Exam Questions PCNSE

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

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

NEW QUESTION 1
A network security engineer has applied a File Blocking profile to a rule with the action of Block. The user of a Linux CLI operating system has opened a ticket. The ticket states that the user is being blocked by the firewall when trying to download a TAR file. The user is getting no error response on the system.
Where is the best place to validate if the firewall is blocking the user's TAR file?

A. URL Filtering log
B. Data Filtering log
C. Threat log
D. WildFire Submissions log

Answer: B

NEW QUESTION 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 13
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 14
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 15
A firewall has been assigned to a new template stack that contains both "Global" and "Local" templates in Panorama, and a successful commit and push has been performed. While validating the configuration on the local firewall, the engineer discovers that some settings are not being applied as intended.
The setting values from the "Global" template are applied to the firewall instead of the "Local" template that has different values for the same settings.
What should be done to ensure that the settings in the "Local" template are applied while maintaining settings from both templates?

A. Move the "Global" template above the "Local" template in the template stack.
B. Perform a commit and push with the "Force Template Values" option selected.
C. Move the "Local" template above the "Global" template in the template stack.
D. Override the values on the local firewall and apply the correct settings for each value.

Answer: C

NEW QUESTION 20
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

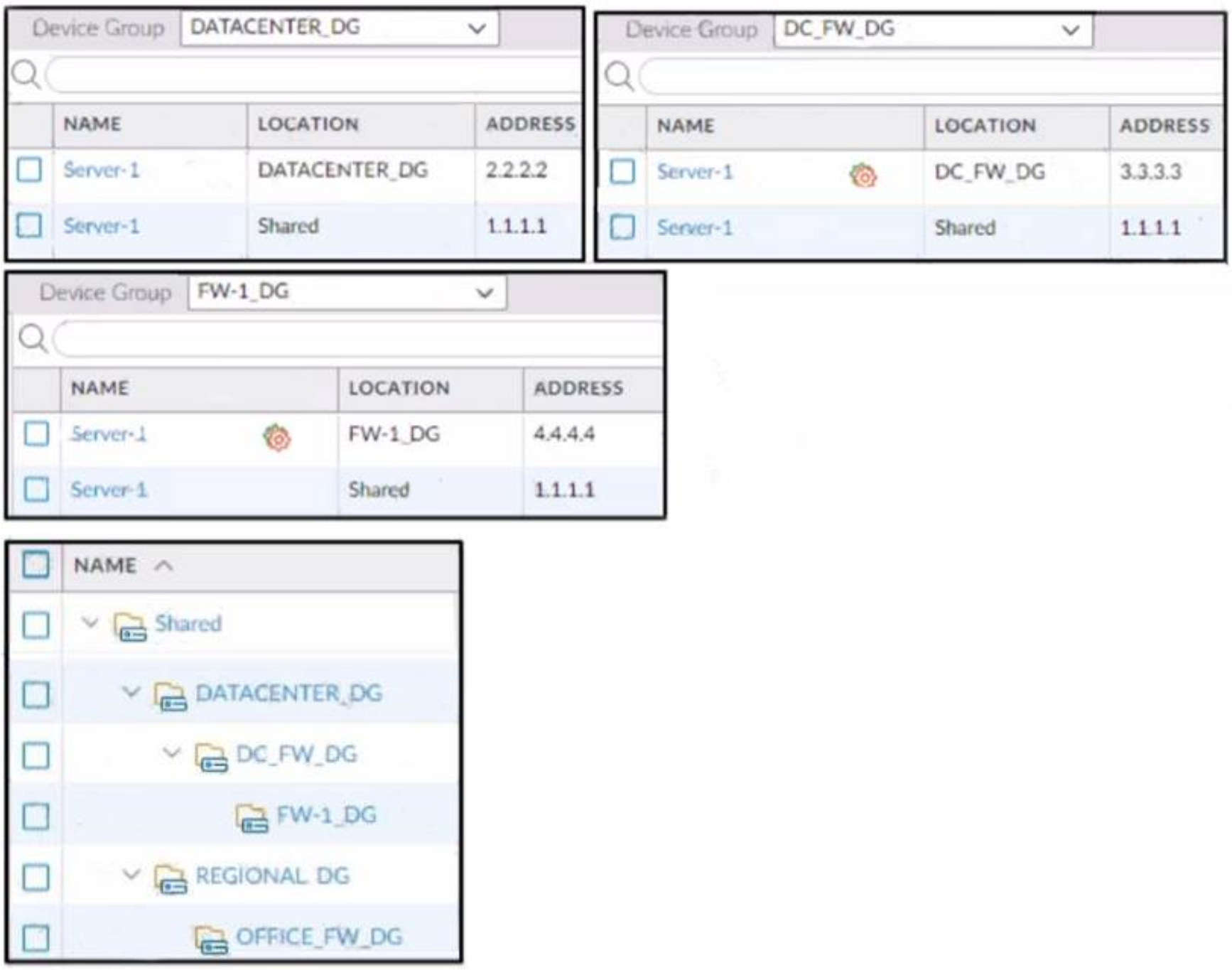
Explanation:
Use only signed certificates, not CA certificates, in SSL/TLS service profiles. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure-an-ssltls-service

