Paloalto-Networks

Exam Questions PCNSE

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

NEW QUESTION 1
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 2
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 3
A firewall engineer creates a new App-ID report under Monitor > Reports > Application Reports > New Applications to monitor new applications on the network and better assess any Security policy updates the engineer might want to make.
How does the firewall identify the New App-ID characteristic?

A. It matches to the New App-IDs downloaded in the last 90 days.
B. It matches to the New App-IDs in the most recently installed content releases.
C. It matches to the New App-IDs downloaded in the last 30 days.
D. It matches to the New App-IDs installed since the last time the firewall was rebooted.

Answer: B

Explanation:
The New App-ID characteristic enables the firewall to monitor new applications on the network, so that the engineer can better assess the security policy updates they might want to make. The New App-ID characteristic always matches to only the new App-IDs in the most recently installed content releases. When a new content release is installed, the New App-ID characteristic automatically begins to match only to the new App-IDs in that content release version. This way, the engineer can see how the newly-categorized applications might impact security policy enforcement and make any necessary
adjustments. References: Monitor New App-IDs

NEW QUESTION 4
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 5
Which statement about High Availability timer settings is true?

A. Use the Critical timer for faster failover timer settings.
B. Use the Aggressive timer for faster failover timer settings
C. Use the Moderate timer for typical failover timer settings
D. Use the Recommended timer for faster failover timer settings.

Answer:

D

Explanation:
Recommended: Use for typical failover timer settings. Unless you're sure that you need different settings, the best practice is to use the Recommended settings.
Aggressive: Use for faster failover timer settings.
Advanced: Allows you to customize the values to suit your network requirement for each of the following timers:

NEW QUESTION 6
Which type of zone will allow different virtual systems to communicate with each other?

A. Tap
B. External
C. Virtual Wire
D. Tunnel

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/virtual-systems/communication-between-virtual-s

NEW QUESTION 7
A security engineer needs firewall management access on a trusted interface.
Which three settings are required on an SSL/TLS Service Profile to provide secure Web UI authentication? (Choose three.)

A. Minimum TLS version
B. Certificate
C. Encryption Algorithm
D. Maximum TLS version
E. Authentication Algorithm

Answer: ABD

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssltls-service

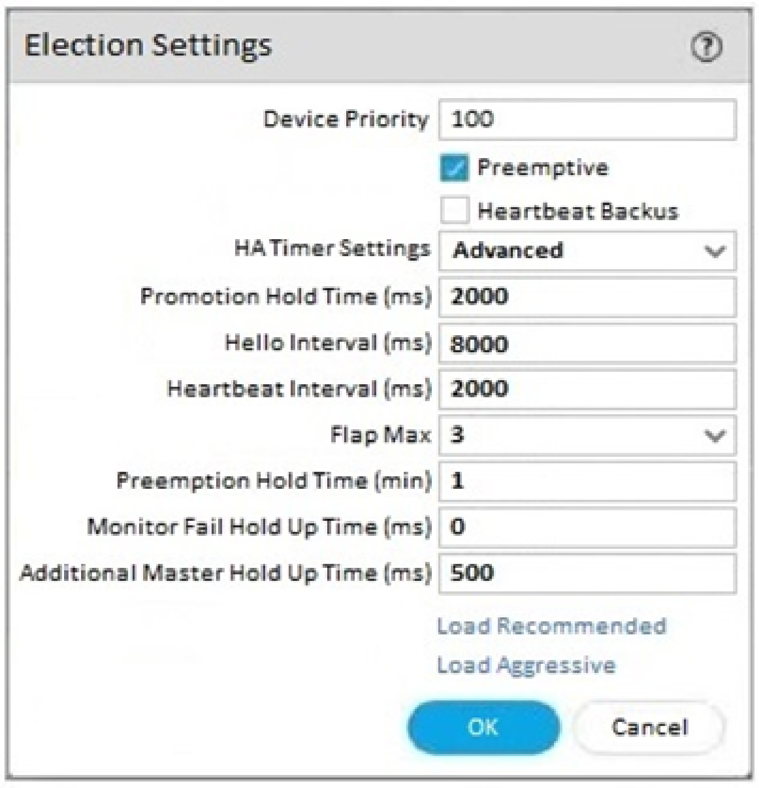
NEW QUESTION 8
An engineer needs to configure a standardized template for all Panorama-managed firewalls. These settings will be configured on a template named "Global" and will be included in all template stacks.
Which three settings can be configured in this template? (Choose three.)

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

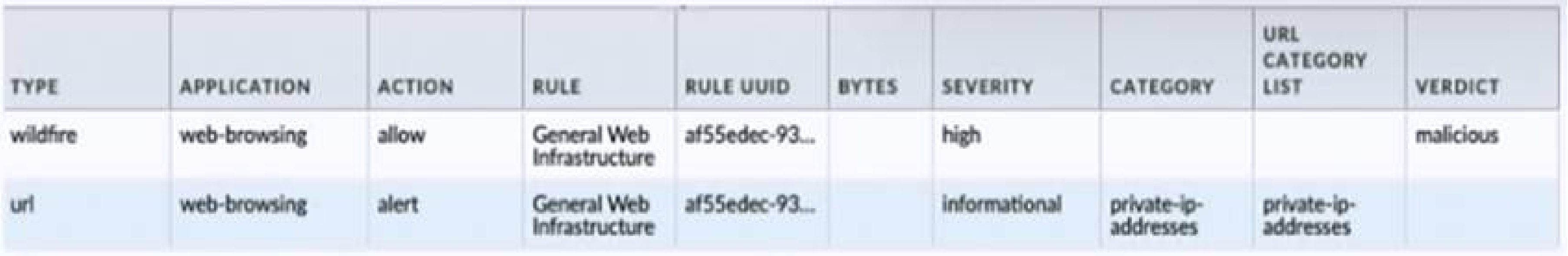
NEW QUESTION 10
In a security-first network, what is the recommended threshold value for apps and threats to be dynamically updated?

A. 1 to 4 hours
B. 6 to 12 hours
C. 24 hours
D. 36 hours

Answer: B

Explanation:
Schedule content updates so that they download-and-install automatically. Then, set a Threshold that determines the amount of time the firewall waits before installing the latest content. In a security-first network, schedule a six to twelve hour threshold.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-thr
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/software-and-content-updates/best-practices-for

NEW QUESTION 10
Given the following snippet of a WildFire submission log did the end-user get access to the requested information and why or why not?



