAME	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	DSCP/TOS	CLASS
1	Class-1Apps	any	any	INTERNET	any	smtp ssh telnet	any	any	1
2	Class-2Apps	any	any	INTERNET	any	google-meet webex zoom	any	any	2
3	Class-3Apps	any	any	INTERNET	any	dns google-video youtube-stre...	any	any	3
4	Class-4Apps	any	any	INTERNET	any	facetime	any	any	4

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 70
Cortex XDR notifies an administrator about grayware on the endpoints. There are no entries about grayware in any of the logs of the corresponding firewall. Which setting can the administrator configure on the firewall to log grayware verdicts?

A. within the log forwarding profile attached to the Security policy rule
B. within the log settings option in the Device tab
C. in WildFire General Settings, select "Report Grayware Files"
D. in Threat General Settings, select "Report Grayware Files"

Answer: C

NEW QUESTION 73
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 77
An engineer has been tasked with reviewing traffic logs to find applications the firewall is unable to identify with App-ID. Why would the application field display as incomplete?

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

Answer: C

NEW QUESTION 78
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 83
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 86
An engineer decides to use Panorama to upgrade devices to PAN-OS 10.2. Which three platforms support PAN-OS 10 2? (Choose three.)

A. PA-5000 Series
B. PA-500
C. PA-800 Series
D. PA-220
E. PA-3400 Series

Answer: CDE

Explanation:
According to the Palo Alto Networks Compatibility Matrix1, the three platforms that support PAN-OS 10.2 are:

- PA-800 Series2
- PA-2202
- PA-3400 Series2

The PA-5000 Series and PA-500 do not support PAN-OS 10.22.
To upgrade devices to PAN-OS 10.2 using Panorama, you need to determine the upgrade path3, upgrade Panorama itself4, and then upgrade the firewalls using Panorama5.

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 93
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

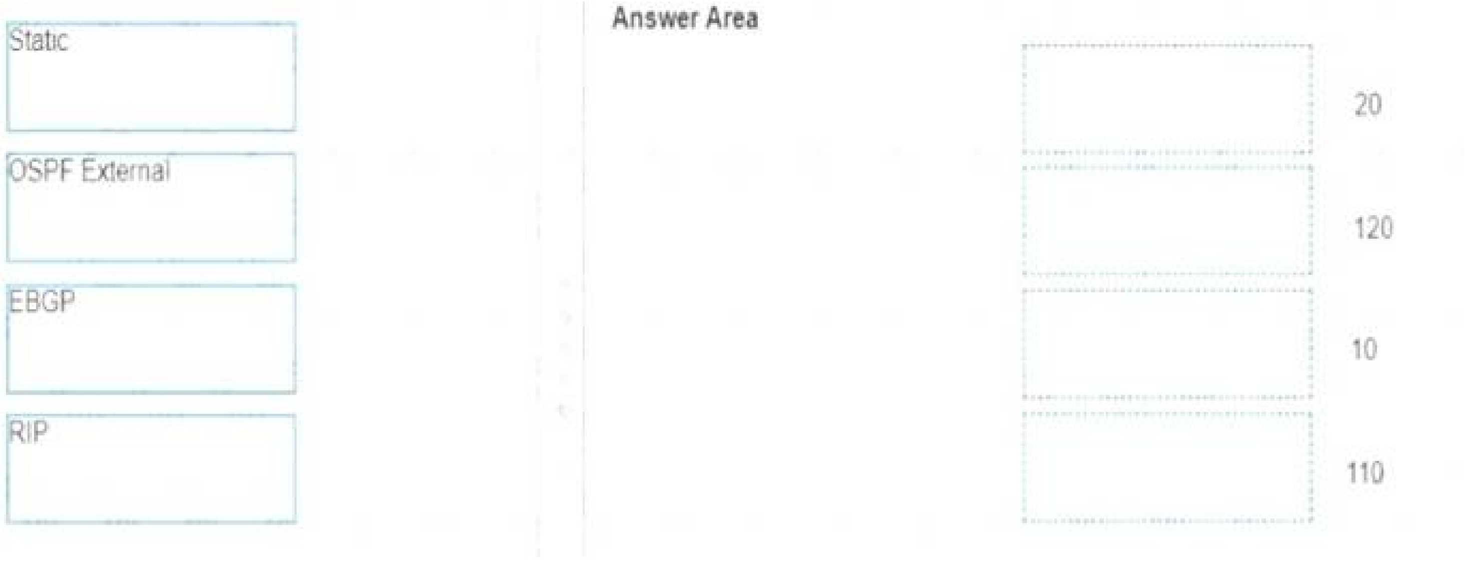
NEW QUESTION 98
A firewall administrator requires an A/P HA pair to fail over more quickly due to critical business application uptime requirements.
What is the correct setting?