NEW QUESTION 23
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 26
Refer to the exhibit.



Review the screenshots and consider the following information:
• FW-1 is assigned to the FW-1_DG device group, and FW-2 is assigned to OFFICE_FW_DG.
• There are no objects configured in REGIONAL_DG and OFFICE_FW_DG device groups.
Which IP address will be pushed to the firewalls inside Address Object Server-1?

A. Server-1 on FW-1 will have IP 1.1.1.1. Server-1 will not be pushed to FW-2.
B. Server-1 on FW-1 will have IP 3.3.3.3. Server-1 will not be pushed to FW-2.
C. Server-1 on FW-1 will have IP 2.2.2.2. Server-1 will not be pushed to FW-2.
D. Server-1 on FW-1 will have IP 4.4.4.4. Server-1 on FW-2 will have IP 1.1.1.1.

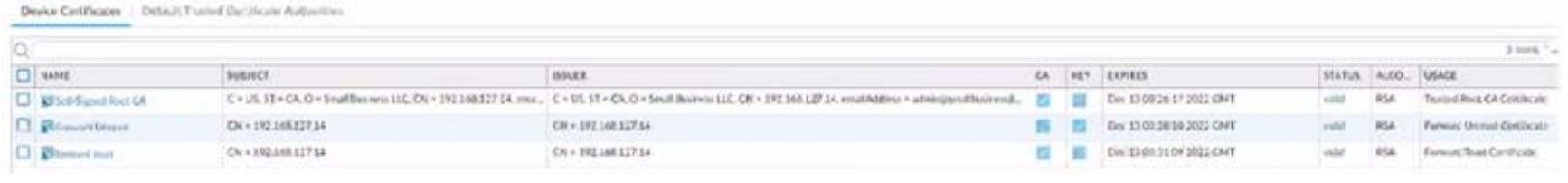
Answer: C

NEW QUESTION 30
An engineer is pushing configuration from Panorama lo a managed firewall.
What happens when the pushed Panorama configuration has Address Object names that duplicate the Address Objects already configured on the firewall?

A. The firewall rejects the pushed configuration, and the commit fails.
B. The firewall renames the duplicate local objects with "-1" at the end signifying they are clones; it willupdate the references to the objects accordingly and fully commit the pushed configuration.
C. The firewall fully commits all of the pushed configuration and overwrites its locally configured objects
D. The firewall ignores only the pushed objects that have the same name as the locally configured objects, and it will commit the rest of the pushed configuration.

Answer: A

NEW QUESTION 35
Review the screenshot of the Certificates page.



An administrator tor a small LLC has created a series of certificates as shown, to use tor a planned Decryption roll out The administrator has also installed the sell-signed root certificate <n all client systems When testing, they noticed that every time a user visited an SSL site they received unsecured website warnings What is the cause of the unsecured website warnings.

