Paloalto-Networks

Exam Questions PCNSE

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

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

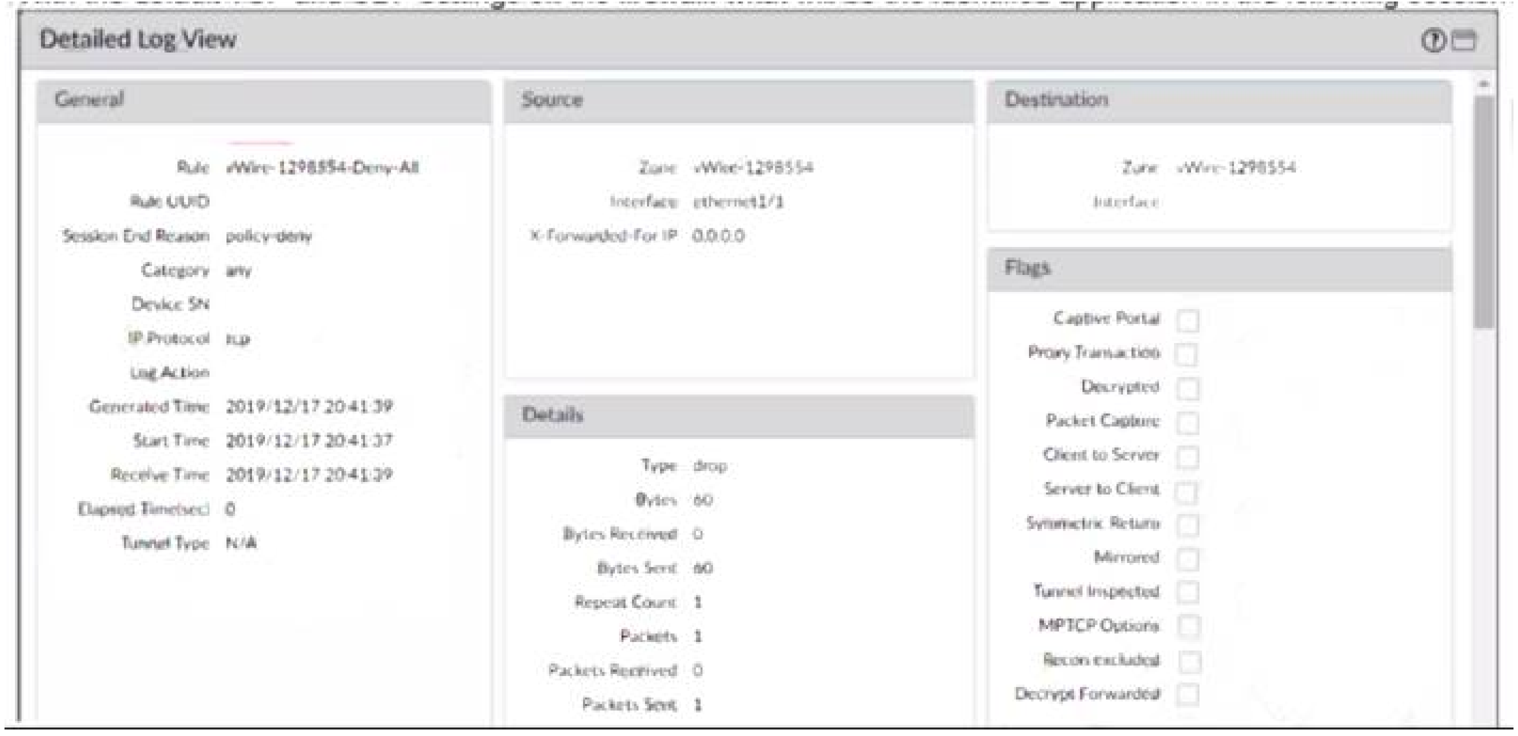
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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
An engineer is troubleshooting a traffic-routing issue. What is the correct packet-flow sequence?

A. PBF > Zone Protection Profiles > Packet Buffer Protection
B. BGP > PBF > NAT
C. PBF > Static route > Security policy enforcement
D. NAT > Security policy enforcement > OSPF

Answer: C

Explanation:
The correct packet-flow sequence is C. PBF > Static route > Security policy enforcement. This sequence describes the order of operations that the firewall performs when processing a packet. PBF stands for
Policy-Based Forwarding, which is a feature that allows the firewall to override the routing table and forward
traffic based on the source and destination addresses, application, user, or service. PBF is evaluated before the static route lookup, which is the default method of forwarding traffic based on the destination address and the longest prefix match. Security policy enforcement is the stage where the firewall applies the security policy rules to allow or block traffic based on various criteria, such as zone, address, port, user, application, etc12. References: Policy-Based Forwarding, Packet Flow Sequence in PAN-OS

NEW QUESTION 3
A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours.
Which two steps are likely to mitigate the issue? (Choose TWO)

A. Exclude video traffic
B. Enable decryption
C. Block traffic that is not work-related
D. Create a Tunnel Inspection policy

Answer: AC

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PP3ICAW

NEW QUESTION 4
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 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
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

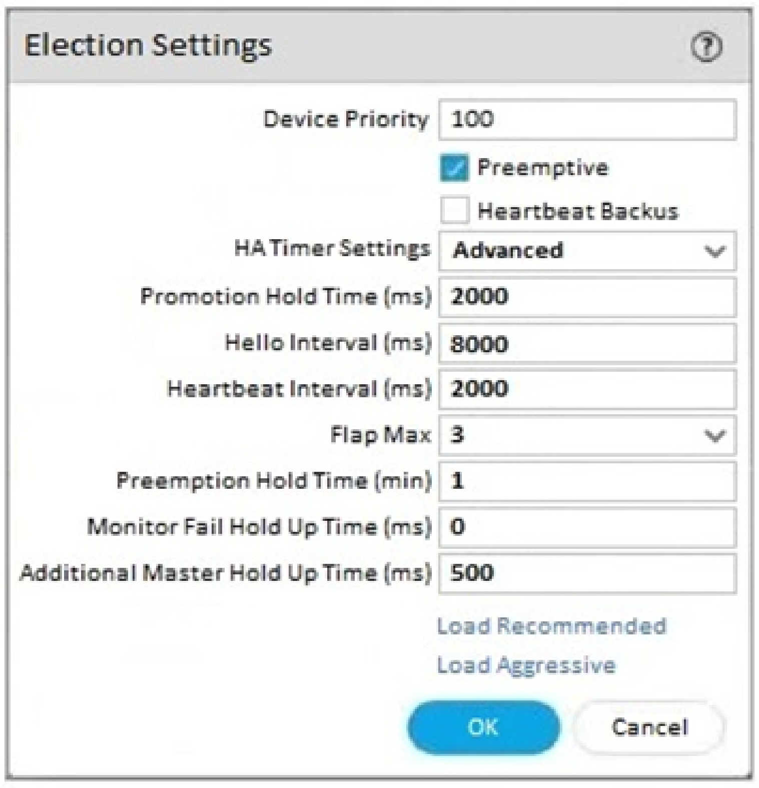
NEW QUESTION 7
An engineer needs to configure a standardized template for all Panorama-managed firewalls. These settings will be configured on a template named "Global" and will be included in all template stacks.
Which three settings can be configured in this template? (Choose three.)

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 8
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 9
An engineer is configuring a template in Panorama which will contain settings that need to be applied to all firewalls in production.
Which three parts of a template an engineer can configure? (Choose three.)

A. NTP Server Address
B. Antivirus Profile
C. Authentication Profile
D. Service Route Configuration
E. Dynamic Address Groups

Answer: ACD

Explanation:
> A, C, and D are the correct answers because they are the parts of a template that an engineer can configure in Panorama. A template is a collection of device and network settings that can be pushed to multiple firewalls from Panorama1. A template can contain settings such as2:
> A: NTP Server Address: This is the address of the Network Time Protocol server that synchronizes the time on the firewall.
> C: Authentication Profile: This is the profile that defines how the firewall authenticates users and administrators.
> D: Service Route Configuration: This is the configuration that specifies which interface and source IP address the firewall uses to access external services, such as DNS, email, syslog, etc.

NEW QUESTION 10
An administrator is using Panorama to manage multiple firewalls. After upgrading all devices to the latest PAN-OS software, the administrator enables log forwarding from the firewalls to Panorama.
However, pre-existing logs from the firewalls are not appearing in Panorama.
Which action should be taken to enable the firewalls to send their pre-existing logs to Panorama?

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

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/use-the-cli/use-secure-copy-to-import-and

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

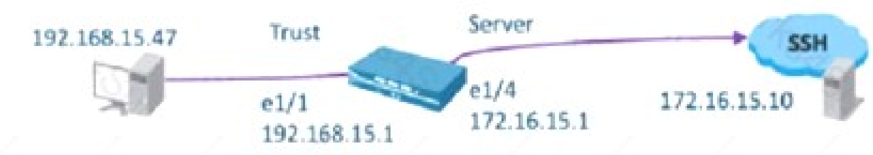
A. The firewall denied the traffic before the application match could be performed.