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

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activepassive-ha/configure In an A/P HA pair, HA (High Availability) timers are used to determine how quickly the firewall should fail over in case of a failure. Typically, the firewall administrator can choose between several predefined timer profiles such as "normal", "aggressive", and "fast".
Changing the HA timer profile to "user-defined" and manually setting the timers would allow the administrator to fine-tune the failover timing and make sure it meets the uptime requirements for the critical business applications. This approach allows the administrator to set the timers to the lowest possible value without compromising the stability and security of the firewall.

NEW QUESTION 102
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 104

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

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

Answer: A

Explanation:
To configure LDAP authentication on Panorama, you need to23:

- Define an LDAP server profile that specifies the connection details and credentials for accessing the LDAP server.
- Define an authentication profile that references the LDAP server profile and defines how users authenticate to Panorama (such as username format and password expiration).
- Define an authentication sequence (optional) that allows users to authenticate using multiple methods (such as local database, LDAP, RADIUS, etc.).
- Assign the authentication profile or sequence to a Panorama administrator role or a device group role

NEW QUESTION 107
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 111
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 112
What can be used to create dynamic address groups?

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

Answer: C

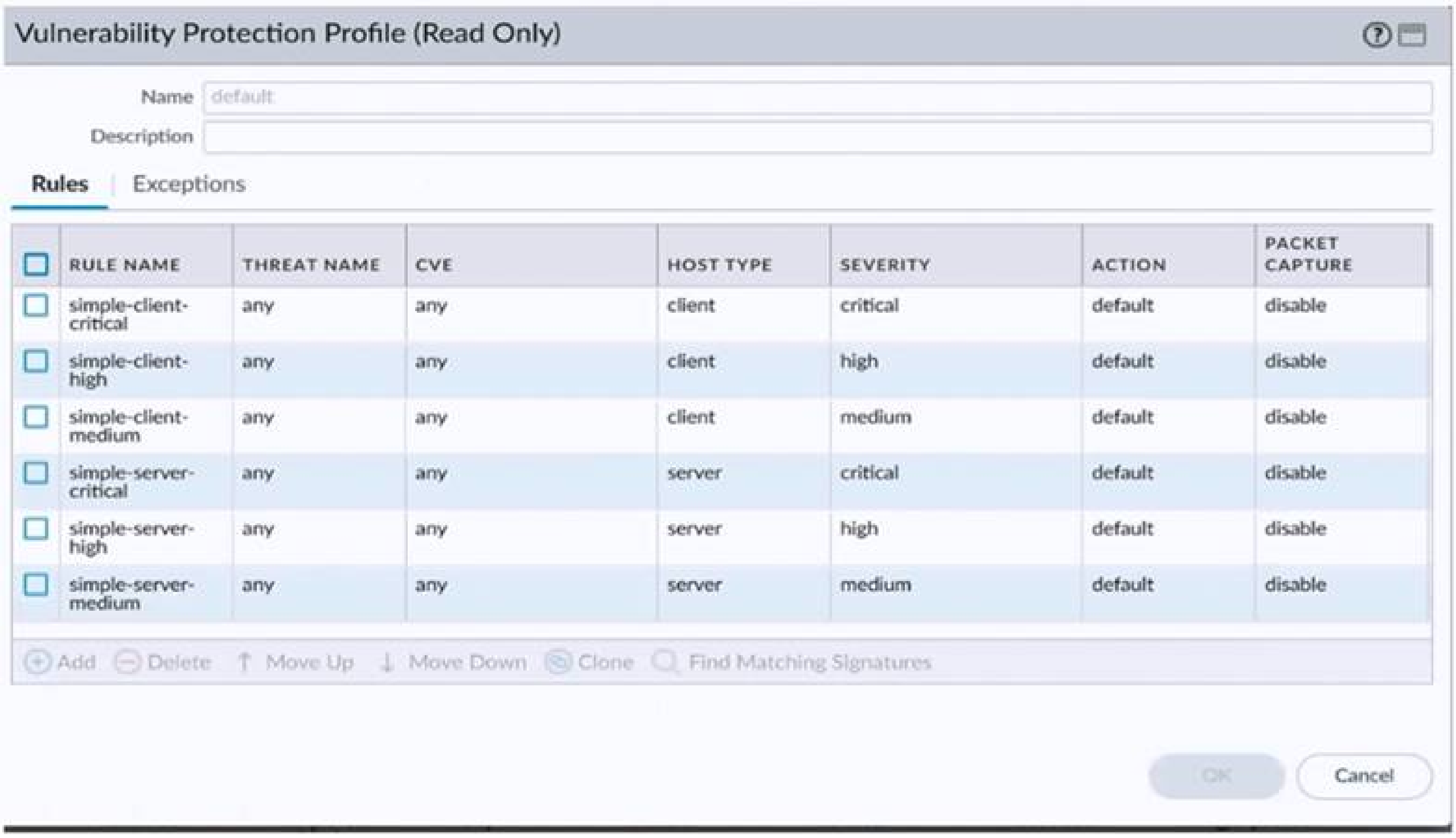
NEW QUESTION 114
Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

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 117
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?



Vulnerability Protection Profile (Read Only)

Name: default

Description:

Rules | Exceptions

□	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
□	simple-client-critical	any	any	client	critical	default	disable
□	simple-client-high	any	any	client	high	default	disable
□	simple-client-medium	any	any	client	medium	default	disable
□	simple-server-critical	any	any	server	critical	default	disable
□	simple-server-high	any	any	server	high	default	disable
□	simple-server-medium	any	any	server	medium	default	disable

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

Answer: A

NEW QUESTION 122
An administrator is receiving complaints about application performance degradation. After checking the ACC. the administrator observes that there Is an excessive amount of SSL traffic
Which three elements should the administrator configure to address this issue? (Choose three.)