A. The forward trust certificate has not been signed by the set-singed root CA certificate
B. The self-signed CA certificate has the same CN as the forward trust and untrust certificates
C. The forward untrust certificate has not been signed by the self-singed root CA certificate
D. The forward trust certificate has not been installed in client systems

Answer: C

NEW QUESTION 40
Which statement is correct given the following message from the PanGPA log on the GlobalProtect app? Failed to connect to server at port:47 67

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

Answer: D

NEW QUESTION 44
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 45
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

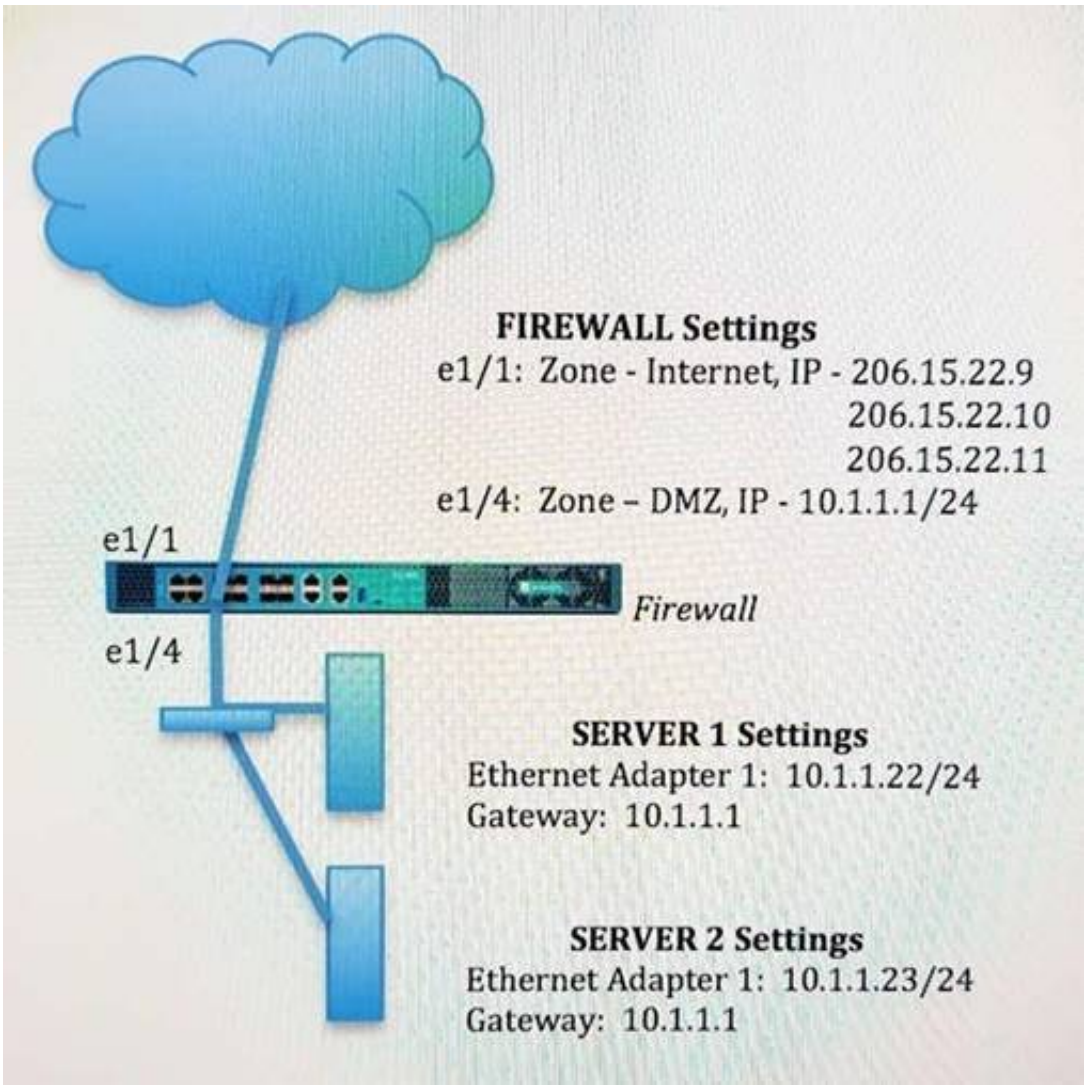
NEW QUESTION 47
An engineer has been asked to limit which routes are shared by running two different areas within an OSPF implementation. However, the devices share a common link for communication. Which virtual router configuration supports running multiple instances of the OSPF protocol over a single link?

