Paloalto-Networks

Exam Questions PCNSE

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

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

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

Answer: B

NEW QUESTION 2
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 3
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 4
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 5
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 6
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 7
Using multiple templates in a stack to manage many firewalls provides which two advantages? (Choose two.)

A. inherit address-objects from templates
B. define a common standard template configuration for firewalls
C. standardize server profiles and authentication configuration across all stacks
D. standardize log-forwarding profiles for security polices across all stacks

Answer: BD

NEW QUESTION 8
An engineer is deploying multiple firewalls with common configuration in Panorama. What are two benefits of using nested device groups? (Choose two.)

A. Inherit settings from the Shared group
B. Inherit IPSec crypto profiles
C. Inherit all Security policy rules and objects
D. Inherit parent Security policy rules and objects

Answer: BD

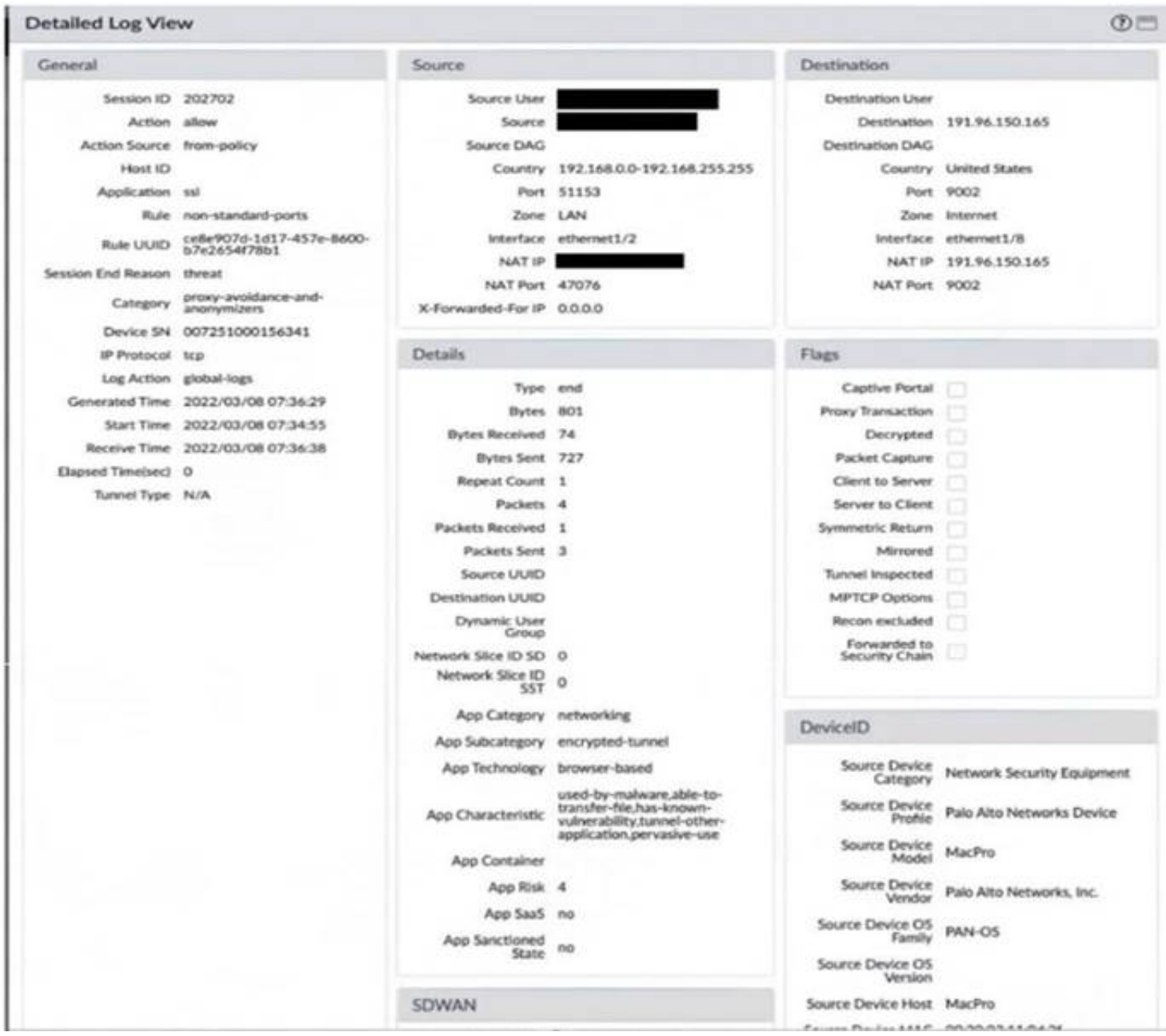
Explanation:
* B. Inherit IPSec crypto profiles
This is correct because IPSec crypto profiles are one of the objects that can be inherited from a parent device group1. You can also create IPSec crypto profiles for use in shared or device group polic1y.
* D. Inherit parent Security policy rules and objects
This is correct because Security policy rules and objects are also inheritable from a parent device group1. You can also create Security policy rules and objects for use in shared or device group policy1.

NEW QUESTION 9
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 10
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 10
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 11
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 14
Which benefit do policy rule UUIDs provide?

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

Answer: A

NEW QUESTION 18
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 19
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