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 14
Which GloDalProtecI 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 19
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:

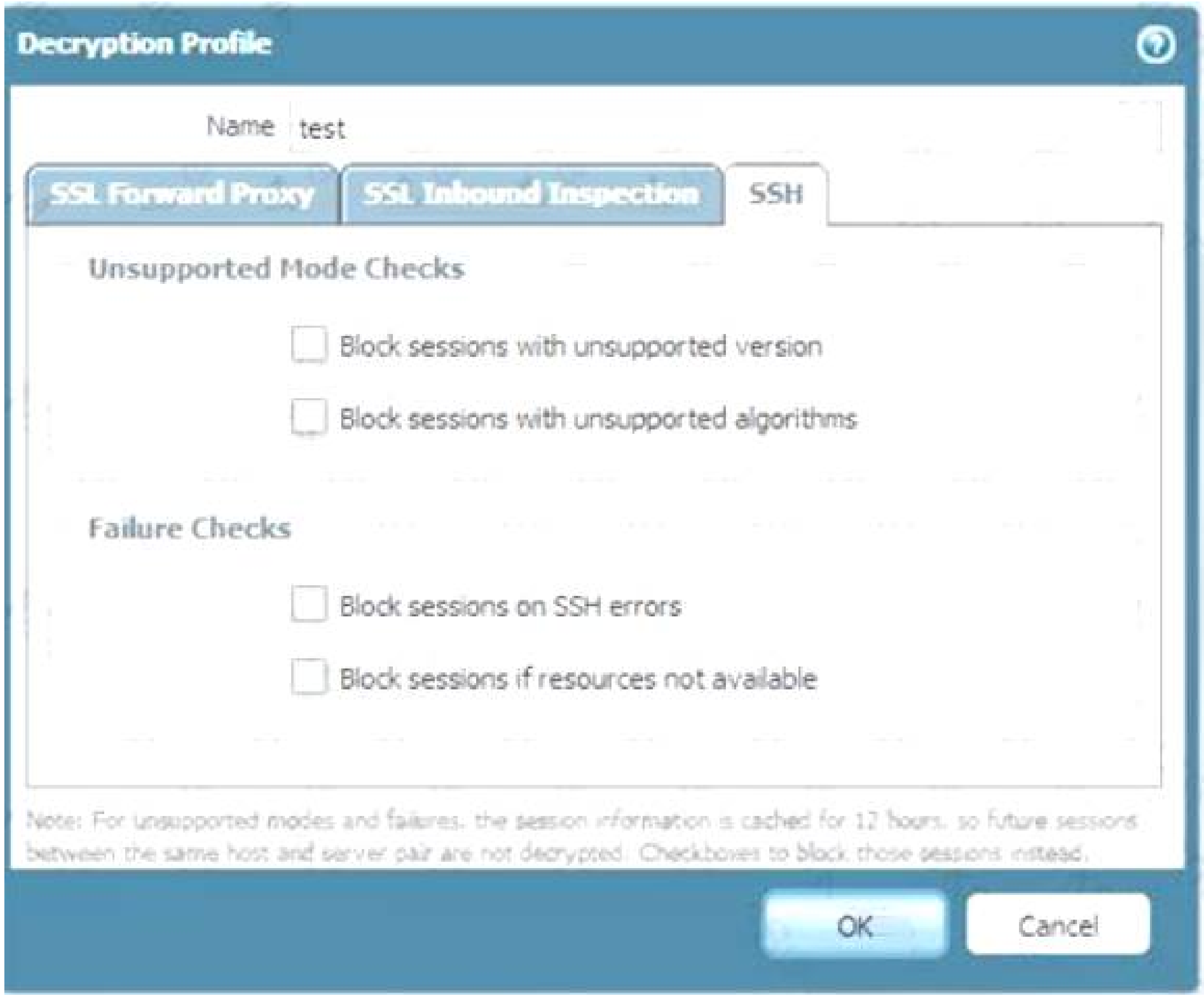
- B: A private key. This is the key that the firewall uses to sign the certificates that it generates for the decrypted sessions. The private key must be securely stored on the firewall and not shared with anyone1.
- D: A certificate authority (CA) certificate. This is the certificate that the firewall 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 24
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



Decryption Profile

Name: test

SSL Forward Proxy | SSL Inbound Inspection | SSH

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.

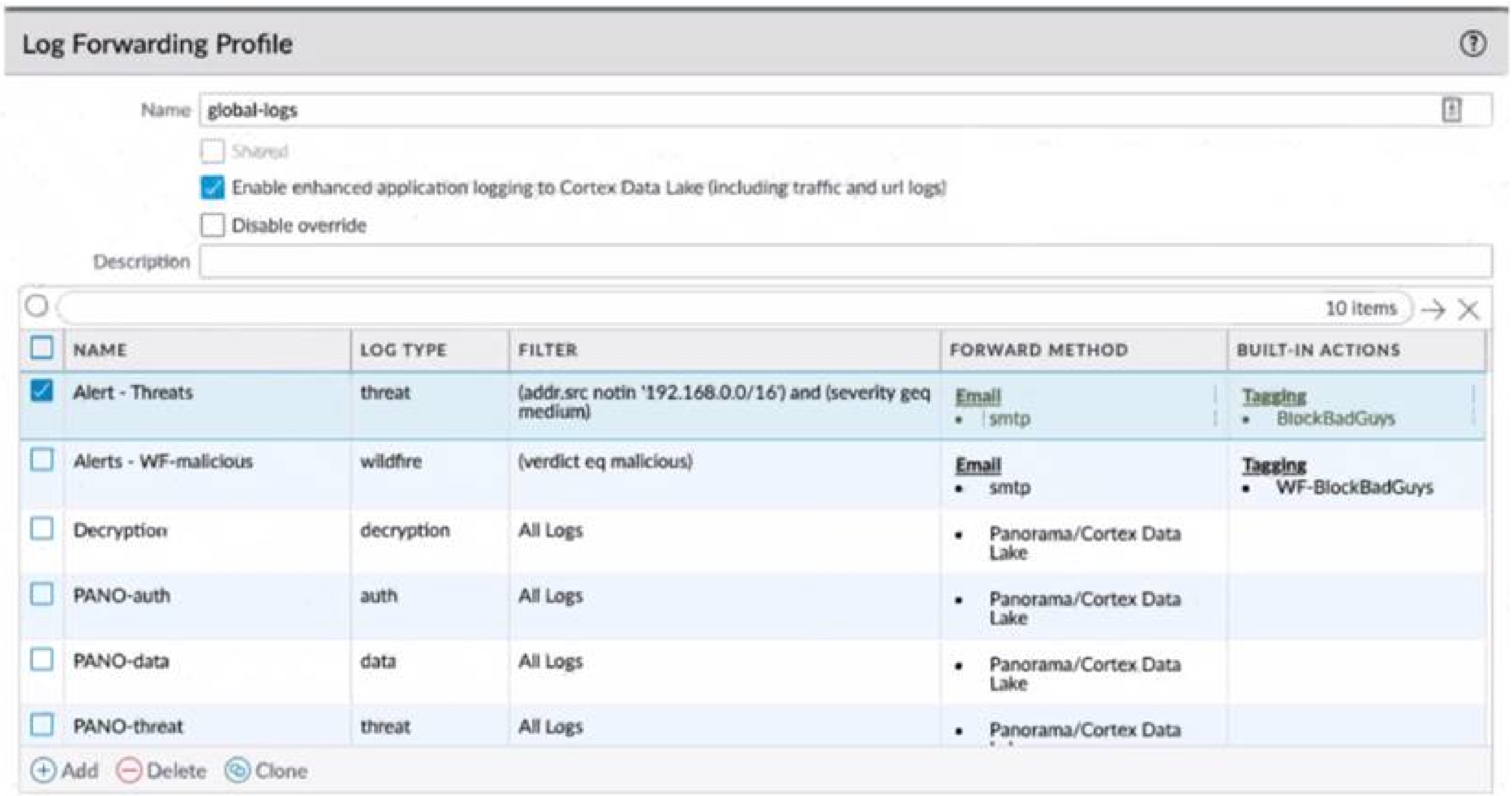
NEW QUESTION 29
An engineer is designing a deployment of multi-vsys firewalls.
What must be taken into consideration when designing the device group structure?

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 31
Review the images.



