

# Practice Exam Questions



## Palo Alto Networks Certified Network Security Engineer



**EXAMKILLER**

Help Pass Your Exam At First Try

# **Paloalto Networks**

## **Exam PCNSE**

**Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS  
10.2**

**Version: 36.1**

**[ Total Questions: 307 ]**

**Question No : 1**

A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg.txt. The firewall is currently running PAN-OS 10.0 and using a lab config. The contents of init-cfg.txt in the USB flash drive are as follows:

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsyst,jumbo-frame
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command: > request resort system. Upon restart, the firewall fails to begin the bootstrapping process. The failure is caused because

- A. Firewall must be in factory default state or have all private data deleted for bootstrapping
- B. The hostname is a required parameter, but it is missing in init-cfg.txt
- C. The USB must be formatted using the ext3 file system, FAT32 is not supported
- D. PANOS version must be 91.x at a minimum but the firewall is running 10.0.x
- E. The bootstrap.xml file is a required file but it is missing

**Answer: C**

**Explanation:** <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive.html#id8378007f-d6e5-4f2d-84a4-5d50b0b3ad7d>

### Question No : 2

Where is information about packet buffer protection logged?

- A. Alert entries are in the Alarms log. Entries for dropped traffic, discarded sessions, and blocked IP address are in the Threat log
- B. All entries are in the System log
- C. Alert entries are in the System log. Entries for dropped traffic, discarded sessions and blocked IP addresses are in the Threat log
- D. All entries are in the Alarms log

Answer: D

WHICH SYSTEM LOGS AND THREAT LOGS ARE GENERATED WHEN PACKET BUFFER PROTECTION

Created On 10/29/19 15:51 PM - Last Modified 04/27/20 22:13 PM

ZONE PROTECTION ZONE AND DOS PROTECTION 8.1 8.0 9.0 HARDWARE

**Question**  
Which system logs and threat logs are generated when packet buffer protection is enabled?

**Environment**

- PAN-OS 8.x
- PBP

**Answer**  
The firewall records alert events in the System log and events for dropped traffic, discarded sessions, and blocked IP address in the Threat log.

- System logs:  
Logs:  
Monitor>System  
Packet buffer congestion  
Severity: Informational
- Threat logs:

**Explanation:**

Graphical user interface, text, application

Description automatically generated

### Question No : 3

An engineer troubleshooting a VPN issue needs to manually initiate a VPN tunnel from the CLI.

Which CLI command can the engineer use?

- A. test vpn flow
- B. test vpn lke—sa
- C. test vpn tunnel
- D. test vpn gateway