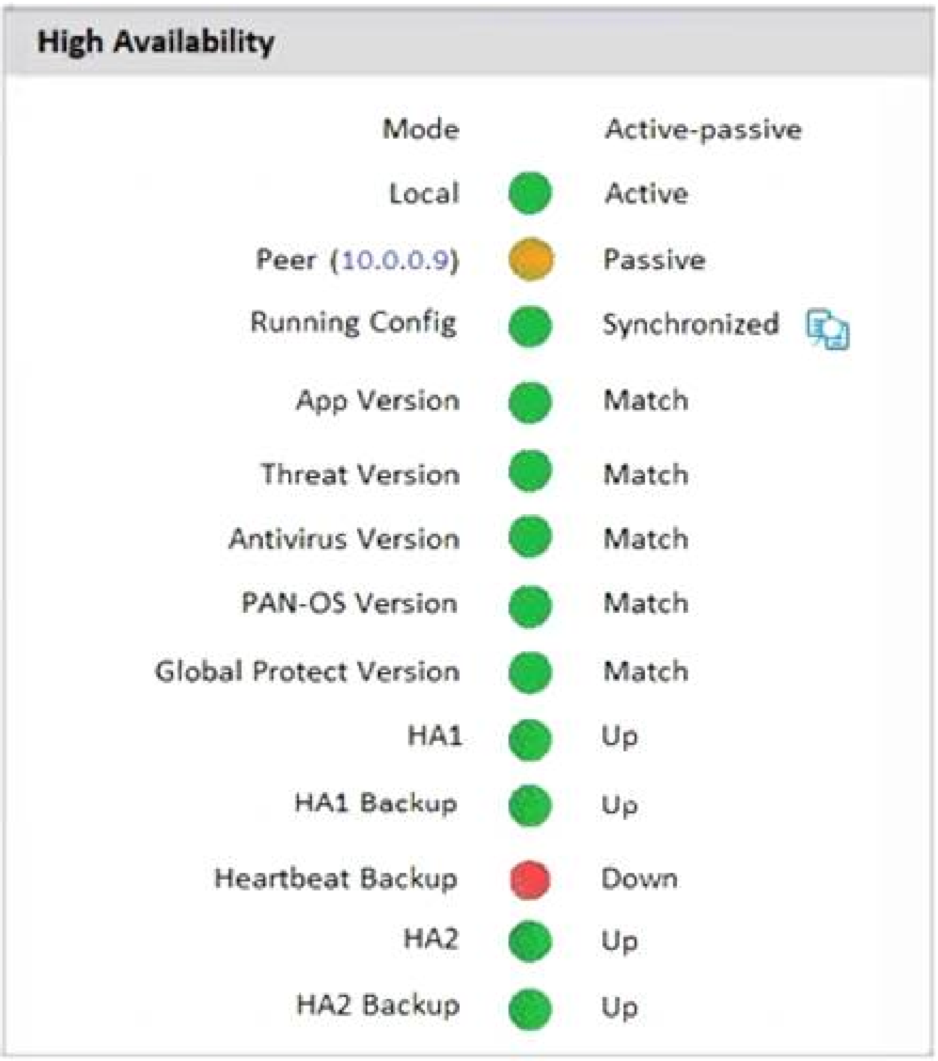
TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	web-browsing	allow	General Web Infrastructure	af55edec-93...		high			malicious
url	web-browsing	alert	General Web Infrastructure	af55edec-93...		informational	private-ip-addresses	private-ip-addresses	

A. Yes, because the action is set to alert
B. No, because this is an example from a defeated phishing attack
C. No, because the severity is high and the verdict is malicious.
D. Yes, because the action is set to allow.

Answer: D

Explanation:
https://live.paloaltonetworks.com/t5/general-topics/wildfire-submission-entries-with-severity-high-showing-acti

NEW QUESTION 13
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 17
Which two policy components are required to block traffic in real time using a dynamic user group (DUG)? (Choose two.)

A. A Deny policy for the tagged traffic
B. An Allow policy for the initial traffic
C. A Decryption policy to decrypt the traffic and see the tag
D. A Deny policy with the "tag" App-ID to block the tagged traffic

Answer: AB

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups Use the dynamic user group in a policy to regulate traffic for the members of the group. You will need to
configure at least two rules: one to allow initial traffic to populate the dynamic user group and one to deny traffic for the activity you want to prevent (in this case, questionable-activity). To tag users, the rule to allow traffic must have a higher rule number in your rulebase than the rule that denies traffic.
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-dynamic-user-groups-in-policy

NEW QUESTION 18
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 20
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

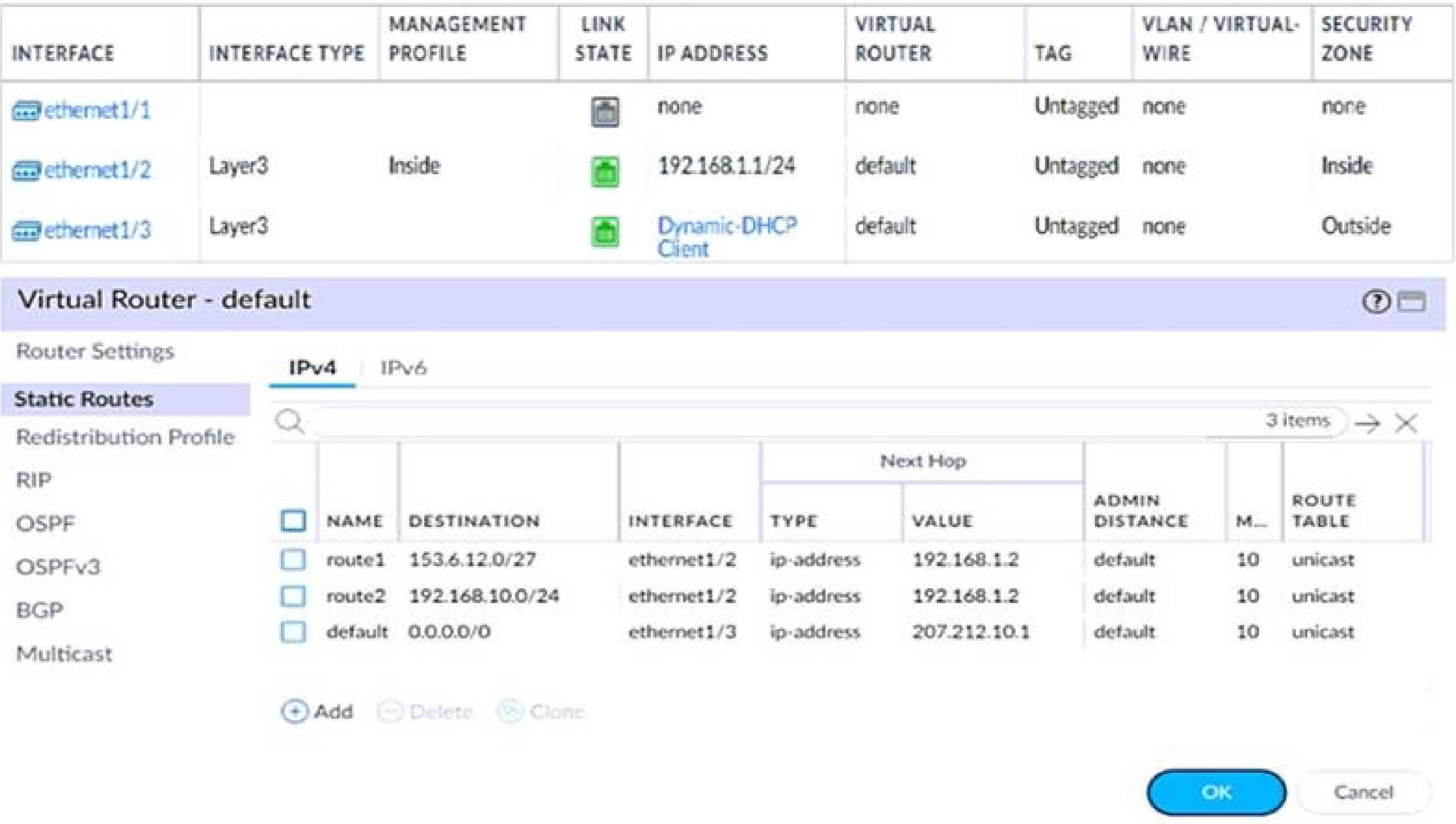
NEW QUESTION 21
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)

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 25
A firewall engineer creates a destination static NAT rule to allow traffic from the internet to a webserver hosted behind the edge firewall. The pre-NAT IP address of the server is 153.6 12.10, and the post-NAT IP address is 192.168.10.10. Refer to the routing and interfaces information below.



