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

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

Answer: ABC

NEW QUESTION 3
A Security policy rule is configured with a Vulnerability Protection Profile and an action of "Deny." Which action will this configuration cause on the matched traffic?

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

Answer: D

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

NEW QUESTION 4
Your company occupies one floor in a single building. You have two Active Directory domain controllers on a single network. The firewall's management-plane resources are lightly utilized.
Given the size of this environment, which User-ID collection method is sufficient?

A. Citrix terminal server agent deployed on the network
B. Windows-based agent deployed on each domain controller
C. PAN-OS integrated agent deployed on the firewall
D. a syslog listener

Answer: C

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
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 7
Match each GlobalProtect component to the purpose of that component

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The GlobalProtect portal provides the management functions for your GlobalProtect infrastructure The GlobalProtect gateways provide security enforcement for traffic from GlobalProtect apps
The GlobalProtect app software runs on endpoints and enables access to your network resources

NEW QUESTION 8
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

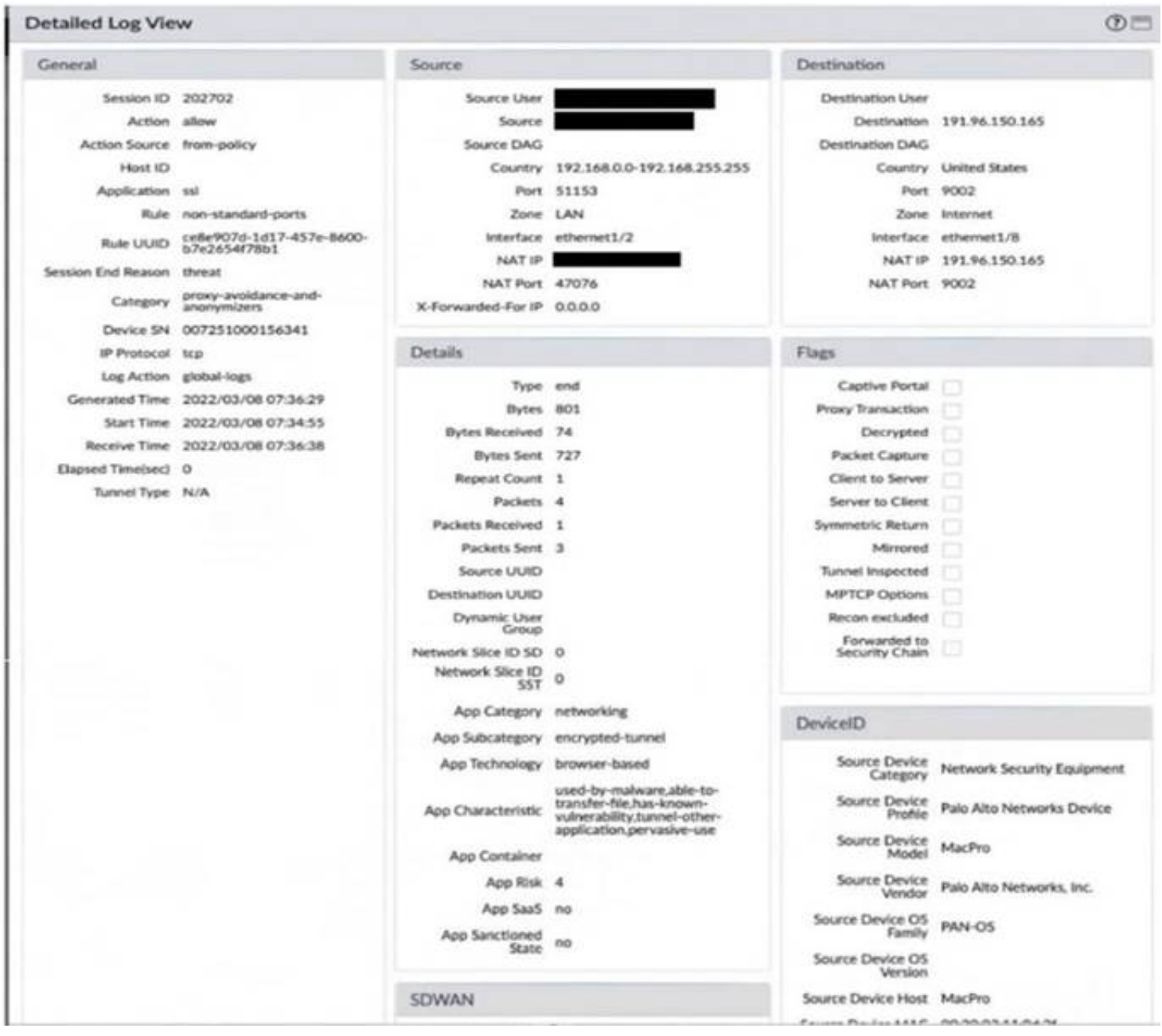
NEW QUESTION 9
How can Panorama help with troubleshooting problems such as high CPU or resource exhaustion on a managed firewall?