A. ASBR
B. ECMP
C. OSPFv3
D. OSPF

Answer: C

Explanation:
Support for multiple instances per link—With OSPFv3, you can run multiple instances of the OSPF protocol over a single link. This is accomplished by assigning an OSPFv3 instance ID number. An interface that is assigned to an instance ID drops packets that contain a different ID.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/ospf/ospf-concepts/ospfv3

NEW QUESTION 49
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 52
An administrator Just enabled HA Heartbeat Backup on two devices However, the status on tie firewall's dashboard is showing as down High Availability.
What could an administrator do to troubleshoot the issue?

A. Goto Device > High Availability> General > HA Pair Settings > Setup and configuring the peer IP for heartbeat backup
B. Check peer IP address In the permit list In Device > Setup > Management > Interfaces > Management Interface Settings
C. Go to Device > High Availability > HA Communications> General> and check the Heartbeat Backup under Election Settings
D. Check peer IP address for heartbeat backup to Device > High Availability > HA Communications > Packet Forwarding settings.

Answer: B

Explanation:
If the HA status is showing as down after enabling HA Heartbeat Backup on two devices, an administrator could troubleshoot the issue by checking the peer IP address in the permit list in Device > Setup > Management > Interfaces > Management Interface Settings. This is described in the Palo Alto Networks PCNSE Study Guide in Chapter 7: High Availability, under the section "Configure Heartbeat Backup for Redundancy":
"Verify that the management interface's permitted IP addresses on each peer includes the IP address of the other peer's Heartbeat Backup interface."

NEW QUESTION 57
What is the function of a service route?

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

Answer: C

NEW QUESTION 62
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 67
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 71
A network security administrator has an environment with multiple forms of authentication. There is a network access control system in place that authenticates and restricts access for wireless users, multiple Windows domain controllers, and an MDM solution for company-provided smartphones. All of these devices have

their authentication events logged.
Given the information, what is the best choice for deploying User-ID to ensure maximum coverage?

A. Syslog listener
B. agentless User-ID with redistribution
C. standalone User-ID agent
D. captive portal

Answer: C

NEW QUESTION 74
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 76
A network administrator plans a Prisma Access deployment with three service connections, each with a BGP peering to a CPE. The administrator needs to minimize the BGP configuration and management overhead on on-prem network devices.
What should the administrator implement?

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

Answer: C

NEW QUESTION 79
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: D

NEW QUESTION 82
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 83
Given the following snippet of a WildFire submission log. did the end-user get access to the requested information and why or why not?

TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-2...		low	any		
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-		low	any		

A. Ye
B. because the action is set to "allow "
C. No because WildFire categorized a file with the verdict "malicious"
D. Yes because the action is set to "alert"
E. No because WildFire classified the seventy as "high."

Answer: A

NEW QUESTION 88
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 92
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 93
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 97
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 102
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

