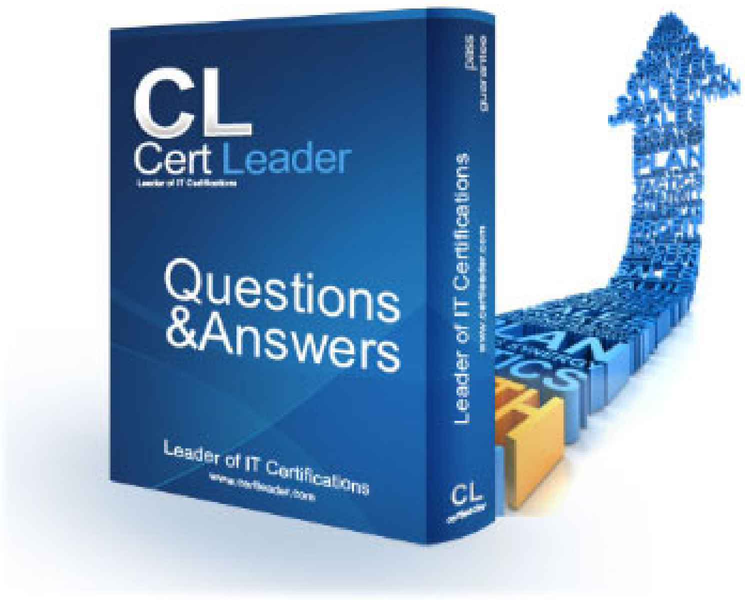
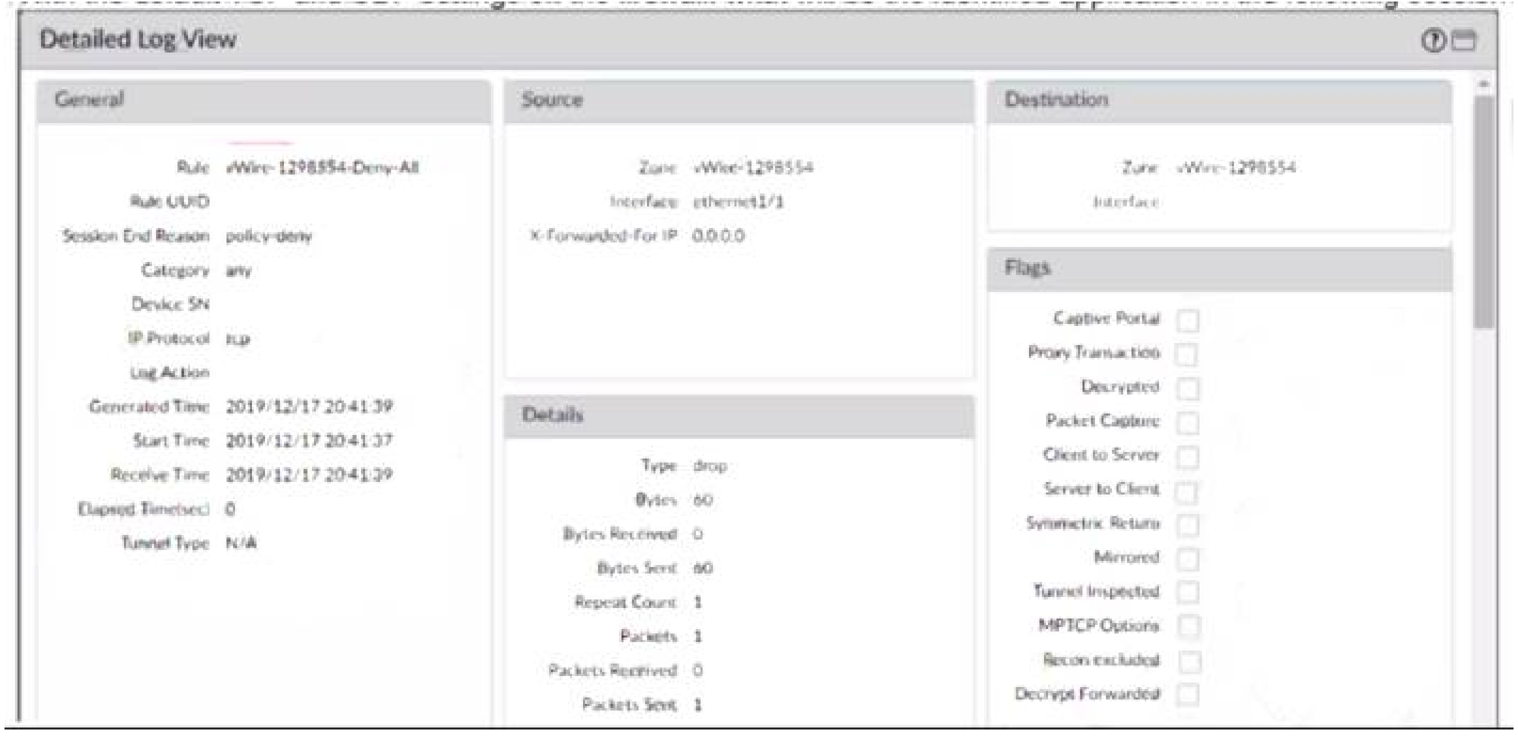
PCNSE Dumps

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

https://www.certleader.com/PCNSE-dumps.html



NEW QUESTION 1
With the default TCP and UDP settings on the firewall, what will be the identified application in the following session?


Detailed Log View

General

Rule	vWire-1298554-Deny-All
Rule UUID	
Session End Reason	policy-deny
Category	any
Device SN	
IP Protocol	tcp
Log Action	
Generated Time	2019/12/17 20:41:39
Start Time	2019/12/17 20:41:37
Receive Time	2019/12/17 20:41:39
Elapsed Time(sec)	0
Tunnel Type	N/A

Source

Zone	vWire-1298554
Interface	ethernet1/1
X-Forwarded-For IP	0.0.0.0

Details

Type	drop
Bytes	60
Bytes Received	0
Bytes Sent	60
Repeat Count	1
Packets	1
Packets Received	0
Packets Sent	1

Destination

Zone	vWire-1298554
Interface	

Flags

Captive Portal	□
Proxy Transaction	□
Decrypted	□
Packet Capture	□
Client to Server	□
Server to Client	□
Symmetric Return	□
Mirrored	□
Tunnel Inspected	□
MPTCP Options	□
Recon excluded	□
Decrypt Forwarded	□

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

Answer: D

Explanation:
Traffic didnt match any other policies and so landed at the implicit "deny all" policy. If it's deny all, the traffic was dropped before the application could be determined. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

NEW QUESTION 2
A firewall engineer creates a NAT rule to translate IP address 1.1.1.10 to 192.168.1.10. The engineer also plans to enable DNS rewrite so that the firewall rewrites the IPv4 address in a DNS response based on the original destination IP address and translated destination IP address configured for the rule. The engineer wants the firewall to rewrite a DNS response of 1.1.1.10 to 192.168.1.10.
What should the engineer do to complete the configuration?

A. Create a U-Turn NAT to translate the destination IP address 192.168.1.10 to 1.1.1.10 with the destination port equal to UDP/53.
B. Enable DNS rewrite under the destination address translation in the Translated Packet section of the NAT rule with the direction Forward.
C. Enable DNS rewrite under the destination address translation in the Translated Packet section of the NAT rule with the direction Reverse.
D. Create a U-Turn NAT to translate the destination IP address 1.1.1.10 to 192.168.1.10 with the destination port equal to UDP/53.

Answer: B

Explanation:
If the DNS response matches the Original Destination Address in the rule, translate the DNS response using the same translation the rule uses. For example, if the rule translates IP address 1.1.1.10 to 192.168.1.10, the firewall rewrites a DNS response of 1.1.1.10 to 192.168.1.10.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/source-nat-and-destination-nat/desti

NEW QUESTION 3
To ensure that a Security policy has the highest priority, how should an administrator configure a Security policy in the device group hierarchy?

A. Add the policy to the target device group and apply a master device to the device group.
B. Reference the targeted device's templates in the target device group.
C. Clone the security policy and add it to the other device groups.
D. Add the policy in the shared device group as a pre-rule

Answer: D

Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-device-groups/man
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-conf

NEW QUESTION 4
An engineer configures a specific service route in an environment with multiple virtual systems instead of using the inherited global service route configuration.
What type of service route can be used for this configuration?

A. IPv6 Source or Destination Address
B. Destination-Based Service Route
C. IPv4 Source Interface
D. Inherit Global Setting

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/virtual-systems/customize-service-routes-for-a-vir

NEW QUESTION 5
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: C

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. The following link has a video that demonstrates that B is the correct answer.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNfeCAG

NEW QUESTION 6
When you import the configuration of an HA pair into Panorama, how do you prevent the import from affecting ongoing traffic?