A. Firewalls send SNMP traps to Panorama when resource exhaustion is detected Panorama generates a system log and can send email alerts
B. Panorama provides visibility into all the system and traffic logs received from firewalls it does not offer any ability to see or monitor resource utilization on managed firewalls
C. Panorama monitors all firewalls using SNMP It generates a system log and can send email alerts when resource exhaustion is detected on a managed firewall
D. Panorama provides information about system resources of the managed devices in the Managed Devices> Health menu

Answer: D

Explanation:
Panorama can help with troubleshooting problems such as high CPU or resource exhaustion on a managed firewall by providing information about system resources of the managed devices in the Managed Devices > Health menu. This is explained in the Palo Alto Networks PCNSE Study Guide in Chapter 13: Panorama, under the section "Monitoring Managed Firewalls with Panorama":
"The Panorama web interface provides information about the system resources of the managed devices. In the Managed Devices > Health menu, you can view the CPU, memory, and disk usage of each managed device. This information can help you troubleshoot problems such as high CPU or resource exhaustion on a managed firewall."

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
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 12
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

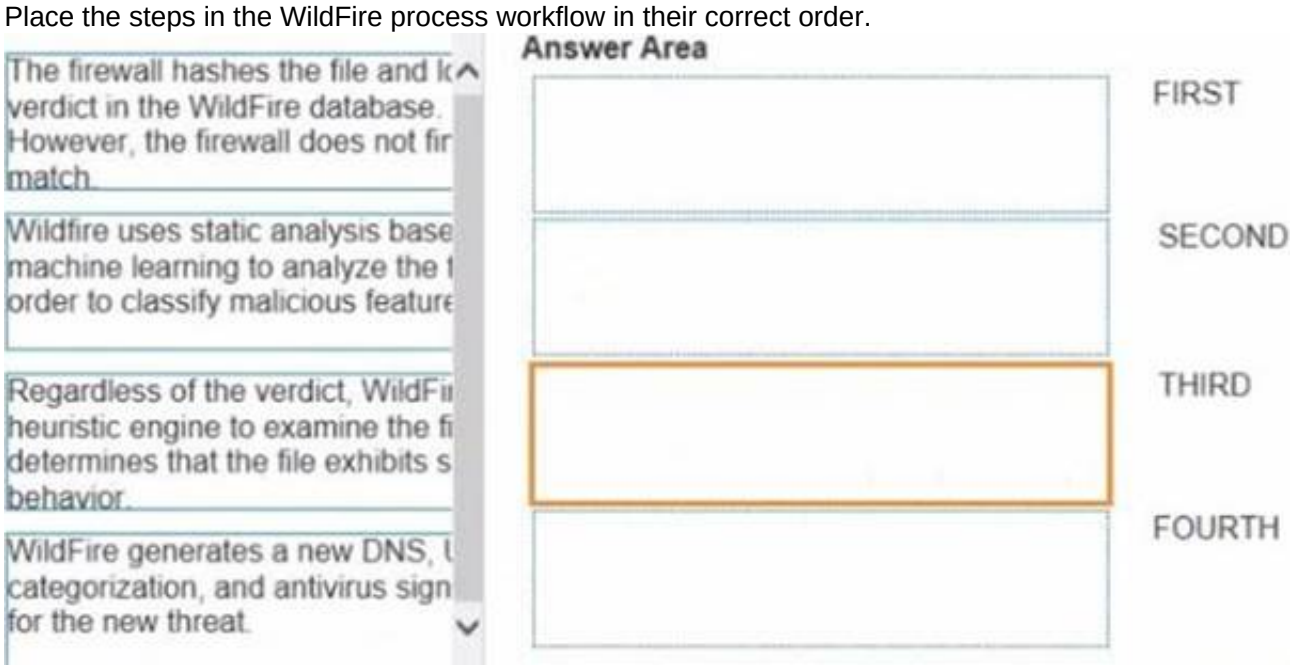
Explanation:
URL filtering is a feature in Palo Alto Networks firewalls that allows administrators to block access to specific URLs [1]. This feature can be configured via four different objects: Custom URL categories in URL Filtering profiles, PAN-DB URL categories in URL Filtering profiles, External 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 15
Which configuration is backed up using the Scheduled Config Export feature in Panorama?