Log Forwarding Profile

Name: global-logs

□ Shared

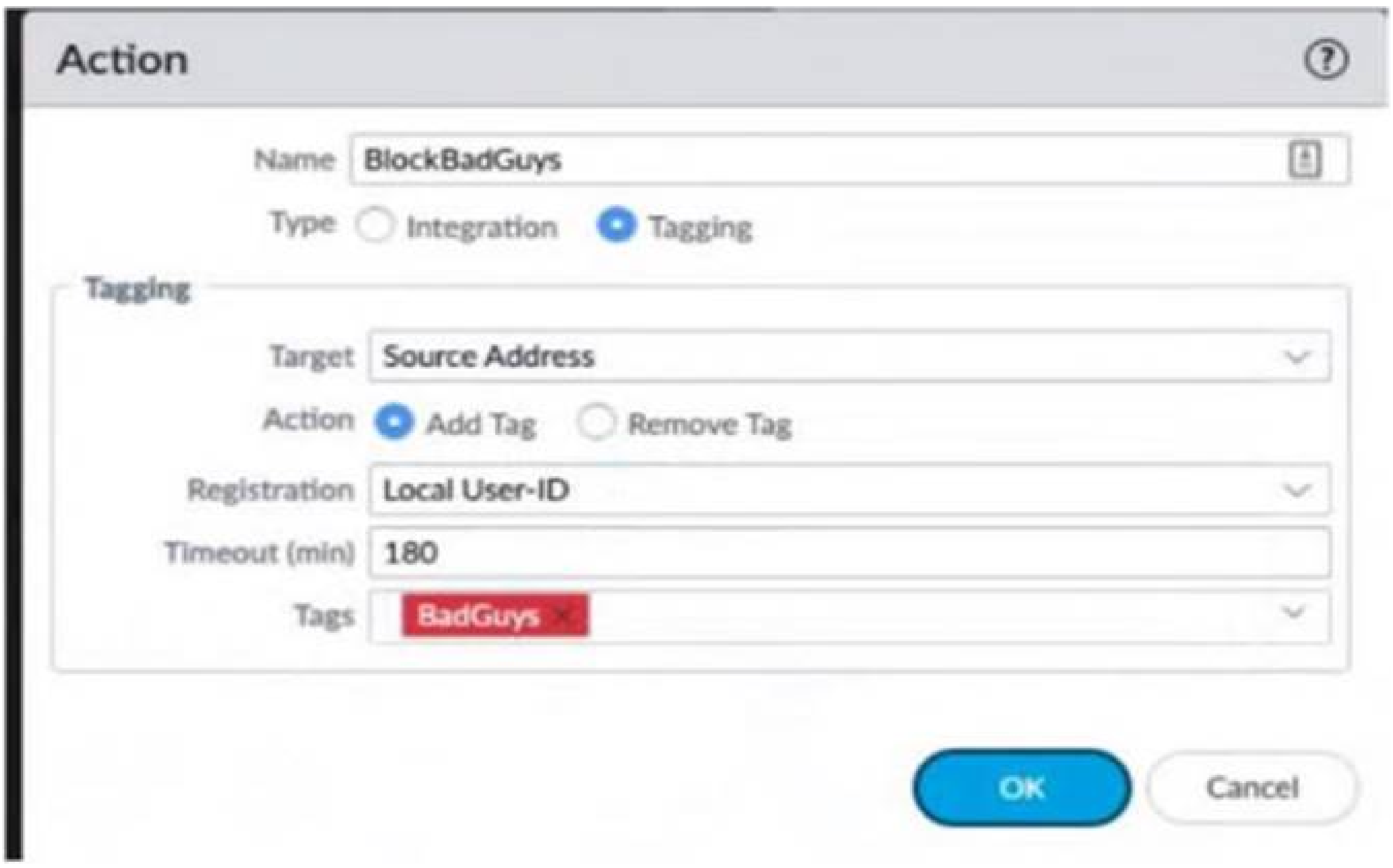
☑ Enable enhanced application logging to Cortex Data Lake (including traffic and url logs)

□ Disable override

Description

10 items

□	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
☑	Alert - Threats	threat	(addr.src notin '192.168.0.0/16') and (severity geq medium)	Email • smtp	Tagging • BlockBadGuys
□	Alerts - WF-malicious	wildfire	(verdict eq malicious)	Email • smtp	Tagging • WF-BlockBadGuys
□	Decryption	decryption	All Logs	• Panorama/Cortex Data Lake	
□	PANO-auth	auth	All Logs	• Panorama/Cortex Data Lake	
□	PANO-data	data	All Logs	• Panorama/Cortex Data Lake	
□	PANO-threat	threat	All Logs	• Panorama/Cortex Data	



Action

Name: BlockBadGuys

Type: ○ Integration ● Tagging

Tagging

Target: Source Address

Action: ● Add Tag ○ Remove Tag

Registration: Local User-ID

Timeout (min): 180

Tags: BadGuys

A firewall policy that permits web traffic includes the global-logs policy is depicted What is the result of traffic that matches the "Alert - Threats" Profile Match List?

A. The source address of SMTP traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.
B. The source address of traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.
C. The source address of traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.
D. The source address of SMTP traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.

Answer: C

NEW QUESTION 33
A company has configured a URL Filtering profile with override action on their firewall. Which two profiles are needed to complete the configuration? (Choose two)

A. SSL/TLS Service
B. HTTP Server
C. Decryption
D. Interface Management

Answer: AD

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRdCAK https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/configure-url-filtering
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/allow-password-access-to-certain-site

NEW QUESTION 34
Which two key exchange algorithms consume the most resources when decrypting SSL traffic? (Choose two.)

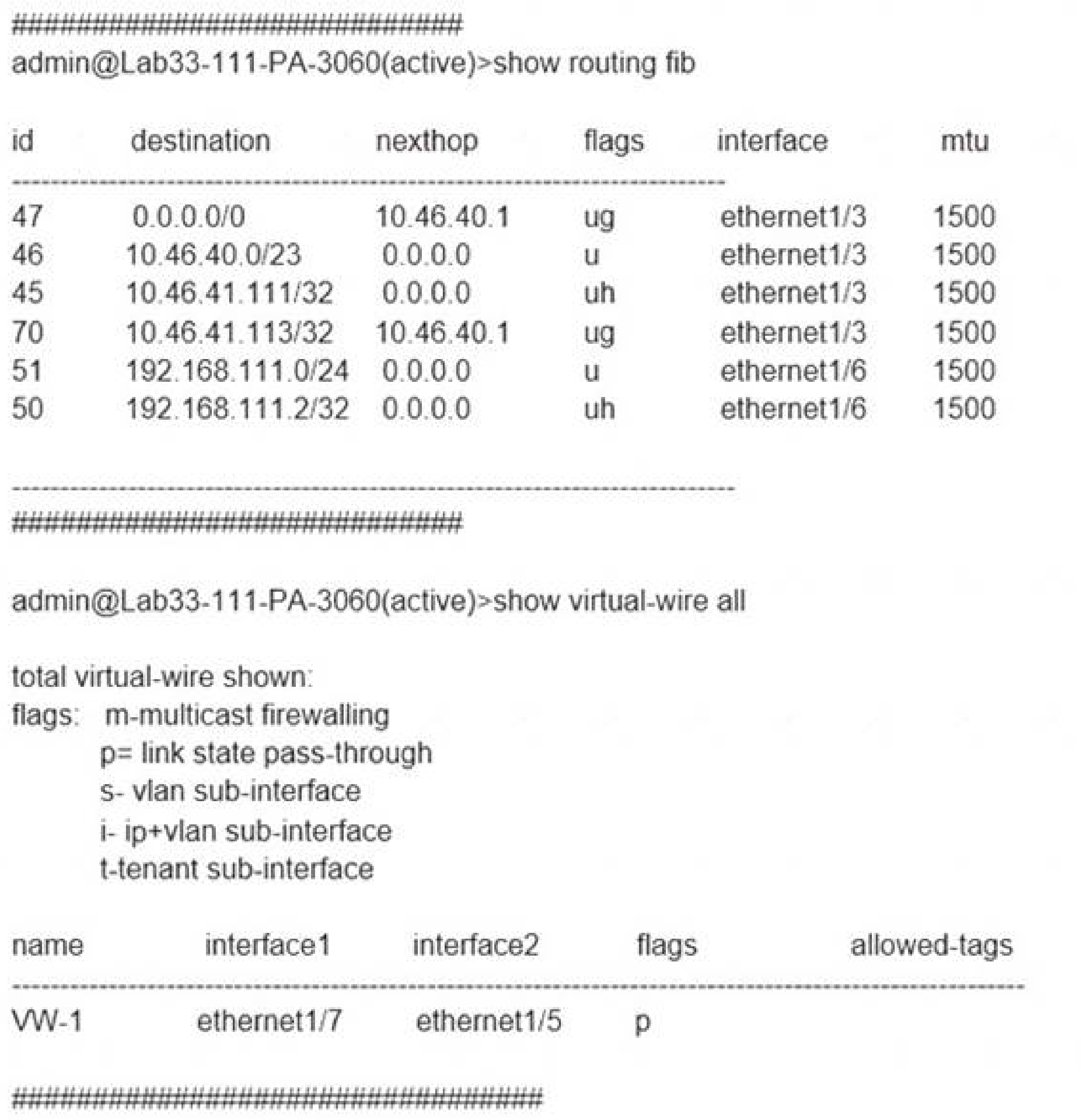
A. ECDSA

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 35
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