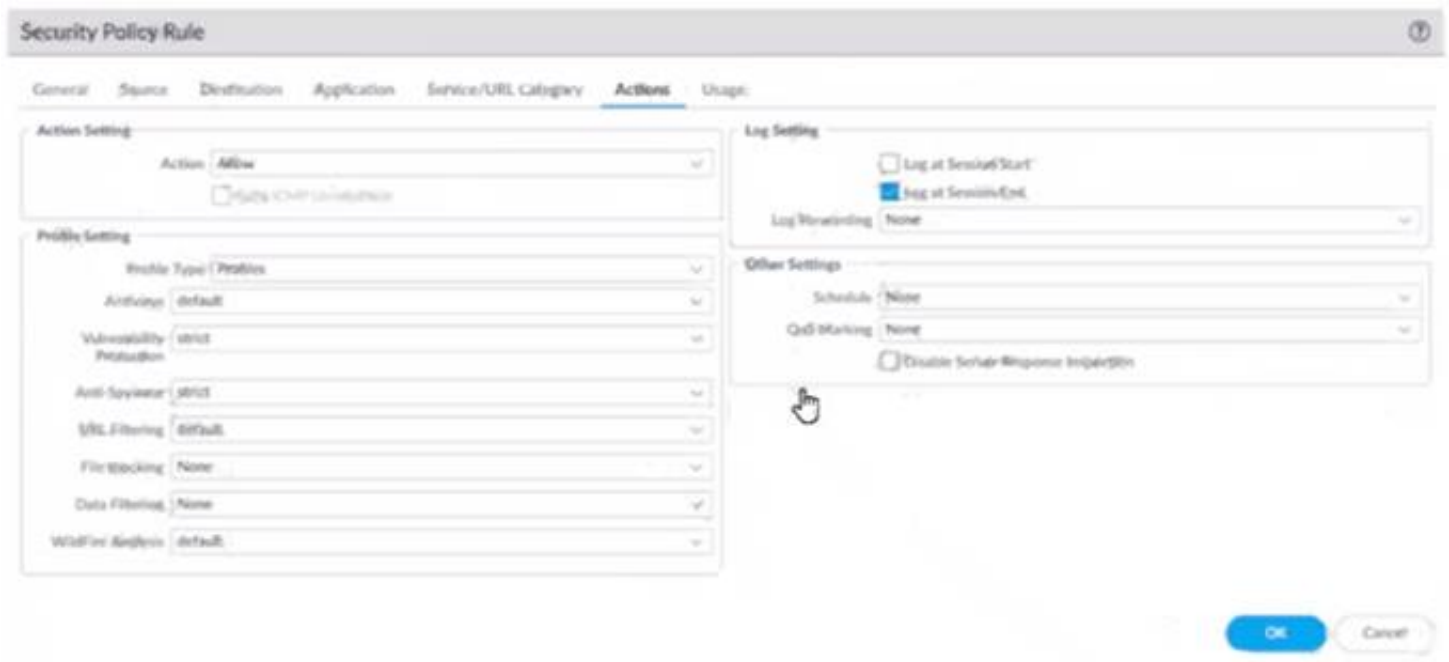
NEW QUESTION 107
An engineer is in the planning stages of deploying User-ID in a diverse directory services environment. Which server OS platforms can be used for server monitoring with User-ID?