A. Panorama running configuration
B. Panorama candidate configuration
C. Panorama candidate configuration and candidate configuration of all managed devices
D. Panorama running configuration and running configuration of all managed devices

Answer: D

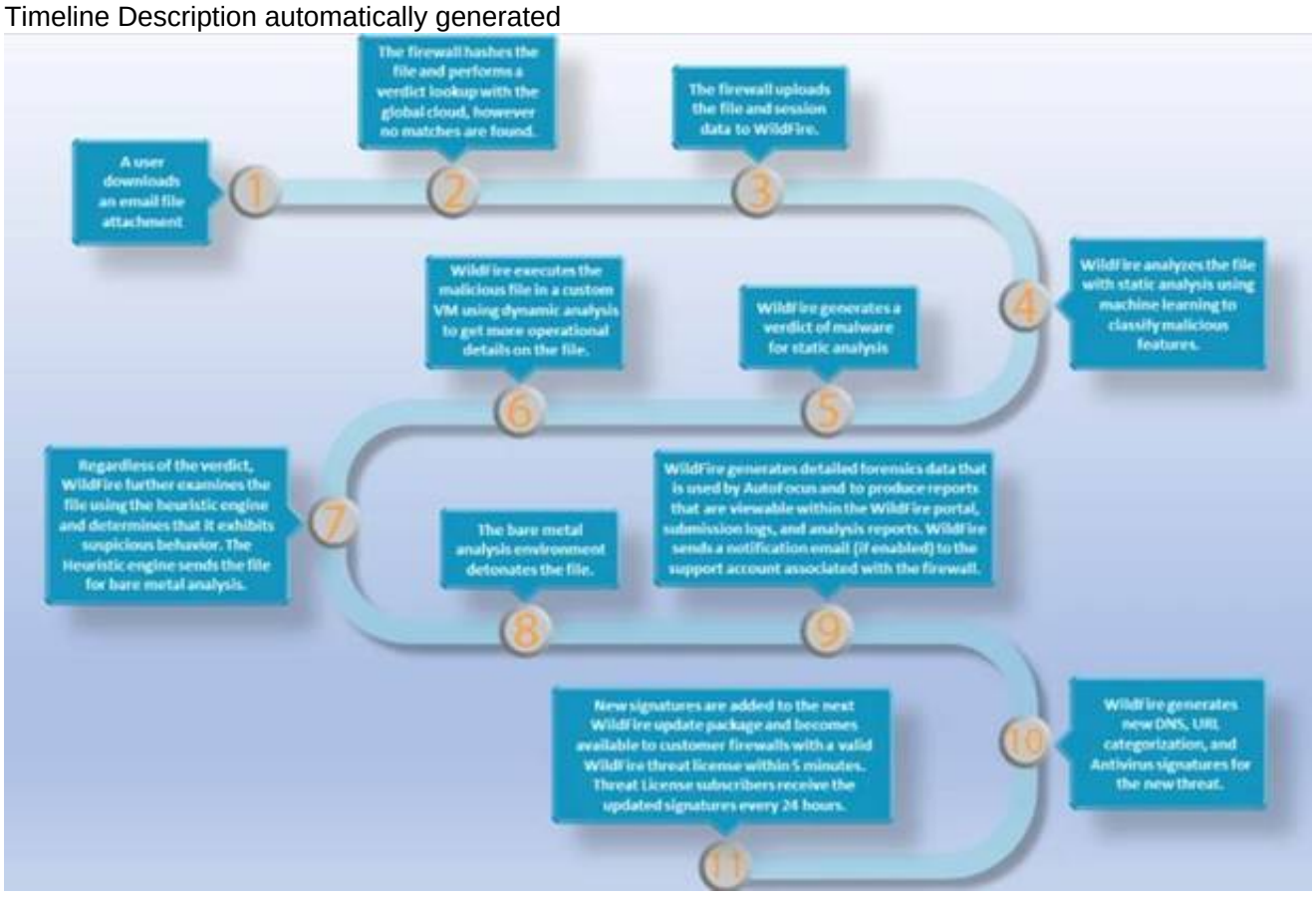
NEW QUESTION 17
Place the steps in the WildFire process workflow in their correct order.