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

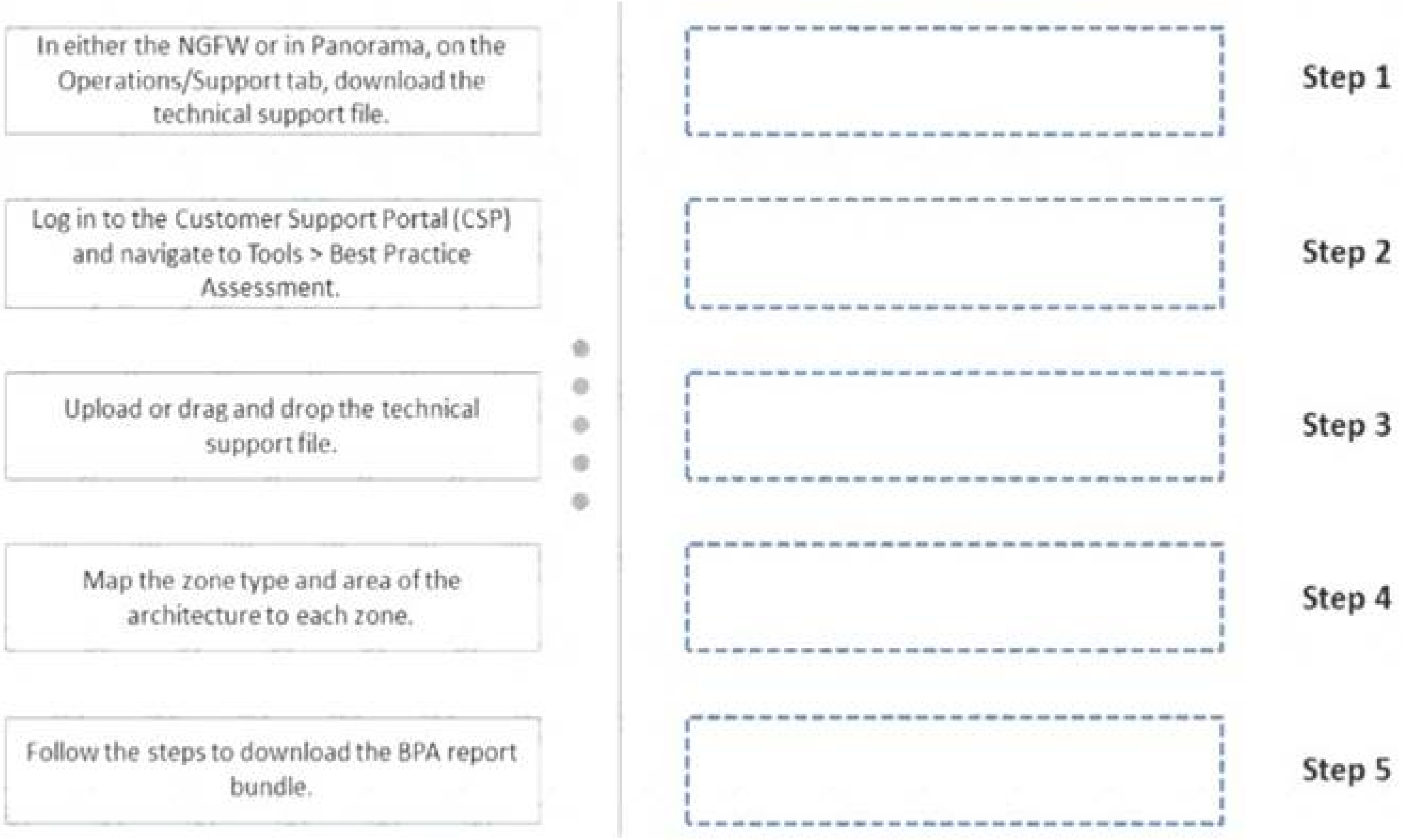
Answer: BCD

NEW QUESTION 125
Which statement is correct given the following message from the PanGPA log on the GlobalProtect app? Failed to connect to server at port:47 67

A. The PanGPS process failed to connect to the PanGPA process on port 4767
B. The GlobalProtect app failed to connect to the GlobalProtect Portal on port 4767
C. The PanGPA process failed to connect to the PanGPS process on port 4767
D. The GlobalProtect app failed to connect to the GlobalProtect Gateway on port 4767

Answer: D

NEW QUESTION 127
Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.



In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.

Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.

Upload or drag and drop the technical support file.

Map the zone type and area of the architecture to each zone.

Follow the steps to download the BPA report bundle.

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 128
An engineer has discovered that certain real-time traffic is being treated as best effort due to it exceeding defined bandwidth Which QoS setting should the engineer adjust?

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

Answer: C

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

NEW QUESTION 130
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 133
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 138
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 139
An administrator allocates bandwidth to a Prisma Access Remote Networks compute location with three remote networks.
What is the minimum amount of bandwidth the administrator could configure at the compute location?