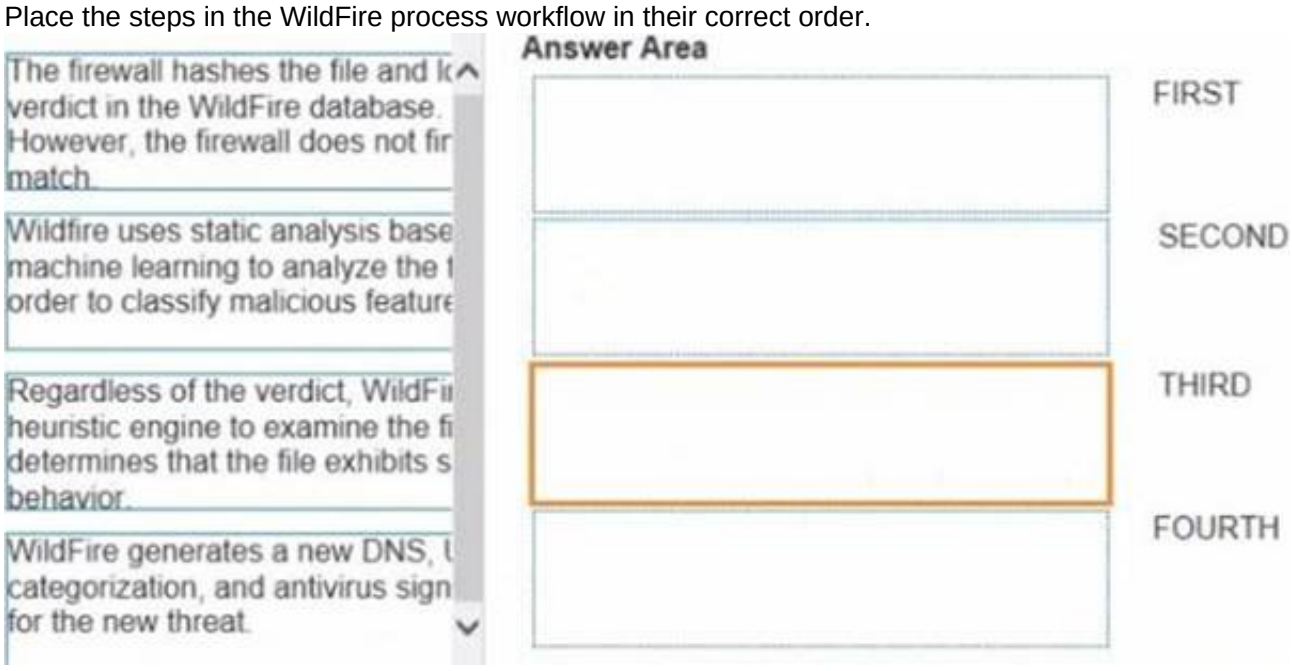
Explanation:
URL filtering is a feature in Palo Alto Networks firewalls that allows administrators to block access to specific URLs [1]. This feature can be configured via four different objects: Custom URL categories in URL Filtering profiles, PAN-DB URL categories in URL Filtering profiles, External 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 22
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

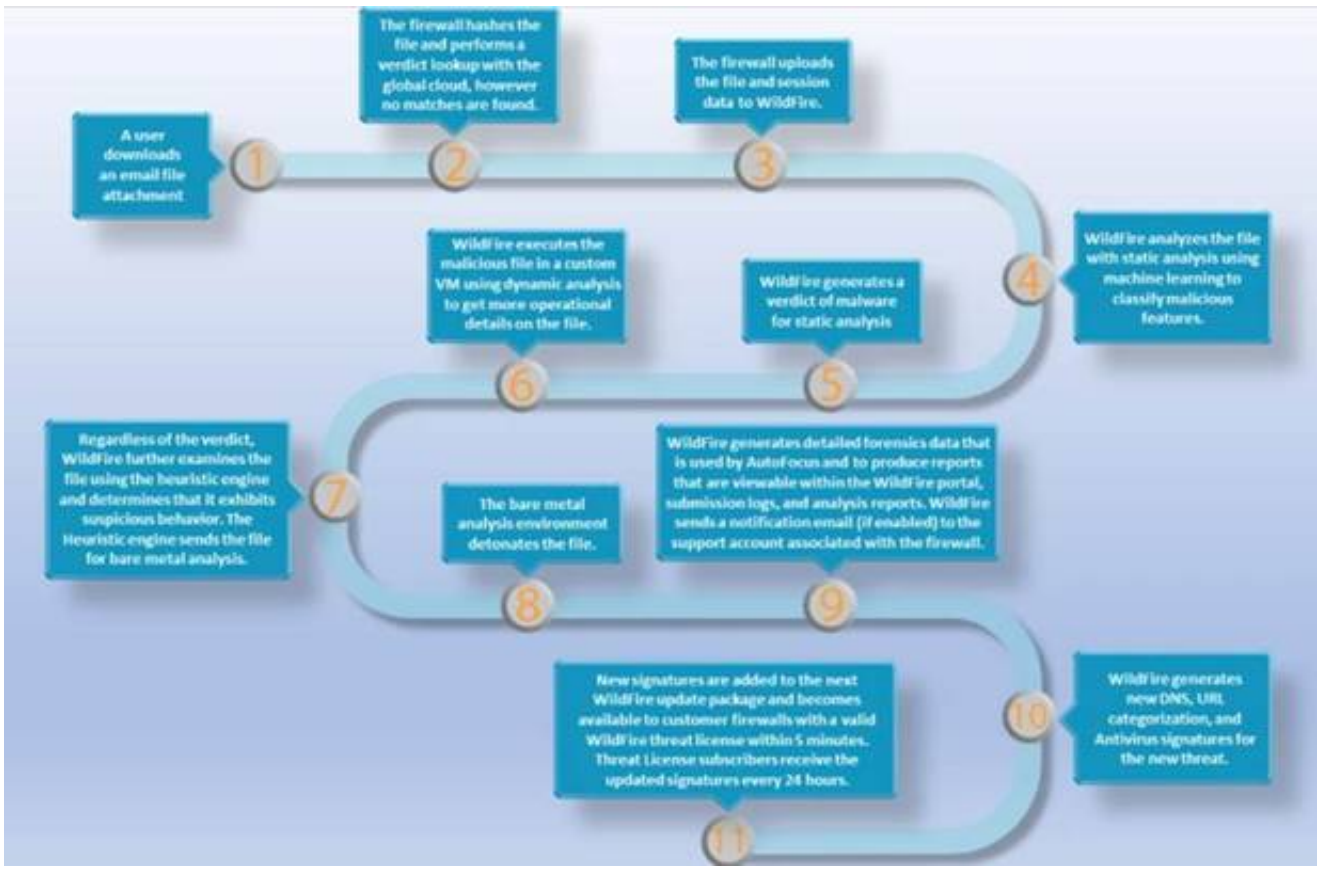
NEW QUESTION 25
Place the steps in the WildFire process workflow in their correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Timeline Description automatically generated



https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/about-wildfire.html

NEW QUESTION 29
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 34
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 39
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 43
Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

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

Answer: ACD

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

NEW QUESTION 47
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 50
A network security engineer must implement Quality of Service policies to ensure specific levels of delivery guarantees for various applications in the environment They want to ensure that they know as much as they can about QoS before deploying.
Which statement about the QoS feature is correct?

A. QoS is only supported on firewalls that have a single virtual system configured
B. QoS can be used in conjunction with SSL decryption
C. QoS is only supported on hardware firewalls
D. QoS can be used on firewalls with multiple virtual systems configured

Answer: D

NEW QUESTION 55
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 58
A company is looking to increase redundancy in their network. Which interface type could help accomplish this?