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 22
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 26
An engineer is planning an SSL decryption implementation
Which of the following statements is a best practice for SSL decryption?

A. Use the same Forward Trust certificate on all firewalls in the network.
B. Obtain a certificate from a publicly trusted root CA for the Forward Trust certificate.
C. Obtain an enterprise CA-signed certificate for the Forward Trust certificate.
D. Use an enterprise CA-signed certificate for the Forward Untrust certificate.

Answer: C

NEW QUESTION 30
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 32
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 33
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 34
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 38
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 39
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 44
A network administrator wants to use a certificate for the SSL/TLS Service Profile. Which type of certificate should the administrator use?

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

Answer: D

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

NEW QUESTION 45
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 50
An administrator has 750 firewalls. The administrator's central-management Panorama instance deploys dynamic updates to the firewalls. The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls.
If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the configuration does not appear, what is the root cause?

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

Answer: D

NEW QUESTION 55
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 58
An existing NGFW customer requires direct interne! access offload locally at each site and iPSec connectivity to all branches over public internet. One requirement is mat no new SD-WAN hardware be introduced to the environment.
What is the best solution for the customer?

A. Configure a remote network on PAN-OS
B. Upgrade to a PAN-OS SD-WAN subscription
C. Deploy Prisma SD-WAN with Prisma Access
D. Configure policy-based forwarding

Answer: B

NEW QUESTION 60
A network security engineer is attempting to peer a virtual router on a PAN-OS firewall with an external router using the BGP protocol. The peer relationship is not establishing.
What command could the engineer run to see the current state of the BGP state between the two devices?

A. show routing protocol bgp state
B. show routing protocol bgp peer
C. show routing protocol bgp summary

D. show routing protocol bgp rib-out

Answer: B

NEW QUESTION 62
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 66
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 68
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 70
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 72
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 77
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 80
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 81
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 82
An engineer discovers the management interface is not routable to the User-ID agent What configuration is needed to allow the firewall to communicate to the User-ID agent?

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

Answer: C

Explanation:
To allow the firewall to communicate with the User-ID agent, you need to configure a custom service route f the UID Agent23. A custom service route allows you to specify which interface and source IP address the firewall uses to connect to a specific destination service. By default, the firewall uses its management interface for services such as User-ID, but you can override this behavior by creating a custom service route.
To configure a custom service route for the UID Agent, you need to do the following steps:

- Go to Device > Setup > Services and click Service Route Configuration.
- In the Service column, select User-ID Agent from the drop-down list.
- In the Interface column, select an interface that can reach the User-ID agent server from the drop-down list.
- In the Source Address column, select an IP address that belongs to that interface from the drop-down list.
- Click OK and Commit your changes.

The correct answer is C. Create a custom service route for UID Agent

NEW QUESTION 84
The administrator for a small company has recently enabled decryption on their Palo Alto Networks firewall using a self-signed root certificate. They have also created a Forward Trust and Forward Untrust certificate and set them as such

The admin has not yet installed the root certificate onto client systems What effect would this have on decryption functionality?