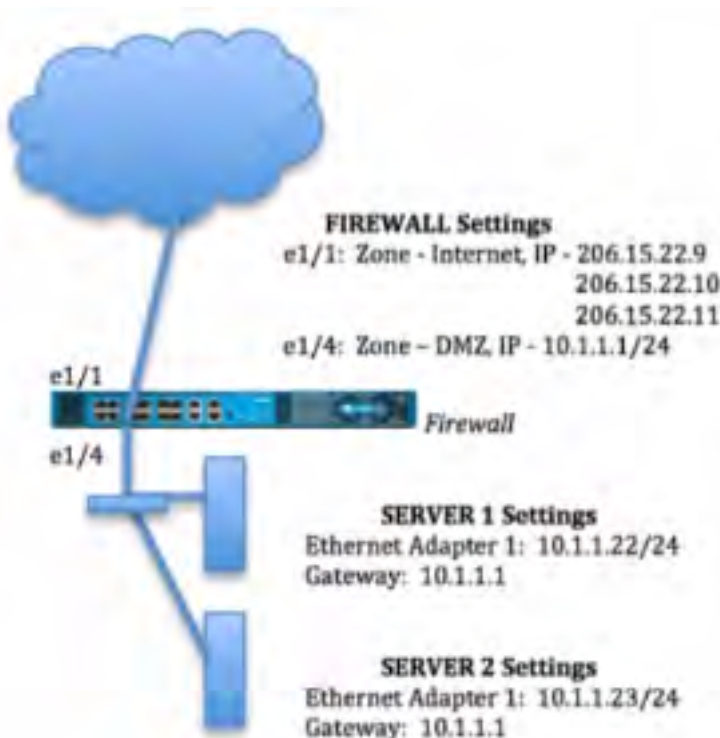
**Answer: D**

**Explanation:** The engineer can use the test vpn gateway CLI command to manually initiate a VPN tunnel from the CLI. This command allows the engineer to specify the name of the VPN gateway and the IP address of the peer to initiate an IKE negotiation and establish a VPN tunnel. Option A is incorrect because test vpn flow is not a valid CLI command. Option B is incorrect because test vpn ike-sa is a CLI command that displays information about the IKE security associations, not initiates a VPN tunnel. Option C is incorrect because test vpn tunnel is a CLI command that displays information about the IPSec security associations, not initiates a VPN tunnel.

**Question No : 4**

An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22.

Based on the image, which NAT rule will forward web-browsing traffic correctly?



A)

Source IP: Any  
Destination IP: 206.15.22.9  
Source Zone: Internet  
Destination Zone: DMZ  
Destination Service: 80/TCP  
Action: Destination NAT  
Translated IP: 10.1.1.22  
Translated Port: 80/TCP

B)

Source IP: Any  
Destination IP: 206.15.22.9  
Source Zone: Internet  
Destination Zone Internet  
Destination Service: 80/TCP  
Action: Destination NAT  
Translated IP: 10.1.1.22  
Translated Port: None

C)

Source IP: Any  
Destination IP: 206.15.22.9  
Source Zone: Internet  
Destination Zone: DMZ  
Destination Service: 80/TCP  
Action: Destination NAT  
Translated IP: 10.2.2.23  
Translated Port: 53/UDP

D)

Source IP: Any  
Destination IP: 206.15.22.9  
Source Zone: Internet  
Destination Zone: DMZ  
Destination Service: 80/TCP  
Action: Destination NAT  
Translated IP: 10.1.1.22  
Translated Port: 80/TCP

- A. Option
- B. Option
- C. Option



D. Option

**Answer: B**

**Explanation:** <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping.html>

#### Question No : 5

A company is using wireless controllers to authenticate users. Which source should be used for User-ID mappings?

- A. Syslog
- B. XFF headers
- C. server monitoring
- D. client probing

**Answer: A**

**Explanation:** <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/user-id-overview>

#### Question No : 6

An engineer wants to configure aggregate interfaces to increase bandwidth and redundancy between the firewall and switch. Which statement is correct about the configuration of the interfaces assigned to an aggregate interface group?

- A. They can have a different bandwidth.
- B. They can have a different interface type such as Layer 3 or Layer 2.
- C. They can have a different interface type from an aggregate interface group.
- D. They can have different hardware media such as the ability to mix fiber optic and copper.

**Answer: D**

**Explanation:** <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/configure-an-aggregate-interface-group>

**Question No : 7**

The administrator for a small company has recently enabled decryption on their Palo Alto Networks firewall using a self-signed root certificate. They have also created a Forward Trust and Forward Untrust certificate and set them as such

The admin has not yet installed the root certificate onto client systems

What effect would this have on decryption functionality?

- A. Decryption will function and there will be no effect to end users
- B. Decryption will not function because self-signed root certificates are not supported
- C. Decryption will not function until the certificate is installed on client systems
- D. Decryption will function but users will see certificate warnings for each SSL site they visit

**Answer: D**

**Explanation:**

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEZCA0>

**Question No : 8**

An engineer is in the planning stages of deploying User-ID in a diverse directory services environment.

Which server OS platforms can be used for server monitoring with User-ID?

- A. Microsoft Terminal Server, Red Hat Linux, and Microsoft Active Directory
- B. Microsoft Active Directory, Red Hat Linux, and Microsoft Exchange
- C. Microsoft Exchange, Microsoft Active Directory, and Novell eDirectory
- D. Novell eDirectory, Microsoft Terminal Server, and Microsoft Active Directory

**Answer: B**

**Explanation:** <https://docs.paloaltonetworks.com/compatibility-matrix/user-id-agent/which-servers-can-the-user-id-agent-monitor>

**Question No : 9**

A company with already deployed Palo Alto firewalls has purchased their first Panorama server. The security team has already configured all firewalls with the Panorama IP address and added all the firewall serial numbers in Panorama. What are the next steps to



migrate configuration from the firewalls to Panorama?