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1			▨	none	none	Untagged	none	none
ethernet1/2	Layer3	Inside	🟩	192.168.1.1/24	default	Untagged	none	Inside
ethernet1/3	Layer3		🟩	Dynamic-DHCP Client	default	Untagged	none	Outside

Virtual Router - default

				Next Hop				
□	NAME	DESTINATION	INTERFACE	TYPE	VALUE	ADMIN DISTANCE	M...	ROUTE TABLE
□	route1	153.6.12.0/27	ethernet1/2	ip-address	192.168.1.2	default	10	unicast
□	route2	192.168.10.0/24	ethernet1/2	ip-address	192.168.1.2	default	10	unicast
□	default	0.0.0.0/0	ethernet1/3	ip-address	207.212.10.1	default	10	unicast

What should the NAT rule destination zone be set to?

A. None
B. Outside
C. DMZ
D. Inside

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/nat-configuration-examples/destin

NEW QUESTION 26
Which log type would provide information about traffic blocked by a Zone Protection profile?

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

Answer: D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhzCAC

- D is the correct answer because the threat log type would provide information about traffic blocked by a Zone Protection profile. This is because Zone Protection profiles are used to protect the network from attacks, including common flood, reconnaissance attacks, and other packet-based attacks1. These attacks are classified as threats by the firewall and are logged in the threat log2. The threat log displays information such as the source and destination IP addresses, ports, zones, applications, threat types, actions, and severity of the threats2.

Verified References:

- 1: Zone protection profiles - Palo Alto Networks Knowledge Base
- 2: Threat Log Fields - Palo Alto Networks

NEW QUESTION 30
Which three multi-factor authentication methods can be used to authenticate access to the firewall? (Choose three.)

A. Voice
B. Fingerprint
C. SMS
D. User certificate
E. One-time password

Answer: CDE

Explanation:
The firewall can use three multi-factor authentication methods to authenticate access to the firewall: SMS, user certificate, and one-time password. These methods can be used in combination with other authentication factors, such as username and password, to provide stronger security for accessing the firewall web interface or CLI. The firewall can integrate with various MFA vendors that support these methods through RADIUS or SAML protocols5. Voice and fingerprint are not supported by the firewall as MFA methods. References: MF Vendor Support, PCNSE Study Guide (page 48)

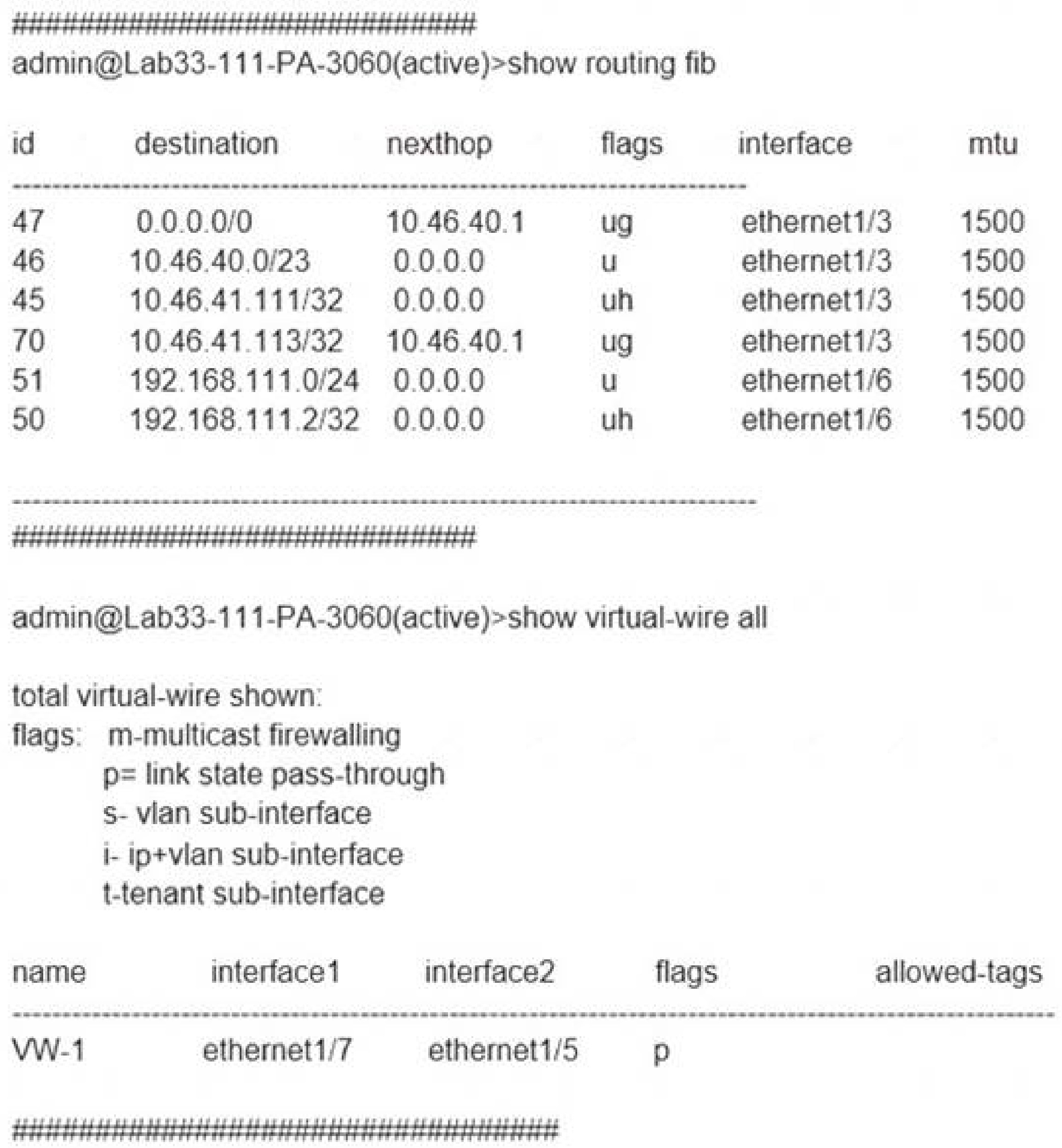
NEW QUESTION 35
If a URL is in multiple custom URL categories with different actions, which action will take priority?

