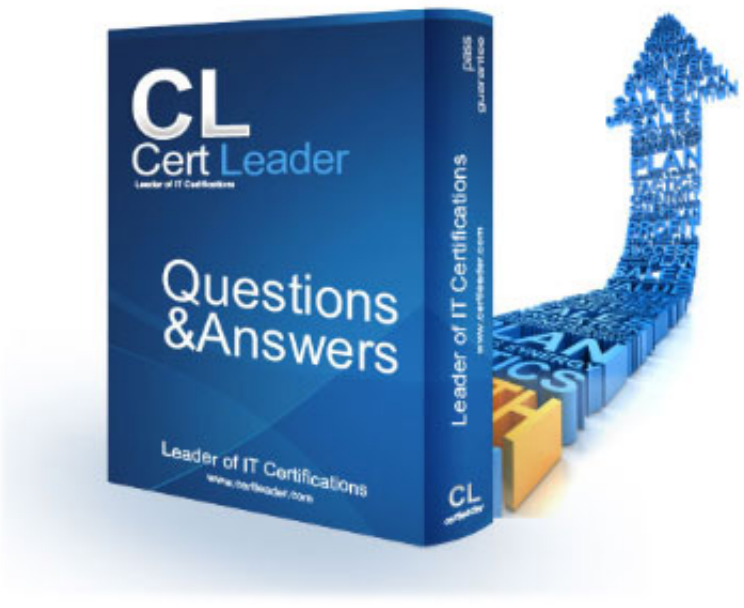
PCNSE Dumps

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

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



NEW QUESTION 1
A firewall engineer creates a NAT rule to translate IP address 1.1.1.10 to 192.168.1.10. The engineer also plans to enable DNS rewrite so that the firewall rewrites the IPv4 address in a DNS response based on the original destination IP address and translated destination IP address configured for the rule. The engineer wants the firewall to rewrite a DNS response of 1.1.1.10 to 192.168.1.10.
What should the engineer do to complete the configuration?

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

Answer: B

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

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

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

Answer: B

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

NEW QUESTION 4
An engineer troubleshoots a high availability (HA) link that is unreliable. Where can the engineer view what time the interface went down?

A. Monitor > Logs > System
B. Device > High Availability > Active/Passive Settings
C. Monitor > Logs > Traffic
D. Dashboard > Widgets > High Availability

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oNlUCAU&lang=en_US

NEW QUESTION 5
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)