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

Answer: D

Explanation:
An aggregate group increases the bandwidth between peers by load balancing traffic across the combined interfaces. It also provides redundancy
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/configure-interfaces/configure-an-agg

NEW QUESTION 59
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 61
Which three firewall multi-factor authentication factors are supported by PAN-OS? (Choose three)

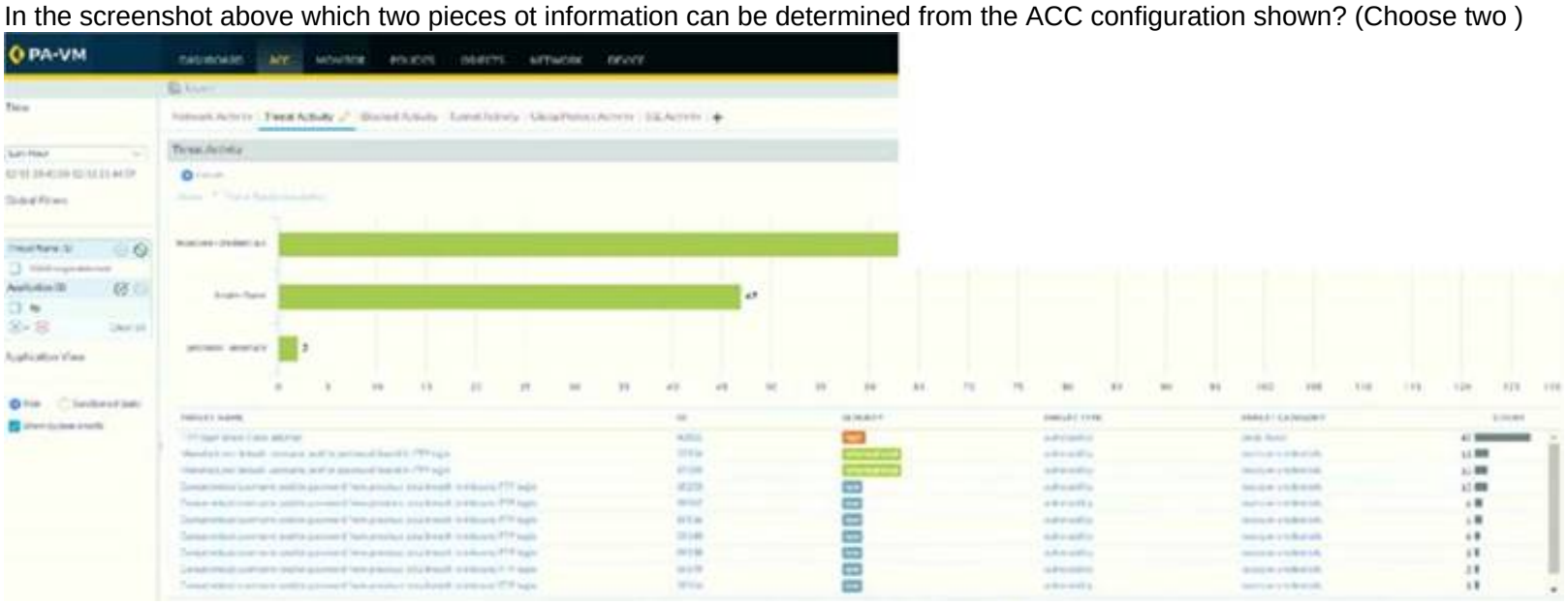
A. SSH key
B. User logon
C. Short message service
D. One-Time Password
E. Push

Answer: BDE

Explanation:
According to Palo Alto Networks documentation123, multi-factor authentication (MFA) is a method of verifying a user's identity using two or more factors, such as something they know, something they have, or something they are.
The firewall supports MFA for administrative access, GlobalProtect VPN access, and Captive Portal access. The firewall can integrate with external MFA providers such as RSA SecurID, Duo Security, or Okta Verify.
The three firewall MFA factors that are supported by PAN-OS are:

- User logon: This is something the user knows, such as a username and password.
- One-Time Password: This is something the user has, such as a code generated by an app or sent by email or SMS.
- Push: This is something the user is, such as a biometric verification or a device approval.

NEW QUESTION 63
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 65
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 70
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 75
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 78
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 81
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 84
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 85
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 87
Which log type would provide information about traffic blocked by a Zone Protection profile?

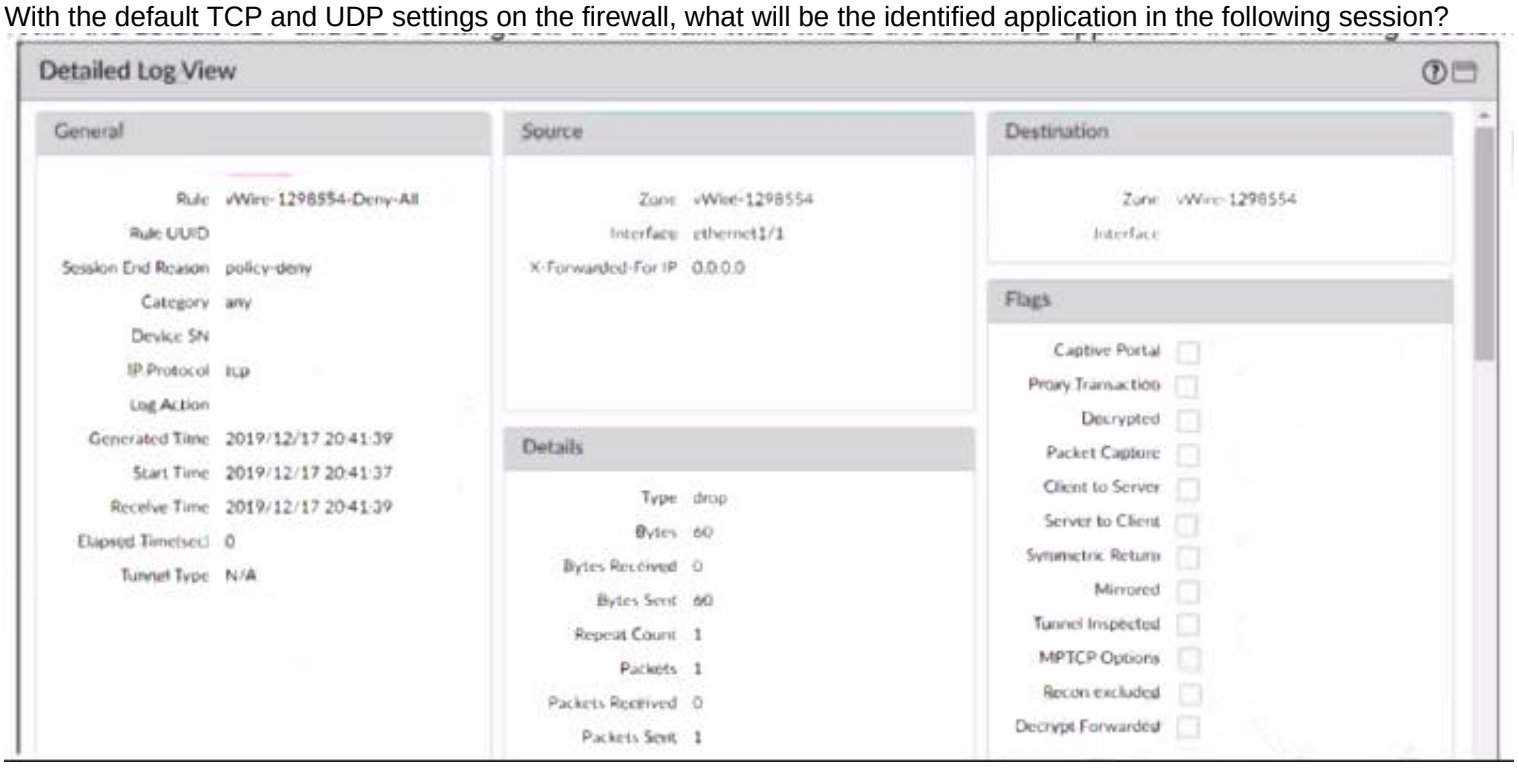
A. Data Filtering
B. IP-Tag
C. Traffic
D. Threat