A. 90Mbps
B. 300 Mbps
C. 75Mbps
D. 50Mbps

Answer: D

Explanation:
The number you specify for the bandwidth applies to both the egress and ingress traffic for the remote network connection. If you specify a bandwidth of 50 Mbps, Prisma Access provides you with a remote network connection with 50 Mbps of bandwidth on ingress and 50 Mbps on egress. Your bandwidth speeds can go up to 10% over the specified amount without traffic being dropped; for a 50 Mbps connection, the maximum bandwidth allocation is 55 Mbps on ingress and 55 Mbps on egress (50 Mbps plus 10% overage allocation).
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-for-netw

NEW QUESTION 144
Where can an administrator see both the management-plane and data-plane CPU utilization in the WebUI?

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

Answer: A

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

NEW QUESTION 145
What is the function of a service route?

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

Answer: C

NEW QUESTION 148
A prospect is eager to conduct a Security Lifecycle Review (SLR) with the aid of the Palo Alto Networks NGFW.
Which interface type is best suited to provide the raw data for an SLR from the network in a way that is minimally invasive?

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

Answer: C

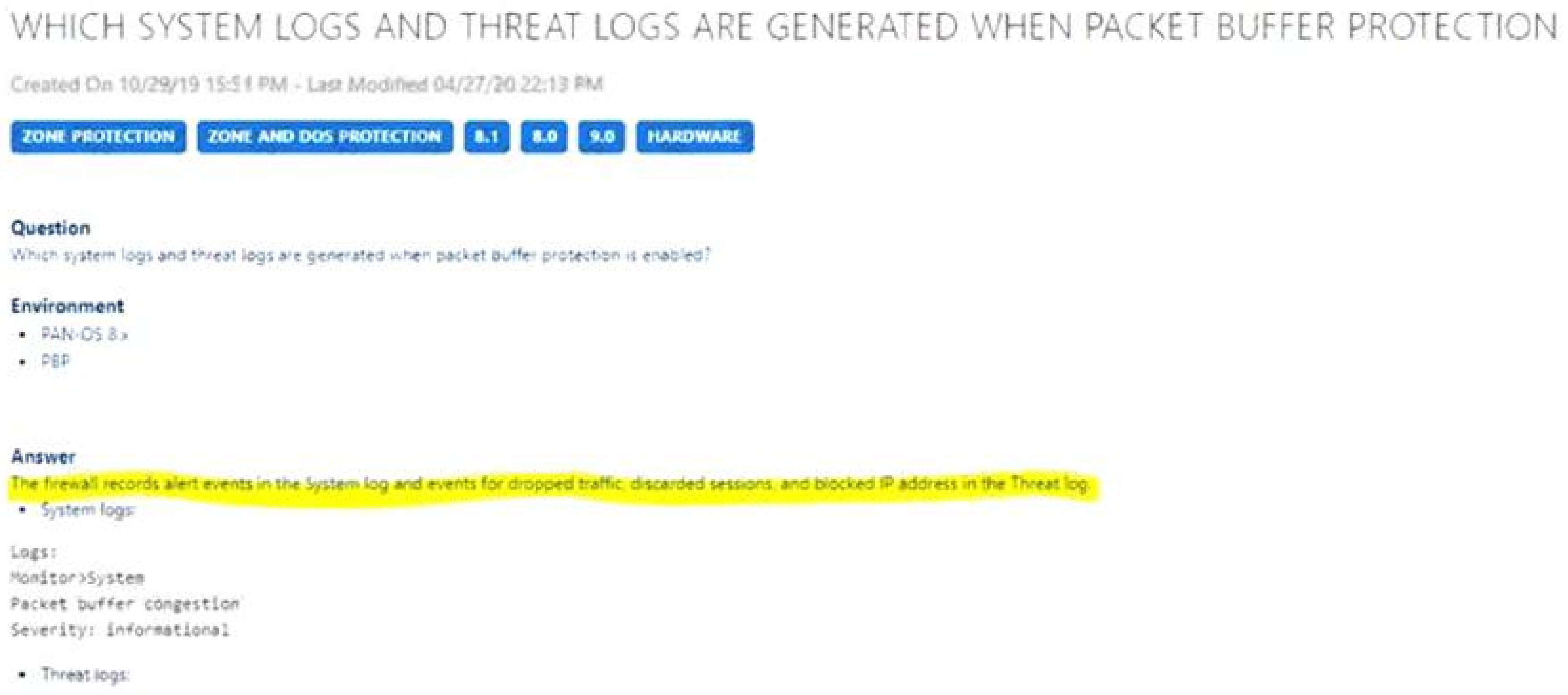
NEW QUESTION 153
Where is information about packet buffer protection logged?