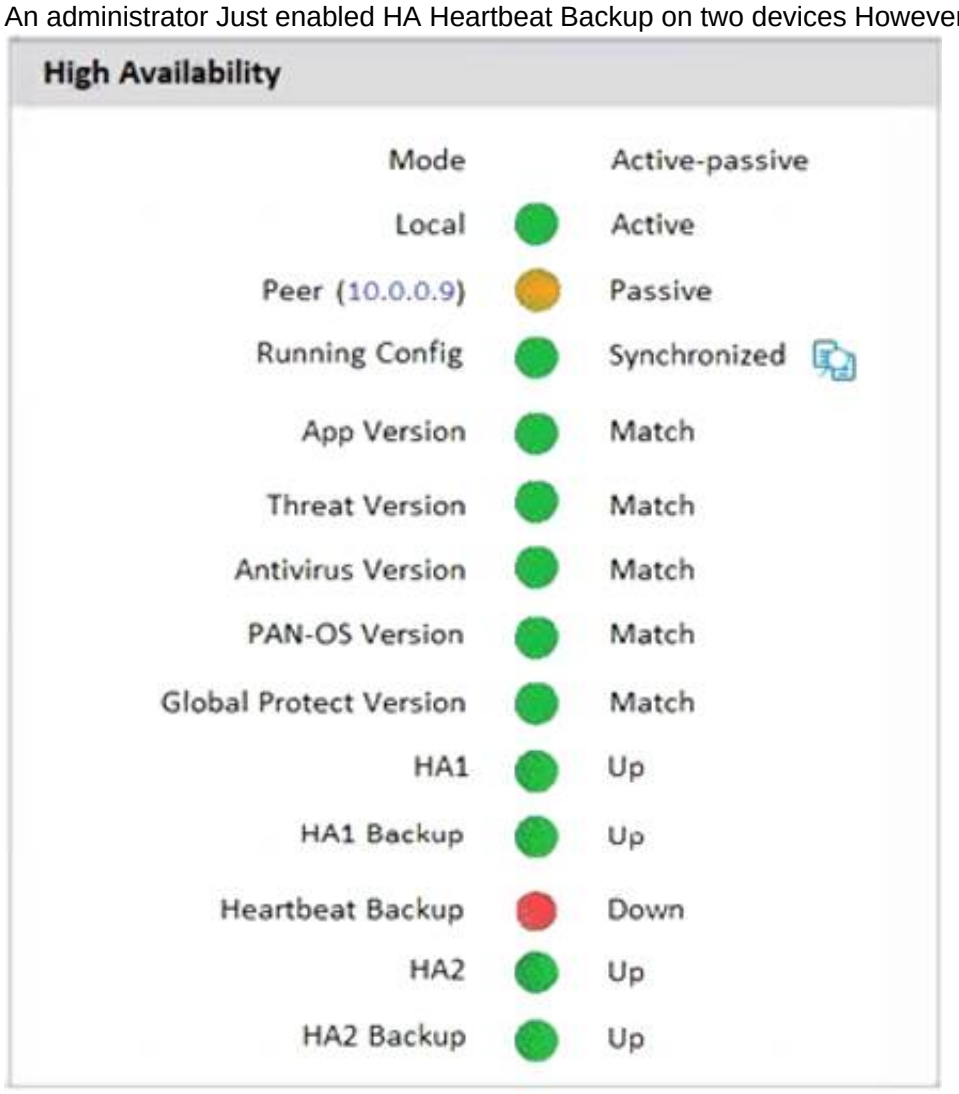
NEW QUESTION 6
In a security-first network, what is the recommended threshold value for apps and threats to be dynamically updated?

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 7
An administrator Just enabled HA Heartbeat Backup on two devices However, the status on tie firewall's dashboard is showing as down High Availability.



What could an administrator do to troubleshoot the issue?

A. 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 8
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 9
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 10
An engineer is configuring a firewall with three interfaces:
• MGT connects to a switch with internet access.
• Ethernet1/1 connects to an edge router.
• Ethernet1/2 connects to a visualization network.
The engineer needs to configure dynamic updates to use a dataplane interface for internet traffic. What should be configured in Setup > Services > Service Route Configuration to allow this traffic?