Answer: D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clm9CAC
Zone Protection profile is a set of security policies that you can apply to an interface or zone to protect it from reconnaissance, flooding, brute force, and other types of attacks.
The log type that would provide information about traffic blocked by a Zone Protection profile is Thre4at. This log type records events such as packet-based

attacks, spyware, viruses, vulnerability exploits, and URL filtering.

NEW QUESTION 92
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 97
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 102
A firewall administrator needs to be able to inspect inbound HTTPS traffic on servers hosted in their DMZ to prevent the hosted service from being exploited. Which combination of features can allow PAN-OS to detect exploit traffic in a session with TLS encapsulation?

A. Decryption policy and a Data Filtering profile
B. a WildFire profile and a File Blocking profile
C. Vulnerability Protection profile and a Decryption policy
D. a Vulnerability Protection profile and a QoS policy

Answer: C

NEW QUESTION 107
An administrator needs to evaluate a recent policy change that was committed and pushed to a firewall device group.
How should the administrator identify the configuration changes?

A. review the configuration logs on the Monitor tab
B. click Preview Changes under Push Scope
C. use Test Policy Match to review the policies in Panorama
D. context-switch to the affected firewall and use the configuration audit tool

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-co

NEW QUESTION 112
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 115
An engineer is bootstrapping a VM-Series Firewall Other than the 'config folder, which three directories are mandatory as part of the bootstrap package directory structure? (Choose three.)

A. /software
B. /opt
C. /license
D. /content
E. /plugins

Answer: AD

NEW QUESTION 118
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 119
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 122
Which statement best describes the Automated Commit Recovery feature?

A. It performs a connectivity check between the firewall and Panorama after every configuration commit on the firewal
B. It reverts the configuration changes on the firewall if the check fails.
C. It restores the running configuration on a firewall and Panorama if the last configuration commit fails.
D. It performs a connectivity check between the firewall and Panorama after every configuration commit on the firewal
E. It reverts the configuration changes on the firewall and on Panorama if the check fails.
F. It restores the running configuration on a firewall if the last configuration commit fails.

Answer: A

NEW QUESTION 126
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

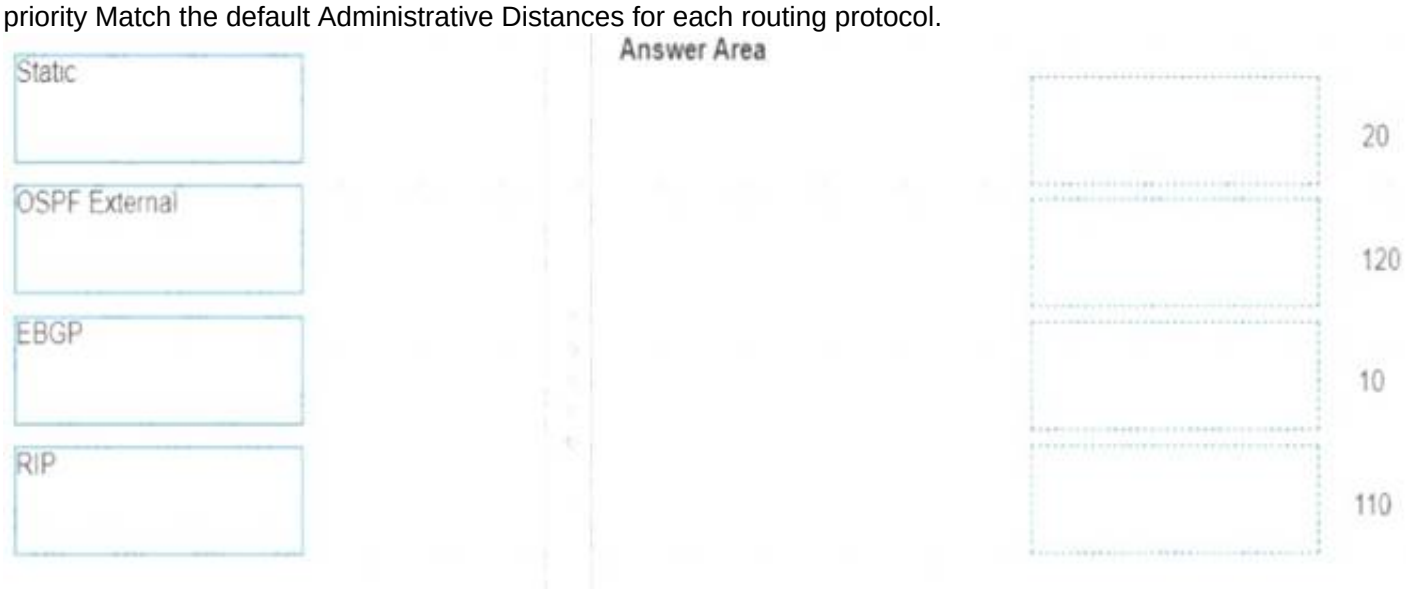
Answer: C

NEW QUESTION 129
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 132
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 136
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 138
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 143
What can be used to create dynamic address groups?