A. Allow
B. Override
C. Block
D. Alert

Answer: C

Explanation:
When a URL matches multiple categories, the category chosen is the one that has the most severe action defined below (block being most severe and allow least severe).
1 block
2 override
3 continue
4 alert
5 allow https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClsmCAC

NEW QUESTION 40
Refer to the exhibit.



```
################################
admin@Lab33-111-PA-3060(active)>show routing fib

id      destination        nexthop       flags     interface        mtu
---------------------------------------------------------------------------
47       0.0.0.0/0         10.46.40.1    ug        ethernet1/3      1500
46      10.46.40.0/23       0.0.0.0      u         ethernet1/3      1500
45      10.46.41.111/32     0.0.0.0      uh        ethernet1/3      1500
70      10.46.41.113/32    10.46.40.1    ug        ethernet1/3      1500
51      192.168.111.0/24    0.0.0.0      u         ethernet1/6      1500
50      192.168.111.2/32    0.0.0.0      uh        ethernet1/6      1500

---------------------------------------------------------------------------
################################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p= link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name         interface1      interface2      flags         allowed-tags
----------------------------------------------------------------------------------
VW-1        ethernet1/7      ethernet1/5      p

######################################
```

Which will be the egress interface if the traffic's ingress interface is ethernet1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

A. ethernet1/6
B. ethernet1/3
C. ethernet1/7
D. ethernet1/5

Answer: D

Explanation:
In the second image, VW ports mentioned are 1/5 and 1/7. Hence it can not be a part of any other routing. So if any traffic coming as ingress from 1/7, it has to go out via 1/5.
The egress interface for the traffic with ingress interface ethernet1/7, source 192.168.111.3, and destination 10.46.41.113 will be ethernet1/5. This is because the traffic will match the virtual wire with interfaces ethernet1/5 and ethernet1/7, which is configured to allow VLAN-tagged traffic with tags 10 and 201. The traffic will also match the security policy rule that allows traffic from zone Trust to zone Untrust, which are assigned to ethernet1/7 and ethernet1/5 respectively2. Therefore, the traffic will be forwarded to the same interface from which it was received, which is ethernet1/53.

NEW QUESTION 41
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 43
An administrator is troubleshooting why video traffic is not being properly classified. If this traffic does not match any QoS classes, what default class is assigned?

A. 1
B. 2

C. 3
D. 4

Answer: D

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/quality-of-service/qos-concepts/qos-classes

NEW QUESTION 44
An engineer is tasked with deploying SSL Forward Proxy decryption for their organization. What should they review with their leadership before implementation?

A. Browser-supported cipher documentation
B. Cipher documentation supported by the endpoint operating system
C. URL risk-based category distinctions
D. Legal compliance regulations and acceptable usage policies

Answer: D

Explanation:
The engineer should review the legal compliance regulations and acceptable usage policies with their leadership before implementing SSL Forward Proxy decryption for their organization. SSL Forward Proxy decryption allows the firewall to decrypt and inspect the traffic from internal users to external servers. This can raise privacy and legal concerns for the users and the organization. Therefore, the engineer should ensure that the leadership is aware of the implications and benefits of SSL Forward Proxy decryption and that they have a clear policy for informing and obtaining consent from the users. Option A is incorrect because browser-supported cipher documentation is not relevant for SSL Forward Proxy decryption. The firewall uses its own cipher suite to negotiate encryption with the external server, regardless of the browser settings. Option B is incorrect because cipher documentation supported by the endpoint operating system is not relevant for SSL Forward Proxy decryption. The firewall uses its own cipher suite to negotiate encryption with the external server, regardless of the endpoint operating system. Option C is incorrect because URL risk-based category distinctions are not relevant for SSL Forward Proxy decryption. The firewall can decrypt and inspect traffic based on any URL category, not just risk-based ones.
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-concepts "Understand local laws and regulations about the traffic you can legally decrypt and user notification requirements."

NEW QUESTION 48
When an engineer configures an active/active high availability pair, which two links can they use? (Choose two)

A. HSCI-C
B. Console Backup
C. HA3
D. HA2 backup

Answer: CD

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activeactive-ha/prerequisit
These are the two links that can be used to configure an active/active high availability pair. An active/active high availability pair consists of two firewalls that are both active and share the traffic load between them1. To configure an active/active high availability pair, the following links are required2:

- HA1: This is the control link that is used for exchanging heartbeat messages and configuration synchronization between the firewalls. It can be a dedicated interface or a subinterface. It can also have a backup link for redundancy.
- HA2: This is the data link that is used for forwarding sessions from one firewall to another in case of failover or load balancing. It can be a dedicated interface or a subinterface. It can also have a backup link for redundancy.
- HA3: This is the session owner synchronization link that is used for synchronizing session information between the firewalls in different virtual systems. It can be a dedicated interface or a subinterface. It is only required for active/active high availability pairs, not for active/passive pairs.

NEW QUESTION 53
An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Link and Path Monitoring is enabled with the Failure Condition set to "any." There is one link group configured containing member interfaces ethernet1/1 and ethernet1/2 with a Group Failure Condition set to "all."
Which HA state will the Active firewall go into if ethernet1/1 link goes down due to a failure?'

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

Answer: D

NEW QUESTION 54
An administrator has configured OSPF with Advanced Routing enabled on a Palo Alto Networks firewall running PAN-OS 10.2. After OSPF was configured, the administrator noticed that OSPF routes were not being learned.
Which two actions could an administrator take to troubleshoot this issue? (Choose two.)

A. Run the CLI command show advanced-routing ospf neighbor
B. In the WebUI, view the Runtime Stats in the virtual router
C. Look for configuration problems in Network > virtual router > OSPF
D. In the WebUI, view Runtime Stats in the logical router

Answer: AD

Explanation:
A:

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-virtual-routers/more
D:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/cli-cheat-sheets/cli-cheat-sheet-networking

NEW QUESTION 55
Which statement regarding HA timer settings is true?

A. Use the Recommended profile for typical failover timer settings
B. Use the Moderate profile for typical failover timer settings
C. Use the Aggressive profile for slower failover timer settings.
D. Use the Critical profile for faster failover timer settings.