A. Set the passive link state to shutdown".
B. Disable config sync.
C. Disable the HA2 link.
D. Disable HA.

Answer: B

Explanation:
To prevent the import from affecting ongoing traffic when you import the configuration of an HA pair into Panorama, you should disable config sync on both firewalls. Config sync is a feature that enables the firewalls in an HA pair to synchronize their configurations and maintain consistency. However, when you import the configuration of an HA pair into Panorama, you want to avoid any changes to the firewall configuration until you verify and commit the imported configuration on Panorama. Therefore, you should disable config sync before importing the configuration, and re-enable it after committing the changes on
Panorama12. References: Migrate a Firewall HA Pair to Panorama Management, PCNSE Study Guide (page 50)

NEW QUESTION 7
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 in the User Credential Submission column and set action to block Select the User credential Detection tab and select Use Domain Credential Filter 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 on Site Access column and set action to block Click the User credential Detection tab and select IP User Mapping Commit
D. 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

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-u https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/prevent-credential-phishing/set-up-cre

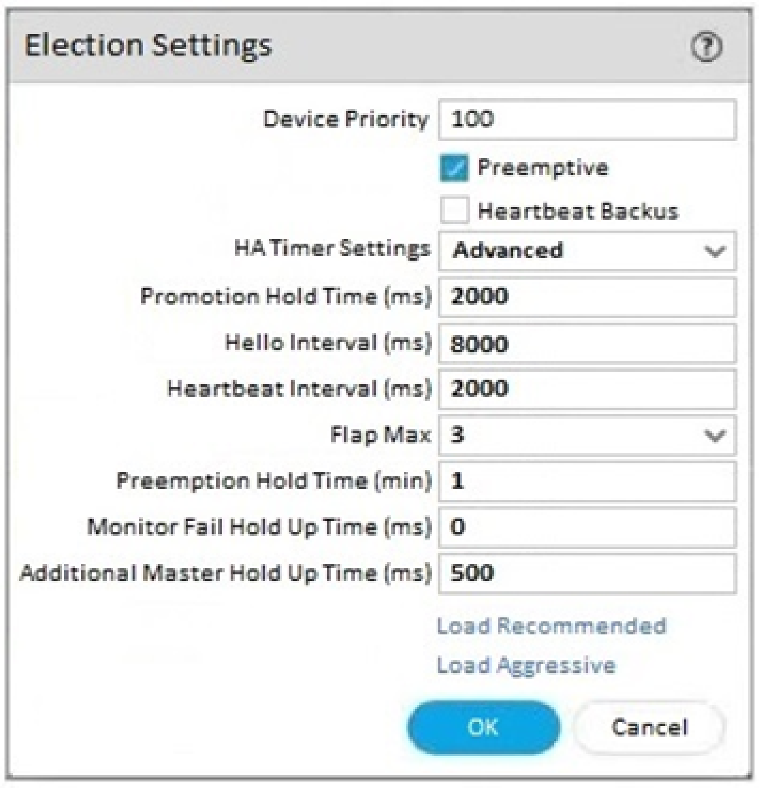
NEW QUESTION 8
An engineer needs to configure a standardized template for all Panorama-managed firewalls. These settings will be configured on a template named "Global" and will be included in all template stacks.
Which three settings can be configured in this template? (Choose three.)

A. Log Forwarding profile
B. SSL decryption exclusion
C. Email scheduler
D. Login banner
E. Dynamic updates

Answer: BDE

Explanation:
A template is a set of configuration options that can be applied to one or more firewalls or virtual systems managed by Panorama. A template can include settings from the Device and Network tabs on the firewall web interface, such as login banner, SSL decryption exclusion, and dynamic updates4. These settings can be configured in a template named “Global” and included in all template stacks. A template stack is a group of templates that Panorama pushes to managed firewalls in an ordered hierarchy4. References: Manage Templates and Template Stacks, PCNSE Study Guide (page 50)

NEW QUESTION 9
An engineer is reviewing the following high availability (HA) settings to understand a recent HAfailover event.



Election Settings

Device Priority	100
	☑ Preemptive
	□ Heartbeat Backus
HA Timer Settings	Advanced
Promotion Hold Time (ms)	2000
Hello Interval (ms)	8000
Heartbeat Interval (ms)	2000
Flap Max	3
Preemption Hold Time (min)	1
Monitor Fail Hold Up Time (ms)	0
Additional Master Hold Up Time (ms)	500

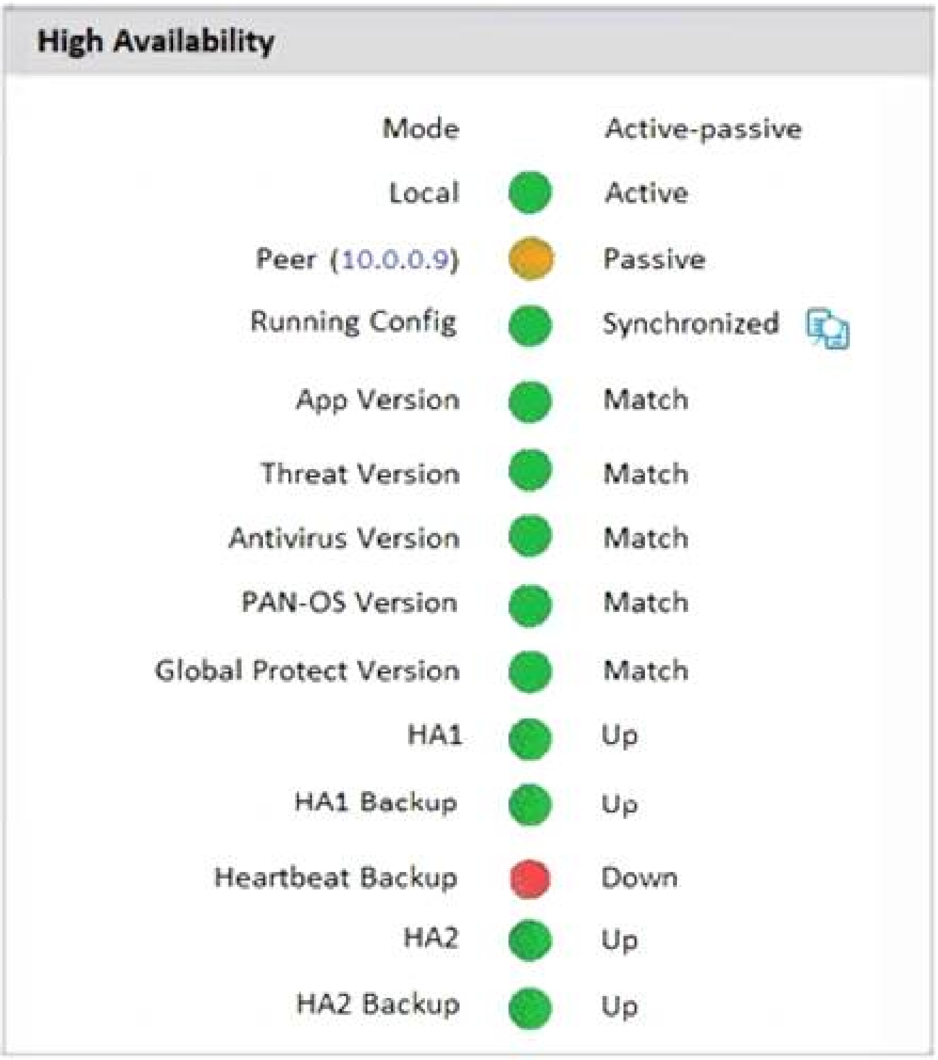
Which timer determines the frequency between packets sent to verify that the HA functionality on the other HA firewall is operational?

A. Monitor Fail Hold Up Time
B. Promotion Hold Time
C. Heartbeat Interval
D. Hello Interval

Answer: D

Explanation:
The timer that determines the frequency between packets sent to verify that the HA functionality on the other HA firewall is operational is the Hello Interval. The Hello Interval is the interval in milliseconds between hello packets that are sent to check the HA status of the peer firewall. The default value for the Hello Interval is 8000 ms for all platforms, and the range is 8000-60000 ms. If the firewall does not receive a hello packet from its peer within the specified interval, it will declare the peer as failed and initiate a failover12. References: H Timers, Layer 3 High Availability with Optimal Failover Times Best Practices
How to Configure Ping Interval/Timeout Settings ... - Palo Alto Networks

NEW QUESTION 10
An administrator Just enabled HA Heartbeat Backup on two devices However, the status on tie firewall's dashboard is showing as down High Availability.



High Availability

Mode		Active-passive
Local	🟢	Active
Peer (10.0.0.9)	🟠	Passive
Running Config	🟢	Synchronized
App Version	🟢	Match
Threat Version	🟢	Match
Antivirus Version	🟢	Match
PAN-OS Version	🟢	Match
Global Protect Version	🟢	Match
HA1	🟢	Up
HA1 Backup	🟢	Up
Heartbeat Backup	🔴	Down
HA2	🟢	Up
HA2 Backup	🟢	Up

What could an administrator do to troubleshoot the issue?

A. Go to 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:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClF4CAK

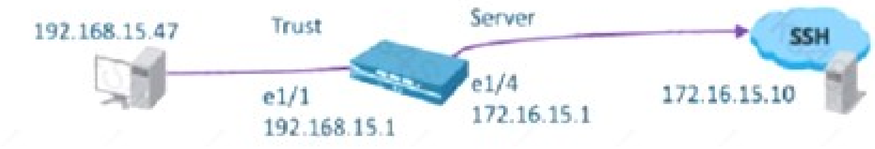
NEW QUESTION 10
Why would a traffic log list an application as "not-applicable”?