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

Answer: C

NEW QUESTION 145
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 148
An engineer needs to redistribute User-ID mappings from multiple data centers. Which data flow best describes redistribution of user mappings?

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

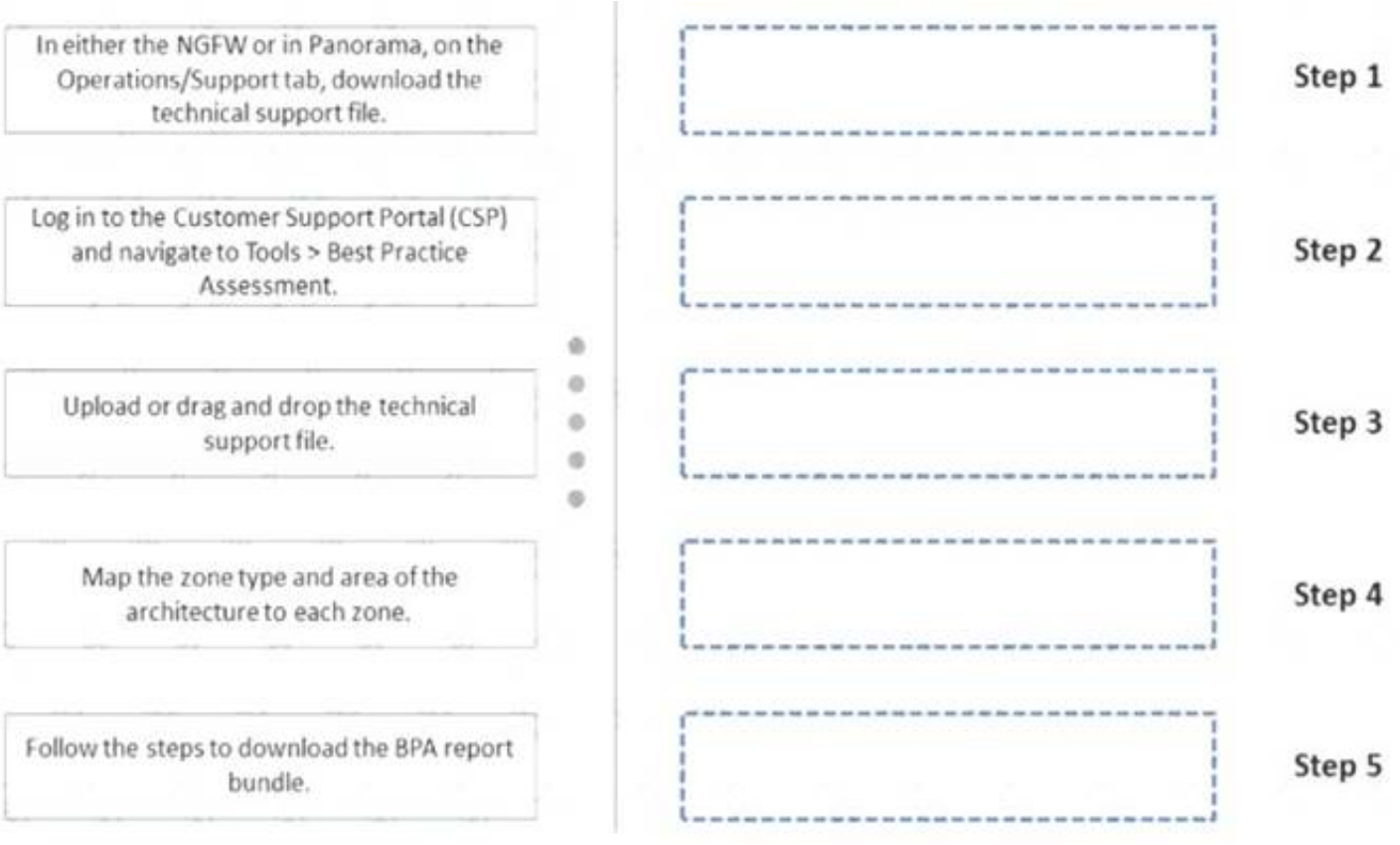
Answer: D

NEW QUESTION 150
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 155
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 157
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 159
A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443 A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.
Which combination of service and application, and order of Security policy rules, needs to be configured to allow cJeartext web-browsing traffic to this server on tcp/443?

A. Rule #1 application: web-browsing; service application-default; action: allow Rule #2- application: ssl; service: application-default; action: allow
B. Rule #1: application; web-browsing; service: service-https; action: allow Rule #2 application: ssl; service: application-default, action: allow
C. Rule #1: application: web-browsing; service: service-http; action: allow Rule #2: application: ssl; service: application-default; action: allow
D. Rule tf1 application: ssl; service: application-default; action: allow Rule #2 application; web-browsing; service application-default; action: allow

Answer: B

NEW QUESTION 163
PBF can address which two scenarios? (Select Two)

A. forwarding all traffic by using source port 78249 to a specific egress interface
B. providing application connectivity the primary circuit fails
C. enabling the firewall to bypass Layer 7 inspection
D. routing FTP to a backup ISP link to save bandwidth on the primary ISP link

Answer: BD

NEW QUESTION 166
In an existing deployment, an administrator with numerous firewalls and Panorama does not see any WildFire logs in Panorama. Each firewall has an active WildFire subscription On each firewall. WildFire togs are available.
This issue is occurring because forwarding of which type of logs from the firewalls to Panorama is missing?