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

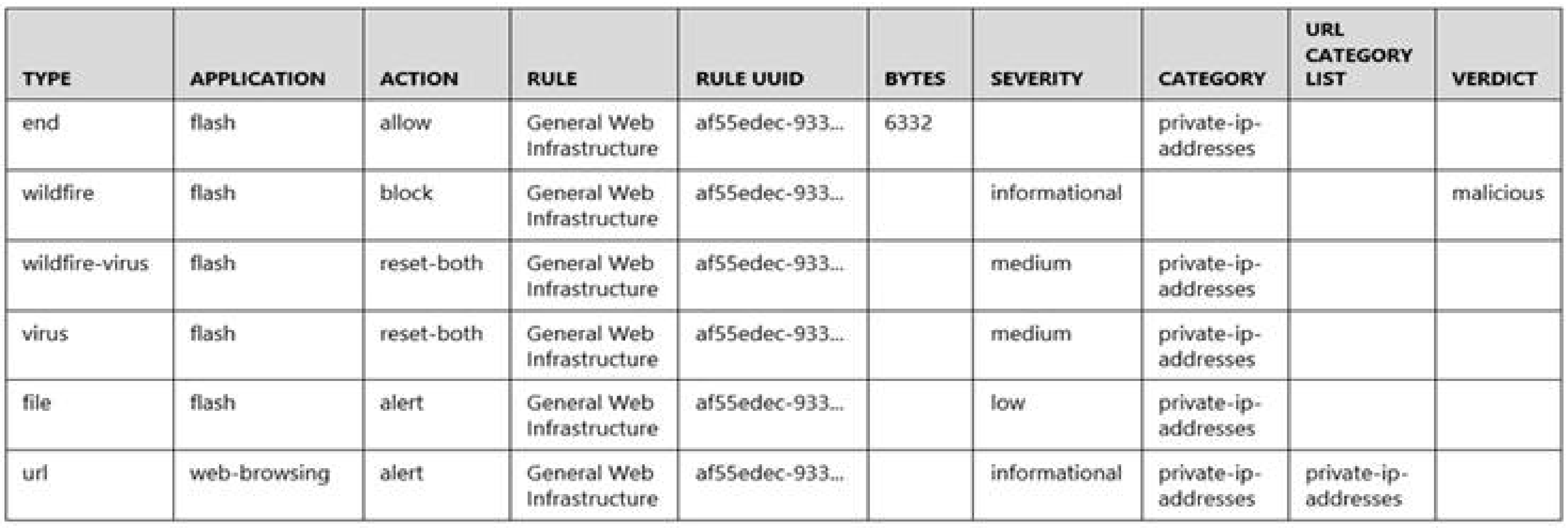
Which will be the egress interface if the traffic's ingress interface is ethernet1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

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 39
Given the following snippet of a WildFire submission log, did the end user successfully download a file?



TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
end	flash	allow	General Web Infrastructure	af55edec-933...	6332		private-ip-addresses		
wildfire	flash	block	General Web Infrastructure	af55edec-933...		informational			malicious
wildfire-virus	flash	reset-both	General Web Infrastructure	af55edec-933...		medium	private-ip-addresses		
virus	flash	reset-both	General Web Infrastructure	af55edec-933...		medium	private-ip-addresses		
file	flash	alert	General Web Infrastructure	af55edec-933...		low	private-ip-addresses		
url	web-browsing	alert	General Web Infrastructure	af55edec-933...		informational	private-ip-addresses	private-ip-addresses	

A. No, because the URL generated an alert.
B. Yes, because both the web-browsing application and the flash file have the 'alert" action.
C. Yes, because the final action is set to "allow."
D. No, because the action for the wildfire-virus is "reset-both."

Answer: C

Explanation:
Based on the snippet of the WildFire submission log provided, it appears that the end user was able to successfully download a file. The key indicator here is that the final action for the web-browsing application and the flash file is set to “allow.” This means that despite any alerts or other actions taken earlier in the process, the ultimate decision was to allow the file to be downloaded.

NEW QUESTION 43
Which three options does Panorama offer for deploying dynamic updates to its managed devices? (Choose three.)

A. Check dependencies
B. Schedules
C. Verify
D. Revert content
E. Install

Answer: BDE

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-de https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-de

NEW QUESTION 47
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 48
Which Panorama feature protects logs against data loss if a Panorama server fails?

A. Panorama HA automatically ensures that no logs are lost if a server fails inside the HA Cluster.
B. Panorama Collector Group with Log Redundancy ensures that no logs are lost if a server fails inside the Collector Group.
C. Panorama HA with Log Redundancy ensures that no logs are lost if a server fails inside the HA Cluster.
D. Panorama Collector Group automatically ensures that no logs are lost if a server fails inside the Collector Group

Answer: B

Explanation:
https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/manage-log-collection/manage-collector-gr "Log redundancy is available only if each Log Collector has the same number of logging disks."
(Recommended) Enable log redundancy across collectors if you are adding multiple Log Collectors to a single Collector group. Redundancy ensures that no logs

are lost if any one Log Collector becomes unavailable. Each log will have two copies and each copy will reside on a different Log Collector. For example, if you have two Log Collectors in the collector group the log is written to both Log Collectors. Enabling redundancy creates more logs and therefore requires more storage capacity, reducing storage capability in half. When a Collector Group runs out of space, it deletes older logs. Redundancy also doubles the log processing traffic in a Collector Group, which reduces its maximum logging rate by half, as each Log Collector must distribute a copy of each log it receives.

NEW QUESTION 53
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 55
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 56
Information Security is enforcing group-based policies by using security-event monitoring on Windows User-ID agents for IP-to-User mapping in the network.
During the rollout, Information Security identified a gap for users authenticating to their VPN and wireless networks.
Root cause analysis showed that users were authenticating via RADIUS and that authentication events were not captured on the domain controllers that were being monitored Information Security found that authentication events existed on the Identity Management solution (IDM). There did not appear to be direct integration between PAN-OS and the IDM solution
How can Information Security extract and learn iP-to-user mapping information from authentication events for VPN and wireless users?

A. Add domain controllers that might be missing to perform security-event monitoring for VPN and wireless users.
B. Configure the integrated User-ID agent on PAN-OS to accept Syslog messages over TLS.
C. Configure the User-ID XML API on PAN-OS firewalls to pull the authentication events directly fromthe IDM solution
D. Configure the Windows User-ID agents to monitor the VPN concentrators and wireless controllers for IP-to-User mapping.

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-i

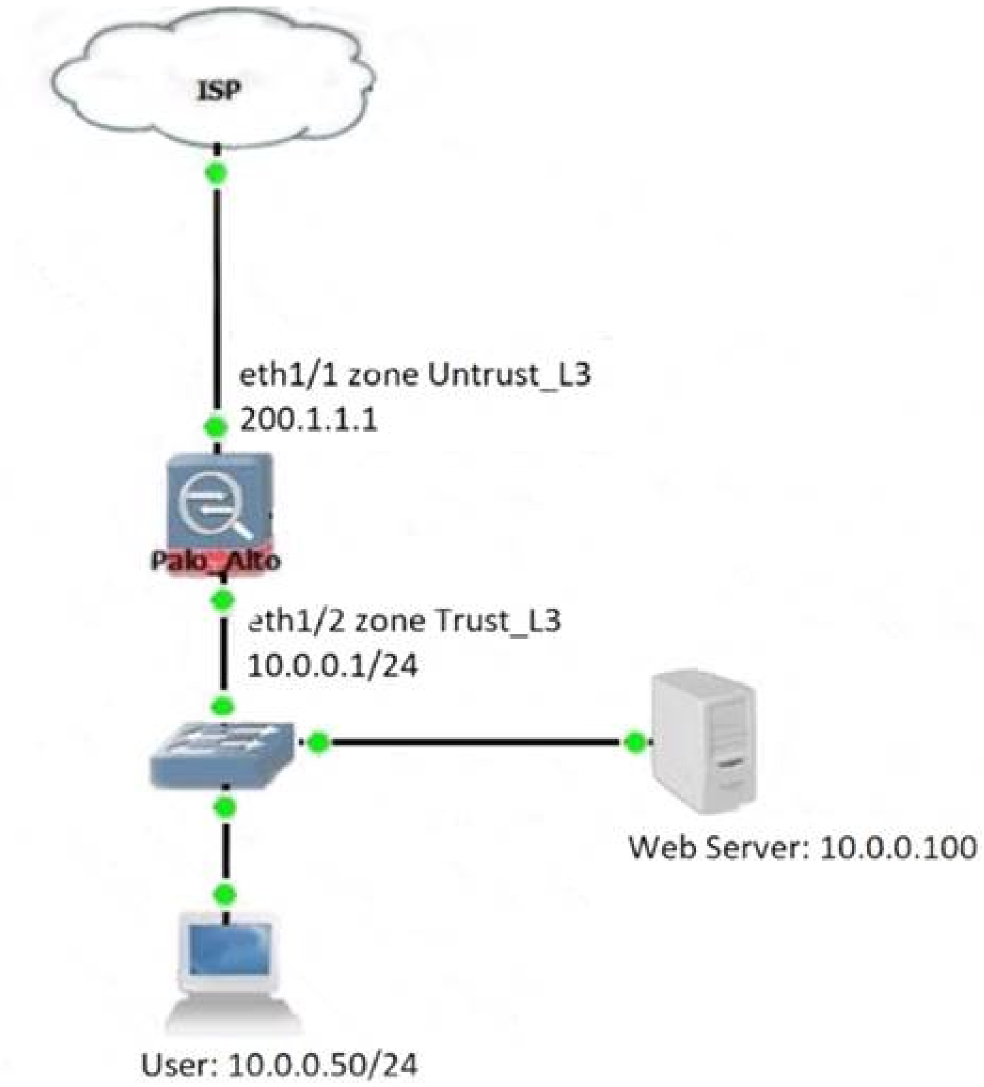
NEW QUESTION 59
An administrator has configured OSPF with Advanced Routing enabled on a Palo Alto Networks firewall running PAN-OS 10.2. After OSPF was configured, the administrator noticed that OSPF routes were not being learned.
Which two actions could an administrator take to troubleshoot this issue? (Choose two.)