A. The firewall denied the traffic before the application match could be performed.
B. The TCP connection terminated without identifying any application data
C. There was not enough application data after the TCP connection was established
D. The application is not a known Palo Alto Networks App-ID.

Answer: A

Explanation:
traffic log would list an application as “not-applicable” if the firewall denied the traffic before the application match could be performed. This can happen if the traffic matches a security rule that is set to deny based on any parameter other than the application, such as source, destination, port, service, etc1. In this case, the firewall does not inspect the application data and discards the traffic, resulting in a “not-applicable” entry in the application field of the traffic log1.

NEW QUESTION 11
Refer to the diagram. Users at an internal system want to ssh to the SSH server. The server is configured to respond only to the ssh requests coming from IP 172.16.16.1.
In order to reach the SSH server only from the Trust zone, which Security rule and NAT rule must be configured on the firewall?



A. NAT Rule:Source Zone: Trust - Source IP: Any - Destination Zone: Server Destination IP: 172.16.15.10 Source Translation: Static IP / 172.16.15.1 Security Rule:Source Zone: Trust - Source IP: Any - Destination Zone: Trust Destination IP: 172.16.15.10 - Application: ssh
B. NAT Rule:Source Zone: Trust Source IP: 192.168.15.0/24 Destination Zone: Trust - Destination IP: 192.168.15.1 Destination Translation: Static IP / 172.16.15.10 Security Rule:Source Zone: Trust Source IP: 192.168.15.0/24 Destination Zone: Server - Destination IP: 172.16.15.10 - Application: ssh
C. NAT Rule:Source Zone: Trust - Source IP: Any - Destination Zone: Trust Destination IP: 192.168.15.1 Destination Translation: Static IP /172.16.15.10 Security Rule:Source Zone: Trust - Source IP: Any - Destination Zone: Server Destination IP: 172.16.15.10 - Application: ssh
D. NAT Rule:Source Zone: Trust Source IP: Any - Destination Zone: Server Destination IP: 172.16.15.10 Source Translation: dynamic-ip-and-port / ethernet1/4 Security Rule:Source Zone: Trust - Source IP: Any - Destination Zone: Server Destination IP: 172.16.15.10 - Application: ssh

Answer: D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhwCAC https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/source-nat-and-destination-nat/sou

NEW QUESTION 15
An engineer is configuring a firewall with three interfaces:
• MGT connects to a switch with internet access.
• Ethernet1/1 connects to an edge router.
• Ethernet1/2 connects to a visualization network.
The engineer needs to configure dynamic updates to use a dataplane interface for internet traffic. What should be configured in Setup > Services > Service Route Configuration to allow this traffic?

A. Set DNS and Palo Alto Networks Services to use the ethernet1/1 source interface.
B. Set DNS and Palo Alto Networks Services to use the ethernet1/2 source interface.
C. Set DNS and Palo Alto Networks Services to use the MGT source interface.
D. Set DDNS and Palo Alto Networks Services to use the MGT source interface.

Answer: A

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGJCA0

NEW QUESTION 20
An engineer troubleshoots a Panorama-managed firewall that is unable to reach the DNS servers configured via a global template. As a troubleshooting step, the engineer needs to configure a local DNS server in place of the template value.
Which two actions can be taken to ensure that only the specific firewall is affected during this process? (Choose two)

A. Configure the DNS server locally on the firewall.
B. Change the DNS server on the global template.
C. Override the DNS server on the template stack.
D. Configure a service route for DNS on a different interface.

Answer: AC

Explanation:
To override a device and network setting applied by a template, you can either configure the setting locally on the firewall or override the setting on the template stack. Configuring the setting locally on the firewall will
copy the setting to the local configuration of the device and will no longer be controlled by the template. Overriding the setting on the template stack will apply the setting to all the firewalls that are assigned to the template stack, unless the setting is also overridden locally on a firewall. Changing the setting on the global

template will affect all the firewalls that inherit the setting from the template, which is not desirable in this scenario. Configuring a service route for DNS on a different interface will not change the DNS server address, but only the interface that the firewall uses to reach the DNS server. References:

- Override a Template Setting
- Overriding Panorama Template settings

NEW QUESTION 22
Which GloDalProtecl gateway setting is required to enable split-tunneting by access route, destination domain and application?

A. Tunnel mode
B. Satellite mode
C. IPSec mode
D. No Direct Access to local networks

Answer: A

Explanation:
https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-gateways/split-tunnel-tra

NEW QUESTION 26
Where can a service route be configured for a specific destination IP?

A. Use Netw ork > Virtual Routers, select the Virtual Router > Static Routes > IPv4
B. Use Device > Setup > Services > Services
C. Use Device > Setup > Services > Service Route Configuration > Customize > Destination
D. Use Device > Setup > Services > Service Route Configuration > Customize > IPv4

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGJCA0

NEW QUESTION 29
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)

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

Answer: ACD

Explanation:
ttps://www.kareemccie.com/2021/05/palo-alto-firewall-packet-flow.html

NEW QUESTION 34
A network administrator wants to deploy SSL Forward Proxy decryption. What two attributes should a forward trust certificate have? (Choose two.)

A. A subject alternative name
B. A private key
C. A server certificate
D. A certificate authority (CA) certificate

Answer: BD

Explanation:
The two attributes that a forward trust certificate should have for SSL Forward Proxy decryption are:

- B: A private key. This is the key that the firewall uses to sign the certificates that it generates for the decrypted sessions. The private key must be securely stored on the firewall and not shared with anyone1.
- D: A certificate authority (CA) certificate. This is the certificate that the firewall uses to issue the certificates for the decrypted sessions. The CA certificate must be trusted by the client browsers and devices that receive the certificates from the firewall1.

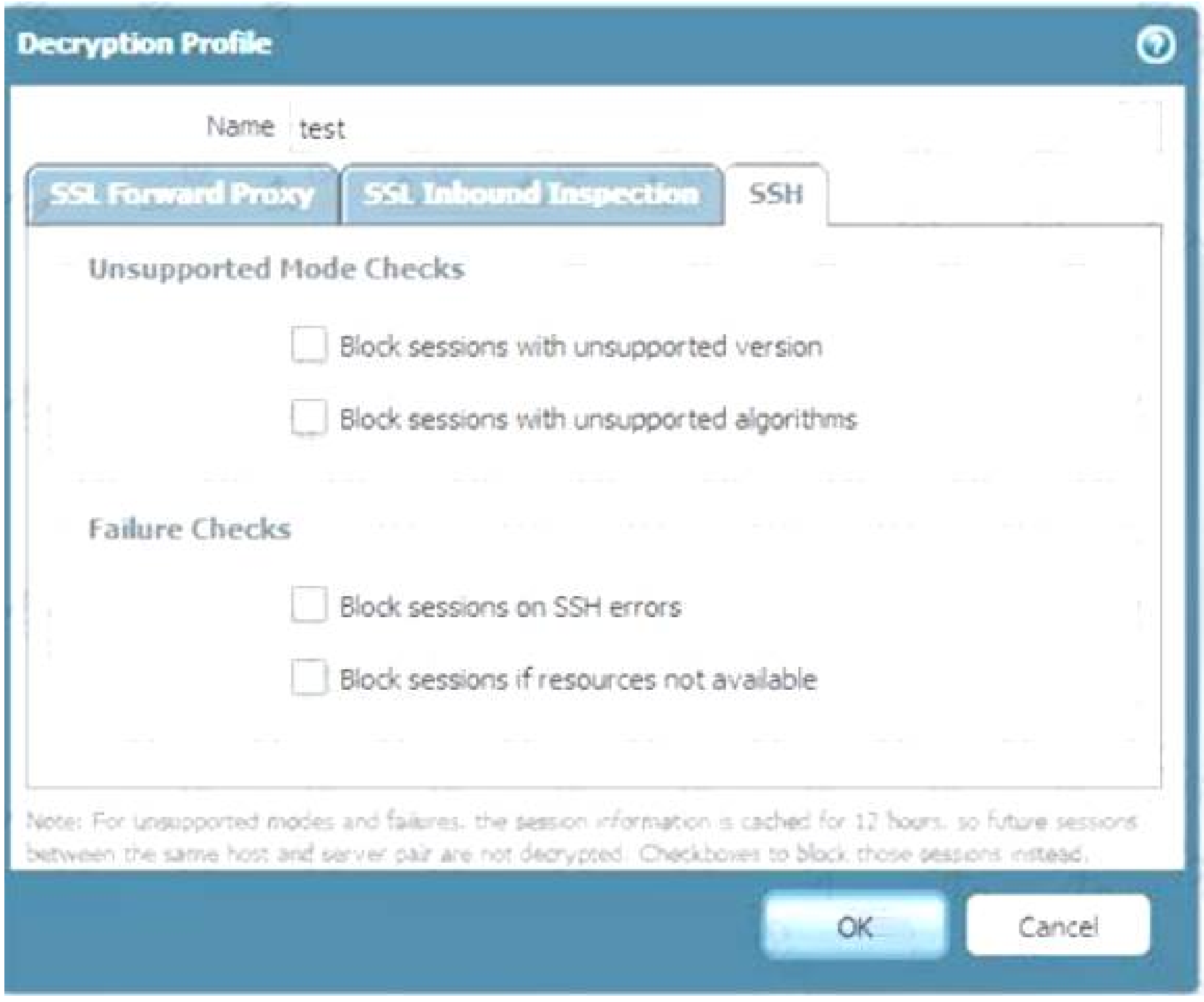
NEW QUESTION 38
An organization wants to begin decrypting guest and BYOD traffic.
Which NGFW feature can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted?