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-timers

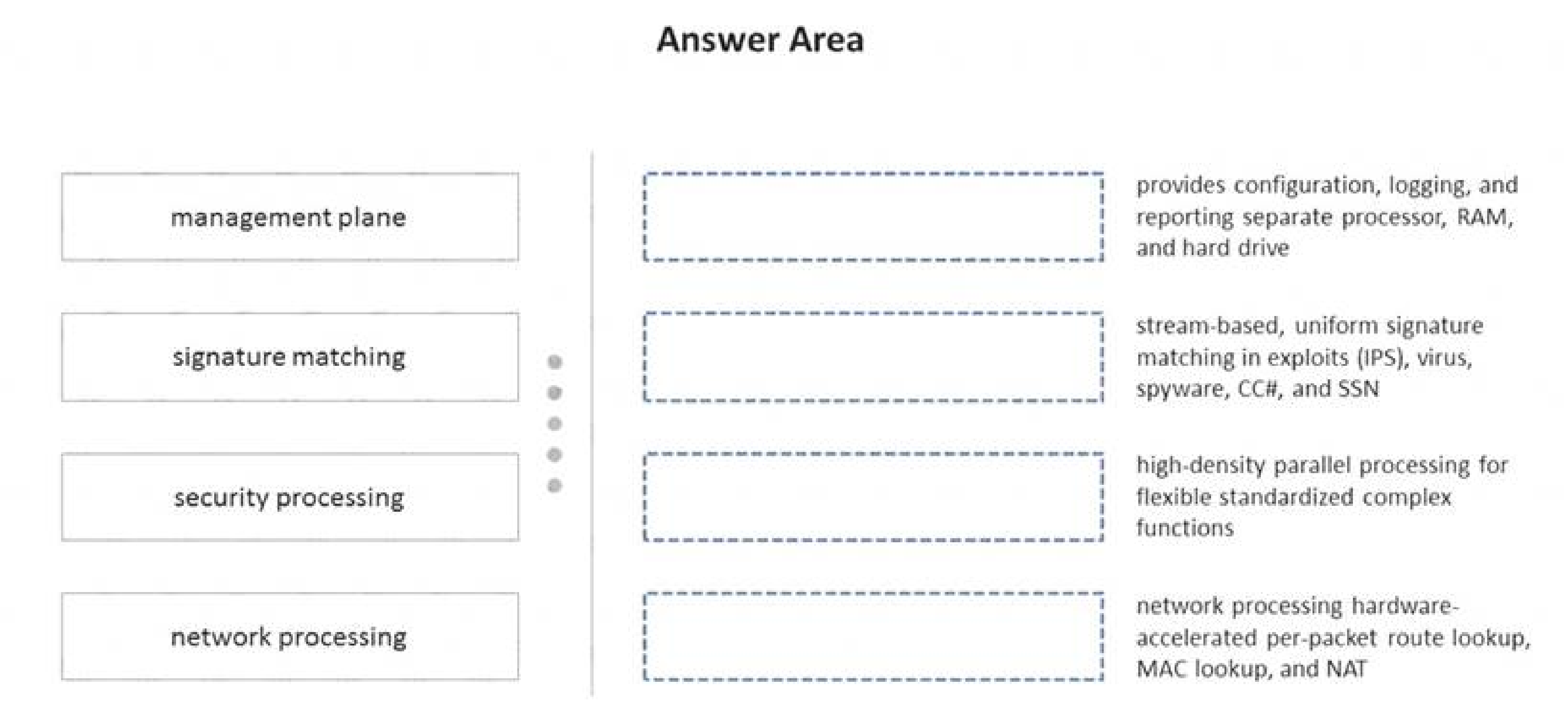
NEW QUESTION 59
Which type of policy in Palo Alto Networks firewalls can use Device-ID as a match condition?

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 60
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 63
Which GlobalProtect gateway selling is required to enable split-tunneling by access route, destination domain, and application?

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

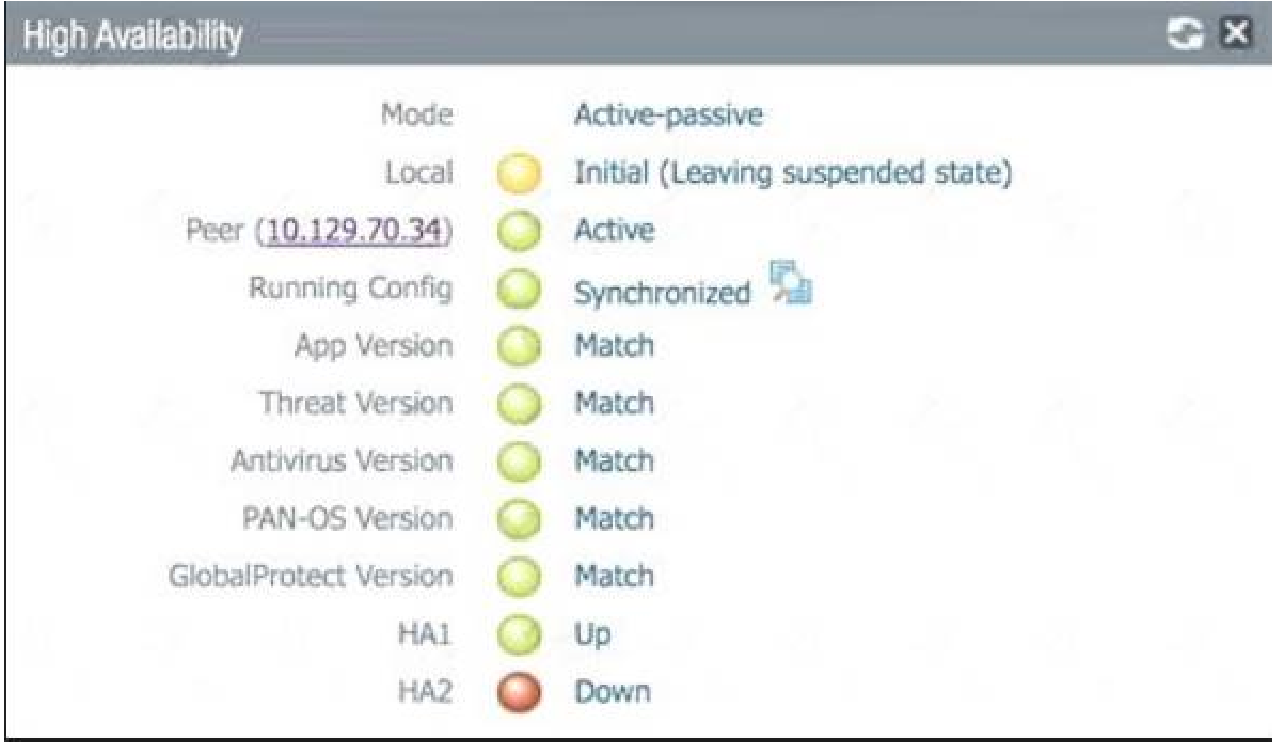
Answer: B

NEW QUESTION 66
An engineer is monitoring an active/active high availability (HA) firewall pair.
Which HA firewall state describes the firewall that is experiencing a failure of a monitored path?

A. Initial
B. Tentative
C. Passive
D. Active-secondary

Answer: B

Explanation:
In an active/active high availability (HA) firewall pair, when a firewall experiences a failure of a monitored path, it enters the “Tentative” state1. This state indicates that the firewall is synchronizing sessions and configurations from its peer due to a failure or a change in monitored objects such as a link or path. The firewall in this state is not fully functional but is working towards resuming normal operations by syncing with its peer. Therefore, the correct answer is B. Tentative.
Firewall Stuck in Initial (Leaving Suspended State) - Palo Alto Networks



High Availability

Mode		Active-passive
Local	●	Initial (Leaving suspended state)
Peer (10.129.70.34)	●	Active
Running Config	●	Synchronized
App Version	●	Match
Threat Version	●	Match
Antivirus Version	●	Match
PAN-OS Version	●	Match
GlobalProtect Version	●	Match
HA1	●	Up
HA2	●	Down

NEW QUESTION 71
What are three tasks that cannot be configured from Panorama by using a template stack? (Choose three.)