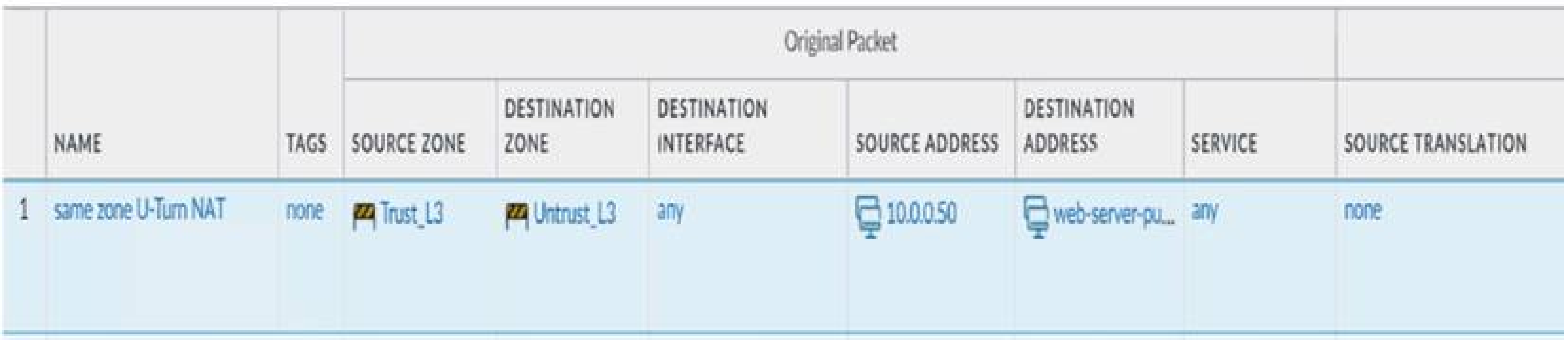
A. Run the CLI command show advanced-routing ospf neighbor
B. In the WebUI, view the Runtime Stats in the virtual router
C. Look for configuration problems in Network > virtual router > OSPF
D. In the WebUI, view Runtime Stats in the logical router

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 62
Review the information below. A firewall engineer creates a U-NAT rule to allow users in the trust zone access to a server in the same zone by using an external, public NAT IP for that server.
Given the rule below, what change should be made to make sure the NAT works as expected?





			Original Packet						
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION
1	same zone U-Turn NAT	none	Trust_L3	Untrust_L3	any	10.0.0.50	web-server-pu...	any	none

A. Change destination NAT zone to Trust_L3.
B. Change destination translation to Dynamic IP (with session distribution) using firewall ethI/2 address.
C. Change Source NAT zone to Untrust_L3.
D. Add source Translation to translate original source IP to the firewall eth1/2 interface translation.

Answer: D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEiCAK

NEW QUESTION 67
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 69
An enterprise Information Security team has deployed policies based on AD groups to restrict user access to critical infrastructure systems. However, a recent phishing campaign against the organization has prompted Information Security to look for more controls that can secure access to critical assets. For users that need to access these systems. Information Security wants to use PAN-OS multi-factor authentication (MFA) integration to enforce MFA.
What should the enterprise do to use PAN-OS MFA?

A. Configure a Captive Portal authentication policy that uses an authentication sequence.
B. Configure a Captive Portal authentication policy that references a RADIUS profile.
C. Create an authentication profile and assign another authentication factor to be used by a Captive Portal authentication policy.
D. Use a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns.

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 assets.
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 71
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.

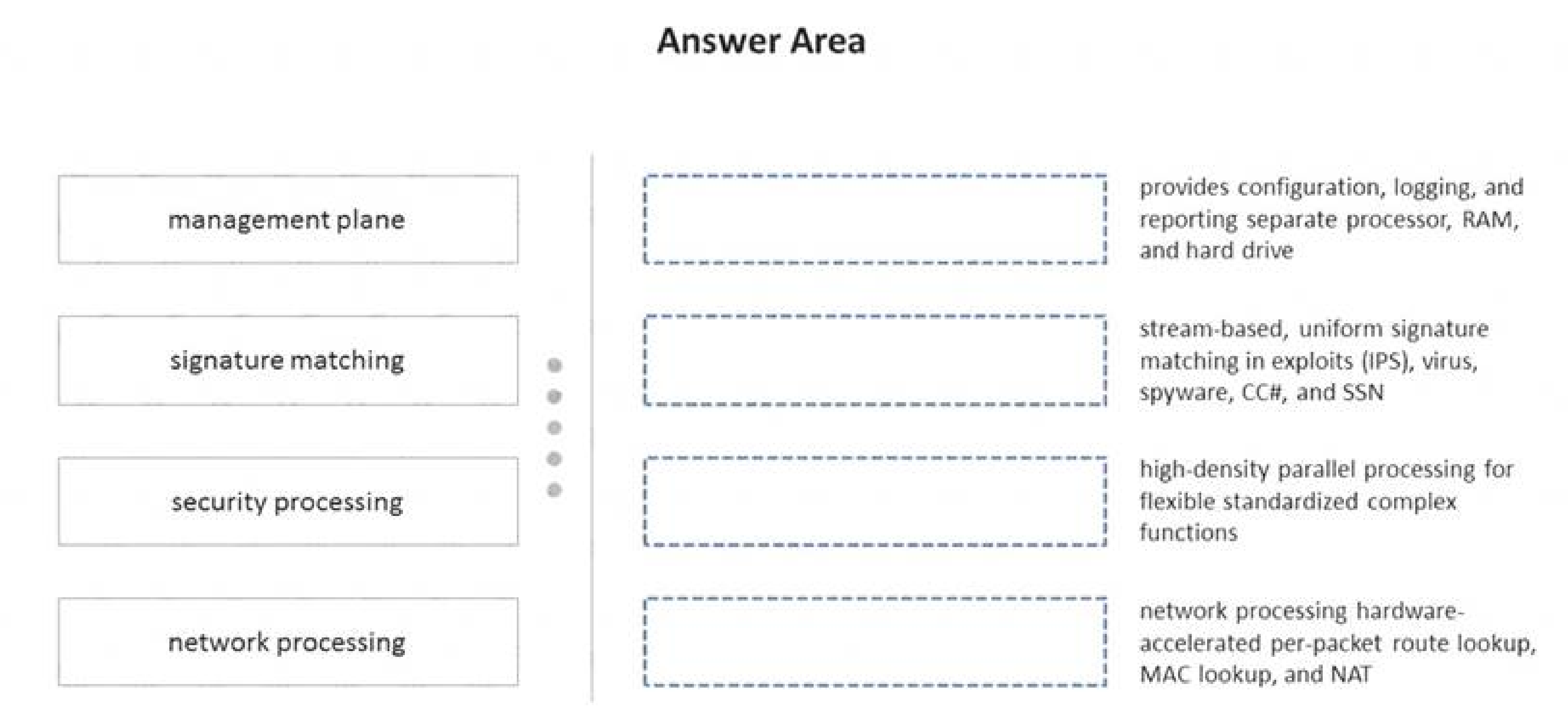
NEW QUESTION 74
An administrator notices that an interface configuration has been overridden locally on a firewall. They require all configuration to be managed from Panorama and overrides are not allowed. What is one way the administrator can meet this requirement?

A. Perform a commit force from the CLI of the firewall.
B. Perform a template commit push from Panorama using the "Force Template Values" option.
C. Perform a device-group commit push from Panorama using the "Include Device and Network Templates" option.
D. Reload the running configuration and perform a Firewall local commit.

Answer: B

Explanation:
The best way for the administrator to meet the requirement of managing all configuration from Panorama and preventing local overrides is B: Perform a template commit push from Panorama using the “Force Template Values” option. This option allows the administrator to overwrite any local configuration on the firewall with the values defined in the template1. This way, the administrator can ensure that the interface configuration and any other

NEW QUESTION 78
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
A network engineer has discovered that asymmetric routing is causing a Palo Alto Networks firewall to drop traffic. The network architecture cannot be changed to correct this.
Which two actions can be taken on the firewall to allow the dropped traffic permanently? (Choose two.)