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

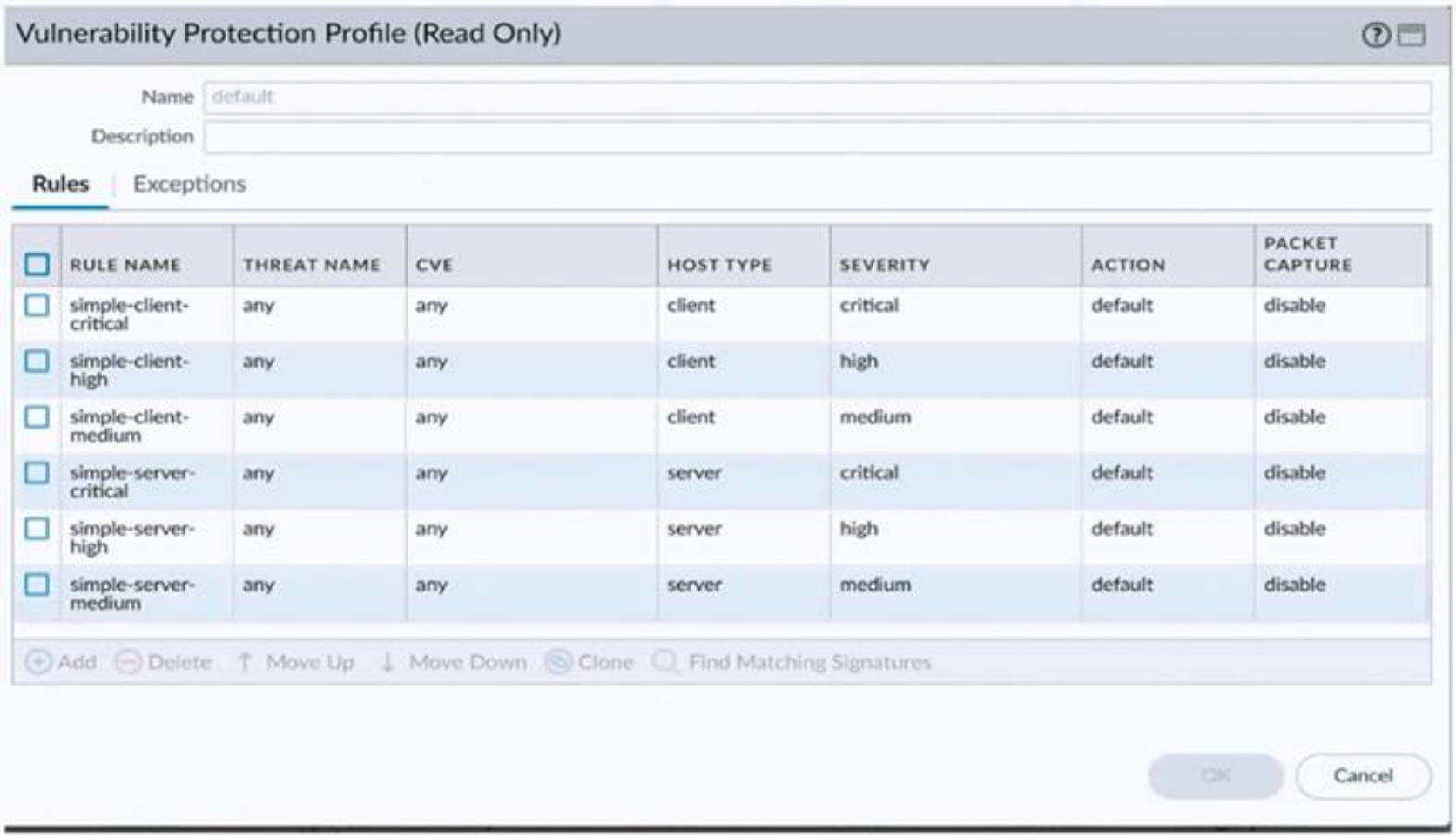
Answer: D

NEW QUESTION 87
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 89
An administrator would like to determine which action the firewall will take for a specific CVE. Given the screenshot below, where should the administrator navigate to view this information?