- A. Use API calls to retrieve the configuration directly from the managed devices
- B. Export Named Configuration Snapshot on each firewall followed by Import Named Configuration Snapshot in Panorama
- C. import Device Configuration to Panorama followed by Export or Push Device Config Bundle
- D. Use the Firewall Migration plugin to retrieve the configuration directly from the managed devices

**Answer: C**

**Explanation:**

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CloRCAS>

#### Question No : 10

After configuring HA in Active/Passive mode on a pair of firewalls the administrator gets a failed commit with the following details.



What are two explanations for this type of issue? (Choose two)

- A. The peer IP is not included in the permit list on Management Interface Settings
- B. The Backup Peer HA1 IP Address was not configured when the commit was issued
- C. Either management or a data-plane interface is used as HA1-backup
- D. One of the firewalls has gone into the suspended state

**Answer: B,C**

**Explanation:** Cause The issue is seen when the HA1-backup is configured with either management (MGT) or an in-band interface. The "Backup Peer HA1 IP Address" is not configured :

[https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UmPCA&lang=en\\_US%E2%80%A9](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UmPCA&lang=en_US%E2%80%A9)

**Question No : 11**

An administrator has two pairs of firewalls within the same subnet. Both pairs of firewalls have been configured to use High Availability mode with Active/Passive. The ARP tables for upstream routes display the same MAC address being shared for some of these firewalls.

What can be configured on one pair of firewalls to modify the MAC addresses so they are no longer in conflict?

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

**Answer: B**

**Explanation:**

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCA>  
S

**change the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet. This will prevent the MAC addresses from conflicting and allow the firewalls to properly route traffic. You can also configure a floating IP between the firewall pairs if necessary.**

**Question No : 12**

A network administrator configured a site-to-site VPN tunnel where the peer device will act as initiator None of the peer addresses are known

What can the administrator configure to establish the VPN connection?

- A. Set up certificate authentication.
- B. Use the Dynamic IP address type.
- C. Enable Passive Mode
- D. Configure the peer address as an FQDN.

**Answer: B**

**Explanation:** According to the documentation, if the peer device has a dynamic IP address, the administrator can configure the peer address as an FQDN and use tunnel monitoring to establish the VPN connection. Tunnel monitoring is a feature that sends periodic ICMP pings to a specified destination IP address across the VPN tunnel and brings down the tunnel interface if the pings fail. This way, the firewall can detect when the peer device changes its IP address and re-establish the VPN connection. References: **1** IPSec VPN Tunnel with Peer Having Dynamic IP Address - Palo Alto Networks **2** Dual ISP VPN site to site Tunnel Failover with Tunnel Monitoring - Palo Alto Networks  
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIIGCA0>

**Question No : 13**

An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

- A. certificate revocation
- B. Content-ID
- C. App-ID
- D. port inspection

**Answer: C**

**Explanation:** QoS natively integrates with App-ID, which is a feature that identifies applications based on their unique characteristics and behaviors, regardless of port, protocol, encryption, or evasive tactics. By using App-ID, QoS can prioritize or limit traffic based on the application name, category, subcategory, technology, or risk level. Certificate revocation is a process of invalidating digital certificates that are no longer trusted or secure. Content-ID is a feature that scans content and data within allowed applications for threats and sensitive data. Port inspection is a method of identifying applications based on the TCP or UDP port numbers they use, which is not reliable or granular enough for QoS purposes. References:

- ✍ <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/quality-of-service/configure-qos>
- ✍ <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id>

**Question No : 14**

Which data flow describes redistribution of user mappings?

- A. User-ID agent to firewall
- B. firewall to firewall
- C. Domain Controller to User-ID agent
- D. User-ID agent to Panorama

**Answer: B**

**Explanation:** <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-firewalls-to-redistribute-user-mapping-information>

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps/firewall-deployment-for-user-id-redistribution.html#ide3661b46-4722-4936-bb9b-181679306809>

### Question No : 15



A firewall administrator wants to avoid overflowing the company syslog server with traffic logs.

What should the administrator do to prevent the forwarding of DNS traffic logs to syslog?