A. Change the firewall management IP address
B. Configure a device block list
C. Add administrator accounts
D. Rename a vsys on a multi-vsys firewall
E. Enable operational modes such as normal mode, multi-vsys mode, or FIPS-CC mode

Answer: ACE

NEW QUESTION 76
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?

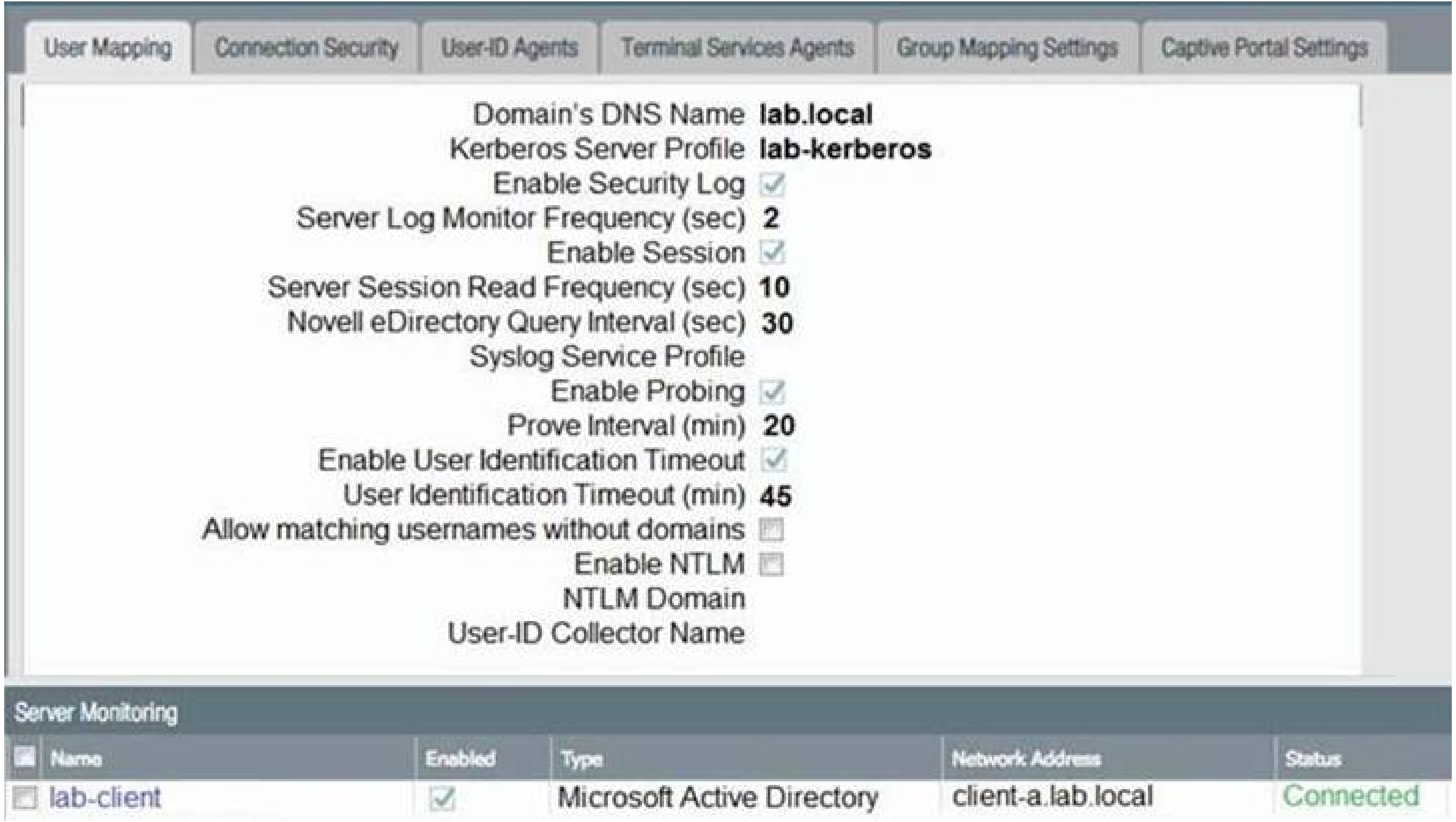
A. In the IKE Gateway configuration, verify that the IP address for each VPN peer is accurate
B. Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure
C. Check whether the VPN peer on one end is set up correctly using policy-based VPN
D. In the IPSec 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 78

Based on the graphic which statement accurately describes the output shown in the Server Monitoring panel?



Domain's DNS Name **lab.local**
Kerberos Server Profile **lab-kerberos**
Enable Security Log ☑
Server Log Monitor Frequency (sec) **2**
Enable Session ☑
Server Session Read Frequency (sec) **10**
Novell eDirectory Query Interval (sec) **30**
Syslog Service Profile
Enable Probing ☑
Prove Interval (min) **20**
Enable User Identification Timeout ☑
User Identification Timeout (min) **45**
Allow matching usernames without domains □
Enable NTLM □
NTLM Domain
User-ID Collector Name

Server Monitoring

□	Name	Enabled	Type	Network Address	Status
□	lab-client	☑	Microsoft Active Directory	client-a.lab.local	Connected

A. The User-ID agent is connected to a domain controller labeled lab-client
B. The host lab-client has been found by a domain controller
C. The host lab-client has been found by the User-ID agent.
D. The User-ID aaent is connected to the firewall labeled lab-client

Answer: A

NEW QUESTION 83
A network security administrator wants to inspect HTTPS traffic from users as it egresses through a firewall to the Internet/Untrust zone from trusted network zones.
The security admin wishes to ensure that if users are presented with invalid or untrusted security certificates, the user will see an untrusted certificate warning.
What is the best choice for an SSL Forward Untrust certificate?

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

Answer: B

Explanation:

- B is the best choice for an SSL Forward Untrust certificate because a self-signed certificate generated on the firewall is not trusted by any client browsers by default1. This means that if the firewall observes an invalid or untrusted security certificate from the server, it will present the self-signed certificate to the client, which will trigger an untrusted certificate warning2. This way, the security admin can ensure that users are aware of any potential risks when accessing HTTPS sites with untrusted certificates.
- A web server certificate signed by the organization’s PKI (A) or a subordinate Certificate Authority certificate signed by the organization’s PKI © are not good choices for an SSL Forward Untrust certificate because they are trusted by the client browsers that have the organization’s root CA installed1. This means that if the firewall observes an invalid or untrusted security certificate from the server, it will present the web server or subordinate CA certificate to the client, which will not trigger an untrusted certificate warning2. This way, the security admin cannot ensure that users are aware of any potential risks when accessing HTTPS sites with untrusted certificates.
- A web server certificate signed by an external Certificate Authority (D) is not a good choice for an SSL Forward Untrust certificate because it is trusted by most client browsers that have the external CA in
their trust store1. This means that if the firewall observes an invalid or untrusted security certificate from the server, it will present the web server certificate to the client, which will not trigger an untrusted certificate warning2. This way, the security admin cannot ensure that users are aware of any potential
risks when accessing HTTPS sites with untrusted certificates.