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

Answer: A

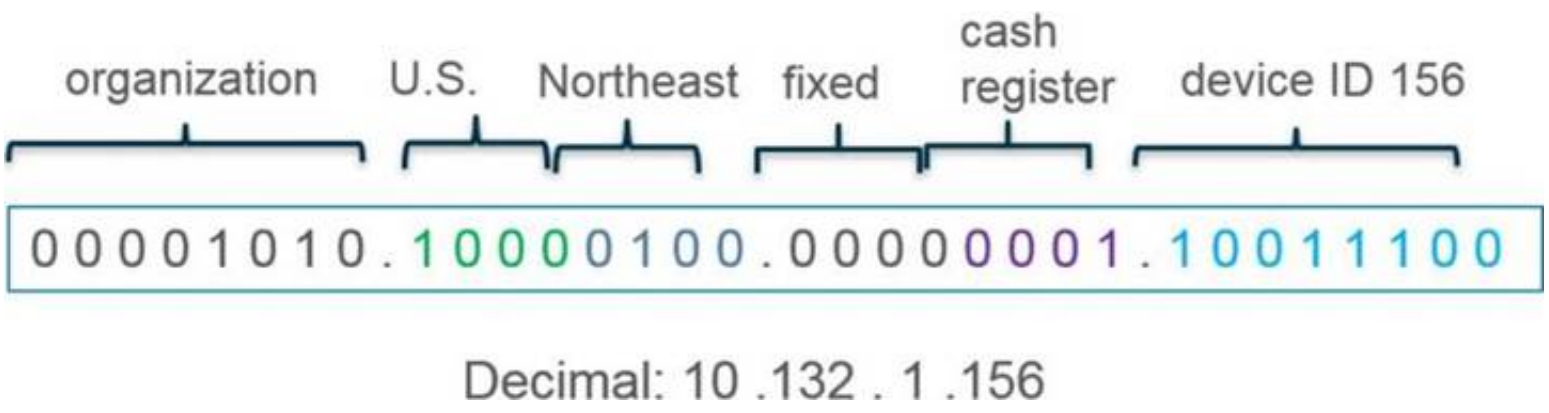
NEW QUESTION 91
An engineer has discovered that certain real-time traffic is being treated as best effort due to it exceeding defined bandwidth Which QoS setting should the engineer adjust?

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 96
What type of address object would be useful for internal devices where the addressing structure assigns meaning to certain bits in the address, as illustrated in the diagram?



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

Answer: B

NEW QUESTION 99
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 104
An administrator is configuring SSL decryption and needs 10 ensure that all certificates for both SSL Inbound inspection and SSL Forward Proxy are installed properly on the firewall. When certificates are being imported to the firewall for these purposes, which three certificates require a private key? (Choose three.)

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

Answer: ABD

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

NEW QUESTION 108
A network security administrator wants to configure SSL inbound inspection.
Which three components are necessary for inspecting the HTTPS traffic as it enters the firewall? (Choose three.)

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

Answer: BCD

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-inbound-inspection

NEW QUESTION 113
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 115
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 118
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 123
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 128
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 131
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 132
Which time determines how long the passive firewall will wait before taking over as the active firewall alter losing communications with the HA peer?

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

Answer: A

NEW QUESTION 134
An administrator has 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 136
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 139
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 140
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 142
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 143
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 144
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 149
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 150
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 151
An administrator is using Panorama to manage me and suspects an IKE Crypto mismatch between peers, from the firewalls to Panorama. However, pre-existing logs from the firewalls are not appearing in Panorama.
Which action should be taken to enable the firewalls to send their pre-existing logs to Panorama?

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

Answer: D

NEW QUESTION 154
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.