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

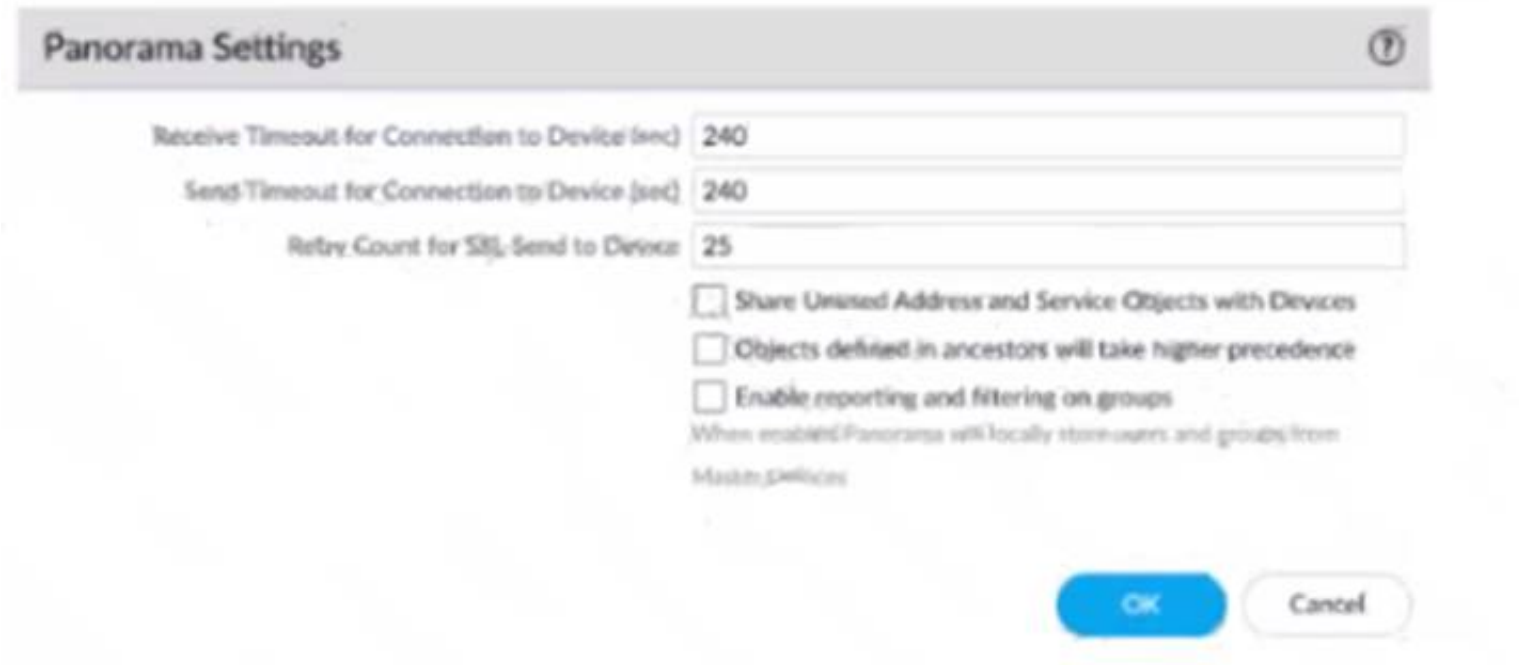
Answer: B

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

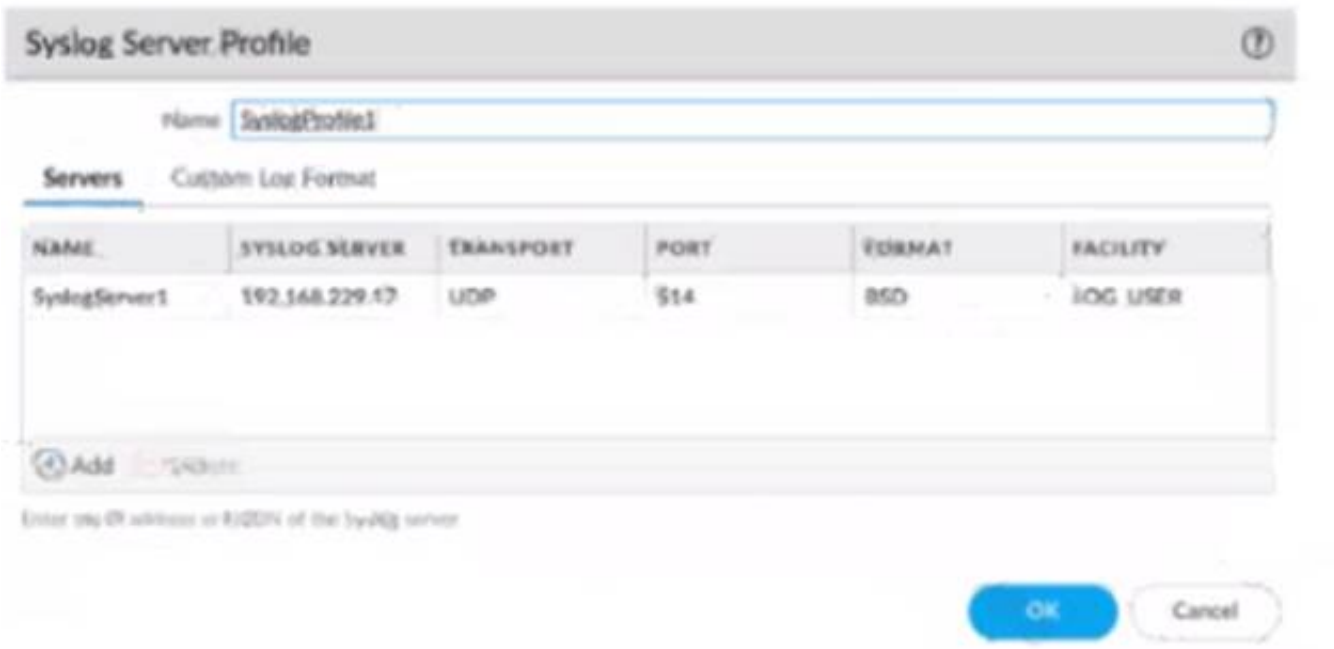
NEW QUESTION 108
An administrator can not see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall.
Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?
A)