Verified References:

- 1: How to Configure SSL Decryption - Palo Alto Networks Knowledge Base
- 2: How to Implement and Test SSL Decryption - Palo Alto Networks Knowledge Base

NEW QUESTION 85
Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

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

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user-mapping/globalprote GlobalProtect is a VPN solution that provides

secure remote access to corporate networks. When a user connects to GlobalProtect, their identity is verified against an LDAP server. This ensures that all IP address-to-user mappings are explicitly known.

NEW QUESTION 86
Which three external authentication services can the firewall use to authenticate admins into the Palo Alto Networks NGFW without creating administrator account on the firewall? (Choose three.)

A. RADIUS
B. TACACS+
C. Kerberos
D. LDAP
E. SAML

Answer: ABE

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

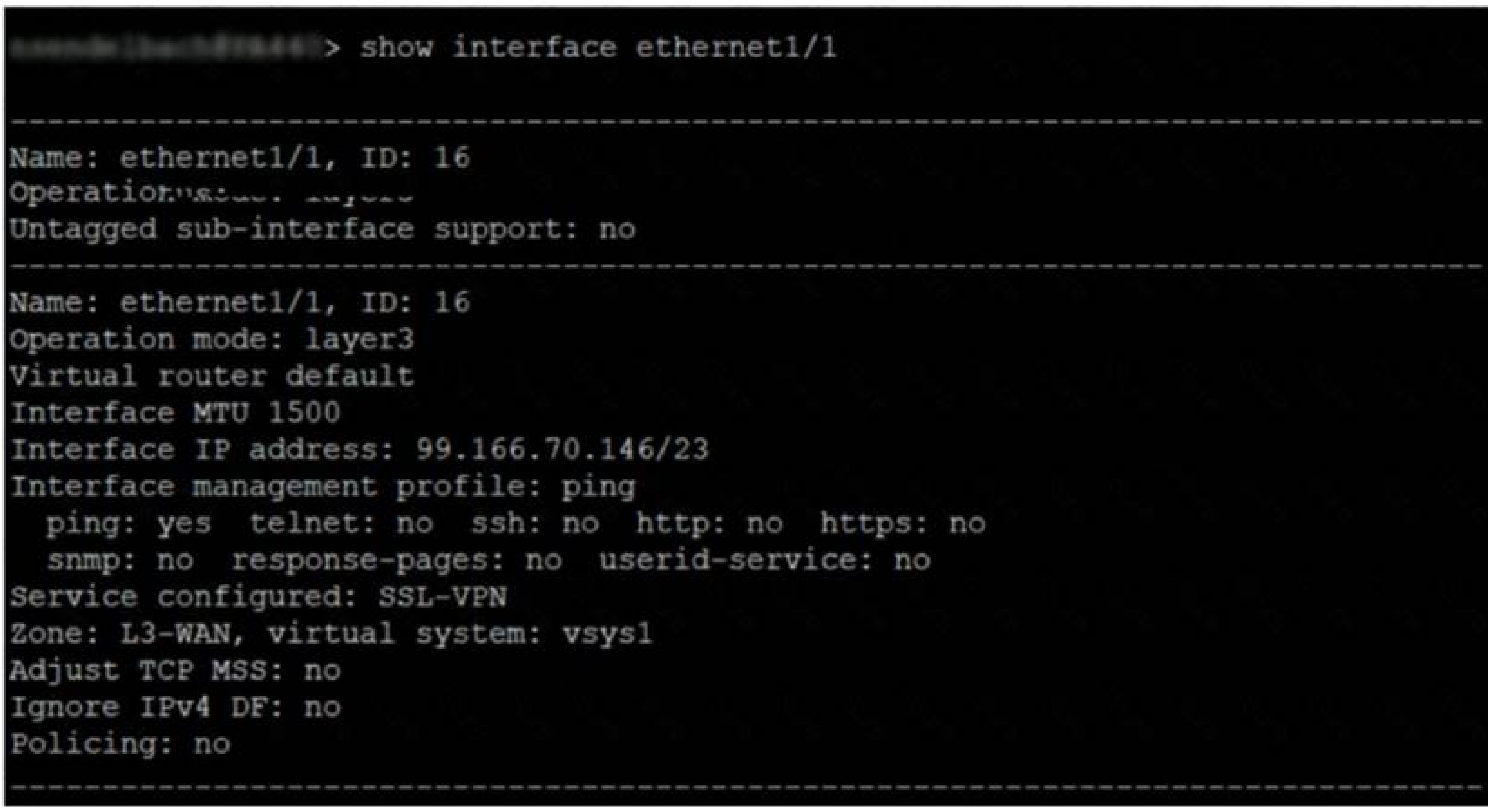
NEW QUESTION 88
A company has recently migrated their branch office's PA-220S to a centralized Panorama. This Panorama manages a number of PA-7000 Series and PA-5200 Series devices All device group and template configuration is managed solely within Panorama
They notice that commit times have drastically 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 91
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 92
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 96
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 101
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.

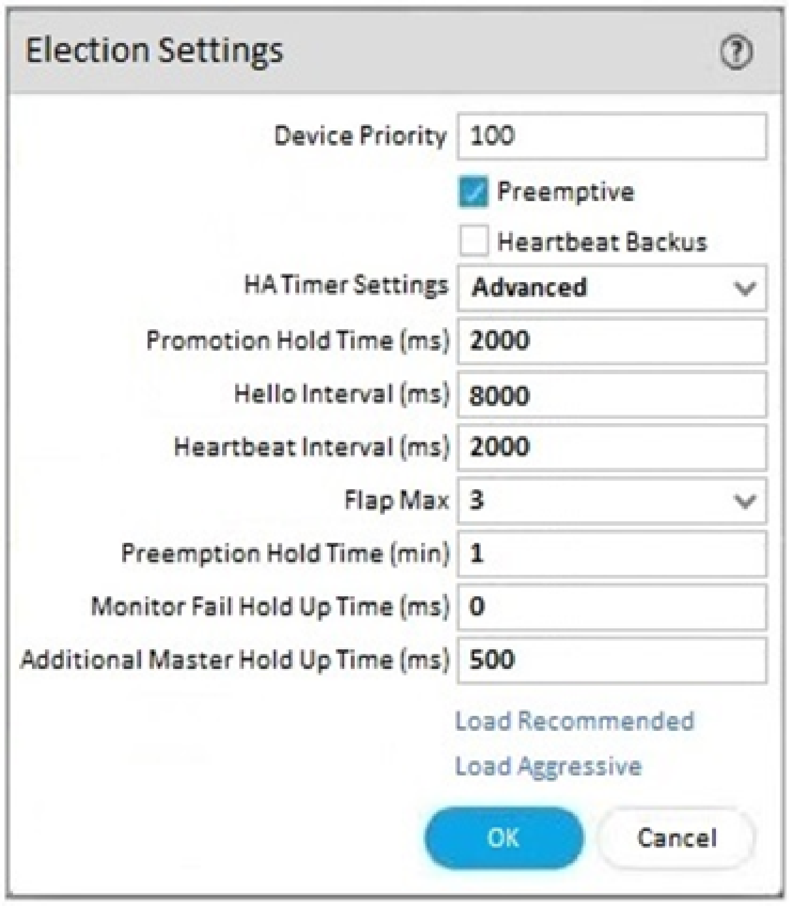
NEW QUESTION 104
An administrator troubleshoots an issue that causes packet drops.
Which log type will help the engineer verify whether packet buffer protection was activated?