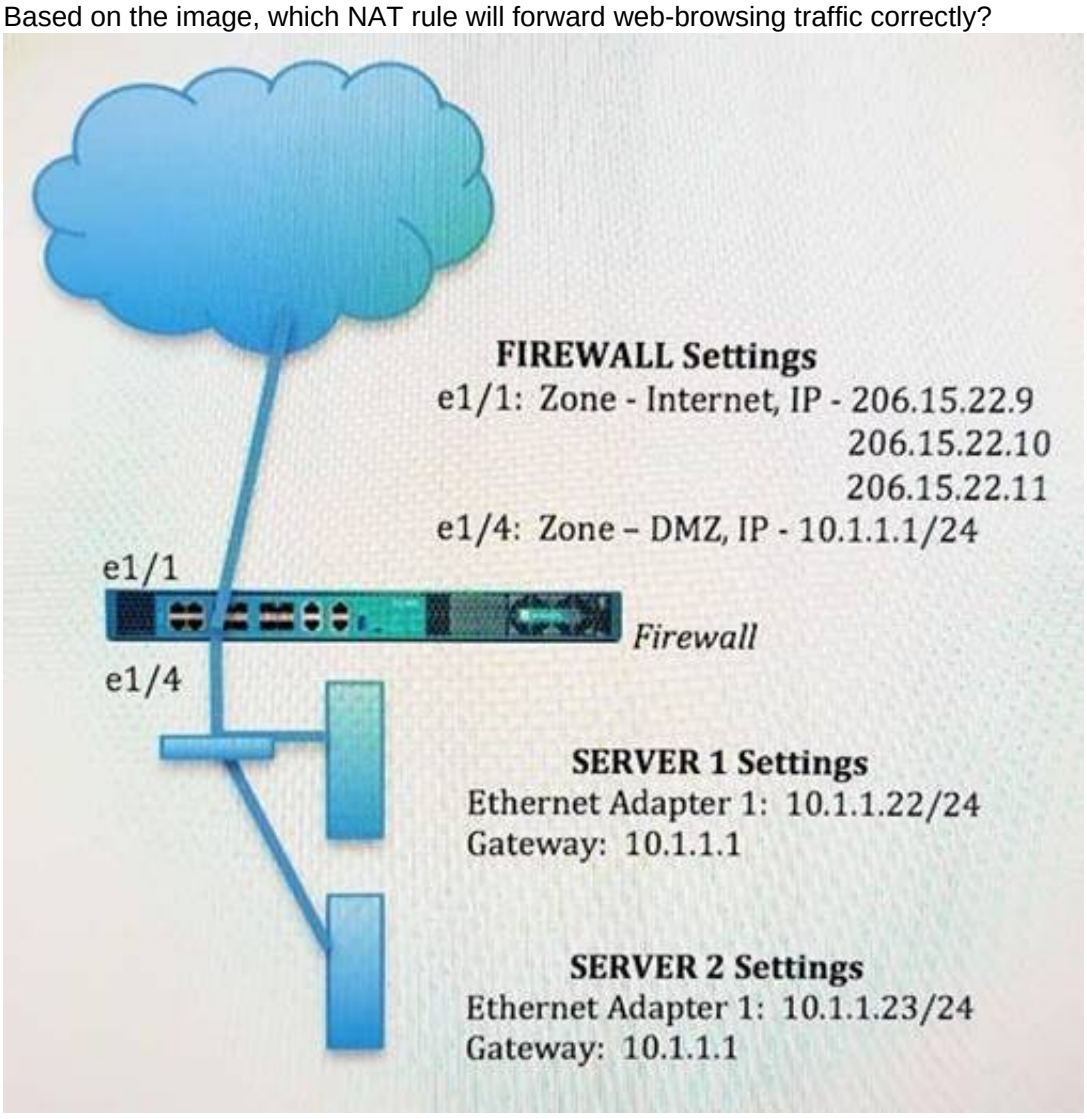
A. Threat logs
B. Traffic togs

C. System logs
D. WildFire logs

Answer: D

Explanation:
When an administrator has numerous firewalls and Panorama, WildFire logs need to be forwarded from the firewalls to Panorama in order for them to be visible in Panorama. WildFire logs contain information about malicious files that have been detected by WildFire and provide detailed information such as the file's hash value, severity, and other attributes. This information can then be used to help identify threats and take appropriate security measures. Proper configuration of forwarding WildFire logs is essential for monitoring malicious activity and ensuring the security of the network.

NEW QUESTION 167
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 171
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 173
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 176
How would an administrator configure a Bidirectional Forwarding Detection profile for BGP after enabling the Advance Routing Engine run on PAN-OS 10.2?

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

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

Answer: B

NEW QUESTION 177
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

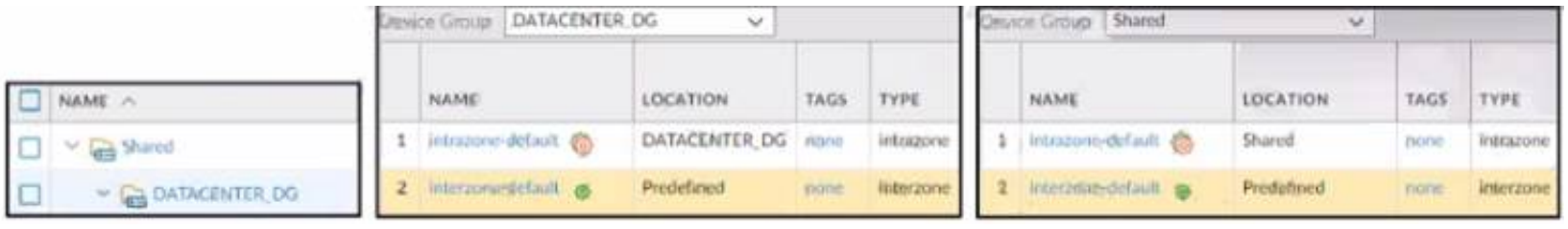
Answer: C

NEW QUESTION 180
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 185
Refer to the exhibit.



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

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

Answer: A

NEW QUESTION 189
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 192
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 197
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 202
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 205
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 209

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 210
When using certificate authentication for firewall administration, which method is used for authorization?

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

Answer: A

NEW QUESTION 215
How should an administrator enable the Advance Routing Engine on a Palo Alto Networks firewall?

A. Enable Advanced Routing Engine in Device > Setup > Session > Session Settings, then commit and reboot.
B. Enable Advanced Routing in Network > Virtual Routers > Redistribution Profiles and then commit.
C. Enable Advanced Routing in Network > Virtual Routers > Router Settings > General, then commit and reboot.
D. Enable Advanced Routing in General Settings of Device > Setup > Management, then commit and reboot

Answer: C

Explanation:
Enable Advanced Routing in Network > Virtual Routers > Router Settings > General, then commit and reboot 1. This means that the administrator can enable advanced routing features such as RIB filtering, BFD, multicast, and redistribution profiles for each virtual router on the firewall. The firewall requires a reboot after enabling advanced routing to apply the changes.

NEW QUESTION 219
What can you use with Global Protect to assign user-specific client certificates to each GlobalProtect user?

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

Answer: C

NEW QUESTION 221
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 225
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)

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

Answer: CDE

NEW QUESTION 230
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 231
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

A. Use the debug dataplane packet-diag set capture stage firewall file command.
B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
C. Use the debug dataplane packet-diag set capture stage management file command.
D. Use the tcpdump command.