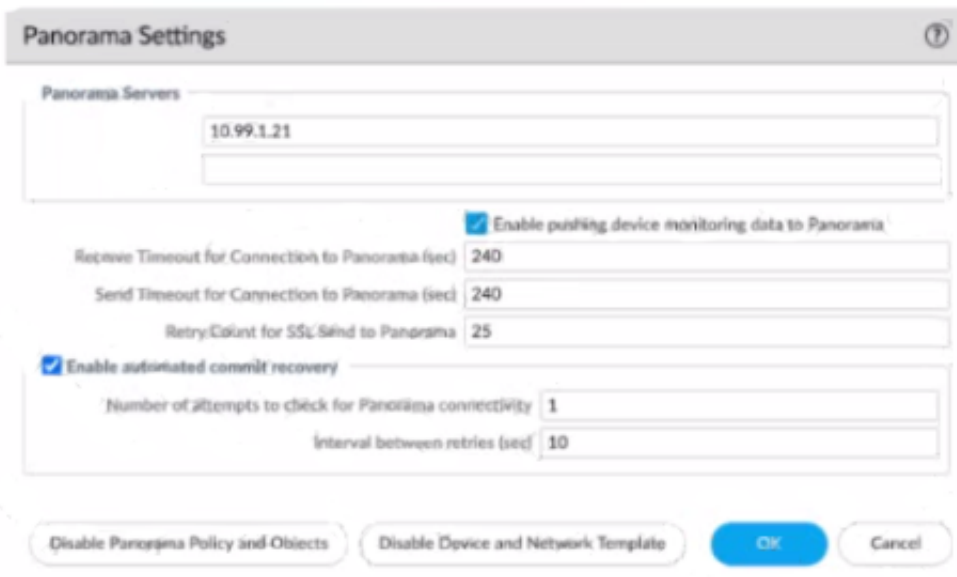
B)



C)



D)



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

Answer: C

NEW QUESTION 112
An administrator is required to create an application-based Security policy rule to allow Evernote. The Evernote application implicitly uses SSL and web browsing. What is the minimum the administrator needs to configure in the Security rule to allow only Evernote?

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

Answer: C

NEW QUESTION 113
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 118
A network security administrator wants to begin inspecting bulk user HTTPS traffic flows egressing out of the internet edge firewall. Which certificate is the best choice to configure as an SSL Forward Trust certificate?

A. A self-signed Certificate Authority certificate generated by the firewall
B. A Machine Certificate for the firewall signed by the organization's PKI
C. A web server certificate signed by the organization's PKI
D. A subordinate Certificate Authority certificate signed by the organization's PKI

Answer: A

NEW QUESTION 122
A network administrator is troubleshooting an issue with Phase 2 of an IPSec VPN tunnel. The administrator determines that the lifetime needs to be changed to match the peer.
Where should this change be made?

A. IKE Gateway profile
B. IPSec Crypto profile
C. IPSec Tunnel settings
D. IKE Crypto profile

Answer: C

NEW QUESTION 125
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 129
Which source is the most reliable for collecting User-ID user mapping?

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

Answer: A

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

NEW QUESTION 134
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 138
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 139
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 140
A remote administrator needs firewall access on an untrusted interface. Which two components are required on the firewall to configure certificate-based administrator authentication to the web UI? (Choose two)

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

Answer: BC

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

NEW QUESTION 144
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 146
An administrator wants to enable WildFire inline machine learning. Which three file types does WildFire inline ML analyze? (Choose three.)

A. MS Office
B. ELF
C. APK
D. VBscripts
E. Powershell scripts

Answer: CDE

NEW QUESTION 147
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

PCNSE Practice Exam Features:

* PCNSE Questions and Answers Updated Frequently

* PCNSE Practice Questions Verified by Expert Senior Certified Staff

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

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