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

Answer: A

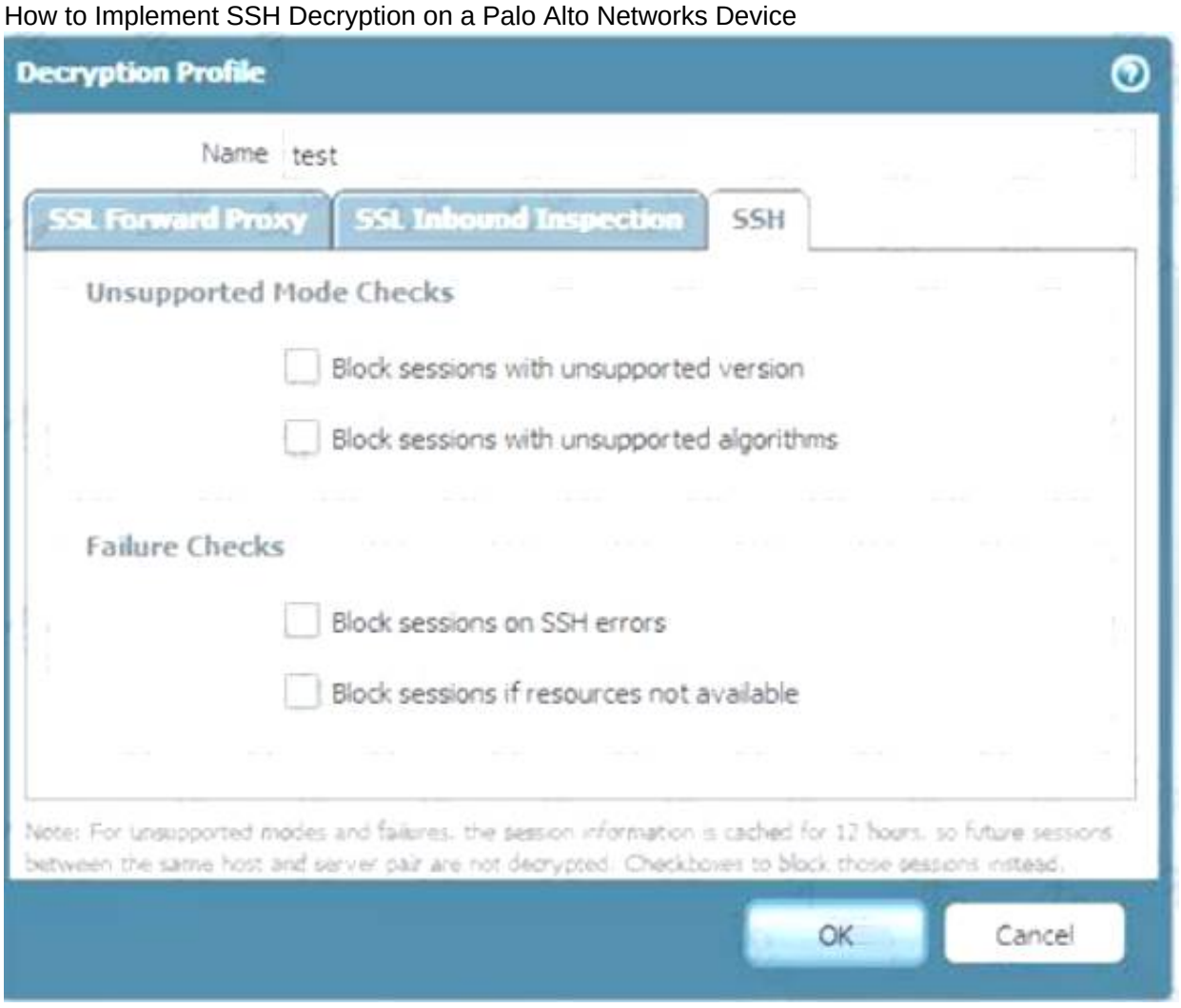
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGJCA0

NEW QUESTION 10
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



NEW QUESTION 13
A network security administrator has been tasked with deploying User-ID in their organization. What are three valid methods of collecting User-ID information in a network? (Choose three.)

A. Windows User-ID agent
B. GlobalProtect
C. XMLAPI
D. External dynamic list
E. Dynamic user groups

Answer: ABC

Explanation:
User-ID is a feature that allows the firewall to identify and classify users and groups on the network based on their usernames, IP addresses, and other attributes1. User-ID information can be collected from various sources, such as:

- A: Windows User-ID agent: A software agent that runs on a Windows server and collects user information from Active Directory domain controllers, Exchange servers, or eDirectory servers2. The agent then sends the user information to the firewall or Panorama for user mapping2.
- B: GlobalProtect: A software agent that runs on the endpoints and provides secure VPN access to the network3. GlobalProtect also collects user information from the endpoints and sends it to the firewall or Panorama for user mapping4.
- C: XMLAPI: An application programming interface that allows external systems or scripts to send user information to the firewall or Panorama in XML format. The XMLAPI can be used to integrate with third-party systems, such as identity providers, captive portals, or custom applications.