A. Authentication Portal
B. SSL Decryption profile
C. SSL decryption policy
D. comfort pages

Answer: A

Explanation:
An authentication portal is a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly

notify them that their traffic will be decrypted. An authentication portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The authentication portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button. The authentication portal can also be configured to use different authentication methods, such as local database, RADIUS, LDAP, Kerberos, or SAML1. By using an authentication portal, the firewall can redirect BYOD users to a web page where they can learn about the decryption policy, download and install the CA certificate, and agree to the terms of use before accessing the network or the internet2.
An SSL decryption profile is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption profile is a set of options that define how the firewall handles SSL/TLS traffic that it decrypts. An SSL decryption profile can include settings such as certificate verification, unsupported protocol handling, session caching, session resumption, algorithm selection, etc3. An SSL decryption profile does not provide any user identification or notification functions.
An SSL decryption policy is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption policy is a set of rules that determine which traffic the firewall decrypts based on various criteria, such as source and destination zones, addresses, users, applications, services, etc. An SSL decryption policy can also specify which type of decryption to apply to the traffic, such as SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy4. An SSL decryption policy does not provide any user identification or notification functions.
Comfort pages are not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. Comfort pages are web pages that the firewall displays to users when it blocks or fails to decrypt certain traffic due to security policy or technical reasons. Comfort pages can include information such as the reason for blocking or failing to decrypt the traffic, the URL of the original site, the firewall serial number, etc5. Comfort pages do not provide any user identification or notification functions before decrypting the traffic.
References: Configure an Authentication Portal, Redirect Users Through an Authentication Portal, SSL Decryption Profile, Decryption Policy, Comfort Pages
How to Implement SSH Decryption on a Palo Alto Networks Device



Name test

Unsupported Mode Checks

□ Block sessions with unsupported version

□ Block sessions with unsupported algorithms

Failure Checks

□ Block sessions on SSH errors

□ Block sessions if resources not available

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Checkboxes to block those sessions instead.

NEW QUESTION 42
Which two profiles should be configured when sharing tags from threat logs with a remote User-ID agent? (Choose two.)

A. Log Ingestion
B. HTTP
C. Log Forwarding
D. LDAP

Answer: BC

Explanation:
>Threat logs, create a log forwarding profile to define how you want the firewall or Panorama to handle logs.
>Configure an HTTP server profile to forward logs to a remote User-ID agent. > Select the log forwarding profile you created then select this server profile as the HTTP server profile https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/use-auto-tagging-to-automate-security-actio

NEW QUESTION 44
An engineer is designing a deployment of multi-vsys firewalls.
What must be taken into consideration when designing the device group structure?

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

Answer: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClETCA0
A device group is a logical grouping of firewalls that share the same security policy rules. A device group can contain multiple vsys and firewalls, including multi-

vsys firewalls. A multi-vsys firewall can have each vsys in a different device group, depending on the desired security policy for each vsys. This allows for granular control and flexibility in managing multi-vsys firewalls with Panorama1. References: Device Group Push to Multi-VSYS Firewall, Configure Virtual Systems, PCNSE Study Guide (page 50)

NEW QUESTION 48
An administrator has two pairs of firewalls within the same subnet. Both pairs of firewalls have been configured to use High Availability mode with Active/Passive. The ARP tables for upstream routes display the same MAC address being shared for some of these firewalls.
What can be configured on one pair of firewalls to modify the MAC addresses so they are no longer in conflict?

A. Configure a floating IP between the firewall pairs.
B. Change the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet.
C. Change the interface type on the interfaces that have conflicting MAC addresses from L3 to VLAN.
D. On one pair of firewalls, run the CLI command: set network interface vlan arp.

Answer: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCAS
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCAS

NEW QUESTION 50
An administrator configures a site-to-site IPsec VPN tunnel between a PA-850 and an external customer on their policy-based VPN devices.
What should an administrator configure to route interesting traffic through the VPN tunnel?

A. Proxy IDs
B. GRE Encapsulation
C. Tunnel Monitor
D. ToS Header

Answer: A

Explanation:
An administrator should configure proxy IDs to route interesting traffic through the VPN tunnel when the peer device is a policy-based VPN device. Proxy IDs are used to identify the traffic that belongs to a particular IPSec VPN and to direct it to the appropriate tunnel. Proxy IDs consist of a local IP address, a remote IP address, and an application (protocol and port numbers). Each proxy ID is considered to be a VPN tunnel and is counted towards the IPSec VPN tunnel capacity of the firewall. Proxy IDs are required for IKEv1 VPNs and optional for IKEv2 VPNs. If the proxy ID is not configured, the firewall uses the default values of source IP: 0.0.0.0/0, destination IP: 0.0.0.0/0, and application: any, which may not match the peer's policy and result in a failure to establish the VPN connection.
References:

- Proxy ID for IPSec VPN
- Set Up an IPSec Tunnel

NEW QUESTION 54
During the process of developing a decryption strategy and evaluating which websites are required for corporate users to access, several sites have been identified that cannot be decrypted due to technical reasons. In this case, the technical reason is unsupported ciphers Traffic to these sites will therefore be blocked if decrypted.
How should the engineer proceed?

A. Install the unsupported cipher into the firewall to allow the sites to be decrypted
B. Allow the firewall to block the sites to improve the security posture.
C. Add the sites to the SSL Decryption Exclusion list to exempt them from decryption.
D. Create a Security policy to allow access to those sites.

Answer: C

Explanation:
If some sites cannot be decrypted due to technical reasons, such as unsupported ciphers, and blocking them is not an option, then the engineer should add the sites to the SSL Decryption Exclusion list to exempt them from decryption. The SSL Decryption Exclusion list is a predefined list of sites that are not subject to SSL decryption by the firewall. The list includes sites that use certificate pinning, mutual authentication, or unsupported cipher suites. The engineer can also add custom sites to the list if they have a valid business reason or technical limitation for not decrypting them34. Adding the sites to the SSL Decryption Exclusion list will allow the traffic to pass through without being decrypted or blocked by the firewall. References: SSL Decryption Exclusion, Troubleshoot Unsupported Cipher Suites

NEW QUESTION 56
Which two key exchange algorithms consume the most resources when decrypting SSL traffic? (Choose two.)

A. ECDSA
B. ECDHE
C. RSA
D. DHE

Answer: BD

Explanation:
The two key exchange algorithms that consume the most resources when decrypting SSL traffic are ECDHE and DHE. These are both Diffie-Hellman based algorithms that enable perfect forward secrecy (PFS), which means that they generate a new and unique session key for each SSL/TLS session, and do not reuse any previous keys. This enhances the security of the encrypted communication, but also increases the computational cost and complexity of the key exchange process. ECDHE stands for Elliptic Curve Diffie-Hellman Ephemeral, which uses elliptic curve cryptography (ECC) to generate the session key. DHE stands for Diffie-Hellman Ephemeral, which uses modular arithmetic to generate the session key. Both ECDHE and DHE require more CPU and memory resources than

RSA, which is a non-PFS algorithm that uses public and private keys to encrypt and decrypt the session key123. References: Key Exchange Algorithms, Best Practices for Enabling SSL Decryption, PCNSE Study Guide (page 60)

NEW QUESTION 61
An organization conducts research on the benefits of leveraging the Web Proxy feature of PAN-OS 11.0. What are two benefits of using an explicit proxy method versus a transparent proxy method? (Choose two.)

A. No client configuration is required for explicit proxy, which simplifies the deployment complexity.
B. Explicit proxy supports interception of traffic using non-standard HTTPS ports.
C. It supports the X-Authenticated-User (XAU) header, which contains the authenticated username in the outgoing request.
D. Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy.

Answer: CD

Explanation:
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-us https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy

NEW QUESTION 63
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. Captive portal
B. Standalone User-ID agent
C. Syslog listener
D. Agentless User-ID with redistribution

Answer: C

Explanation:
A syslog listener is the best choice for deploying User-ID to ensure maximum coverage in an environment with multiple forms of authentication. A syslog listener is a feature that enables the firewall or Panorama to receive syslog messages from other systems and parse them for IP address-to-username mappings. A syslog listener can collect user mapping information from a variety of sources, such as network access control systems, domain controllers, MDM solutions, VPN gateways, wireless controllers, proxies, and more2. A syslog listener can also support multiple platforms and operating systems, such as Windows, Linux, macOS, iOS, Android, etc3. Therefore, a syslog listener can provide a comprehensive and flexible solution for User-ID deployment in a large-scale network. References: Configure a Syslog Listener for User Mapping, User-ID Agent Deployment Guide, PCNSE Study Guide (page 48)

NEW QUESTION 64
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-220
B. PA-800 Series
C. PA-5000 Series
D. PA-500
E. PA-3400 Series

Answer: ABE

Explanation:
https://docs.paloaltonetworks.com/compatibility-matrix/supported-os-releases-by-model/palo-alto-networks-nex

NEW QUESTION 67
Which type of policy in Palo Alto Networks firewalls can use Device-ID as a match condition?