- A. Disable logging on security rules allowing DNS.
- B. Go to the Log Forwarding profile used to forward traffic logs to syslog. Then, under traffic logs match list, create a new filter with application not equal to DNS.
- C. Create a security rule to deny DNS traffic with the syslog server in the destination
- D. Go to the Log Forwarding profile used to forward traffic logs to syslog. Then, under traffic logs match list, create a new filter with application equal to DNS.

**Answer: B**

**Explanation:** A log forwarding profile defines which logs are forwarded to which destinations, such as syslog servers. By creating a filter with application not equal to DNS, the log forwarding profile will exclude DNS traffic logs from being forwarded to syslog. Disabling logging on security rules allowing DNS will prevent the firewall from generating any logs for DNS traffic, which may not be desirable. Creating a security rule to deny DNS traffic with the syslog server in the destination will block the communication between the firewall and the syslog server, which may affect other logs. Creating a filter with application equal to DNS will forward only DNS traffic logs to syslog, which is the opposite of what is required. References:

-  <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-forwarding>
-  <https://docs.paloaltonetworks.com/network-security/security-policy/objects/log-forwarding>

**Question No : 16**

Which CLI command displays the physical media that are connected to ethernet1/8?

- A. > show system state filter-pretty sys.si.p8.stats
- B. > show system state filter-pretty sys.sl.p8.phy
- C. > show interface ethernet1/8
- D. > show system state filter-pretty sys.sl.p8.med

**Answer: B**

**Explanation:** Example output:

```
> show system state filter-pretty sys.s1.p1.phy
```

```
sys.s1.p1.phy: {  
link-partner: { },  
media: CAT5,  
type: Ethernet,  
}
```

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CId3CAC>

**Question No : 17**

An internal system is not functioning. The firewall administrator has determined that the incorrect egress interface is being used. After looking at the configuration, the administrator believes that the firewall is not using a static route.

What are two reasons why the firewall might not use a static route? (Choose two.)

- A. no install on the route
- B. duplicate static route
- C. path monitoring on the static route
- D. disabling of the static route

**Answer: A,C**

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/static-routes/static-route-removal-based-on-path-monitoring.html>

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/static-routes/configure-a-static-route.html>

**Question No : 18**

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

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

**Answer: B,C**

**Explanation:** <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface.html>

**Question No : 19 DRAG DROP**

An engineer is troubleshooting traffic routing through the virtual router. The firewall uses multiple routing protocols, and the engineer is trying to determine routing priority Match the default Administrative Distances for each routing protocol.

Static	<div style="display: flex; align-items: center; justify-content: center;"> <div style="width: 10px; height: 10px; background-color: #ccc; margin-right: 5px;"></div> <div style="width: 10px; height: 10px; background-color: #ccc; margin-right: 5px;"></div> <div style="width: 10px; height: 10px; background-color: #ccc; margin-right: 5px;"></div> <div style="width: 10px; height: 10px; background-color: #ccc; margin-right: 5px;"></div> </div>		20
OSPF External			120
EBGP			10
RIP			110

**Answer:**

Static		Answer Area		EBGP	
Static				EBGP	20
OSPF External				RIP	120
EBGP				Static	10
RIP				OSPF External	110

### Explanation:

- ✍ Static
  - Range is 10-240; default is 10.
- ✍ OSPF Internal
  - Range is 10-240; default is 30.
- ✍ OSPF External
  - Range is 10-240; default is 110.
- ✍ IBGP
  - Range is 10-240; default is 200.
- ✍ EBGP
  - Range is 10-240; default is 20.
- ✍ RIP
  - Range is 10-240; default is 120.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/virtual-routers>

### Question No : 20

When configuring forward error correction (FEC) for PAN-OS SD-WAN, an administrator would turn on the feature inside which type of SD-WAN profile?

- A. Certificate profile
- B. Path Quality profile
- C. SD-WAN Interface profile
- D. Traffic Distribution profile

### Answer: C

**Explanation:** To enable forward error correction (FEC) for PAN-OS SD-WAN, you need to create an SD-WAN Interface Profile that specifies Eligible for Error Correction Profile interface selection and apply the profile to one or more interfaces. Then you need to create an Error Correction Profile to implement FEC or packet duplication. References:



<https://docs.paloaltonetworks.com/sd-wan/2-0/sd-wan-admin/configure-sd-wan/create-an-error-correction-profile>

**Question No : 21**

How can an administrator use the Panorama device-deployment option to update the apps and threat version of an HA pair of managed firewalls?