Answer: D

NEW QUESTION 236
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 239
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 240
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 241
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 245
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 250
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

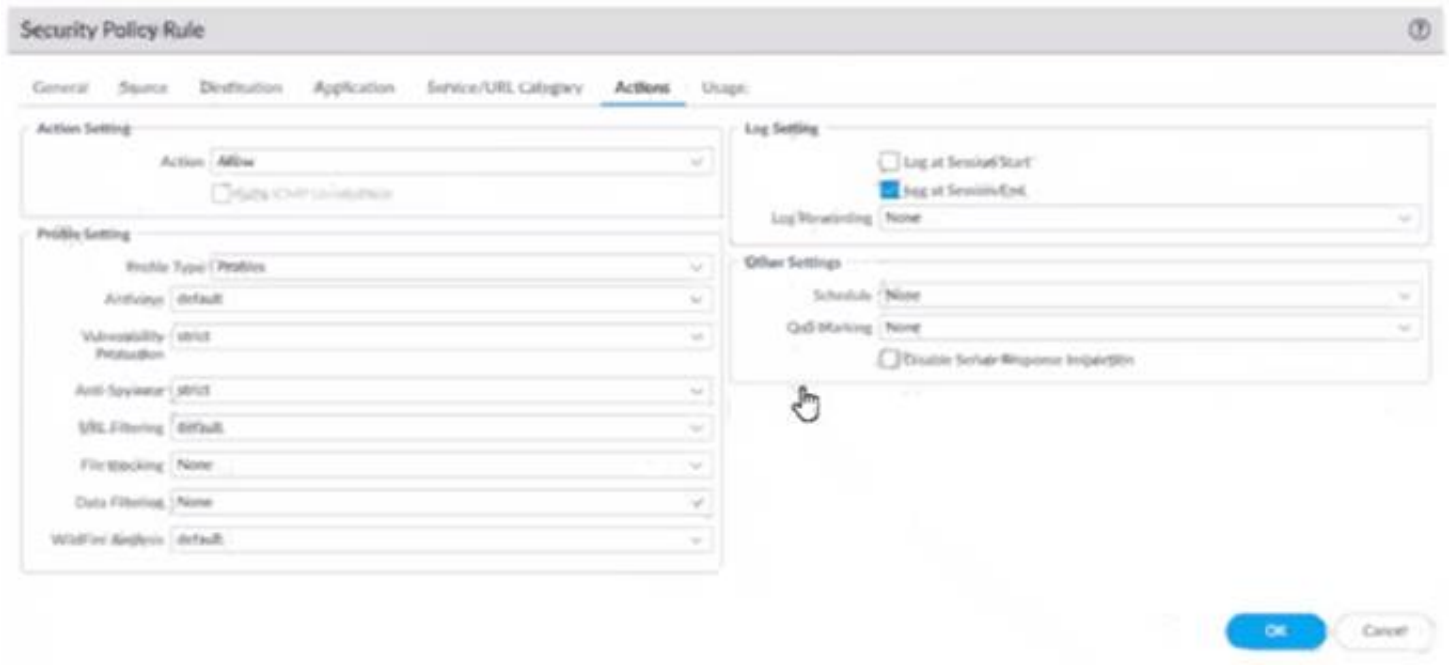
NEW QUESTION 254
An engineer is in the planning stages of deploying User-ID in a diverse directory services environment. Which server OS platforms can be used for server monitoring with User-ID?