A. NAT
B. DOS protection
C. QoS
D. Tunnel inspection

Answer: C

Explanation:
The type of policy in Palo Alto Networks firewalls that can use Device-ID as a match condition is QoS. This is because Device-ID is a feature that allows the firewall to identify and classify devices on the network based on their characteristics, such as vendor, model, OS, and role1. QoS policies are used to allocate bandwidth and prioritize traffic based on various criteria, such as application, user, source, destination, and device2. By using Device-ID as a match condition in QoS policies, the firewall can apply different QoS actions to different types of devices, such as IoT devices, laptops, smartphones, etc3. This can help optimize the network performance and ensure the quality of service for critical applications and devices.

NEW QUESTION 70
An engineer is configuring a Protection profile to defend specific endpoints and resources against malicious activity.
The profile is configured to provide granular defense against targeted flood attacks for specific critical systems that are accessed by users from the internet.
Which profile is the engineer configuring?

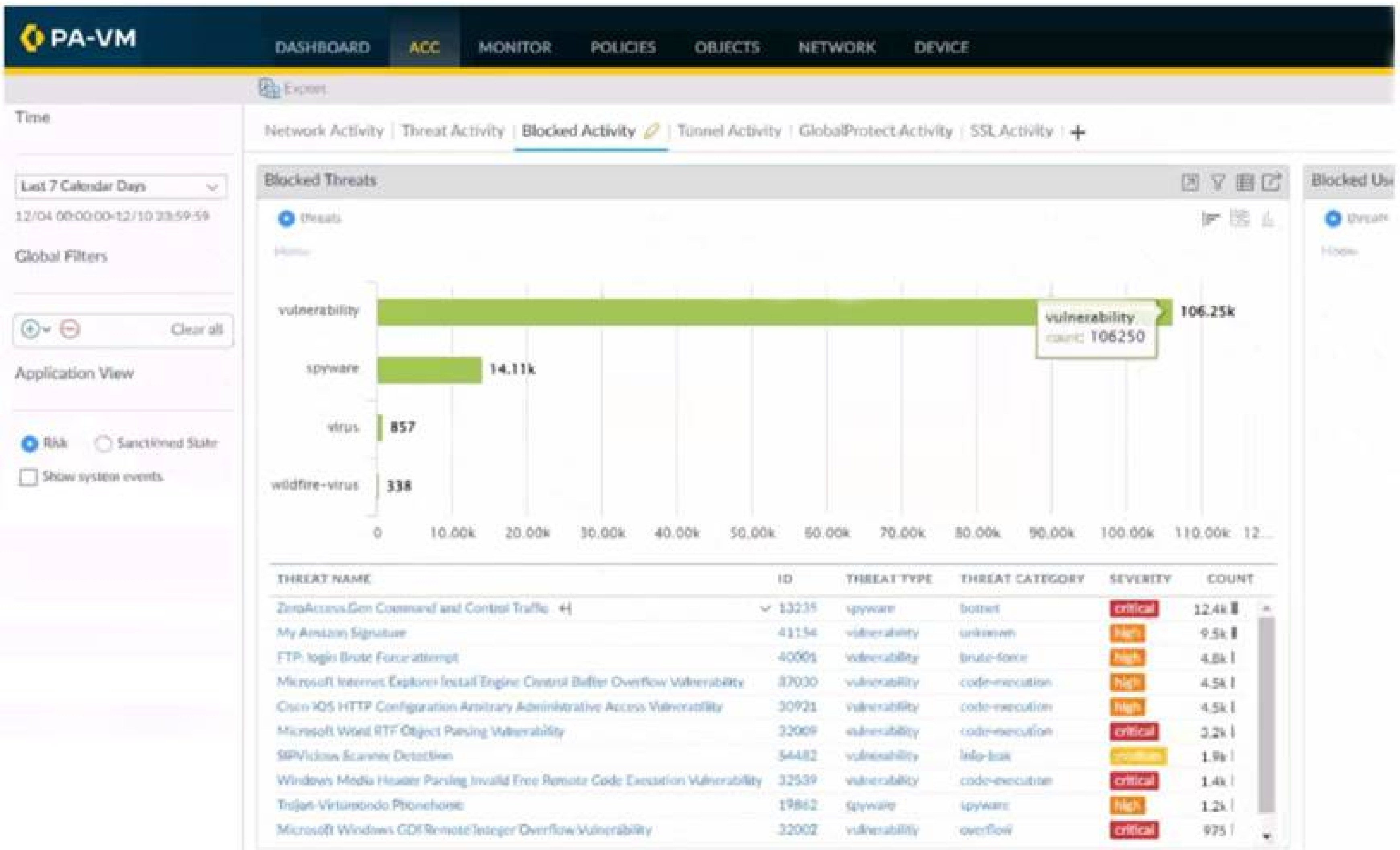
A. Packet Buffer Protection
B. Zone Protection
C. Vulnerability Protection

D. DoS Protection

Answer: D

Explanation:
The engineer is configuring a DoS Protection profile to defend specific endpoints and resources against malicious activity. A DoS Protection profile is a feature that enables the firewall to detect and prevent denial-of-service (DoS) attacks that attempt to overwhelm network resources or disrupt services. A DoS Protection profile can provide granular defense against targeted flood attacks for specific critical systems that are accessed by users from the internet, such as web servers, DNS servers, or VPN gateways. A DoS Protection profile can be applied to a security policy rule that matches the traffic to and from the protected systems, and can specify the thresholds and actions for different types of flood attacks, such as SYN, UDP, ICMP, or other IP floods12. References: DoS Protection, PCNSE Study Guide (page 58)

NEW QUESTION 75
Refer to the exhibit.



THREAT NAME	ID	THREAT TYPE	THREAT CATEGORY	SEVERITY	COUNT
ZeroAccess.Gen Command and Control Traffic	13235	spyware	botnet	critical	12.4k
My Amazon Signature	41154	vulnerability	unknown	high	9.5k
FTP: login Brute Force attempt	40001	vulnerability	brute-force	high	4.8k
Microsoft Internet Explorer Install Engine Control Buffer Overflow Vulnerability	37030	vulnerability	code-execution	high	4.5k
Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability	30921	vulnerability	code-execution	high	4.5k
Microsoft Word RTF Object Parsing Vulnerability	32009	vulnerability	code-execution	critical	3.2k
SIPVicious Scanner Detection	54482	vulnerability	info-leak	medium	1.9k
Windows Media Header Parsing Invalid Free Remote Code Execution Vulnerability	32539	vulnerability	code-execution	critical	1.4k
Trojan-Virtumondo Phonehome	19862	spyware	spyware	high	1.2k
Microsoft Windows GDI Remote Integer Overflow Vulnerability	32002	vulnerability	overflow	critical	975

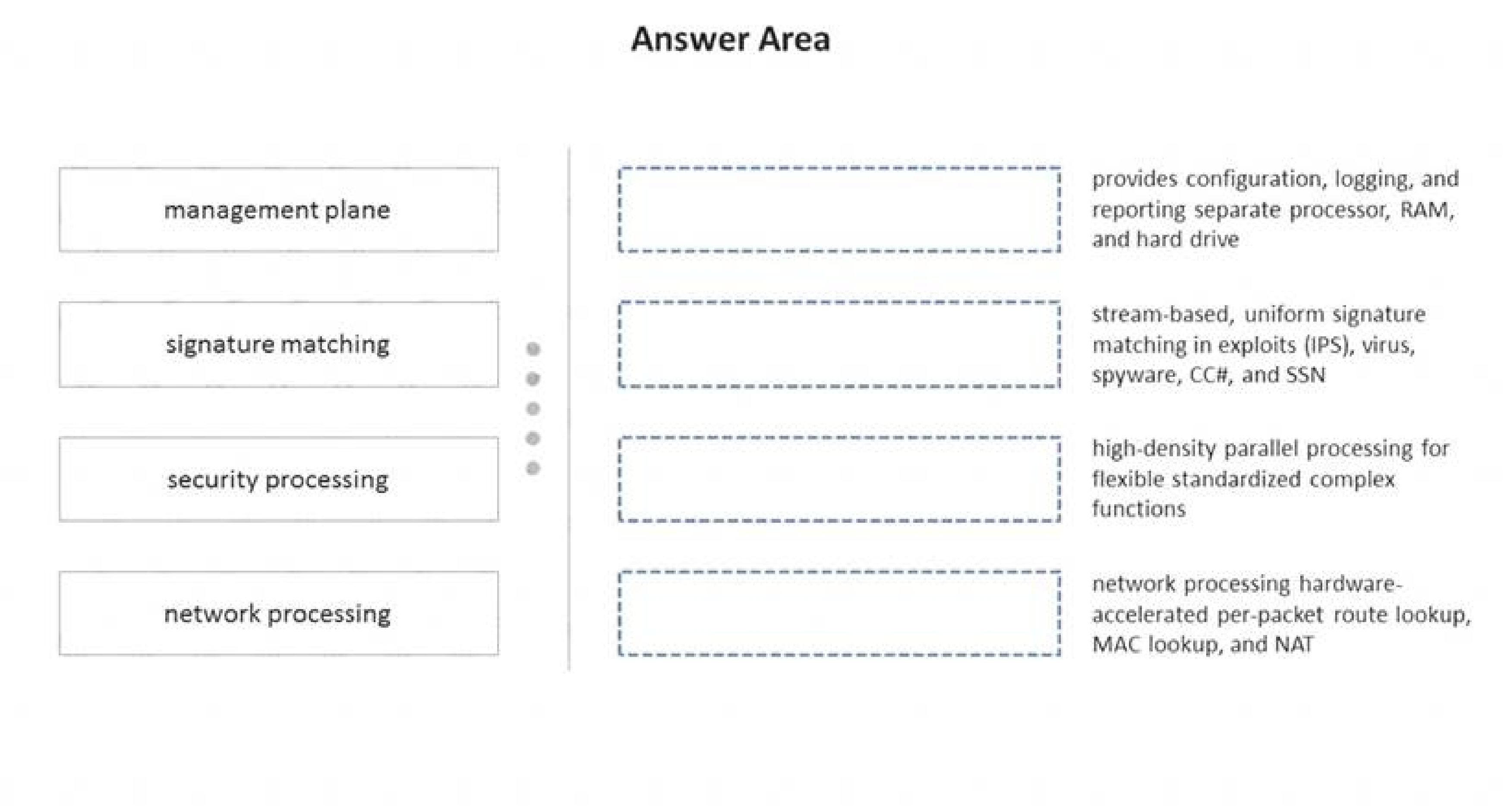
Using the above screenshot of the ACC, what is the best method to set a global filter, narrow down Blocked User Activity, and locate the user(s) that could be compromised by a botnet?