A. Navigate to Network > Zone Protection Click AddSelect Packet Based Attack Protection > TCP/IP Drop Set "Reject Non-syn-TCP" to No Set "Asymmetric Path" to Bypass
B. > set session tcp-reject-non-syn no
C. Navigate to Network > Zone Protection Click AddSelect Packet Based Attack Protection > TCP/IP Drop Set "Reject Non-syn-TCP" to Global Set "Asymmetric Path" to Global
D. # set deviceconfig setting session tcp-reject-non-syn no

Answer: AD

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClG2CAK

NEW QUESTION 86
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

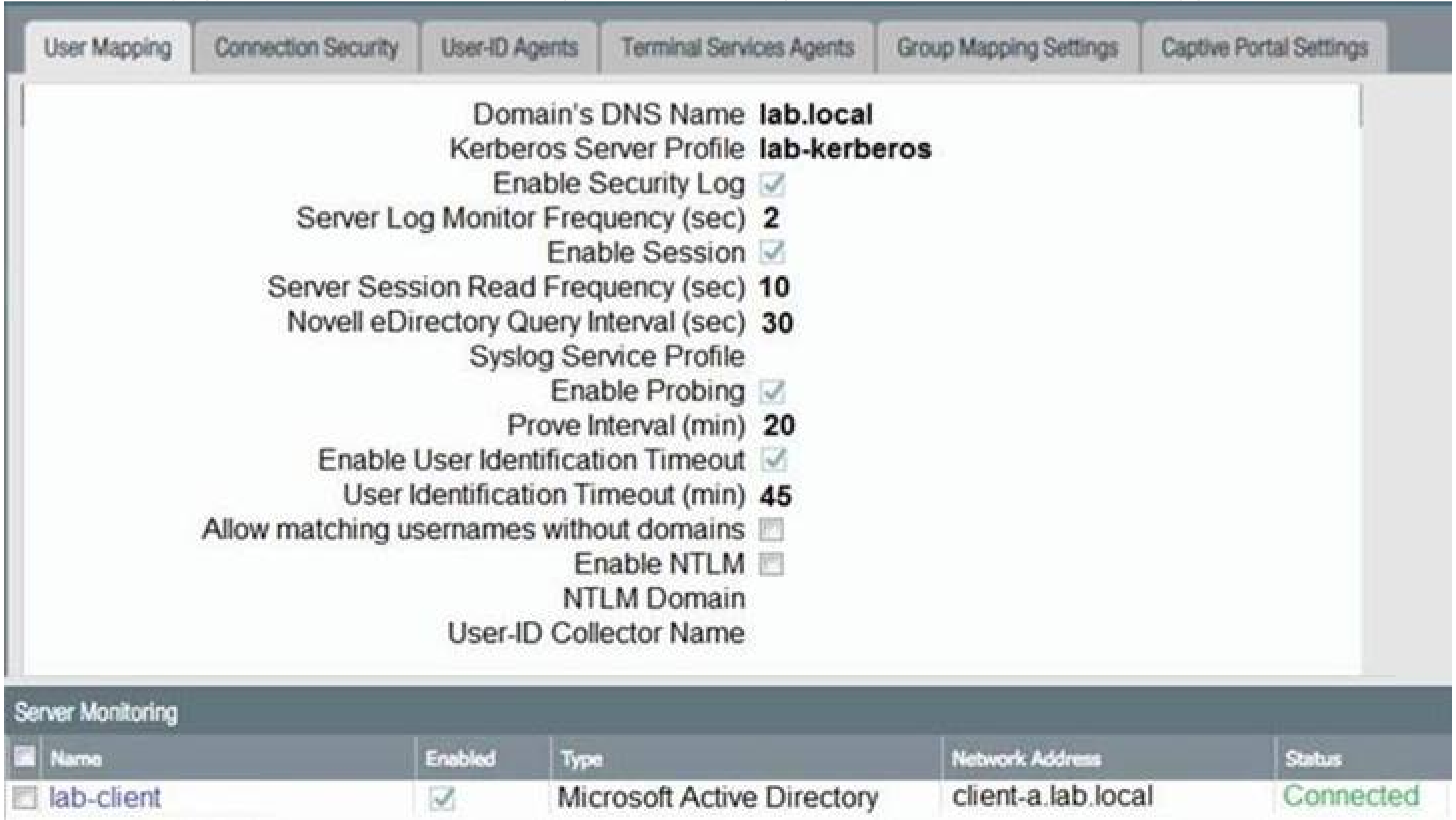
NEW QUESTION 89
Which three items must be configured to implement application override? (Choose three)

A. Custom app
B. Security policy rule
C. Application override policy rule
D. Decryption policy rule
E. Application filter

Answer: ABC

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/policies/policies-application-override
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PPDrCAO

NEW QUESTION 93
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 98
What must be configured to apply tags automatically based on User-ID logs?

A. Device ID
B. Log Forwarding profile
C. Group mapping
D. Log settings

Answer: B

Explanation:
To apply tags automatically based on User-ID logs, the engineer must configure a Log Forwarding profile that specifies the criteria for matching the logs and the tags to apply. The Log Forwarding profile can be attached to a security policy rule or a decryption policy rule to enable auto-tagging for the traffic that matches the rule. The tags can then be used for dynamic address groups, policy enforcement, or
reporting1. References: Use Auto-Tagging to Automate Security Actions, PCNSE Study Guide (page 49)

NEW QUESTION 100
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

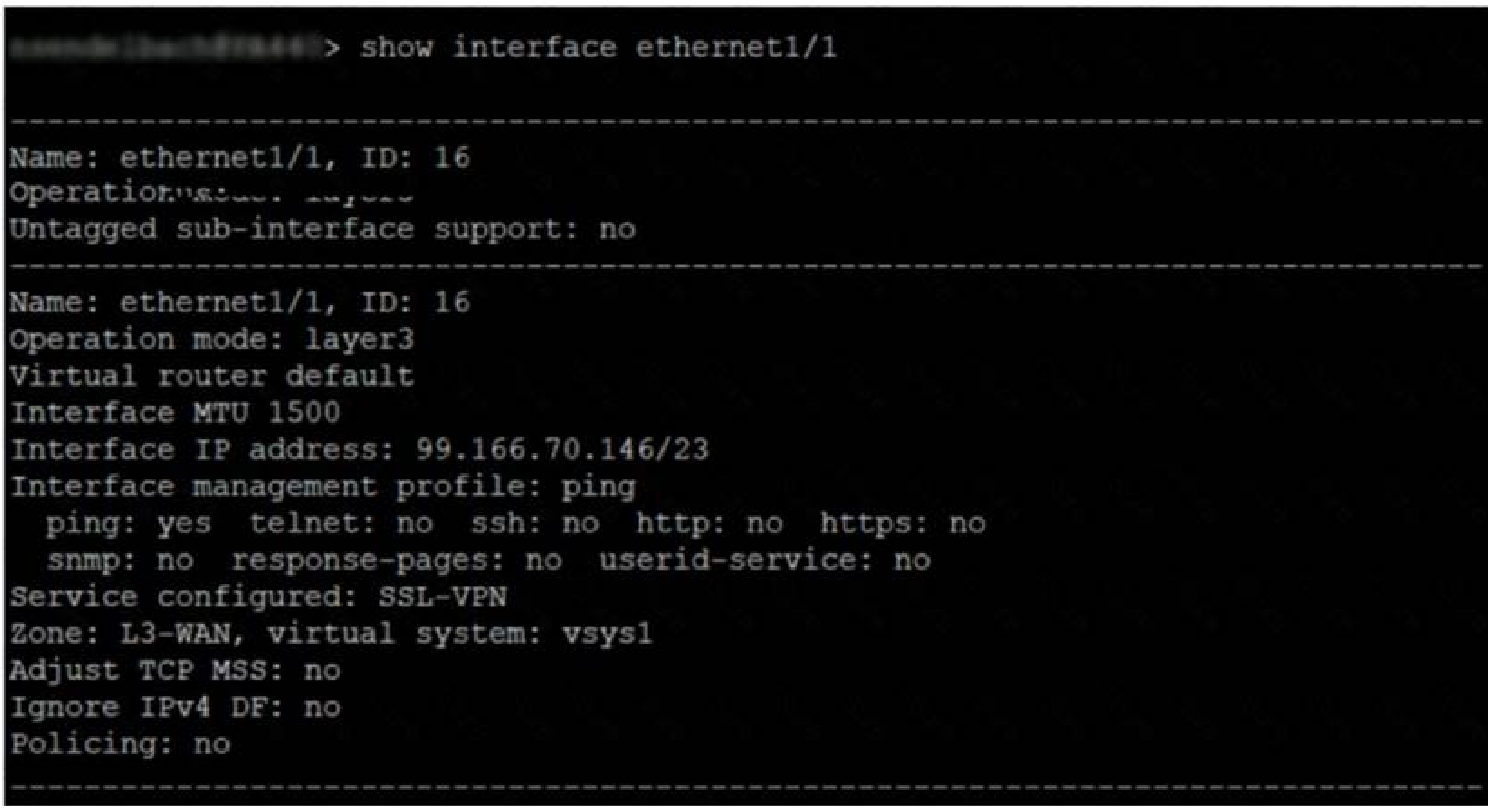
NEW QUESTION 103
A company has recently migrated their branch office's PA-220S to a centralized Panorama. This Panorama manages a number of PA-7000 Series and PA-5200 Series devices All device group and template configuration is managed solely within Panorama
They notice that commit times have drastically 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 104
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)