NEW QUESTION 16
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 21
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 26
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 29
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 32
If an administrator wants to apply QoS to traffic based on source, what must be specified in a QoS policy rule?

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

Answer: C

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

- QoS Policy
- Configure QoS

NEW QUESTION 37
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 38
Based on the graphic which statement accurately describes the output shown in the Server Monitoring panel?

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 43
An engineer manages a high availability network and requires fast failover of the routing protocols. The engineer decides to implement BFD.
Which three dynamic routing protocols support BFD? (Choose three.)

A. OSPF
B. RIP
C. BGP
D. IGRP
E. OSPFv3 virtual link

Answer: ABC

Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/bfd/bfd-overview/bfd-for-dynamic-ro

NEW QUESTION 48
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 51
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 53
After importing a pre-configured firewall configuration to Panorama, what step is required to ensure a commit/push is successful without duplicating local configurations?

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

Answer: C

Explanation:
https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/manage-firewalls/transition-a-firewall-to-pa Push the configuration bundle from Panorama to the newly added firewall to remove all policy rules and objects from its local configuration. This step is necessary to prevent duplicate rule or object names, which would cause commit errors when you push the device group configuration from Panorama to the firewall in the next step.

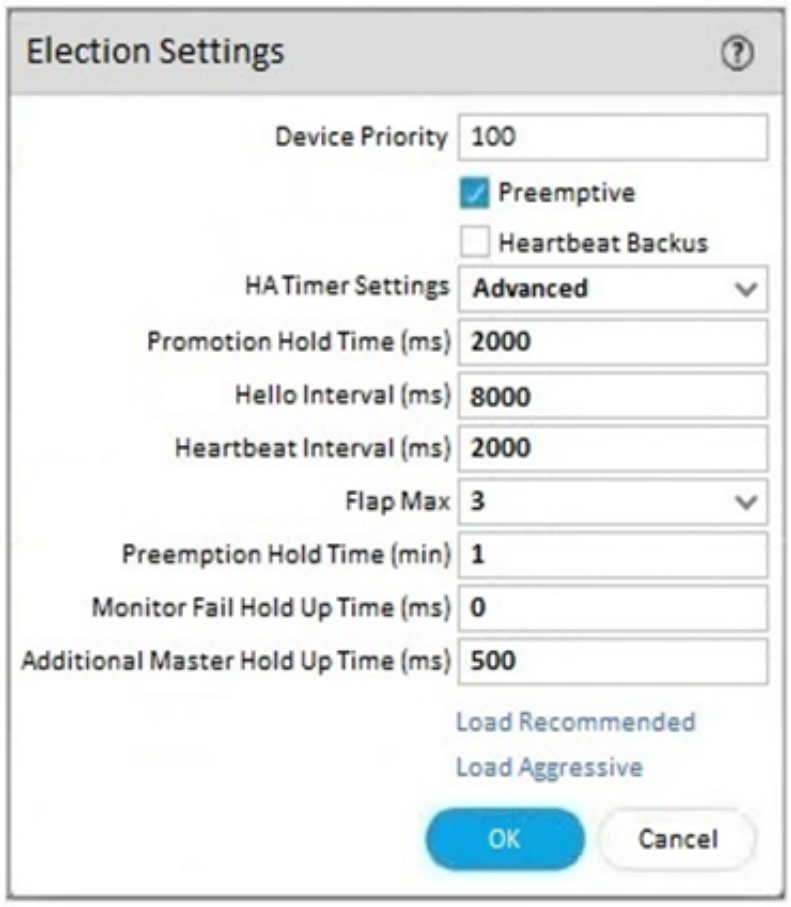
NEW QUESTION 57
The decision to upgrade PAN-OS has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when attempting the install.
When performing an upgrade on Panorama to PAN-OS. what is the potential cause of a failed install?

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 59
An engineer reviews high availability (HA) settings to understand a recent HA failover event. Review the screenshot below.



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 61
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PCNSE Exam with Our Prep Materials Via below:

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