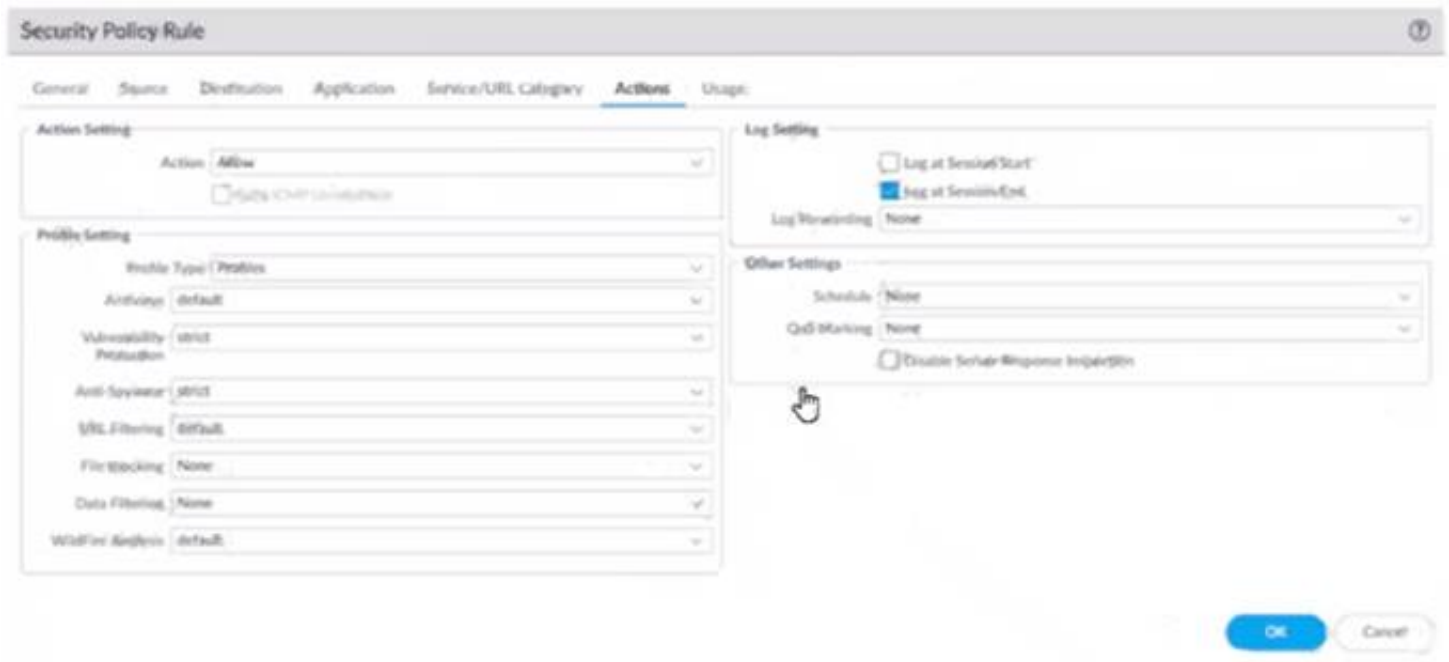
Answer: A

NEW QUESTION 155
A company is using wireless controllers to authenticate users. Which source should be used for User-ID mappings?