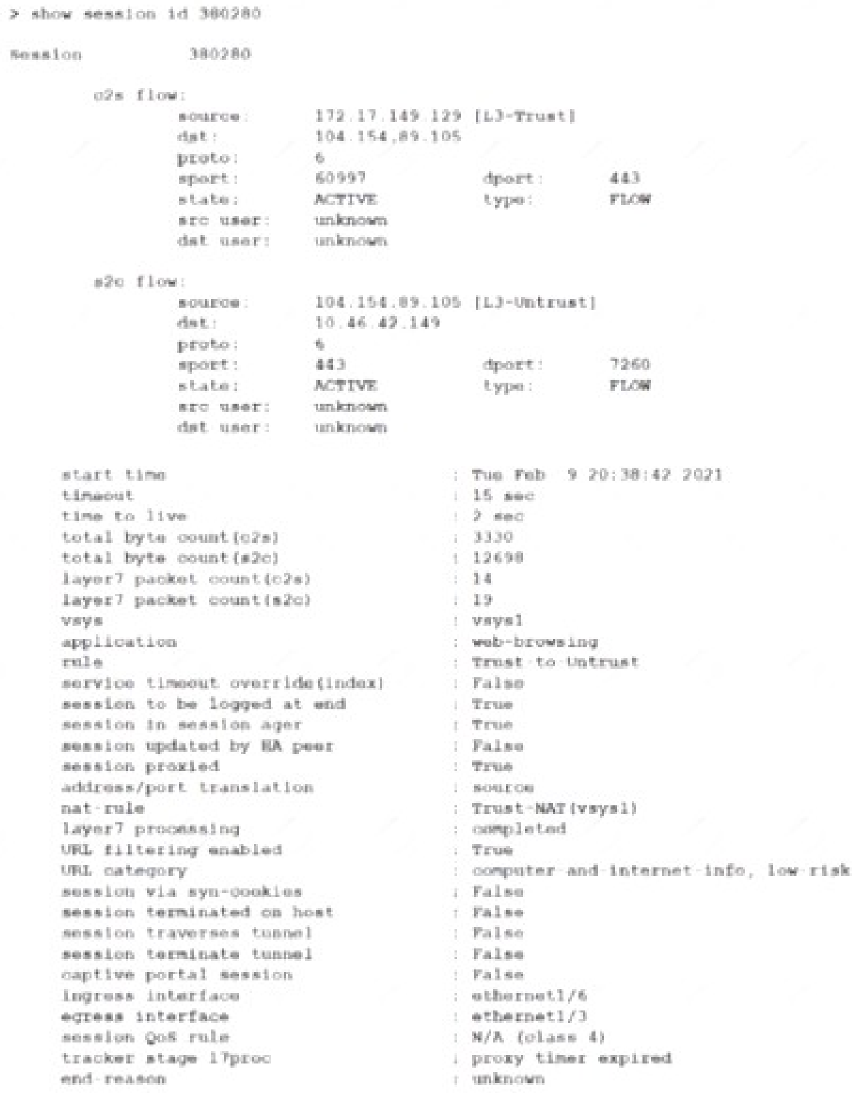
NEW QUESTION 109
What is the best description of the Cluster Synchronization Timeout (min)?

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 111
Which two statements correctly describe Session 380280? (Choose two.)



```
> show session id 380280

Session           380280

        c2s flow:
                source:      172.17.149.129 [L3-Trust]
                dst:         104.154,89.105
                proto:       6
                sport:       60997          dport:       443
                state:       ACTIVE         type:        FLOW
                src user:    unknown
                dst user:    unknown

        s2c flow:
                source:      104.154.89.105 [L3-Untrust]
                dst:         10.46.42.149
                proto:       6
                sport:       443            dport:       7260
                state:       ACTIVE         type:        FLOW
                src user:    unknown
                dst user:    unknown

     start time                           : Tue Feb  9 20:38:42 2021
     timeout                              : 15 sec
     time to live                         : 2 sec
     total byte count(c2s)                : 3330
     total byte count(s2c)                : 12698
     layer7 packet count(c2s)             : 14
     layer7 packet count(s2c)             : 19
     vsys                                 : vsys1
     application                          : web-browsing
     rule                                 : Trust-to-Untrust
     service timeout override(index)      : False
     session to be logged at end          : True
     session in session ager              : True
     session updated by HA peer           : False
     session proxied                      : True
     address/port translation             : source
     nat-rule                             : Trust-NAT(vsys1)
     layer7 processing                    : completed
     URL filtering enabled                : True
     URL category                         : computer-and-internet-info, low-risk
     session via syn-cookies              : False
     session terminated on host           : False
     session traverses tunnel             : False
     session terminate tunnel             : False
     captive portal session               : False
     ingress interface                    : ethernet1/6
     egress interface                     : ethernet1/3
     session QoS rule                     : N/A (class 4)
     tracker stage l7proc                 : proxy timer expired
     end-reason                           : unknown
```

A. The session went through SSL decryption processing.
B. The session has ended with the end-reason unknown.
C. The application has been identified as web-browsing.
D. The session did not go through SSL decryption processing.

Answer: AC

NEW QUESTION 113
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

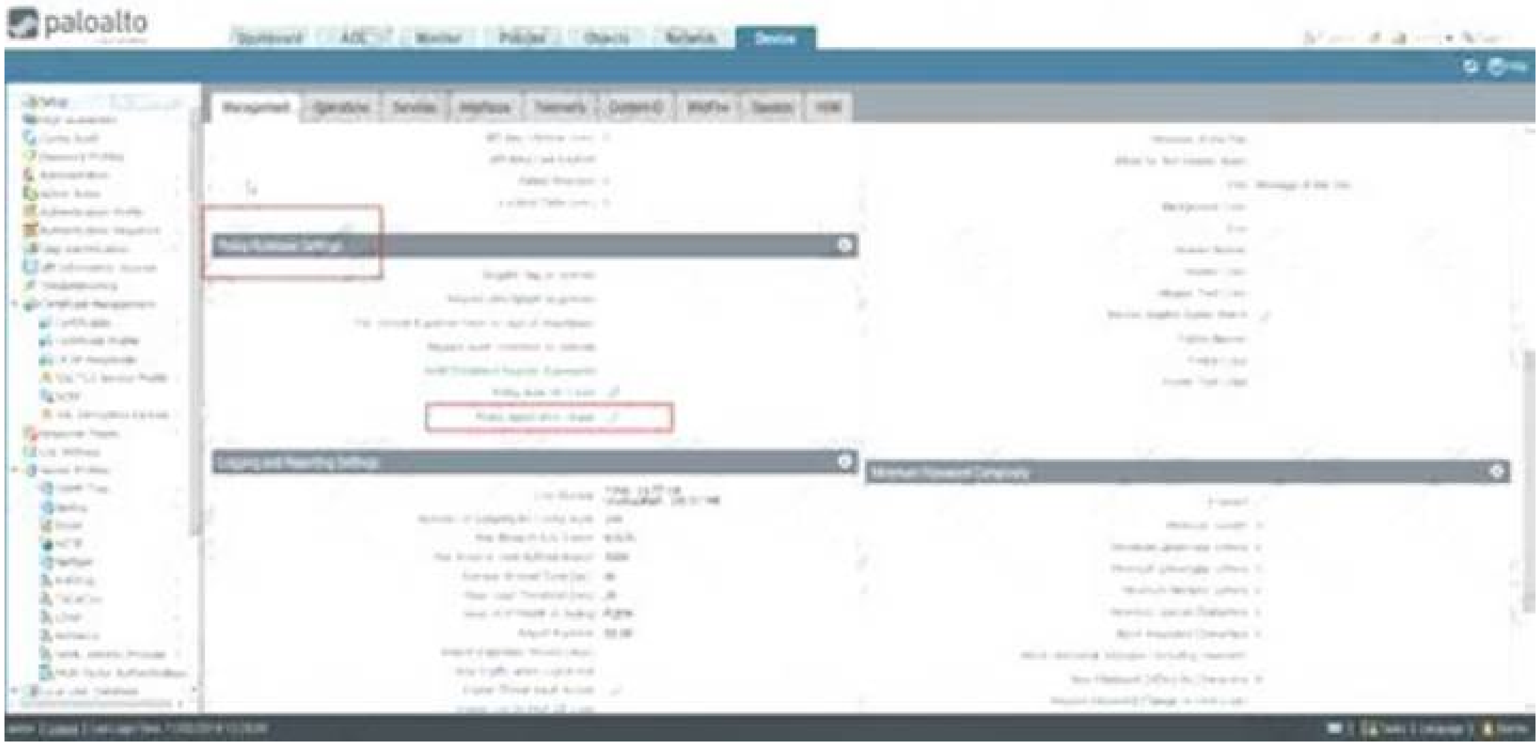
updated before or after upgrading Panorama, depending on the plugin compatibility matrix2. If the plugins are not updated accordingly, the upgrade process may fail or cause issues with Panorama
functionality3. References: Panorama Plugins Upgrade/Downgrade Considerations, Troubleshoot Your Panorama Upgrade, PCNSE Study Guide (page 54)

NEW QUESTION 118
In the New App Viewer under Policy Optimizer, what does the compare option for a specific rule allow an administrator to compare?

A. The running configuration with the candidate configuration of the firewall
B. Applications configured in the rule with applications seen from traffic matching the same rule
C. Applications configured in the rule with their dependencies
D. The security rule with any other security rule selected

Answer: B

Explanation:
The compare option for a specific rule in the New App Viewer under Policy Optimizer allows an administrator to compare the applications configured in the rule with the applications seen from traffic matching the same rule. This helps the administrator to identify any new applications that are not explicitly defined in the rule, but are implicitly allowed by the firewall based on the dependencies of the configured applications. The compare option also shows the usage statistics and risk levels of the applications, and provides suggestions for optimizing the rule by adding, removing, or replacing applications12. References: New App Viewer (Policy Optimizer), PCNSE Study Guide (page 47)
Why use Security Policy Optimizer and what are the benefits?