A. Click the hyperlink for the Zero Access.Gen threat.
B. Click the left arrow beside the Zero Access.Gen threat.
C. Click the source user with the highest threat count.
D. Click the hyperlink for the hotport threat Category.

Answer: B

Explanation:
Hover over an attribute in the table below the chart and click the arrow icon to the right of the attribute. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-the-application-command-center/int

NEW QUESTION 80
Match the terms to their corresponding definitions



Answer Area

management plane

signature matching

security processing

network processing

provides configuration, logging, and reporting separate processor, RAM, and hard drive

stream-based, uniform signature matching in exploits (IPS), virus, spyware, CC#, and SSN

high-density parallel processing for flexible standardized complex functions

network processing hardware-accelerated per-packet route lookup, MAC lookup, and NAT

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A close-up of a computer screen Description automatically generated
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnse-study-guide.p page 83

NEW QUESTION 83
If an administrator wants to apply QoS to traffic based on source, what must be specified in a QoS policy rule?

A. Post-NAT destination address
B. Pre-NAT destination address
C. Post-NAT source address
D. Pre-NAT source address

Answer: C

Explanation:
If an administrator wants to apply QoS to traffic based on source, they must specify the post-NAT source address in a QoS policy rule. This is because QoS is enforced on traffic as it egresses the firewall, and the firewall applies NAT rules before QoS rules. Therefore, the firewall will match the QoS policy rule based on the translated source address, not the original source address. If the administrator uses the pre-NAT source address in the QoS policy rule, the firewall will not be able to identify the traffic correctly and apply the desired QoS treatment. References:

- QoS Policy
- Configure QoS

NEW QUESTION 84
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: D

Explanation:
Regardless of whether you generate Forward Trust certificates from your Enterprise Root CA or use a
self-signed certificate generated on the firewall, generate a separate subordinate Forward Trust CA certificate for each firewall. The flexibility of using separate subordinate CAs enables you to revoke one certificate when you decommission a device (or device pair) without affecting the rest of the deployment and reduces the impact in any situation in which you need to revoke a certificate. Separate Forward Trust CAs on each firewall also helps troubleshoot issues because the CA error message the user sees includes information about the firewall the traffic is traversing. If you use the same Forward Trust CA on every firewall, you lose the granularity of that information.
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy

NEW QUESTION 85
An administrator receives the following error message:

"IKE phase-2 negotiation failed when processing Proxy ID. Received local id 192.168 33 33/24 type IPv4 address protocol 0 port 0, received remote id 172.16 33.33/24 type IPv4 address protocol 0 port 0."
How should the administrator identify the root cause of this error message?

A. In the IKE Gateway configuration, verify that the IP address for each VPN peer is accurate
B. Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure
C. Check whether the VPN peer on one end is set up correctly using policy-based VPN
D. In the IPSec Crypto profile configuration, verify that PFS is either enabled on both VPN peers or disabled on both VPN peers.

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-me The VPN peer on one end is using policy-based VPN. You must configure a Proxy ID on the Palo Alto
Networks firewall.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-me

NEW QUESTION 88
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 3
C. Layer 2
D. Tap
E. Virtual Wire

Answer: BCE

Explanation:
PAN-OS can decrypt and inspect SSL inbound and outbound connections going through the firewall. SSL decryption can occur on interfaces in virtual wire, Layer 2 or Layer 3 mode https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClmyCAC

NEW QUESTION 90
An engineer creates a set of rules in a Device Group (Panorama) to permit traffic to various services for a specific LDAP user group.
What needs to be configured to ensure Panorama can retrieve user and group information for use in these rules?

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

Answer: B

Explanation:
https://live.paloaltonetworks.com/t5/general-topics/what-is-a-master-device-in-device-groups/td-p/15032
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMtpCAG

NEW QUESTION 92
Phase two of a VPN will not establish a connection. The peer is using a policy-based VPN configuration. What part of the configuration should the engineer verify?

A. IKE Crypto Profile
B. Security policy
C. Proxy-IDs
D. PAN-OS versions

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClbXCAS https://live.paloaltonetworks.com/t5/general-topics/phase-2-tunnel-is-not-up/td-p/424789

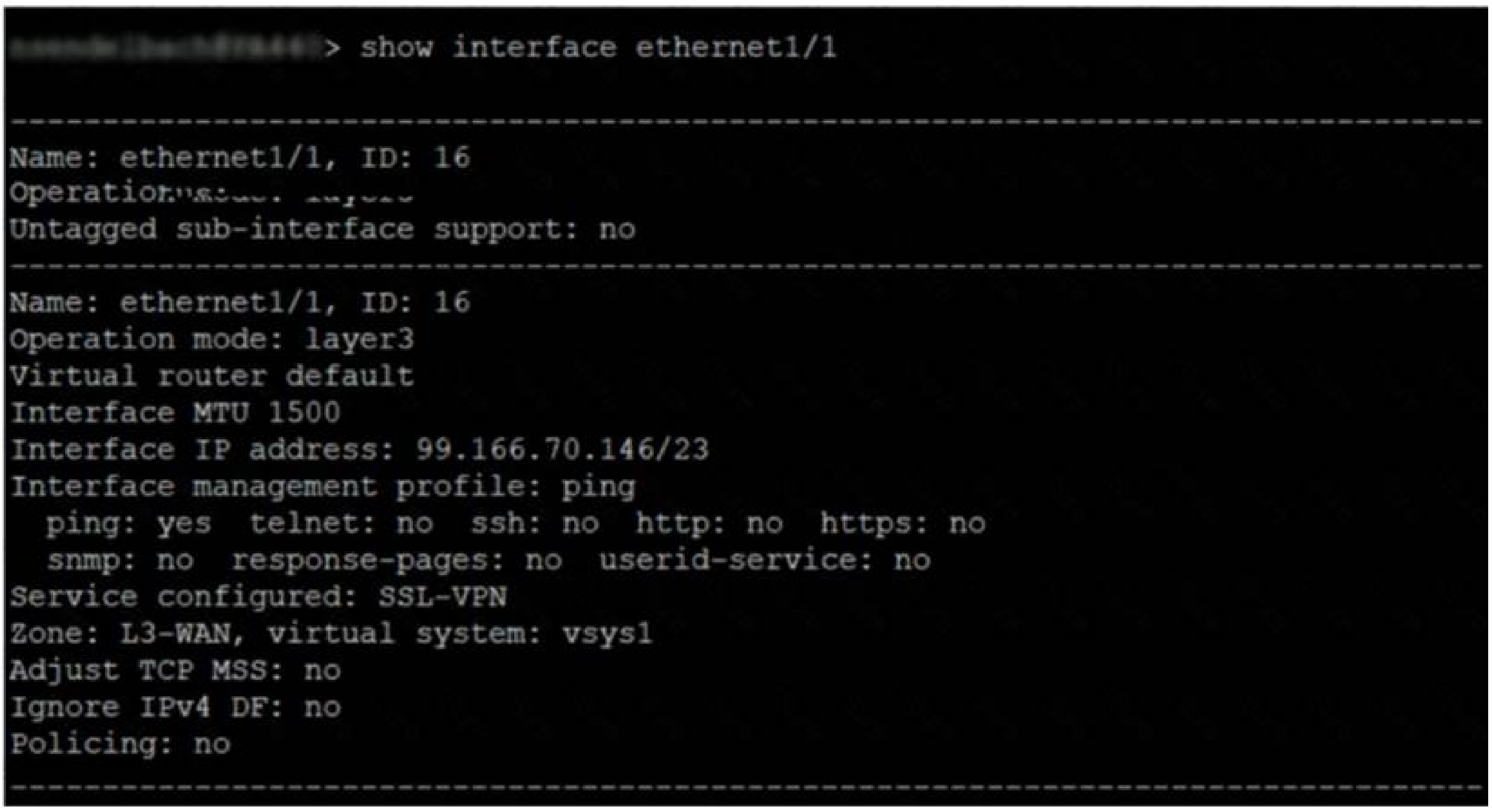
NEW QUESTION 93
A company has recently migrated their branch office's PA-220S to a centralized Panorama. This Panorama manages a number of PA-7000 Series and PA-5200 Series devices All device group and template configuration is managed solely within Panorama
They notice that commit times have drastically increased for the PA-220S after the migration What can they do to reduce commit times?