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

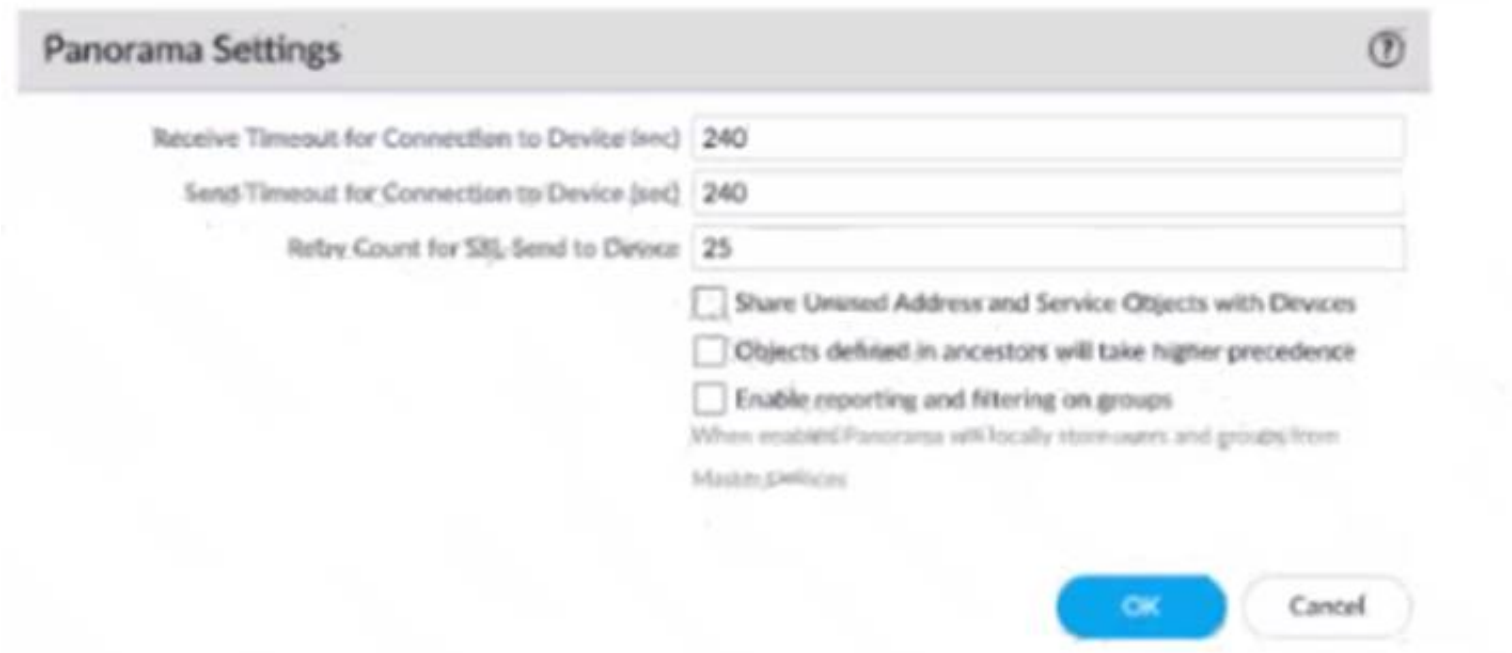
Answer: B

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

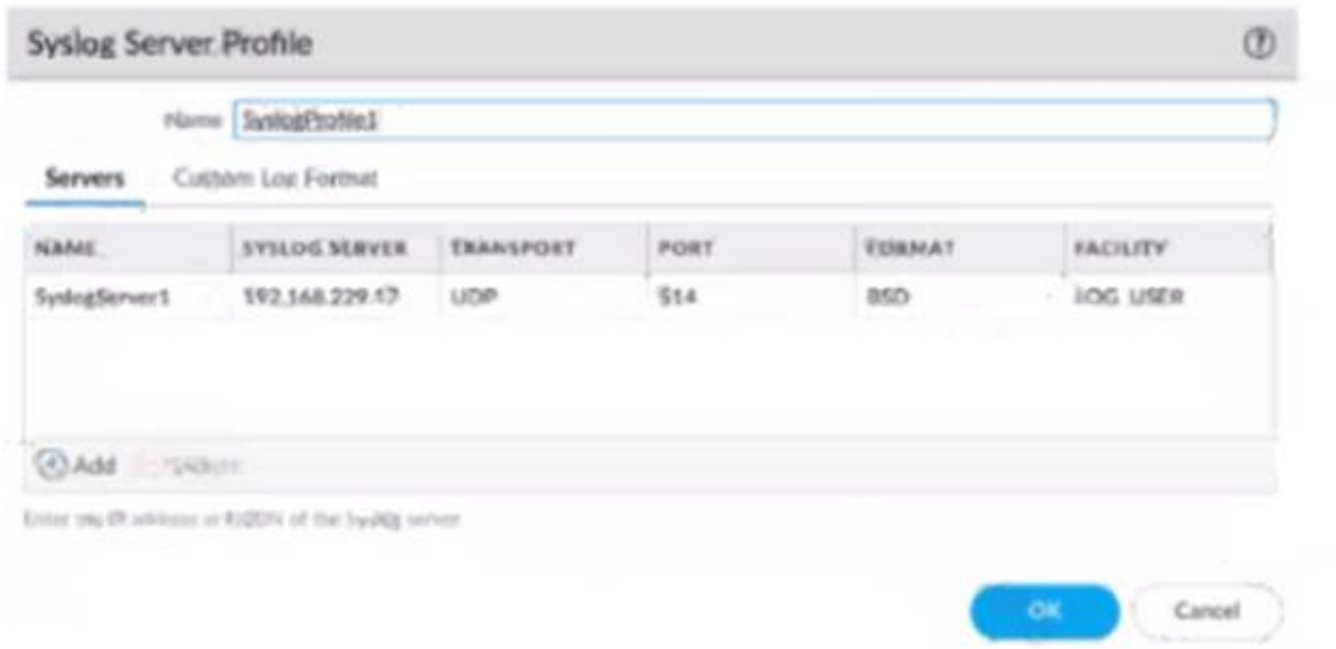
NEW QUESTION 255
An administrator can not see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall.
Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?
A)



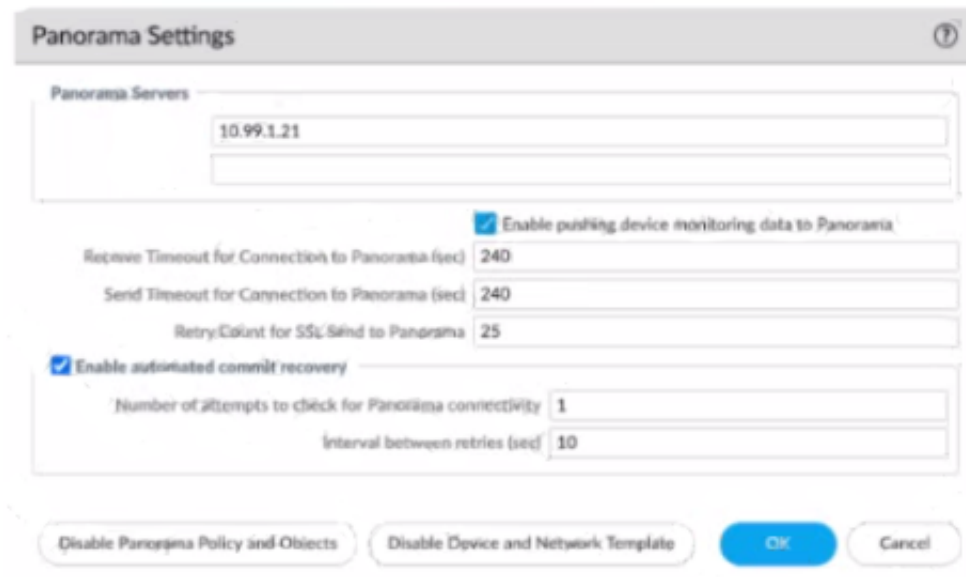
B)



C)



D)



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

Answer: C

NEW QUESTION 260
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 263
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 268
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 271
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 273
An engineer has been given approval to upgrade their environment 10 PAN-OS 10 2
The environment consists of both physical and virtual firewalls a virtual Panorama HA pair, and virtual log collectors
What is the recommended order when upgrading to PAN-OS 10.2?

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

Answer: B

NEW QUESTION 278
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 279
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 283
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same firewall. The update contains an application that matches the same traffic signatures as the custom application.
Which application will be used to identify traffic traversing the firewall?

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

Answer: A

NEW QUESTION 286
What are three valid qualifiers for a Decryption Policy Rule match? (Choose three.)

A. Destination Zone
B. App-ID
C. Custom URL Category
D. User-ID
E. Source Interface

Answer: ACD

NEW QUESTION 290
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 291
An administrator needs to build Security rules in a Device Group that allow traffic to specific users and groups defined in Active Directory
What must be configured in order to select users and groups for those rules from Panorama?

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

Answer: B

NEW QUESTION 293
You need to allow users to access the office-suite applications of their choice. How should you configure the firewall to allow access to any office-suite application?

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

Answer: C

NEW QUESTION 295
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 300
Four configuration choices are listed, and each could be used to block access to a specific URL
II you configured each choice to block the same URL, then which choice would be evaluated last in the processing order to block access to the URL1?

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

Answer: A

NEW QUESTION 302
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 305
A network security engineer configured IP multicast in the virtual router to support a new application. Users in different network segments are reporting that they are unable to access the application.
What must be enabled to allow an interface to forward multicast traffic?

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

Answer: B

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

NEW QUESTION 308
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 310
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 312
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 316
An administrator has configured the Palo Alto Networks NGFW's management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.
Which configuration setting or step will allow the firewall to get automatic application signature updates?

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

Answer: A

NEW QUESTION 317
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 321
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 325
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 329
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 333

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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