A. Alert entries are in the Alarms lo

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

Answer: D

Explanation:
Graphical user interface, text, application Description automatically generated



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

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

ZONE PROTECTION | ZONE AND DOS PROTECTION | 8.1 | 8.0 | 9.0 | HARDWARE

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

Environment
- PAN-OS 8.x
- PBP

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

```
Logs:
Monitor>System
Packet buffer congestion
Severity: informational
```

- Threat logs:

NEW QUESTION 156
What is the best definition of the Heartbeat Interval?

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

Answer: A

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

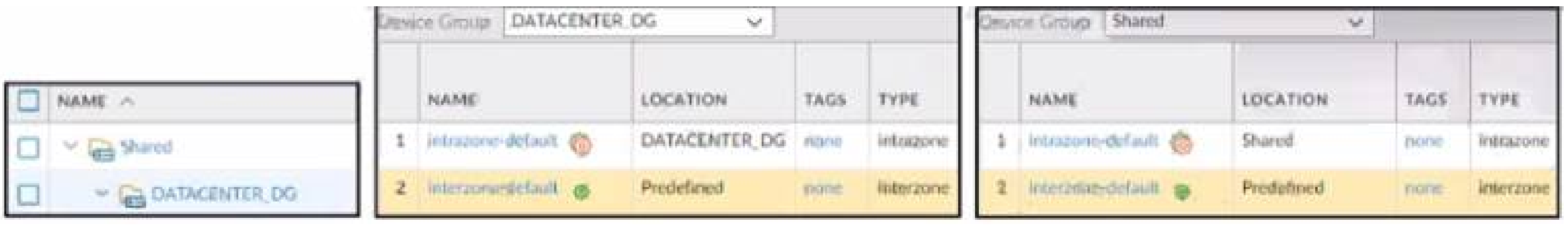
NEW QUESTION 159
A security engineer received multiple reports of an IPSec VPN tunnel going down the night before. The engineer couldn't find any events related to VPN under system togs.
What is the likely cause?

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 161
Refer to the exhibit.



□	NAME ^
□	Shared
□	DATACENTER_DG

Device Group: DATACENTER_DG

	NAME	LOCATION	TAGS	TYPE
1	intrazone-default	DATACENTER_DG	none	intrazone
2	interzone-default	Predefined	none	interzone

Device Group: Shared

	NAME	LOCATION	TAGS	TYPE
1	intrazone-default	Shared	none	intrazone
2	interzone-default	Predefined	none	interzone

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 164
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 167
Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

A. PAN-OS integrated User-ID agent
B. GlobalProtect
C. Windows-based User-ID agent
D. LDAP Server Profile configuration

Answer: B

NEW QUESTION 172
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 174
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 179
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 181
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 182
An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Link and Path Monitoring Is enabled with the Failure Condition set to "any." There is one link group configured containing member interfaces ethernet1/1 and ethernet1/2 with a Group Failure Condition set to "all."
Which HA state will the Active firewall go into if ethernet1/1 link goes down due to a failure?