NEW QUESTION 122
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

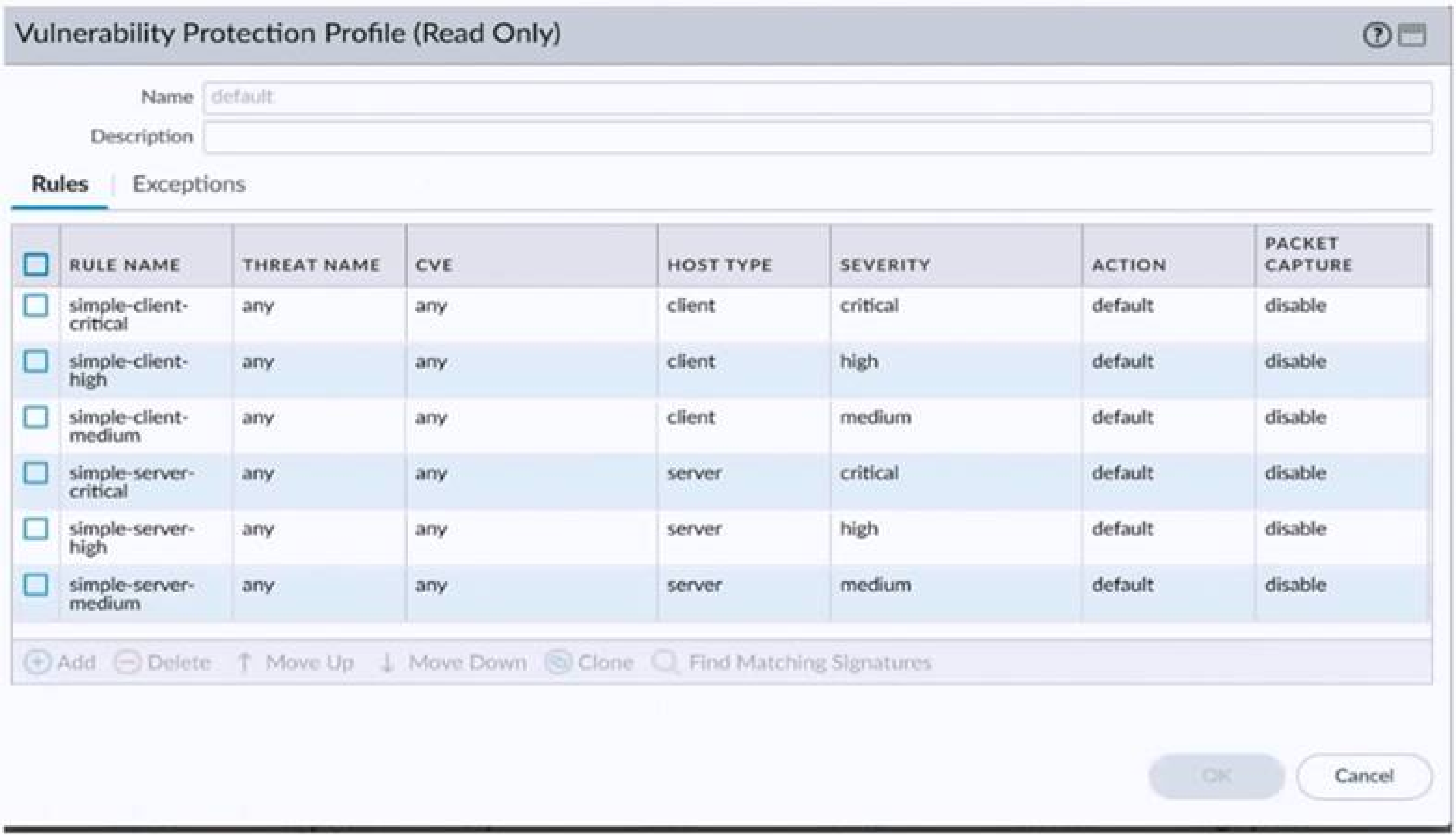
NEW QUESTION 124
An administrator troubleshoots an issue that causes packet drops.
Which log type will help the engineer verify whether packet buffer protection was activated?

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

Answer: C

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

NEW QUESTION 127
An administrator would like to determine which action the firewall will take for a specific CVE. Given the screenshot below, where should the administrator navigate to view this information?



Vulnerability Protection Profile (Read Only)

Name: default

Description:

Rules | Exceptions

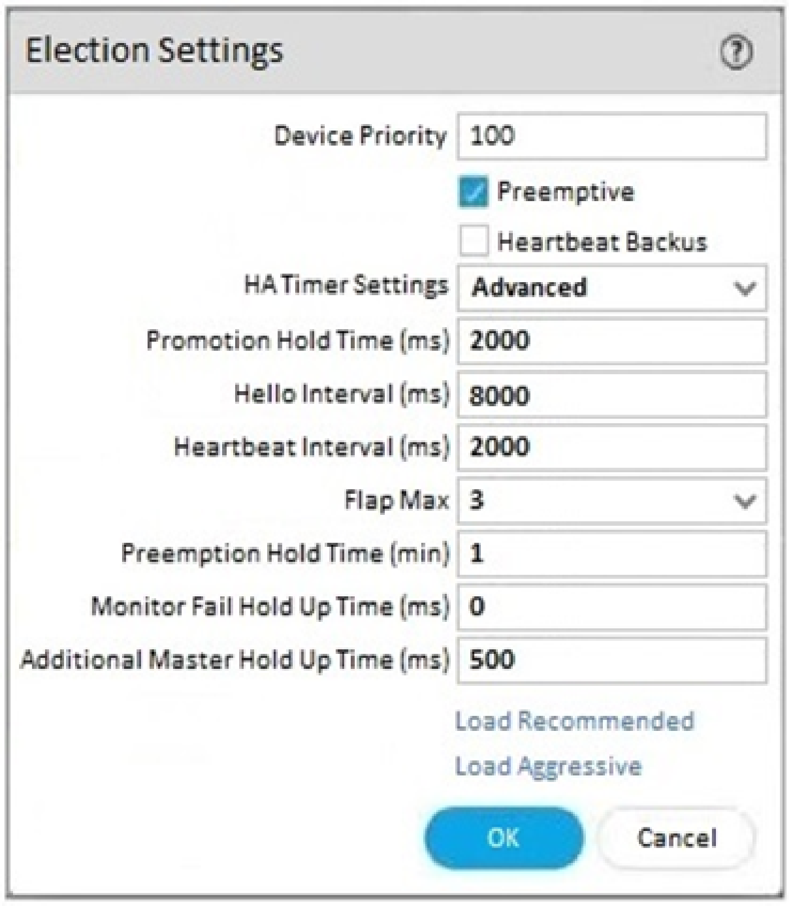
☐	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
☐	simple-client-critical	any	any	client	critical	default	disable
☐	simple-client-high	any	any	client	high	default	disable
☐	simple-client-medium	any	any	client	medium	default	disable
☐	simple-server-critical	any	any	server	critical	default	disable
☐	simple-server-high	any	any	server	high	default	disable
☐	simple-server-medium	any	any	server	medium	default	disable

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

Answer: C

Explanation:
The Exceptions settings allows you to change the response to a specific signature. For example, you can block all packets that match a signature, except for the selected one, which generates an alert. The Exception tab supports filtering functions.
If you not believed, then login the firewall go to Vulnerability > Exceptions and select "Show all signatures". From there you will see all threat information including specific actions.
More detail: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm4yCAC

NEW QUESTION 132
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

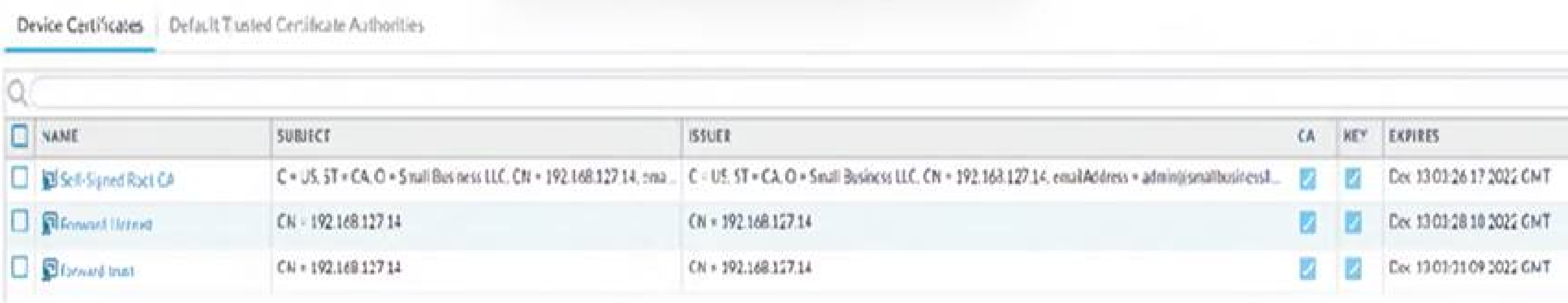
NEW QUESTION 133
Which DoS Protection Profile detects and prevents session exhaustion attacks against specific destinations?

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 136
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@smallbusinessll...	☑	☑	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 140
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 141
......

Relate Links

100% Pass Your PCNSE Exam with Exambible Prep Materials

https://www.exambible.com/PCNSE-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/