A. Syslog
B. XFF headers
C. server monitoring
D. client probing

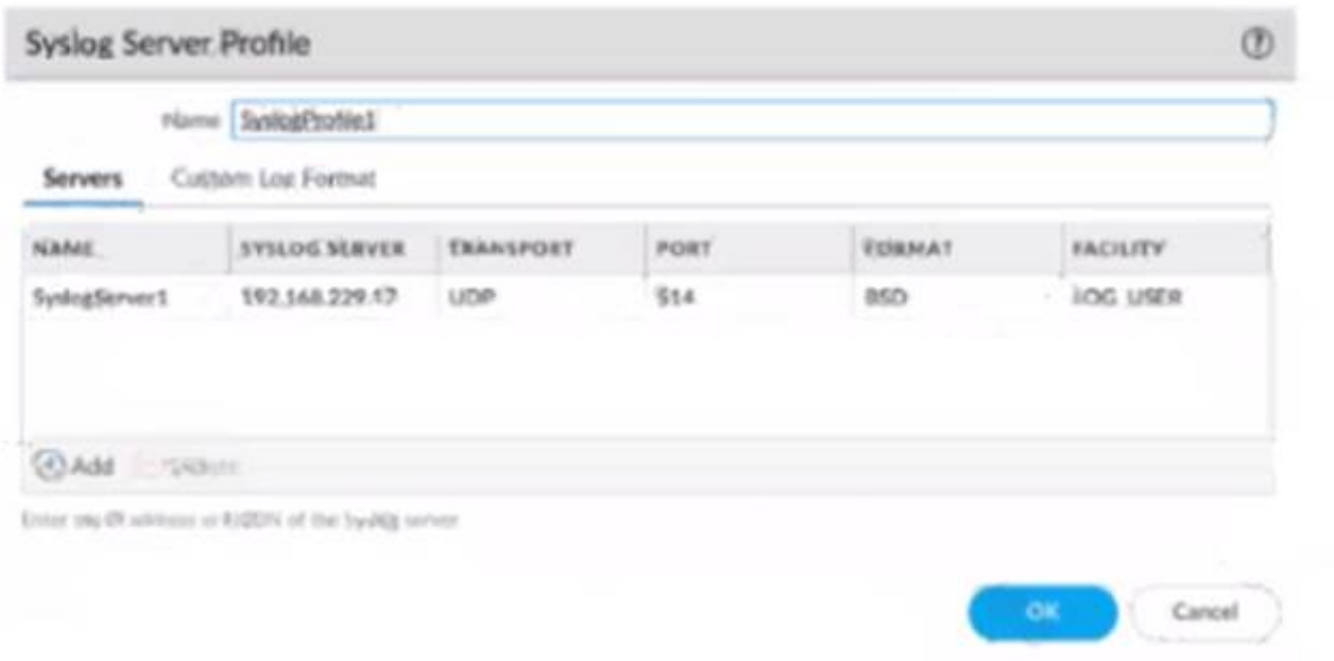
Answer: A

NEW QUESTION 157
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 160
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 161
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 163
A user at an external system with the IP address 65.124.57.5 queries the DNS server at 4. 2.2.2 for the IP address of the web server, www,xyz.com. The DNS server returns an address of 172.16.15.1
In order to reach Ire web server, which Security rule and NAT rule must be configured on the firewall?

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

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

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

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

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

Answer: C

NEW QUESTION 164
A network security engineer wants to prevent resource-consumption issues on the firewall. Which strategy is consistent with decryption best practices to ensure consistent performance?

A. Use RSA in a Decryption profile tor higher-priority and higher-risk traffic, and use less processor-intensive decryption methods for lower-risk traffic
B. Use PFS in a Decryption profile for higher-priority and higher-risk traffic, and use lessprocessor-intensive decryption methods for tower-risk traffic
C. Use Decryption profiles to downgrade processor-intensive ciphers to ciphers that are less processor-intensive
D. Use Decryption profiles to drop traffic that uses processor-intensive ciphers

Answer: B

NEW QUESTION 165
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 168
After importing a pre-configured firewall configuration to Panorama, what step is required to ensure a commit/push is successful without duplicating local configurations?

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

Answer: C

Explanation:
When importing a pre-configured firewall configuration to Panorama, you need to perform the following steps 12:
- Add the serial number of the firewall under Panorama > Managed Devices
- In Panorama, import the firewall’s configuration bundle under Panorama > Setup > Operations > Import device configuration to Panorama
- Commit the changes you made to Panorama
- Perform an Export or push Device Config Bundle operation under Panorama > Setup > Operations

The Export or push Device Config Bundle operation allows you to push a complete configuration bundle from Panorama to a managed firewall without duplicating local configurations3. This operation ensures that any local settings on the firewall are preserved and merged with the settings from Panorama.

NEW QUESTION 173
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 177
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 180
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 184
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 186
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 190
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 194
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 199
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 203
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 204
An administrator needs firewall access on a trusted interface. Which two components are required to configure certificate based, secure authentication to the web UI? (Choose two)

A. certificate profile
B. server certificate
C. SSH Service Profile
D. SSL/TLS Service Profile

Answer: AD

NEW QUESTION 206
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 211
An engineer is configuring SSL Inbound Inspection for public access to a company's application. Which certificate(s) need to be installed on the firewall to ensure that inspection is performed successfully?

A. Self-signed CA and End-entity certificate
B. Root CA and Intermediate CA(s)
C. Self-signed certificate with exportable private key
D. Intermediate CA (s) and End-entity certificate

Answer: D

NEW QUESTION 215
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 218

.....

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