A. Non-functional
B. Passive
C. Active-Secondary
D. Active

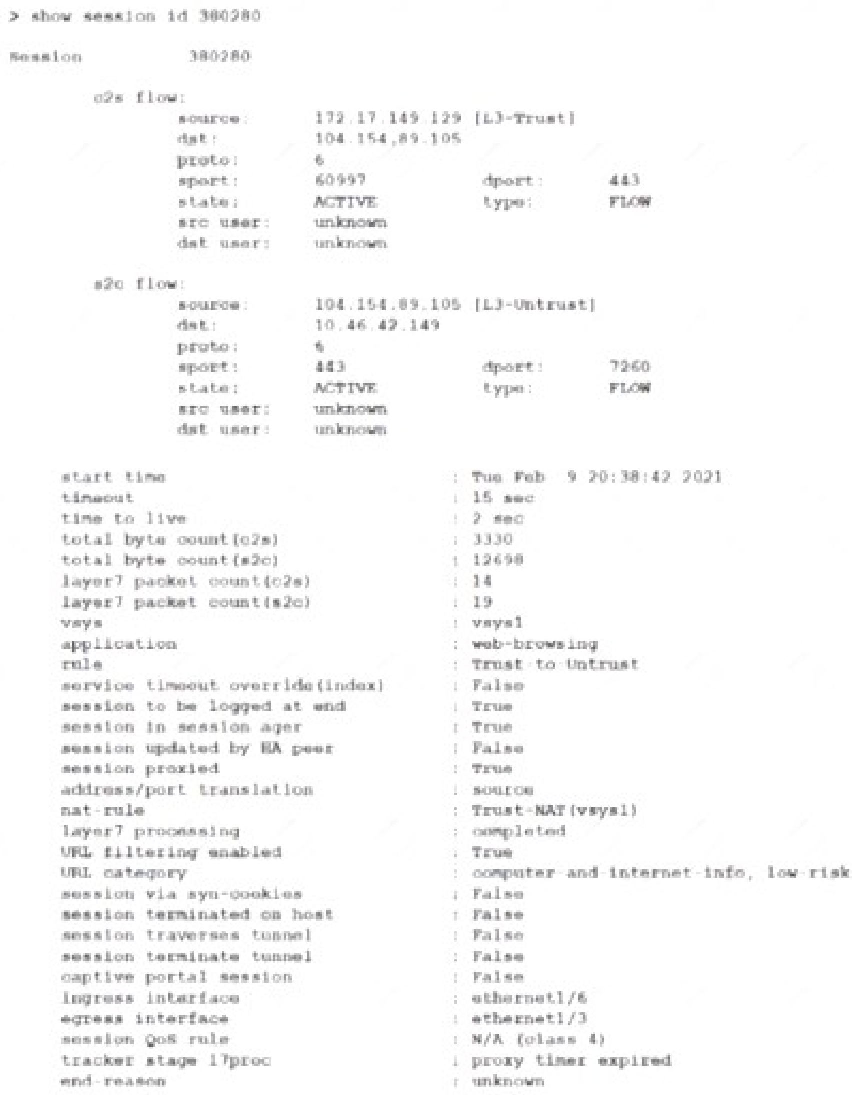
Answer: D

NEW QUESTION 186
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 188
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 191
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 192
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 194
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 198
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 202
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 204
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 205
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 210
A client wants to detect the use of weak and manufacturer-default passwords for loT 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 215
What happens, by default, when the GlobalProtect app fails to establish an IPSec tunnel to the GlobalProtect gateway?

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

Answer: A

NEW QUESTION 219
An administrator is attempting to create policies tor deployment of a device group and template stack. When creating the policies, the zone drop down list does not include the required zone.
What must the administrator do to correct this issue?

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

Answer: D

NEW QUESTION 220
What is the best description of the HA4 Keep-Alive Threshold (ms)?

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

Answer: C

NEW QUESTION 221
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 223
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 226
A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)

A. Virtual router
B. Security zone
C. ARP entries
D. Netflow Profile

Answer: AB

NEW QUESTION 229
You have upgraded your Panorama and Log Collectors lo 10.2 x. Before upgrading your firewalls using Panorama, what do you need do?