A. Disable "Share Unused Address and Service Objects with Devices" in Panorama Settings.
B. Update the apps and threat version using device-deployment
C. Perform a device group push using the "merge with device candidate config" option
D. Use "export or push device config bundle" to ensure that the firewall is integrated with the Panorama config.

Answer: A

Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-device-groups/man
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1CCAS

NEW QUESTION 97
After switching to a different WAN connection, users have reported that various websites will not load, and timeouts are occurring. The web servers work fine from other locations.
The firewall engineer discovers that some return traffic from these web servers is not reaching the users behind the firewall. The engineer later concludes that the maximum transmission unit (MTU) on an upstream router interface is set to 1400 bytes.
The engineer reviews the following CLI output for ethernet1/1.



```
[redacted]> show interface ethernet1/1

-------------------------------------------------------------------------------
Name: ethernet1/1, ID: 16
Operation mode: layer3
Untagged sub-interface support: no
-------------------------------------------------------------------------------
Name: ethernet1/1, ID: 16
Operation mode: layer3
Virtual router default
Interface MTU 1500
Interface IP address: 99.166.70.146/23
Interface management profile: ping
  ping: yes  telnet: no  ssh: no  http: no  https: no
  snmp: no  response-pages: no  userid-service: no
Service configured: SSL-VPN
Zone: L3-WAN, virtual system: vsys1
Adjust TCP MSS: no
Ignore IPv4 DF: no
Policing: no

-------------------------------------------------------------------------------
```

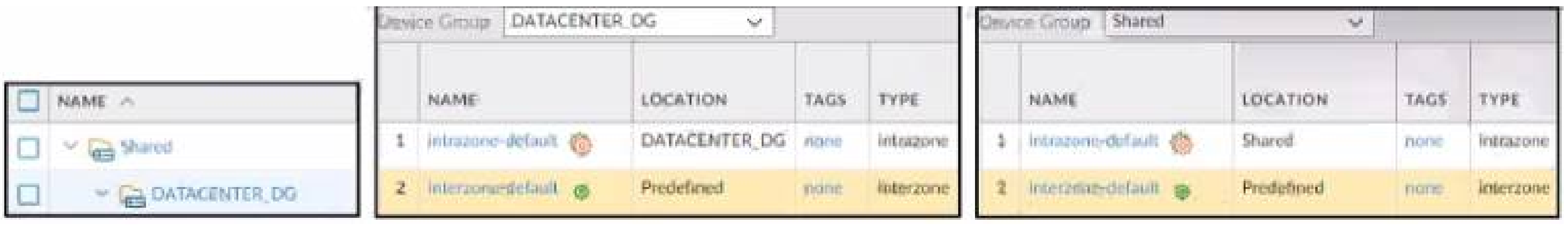
Which setting should be modified on ethernet1/1 to remedy this problem?

A. Lower the interface MTU value below 1500.
B. Enable the Ignore IPv4 Don't Fragment (DF) setting.
C. Change the subnet mask from /23 to /24.
D. Adjust the TCP maximum segment size (MSS) valu
E. *

Answer: D

Explanation:
The engineer should adjust the TCP maximum segment size (MSS) value on ethernet1/1 to remedy this problem. This is because the MTU on an upstream router interface is set to 1400 bytes, which is causing the return traffic from the web servers to not reach the users behind the firewall. By adjusting the TCP MSS value, the engineer can ensure that the return traffic is able to reach the users without any issues.
The TCP MSS is the maximum amount of data that can be transmitted in a single TCP segment, excluding the TCP and IP headers. The TCP MSS is usually derived from the MTU of the underlying network, which is the maximum packet size that can be transmitted without fragmentation. For example, if the MTU is 1500 bytes, which is the default value for ethernet interfaces, then the TCP MSS is 1460 bytes (1500 - 20 bytes for IP header - 20 bytes for TCP header). However, if there are intermediate devices or networks that have a lower MTU than the end-to-end path, then the TCP MSS may need to be adjusted accordingly to avoid packet loss or fragmentation1.
In this case, the firewall has an MTU of 1500 bytes on ethernet1/1, which is connected to a WAN link. However, an upstream router has an MTU of 1400 bytes on its interface, which means that any packet larger than 1400 bytes will be either dropped or fragmented by the router. This can cause problems for the return traffic from the web servers, which may have a TCP MSS of 1460 bytes or higher, depending on their MTU settings. If these packets have the Don't Fragment (DF) bit set in their IP header, which is common for TCP packets, then they will be dropped by the router and never reach the firewall or the users behind it. If they do not have the DF bit set, then they will be fragmented by the router and reassembled by the firewall, which can cause performance degradation and overhead2.
To avoid these problems, the engineer should adjust the TCP MSS value on ethernet1/1 to match or be lower than the MTU of the upstream router. This can be done by using the CLI command set network interface ethernet ethernet1/1 tcp-mss <value> , where <value> is an integer between 64 and 15003. For example, if the engineer sets the TCP MSS value to 1360 bytes (1400 - 20 - 20), then this will ensure that any TCP packet sent or received by ethernet1/1 will not exceed 1400 bytes in total size, and thus will not be dropped or fragmented by the router. This will allow the return traffic from the web servers to reach the users behind the firewall without any issues4.
References: TCP Maximum Segment Size (MSS), Configure Session Settings, TCP MSS Adjustments, PCNSE Study Guide (page 59)

NEW QUESTION 101
Refer to the exhibit.



☐	NAME ^
☐	⌄ Shared
☐	⌄ DATACENTER_DG

Device Group: DATACENTER_DG

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

Device Group: Shared

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

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

A. shared pre-rules DATACENTER DG pre rulesrules configured locally on the firewall shared post-rules DATACENTER_DG post-rules DATACENTER.DG default rules
B. shared pre-rules DATACENTER_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 102
What is the best description of the Cluster Synchronization Timeout (min)?

A. The maximum time that the local firewall waits before going to Active state when another cluster member is preventing the cluster from fully synchronizing
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 maximum interval between hello packets that are sent to verify that the HA functionality on theother firewall is operational

Answer: A

Explanation:
The best description of the Cluster Synchronization Timeout (min) is the maximum time that the local firewall waits before going to Active state when another cluster member is preventing the cluster from fully synchronizing. This is a parameter that can be configured in an HA cluster, which is a group of firewalls that share session state and provide high availability and scalability. The Cluster Synchronization Timeout (min) determines how long the local firewall will wait for the cluster to reach a stable state before it decides to become Active and process traffic. A stable state means that all cluster members are either Active or Passive, and have synchronized their sessions with each other. If there is another cluster member that is in an unknown or unstable state, such as Initializing, Non-functional, or Suspended, then it may prevent the cluster from fully synchronizing and cause a delay in traffic processing. The Cluster Synchronization Timeout (min) can be set to a value between 0 and 30 minutes, with a default of 0. If it is set to 0, then the local firewall will not wait for any other cluster member and will immediately go to Active state. If it is set to a positive value, then the local firewall will wait for that amount of time before going to Active state, unless the cluster reaches a stable state earlier12. References: Configure HA Clustering, PCNSE Study Guide (page 53)
How to Set Session, TCP, and UDP Timeout Values - Palo Alto Networks ...

NEW QUESTION 105
An engineer is monitoring an active/active high availability (HA) firewall pair. Which HA firewall state describes the firewall that is currently processing traffic?

A. Initial
B. Passive
C. Active
D. Active-primary

Answer: C

Explanation:
In an active/active high availability (HA) firewall pair, the firewall that is currently processing traffic is in the “Active” state. This state indicates that the firewall is fully functional and can own sessions and set up sessions. An active firewall can be either active-primary or active-secondary, depending on the Device ID and the HA configuration. An active-primary firewall connects to User-ID agents, runs DHCP server and DHCP relay, and matches NAT and PBF rules with the Device ID of the active-primary firewall. An active-secondary firewall connects to User-ID agents, runs DHCP server, and matches NAT and PBF rules with the Device ID of the active-secondary firewall. An active-secondary firewall does not support DHCP relay1. References: Firewall States, PCNSE Study Guide (page 53)

NEW QUESTION 110
The decision to upgrade PAN-OS has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when attempting the install.
When performing an upgrade on Panorama to PAN-OS. what is the potential cause of a failed install?

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

Answer: A

Explanation:
One of the potential causes of a failed install when upgrading Panorama to PAN-OS is having outdated plugins. Plugins are software extensions that enable Panorama to interact with Palo Alto Networks cloud services and third-party services. Plugins have dependencies on specific PAN-OS versions, so they must be updated before or after upgrading Panorama, depending on the plugin compatibility matrix2. If the plugins are not updated accordingly, the upgrade process may fail or cause issues with Panorama
functionality3. References: Panorama Plugins Upgrade/Downgrade Considerations, Troubleshoot Your Panorama Upgrade, PCNSE Study Guide (page 54)

NEW QUESTION 112
Which two factors should be considered when sizing a decryption firewall deployment? (Choose two.)