A. Data Filtering
B. Configuration
C. Threat
D. Traffic

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNGFCA4

NEW QUESTION 109
An engineer reviews high availability (HA) settings to understand a recent HA failover event. Review the screenshot below.



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 at which the HA peers exchange messages in the form of an ICMP (ping)

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

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/ha-timers

NEW QUESTION 111
Which DoS Protection Profile detects and prevents session exhaustion attacks against specific destinations?

A. Resource Protection
B. TCP Port Scan Protection
C. Packet Based Attack Protection
D. Packet Buffer Protection

Answer: A

Explanation:
IP flood thresholds, you can also use DoS Protection profiles to detect and prevent session exhaustion attacks in which a large number of hosts (bots) establish as many sessions as possible to consume a target's resources. On the profile's Resources Protection tab, you can set the maximum number of concurrent sessions that the device(s) defined in the DoS Protection policy rule to which you apply the profile can receive. When the number of concurrent sessions reaches its maximum limit, new sessions are dropped.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/

NEW QUESTION 116
Which new PAN-OS 11.0 feature supports IPv6 traffic?

A. DHCPv6 Client with Prefix Delegation
B. OSPF
C. DHCP Server
D. IKEv1

Answer: A

Explanation:
https://docs.paloaltonetworks.com/compatibility-matrix/ipv6-support-by-feature/ipv6-support-by-feature-table

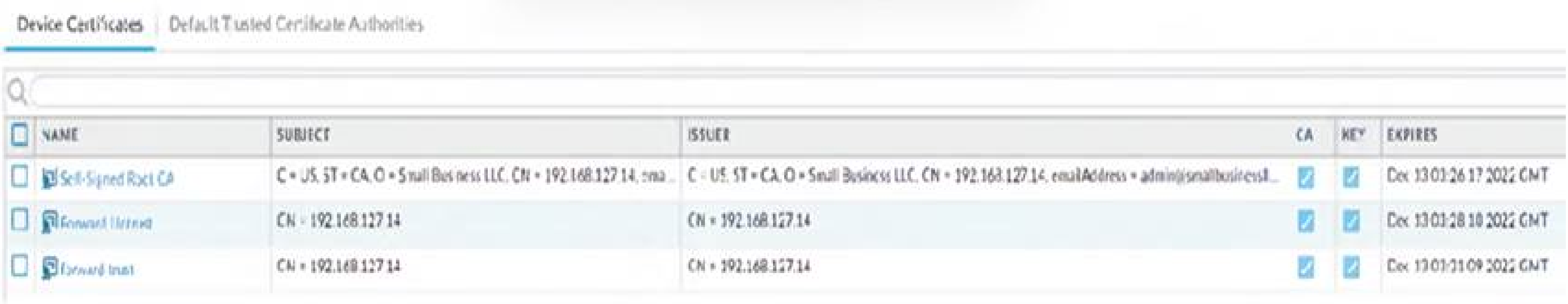
NEW QUESTION 121
An administrator has purchased WildFire subscriptions for 90 firewalls globally. What should the administrator consider with regards to the WildFire infra-structure?

A. To comply with data privacy regulations, WildFire signatures and ver-dicts are not shared globally.
B. Palo Alto Networks owns and maintains one global cloud and four WildFire regional clouds.
C. Each WildFire cloud analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds.
D. The WildFire Global Cloud only provides bare metal analysis.

Answer: C

Explanation:
https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts Each WildFire cloud—global (U.S.), regional, and private—analyzes samples and generates WildFire verdicts independently of the other WildFire clouds. With the exception of WildFire private cloud verdicts, WildFire verdicts are shared globally, enabling WildFire users to access a worldwide database of threat data.
https://docs.paloaltonetworks.com/wildfire/10-1/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts.ht

NEW QUESTION 126
Review the screenshot of the Certificates page.



☐	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@smallbusinessl...	☑	☑	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 129
An engineer must configure a new SSL decryption deployment.
Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

A. A Decryption profile must be attached to the Decryption policy that the traffic matches.
B. A Decryption profile must be attached to the Security policy that the traffic matches.
C. There must be a certificate with only the Forward Trust option selected.
D. There must be a certificate with both the Forward Trust option and Forward Untrust option selected.

Answer: A

Explanation:
To use PAN-OS multi-factor authentication (MFA) to secure access to critical assets, the enterprise should configure a Captive Portal authentication policy that uses an authentication sequence. An authentication sequence is a feature that allows the firewall to enforce multiple authentication methods (factors) for users who access sensitive services or applications. An authentication sequence can include up to four factors, such as login and password, Voice, SMS, Push, or One-time Password (OTP) authentication. The firewall can integrate with MFA vendors through RADIUS or vendor APIs to provide the additional factors12.
To configure an authentication sequence, the enterprise needs to create an authentication profile for each factor and then add them to the sequence in the desired order. The enterprise also needs to create a Captive Portal authentication policy that matches the traffic that requires MFA and applies the authentication sequence to it. The Captive Portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The Captive Portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button34.
When a user tries to access a service or application that matches the Captive Portal authentication policy, the firewall redirects the user to the Captive Portal web form for the first factor. After the user successfully authenticates for the first factor, the firewall prompts the user for the second factor through RADIUS or vendor API integration. The firewall repeats this process until all factors in the sequence are completed or until one factor fails. If all factors are completed successfully, the firewall allows the user to access the service or application. If one factor fails, the firewall denies access and logs an event56.

Configuring a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile is not sufficient to use PAN-OS MFA. This option only provides one factor of authentication through RADIUS integration with an MFA vendor. To use multiple factors of authentication, an authentication sequence is required.
Creating an authentication profile and assigning another authentication factor to be used by a Captive Portal authentication policy is not correct to use PAN-OS MFA. This option does not specify how to create or apply an authentication sequence, which is necessary for enforcing multiple factors of authentication.
Using a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns is not relevant to use PAN-OS MFA. This option is a feature of Palo Alto Networks Cortex XDR™ that helps
protect endpoints from credential theft by malicious actors. It does not provide any MFA functionality for accessing critical assets7.
References: Authentication Sequence, Configure Multi-Factor Authentication, Configure an Authenticatio Portal, Create an Authentication Profile, Create an Authentication Sequence, Create a Captive Portal Authentication Policy, Credential Phishing Agent

NEW QUESTION 133
......