A. Refresh your licenses with Palo Alto Network Support - Panorama/Licenses/Retrieve License Keys from License Server.
B. Re-associate the firewalls in Panorama/Managed Devices/Summary.
C. Commit and Push the configurations to the firewalls.
D. Refresh the Mastor Key in Panorama/Master Key and Diagnostic

Answer: C

NEW QUESTION 234
In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)

A. wildcard server certificate
B. enterprise CA certificate
C. client certificate
D. server certificate
E. self-signed CA certificate

Answer: BE

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

NEW QUESTION 237
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 241
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 246

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 251
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 252
Which Panorama feature protects logs against data loss if a Panorama server fails?

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

Answer: A

NEW QUESTION 255
An administrator has configured PAN-OS SD-WAN and has received a request to find out the reason for a session failover for a session that has already ended Where would you find this in Panorama or firewall logs?

A. Traffic Logs
B. System Logs
C. Session Browser
D. You cannot find failover details on closed sessions

Answer: D

NEW QUESTION 260
A firewall administrator notices that many Host Sweep scan attacks are being allowed through the firewall sourced from the outside zone. What should the firewall administrator do to mitigate this type of attack?

A. Create a DOS Protection profile with SYN Flood protection enabled and apply it to all rules allowing traffic from the outside zone
B. Enable packet buffer protection in the outside zone.
C. Create a Security rule to deny all ICMP traffic from the outside zone.
D. Create a Zone Protection profile, enable reconnaissance protection, set action to Block, and apply it to the outside zone.

Answer: D

NEW QUESTION 264
What is considered the best practice with regards to zone protection?

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

Answer: C

NEW QUESTION 266
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 269
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 273
An engineer wants to implement the Palo Alto Networks firewall in VWire mode on the internet gateway and wants to be sure of the functions that are supported on the vwire interface
What are three supported functions on the VWire interface? (Choose three)

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

Answer: ABE

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

NEW QUESTION 275
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 279
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 281
Which feature checks Panorama connectivity status after a commit?

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

Answer: A

NEW QUESTION 286
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 287
While analyzing the Traffic log, you see that some entries show "unknown-tcp" in the Application column What best explains these occurrences?

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

Answer: C

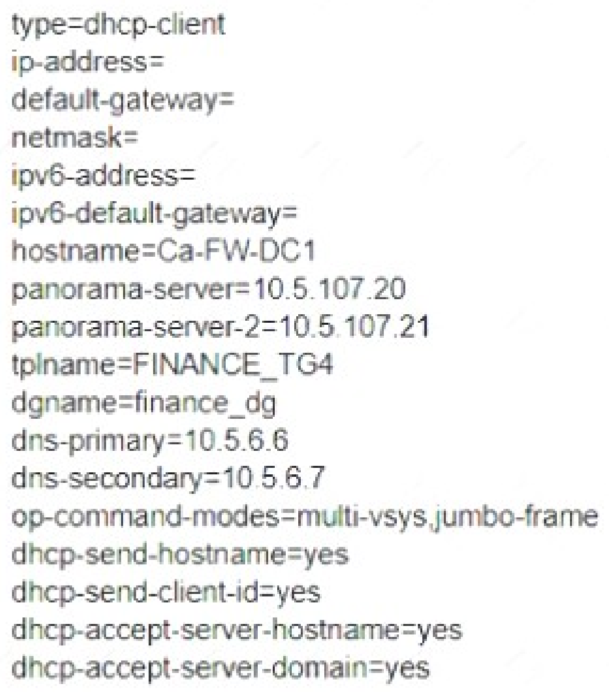
NEW QUESTION 290
An administrator device-group commit push is tailing due to a new URL category How should the administrator correct this issue?

A. verify that the URL seed Tile has been downloaded and activated on the firewall
B. change the new category action to alert" and push the configuration again
C. update the Firewall Apps and Threat version to match the version of Panorama
D. ensure that the firewall can communicate with the URL cloud

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNqw

NEW QUESTION 291
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 292
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 295
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 296
......