A. Encryption algorithm
B. Number of security zones in decryption policies
C. TLS protocol version
D. Number of blocked sessions

Answer: AC

Explanation:
When sizing a decryption firewall deployment, two factors that should be considered are the encryption algorithm and the TLS protocol version. These factors affect the amount of resources and processing power that the firewall needs to decrypt and inspect SSL/TLS traffic.
The encryption algorithm is the method that the server and the client use to encrypt and decrypt the data exchanged in an SSL/TLS session. Different encryption algorithms have different levels of security and performance. For example, AES is a symmetric encryption algorithm that is faster and more efficient than RSA, which is an asymmetric encryption algorithm. However, RSA is more secure than AES because it uses public and private keys to encrypt and decrypt data, while AES uses a single shared key. The firewall must support the encryption algorithms that are used by the servers and clients that it decrypts, and it must have enough CPU and memory resources to handle the decryption workload12.
The TLS protocol version is the standard that defines how the server and the client establish and maintain an SSL/TLS session. Different TLS protocol versions

have different features and requirements for encryption algorithms, cipher suites, certificates, handshake messages, etc. For example, TLS 1.3 is the latest and most secure version of TLS, which supports only strong encryption algorithms and cipher suites, such as AES-GCM and ChaCha20-Poly1305, and requires elliptic curve certificates. The firewall must support the TLS protocol versions that are used by the servers and clients that it decrypts, and it must have enough hardware acceleration resources to handle the decryption speed34.
The number of security zones in decryption policies and the number of blocked sessions are not relevant factors for sizing a decryption firewall deployment. The number of security zones in decryption policies only affects how the firewall matches traffic to decryption rules based on source and destination zones, but it does not affect the decryption performance or resource consumption. The number of blocked sessions only indicate how many sessions are denied by the firewall based on security policy or decryption policy rules, but it does not affect the decryption capacity or throughput56.
References: Encryption Algorithms, TLS Protocol Versions, Decryption Policy, PCNSE Study Guide (pag 60)

NEW QUESTION 116
In a template, which two objects can be configured? (Choose two.)

A. SD-WAN path quality profile
B. Monitor profile
C. IPsec tunnel
D. Application group

Answer: BC

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-network-profiles/ne

NEW QUESTION 119
During the implementation of SSL Forward Proxy decryption, an administrator imports the company's Enterprise Root CA and Intermediate CA certificates onto the firewall. The company's Root and Intermediate CA certificates are also distributed to trusted devices using Group Policy and GlobalProtect. Additional device certificates and/or Subordinate certificates requiring an Enterprise CA chain of trust are signed by the company's Intermediate CA.
Which method should the administrator use when creating Forward Trust and Forward Untrust certificates on the firewall for use with decryption?

A. Generate a single subordinate CA certificate for both Forward Trust and Forward Untrust.
B. Generate a CA certificate for Forward Trust and a self-signed CA for Forward Untrust.
C. Generate a single self-signed CA certificate for Forward Trust and another for Forward Untrust
D. Generate two subordinate CA certificates, one for Forward Trust and one for Forward Untrust.

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy

NEW QUESTION 123
Which three authentication types can be used to authenticate users? (Choose three.)

A. Local database authentication
B. PingID
C. Kerberos single sign-on
D. GlobalProtect client
E. Cloud authentication service

Answer: ACE

Explanation:
The three authentication types that can be used to authenticate users are:

- A: Local database authentication. This is the authentication type that uses the local user database on the firewall or Panorama to store and verify user credentials1.
- C: Cloud authentication service. This is the authentication type that uses a cloud-based identity provider such as Okta, PingOne, or PingFederate, to authenticate users and provide SAML assertions to the firewall or Panorama2.
- E: Kerberos single sign-on. This is the authentication type that uses the Kerberos protocol to authenticate users who are logged in to a Windows domain and provide them with seamless access to resources on the firewall or Panorama3.

NEW QUESTION 125
A firewall engineer reviews the PAN-OS GlobalProtect application and sees that it implicitly uses web-browsing and depends on SSL.
When creating a new rule, what is needed to allow the application to resolve dependencies?

A. Add SSL and web-browsing applications to the same rule.
B. Add web-browsing application to the same rule.
C. Add SSL application to the same rule.
D. SSL and web-browsing must both be explicitly allowed.

Answer: C

Explanation:
'Implicitly Uses' has web-browsing listed. This means that if you allow facebook-posting, that it will also be allowing the web-browsing application implicitly.. In our case, we dont know which APP the question referes too but 'Implicitly means already uses HTTP.

NEW QUESTION 127
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. Create an Application Override using TCP ports 443 and 80.
C. Add the HTT
D. SS
E. and Evernote applications to the same Security policy.
F. Add only the Evernote application to the Security policy rule.

Answer: D

Explanation:
https://live.paloaltonetworks.com/t5/blogs/what-is-application-dependency/ba-p/344330
To create an application-based Security policy rule to allow Evernote, the administrator only needs to add the Evernote application to the Security policy rule. The Evernote application is a predefined App-ID that identifies the traffic generated by the Evernote client or web interface. The Evernote application implicitly uses SSL and web browsing as dependencies, which means that the firewall automatically allows these applications when the Evernote application is allowed. Therefore, there is no need to add HTTP, SSL, or web browsing applications to the same Security policy rule. Adding these applications would broaden the scope of the rule and potentially allow unwanted traffic12. References: App-ID Overview, Create a Security Policy Rule

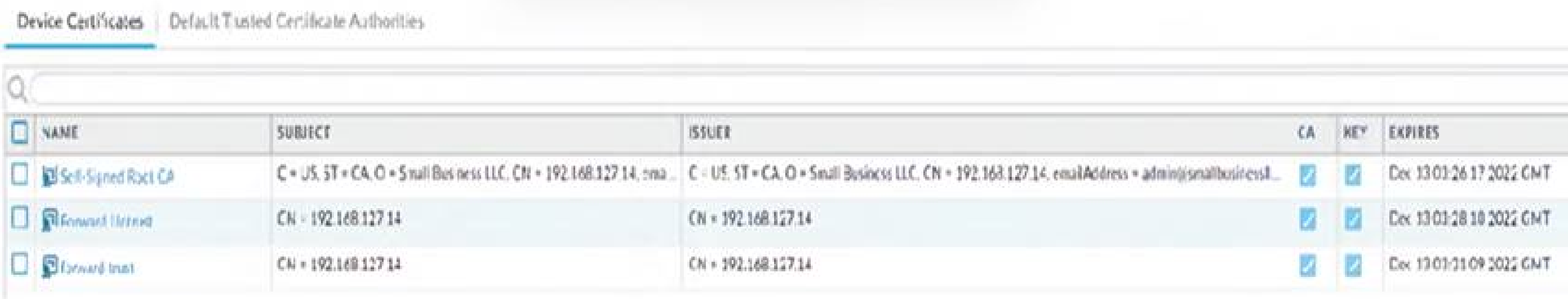
NEW QUESTION 131
Which statement is correct given the following message from the PanGPA log on the GlobalProtect app? Failed to connect to server at port:47 67

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: C

Explanation:
https://knowledgebase.paloaltonetworks.com/kCSArticleDetail?id=kA10g000000PMiD

NEW QUESTION 133
Review the screenshot of the Certificates page.



Device Certificates | Default Trusted Certificate Authorities

□	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES
□	Self-Signed Root CA	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.14, ema...	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.14, emailAddress = admin@smallbusiness...	☑	☑	Dec 13 03:26:17 2022 GMT
□	Forward Untrust	CN = 192.168.127.14	CN = 192.168.127.14	☑	☑	Dec 13 03:28:10 2022 GMT
□	Forward trust	CN = 192.168.127.14	CN = 192.168.127.14	☑	☑	Dec 13 03:31:09 2022 GMT

An administrator for a small LLC has created a series of certificates as shown, to use for a planned Decryption roll out. The administrator has also installed the self-signed root certificate in 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 untrust certificate has not been signed by the self-singed root CA certificate.
B. The forward trust certificate has not been installed in client systems.
C. The self-signed CA certificate has the same CN as the forward trust and untrust certificates.
D. The forward trust certificate has not been signed by the self-singed root CA certificate.

Answer: D

Explanation:
The cause of the unsecured website warnings is that the forward trust certificate has not been signed by the self-signed root CA certificate. The forward trust certificate is used by the firewall to generate a copy of the server certificate for outbound SSL decryption (SSL Forward Proxy). The firewall signs the copy with the forward trust certificate and presents it to the client. The client then verifies the signature using the public key of the CA that issued the forward trust certificate. If the client does not trust the CA, it will display a warning message. Therefore, the forward trust certificate must be signed by a CA that is trusted by the client. In this case, the administrator has installed the self-signed root CA certificate in all client systems, so this CA should be used to sign the forward trust certificate. However, as shown in the screenshot, the forward trust certificate has a different issuer than the self-signed root CA certificate, which means it has not been signed by it. This causes the client to reject the signature and show a warning message. To fix this issue, the administrator should generate a new forward trust certificate and sign it with the self-signed root CA certificate12. References: Keys and Certificates for Decryption Policies, How to Configure SSL Decryptio

NEW QUESTION 138
......