- A. Configure the firewall's assigned template to download the content updates.
- B. Choose the download and install action for both members of the HA pair in the Schedule object.
- C. Switch context to the firewalls to start the download and install process.
- D. Download the apps to the primary; no further action is required.

**Answer: B**

**Explanation:** <https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/use-case-configure-firewalls-using-panorama/set-up-your-centralized-configuration-and-policies/add-the-managed-firewalls-and-deploy-updates>

**Question No : 22**

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 logical router.
- C. In the WebUI, view the Runtime Stats in the virtual router.
- D. Look for configuration problems in Network > virtual router > OSPF

**Answer: A,C**

**Question No : 23**

What is a key step in implementing WildFire best practices?

- A. In a mission-critical network, increase the WildFire size limits to the maximum value.
- B. Configure the firewall to retrieve content updates every minute.
- C. In a security-first network, set the WildFire size limits to the minimum value.
- D. Ensure that a Threat Prevention subscription is active.

**Answer: D**

**Explanation:** In the WildFire best practices linked below, the first step is to "... make sure that you have an active Threat Prevention subscription. Together, WildFire® and Threat Prevention enable comprehensive threat detection and prevention."

<https://docs.paloaltonetworks.com/wildfire/10-1/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices.html>

**Question No : 24**



The image shows a screenshot of the 'Election Settings' dialog box in Palo Alto Networks firewalls. The dialog box has a title bar with a question mark icon. It contains several configuration fields and checkboxes. The 'Device Priority' is set to 100. There are two checkboxes: 'Preemptive' (checked) and 'Heartbeat Backup' (unchecked). The 'HA Timer Settings' dropdown is set to 'Advanced'. The 'Promotion Hold Time (ms)' is 2000, 'Hello Interval (ms)' is 8000, 'Heartbeat Interval (ms)' is 2000, 'Flap Max' is 3, 'Preemption Hold Time (min)' is 1, 'Monitor Fail Hold Up Time (ms)' is 0, and 'Additional Master Hold Up Time (ms)' is 500. At the bottom, there are two radio buttons: 'Load Recommended' (selected) and 'Load Aggressive'. At the very bottom are 'OK' and 'Cancel' buttons.

Setting	Value
Device Priority	100
Preemptive	<input checked="" type="checkbox"/>
Heartbeat Backup	<input type="checkbox"/>
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
Load Recommended	<input checked="" type="radio"/>
Load Aggressive	<input type="radio"/>

Which time determines how long the passive firewall will wait before taking over as the active firewall after losing communications with the HA peer?

- A. Heartbeat Interval
- B. Additional Master Hold Up Time
- C. Promotion Hold Time
- D. Monitor Fail Hold Up Time

**Answer: C**

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

### Question No : 25

How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

- A. Use the debug dataplane packet-diag set capture stage firewall file command.

- B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
- C. Use the debug dataplane packet-diag set capture stage management file command.
- D. Use the tcpdump command.

**Answer: D**

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta-p/62390>

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capture-on-the-management-interface.html>

#### Question No : 26

An engineer is pushing configuration from Panorama to a managed firewall.

What happens when the pushed Panorama configuration has Address Object names that duplicate the Address Objects already configured on the firewall?

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

**Answer: A**

**Explanation:** it fails the commit should the local FW has the same object as the Panorama. on this docs it say "shared" <https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/transition-a-firewall-to-panorama-management/plan-the-transition-to-panorama-management>

#### Question No : 27

What happens when an A/P firewall cluster synchronizes IPsec tunnel security associations (SAs)?

- A. Phase 1 and Phase 2 SAs are synchronized over HA3 links.

- B. Phase 1 SAs are synchronized over HA1 links.
- C. Phase 2 SAs are synchronized over HA2 links.
- D. Phase 1 and Phase 2 SAs are synchronized over HA2 links.

**Answer: C**

**Explanation:** From the Palo Alto documentation below, "when a VPN is terminated on a Palo Alto firewall HA pair, not all IPSEC related information is synchronized between the firewalls... This is an expected behavior. IKE phase 1 SA information is NOT synchronized between the HA firewalls."

And from the second link, "Data link (HA2) is used to sync sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in the HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive). It flows from the active firewall to the passive firewall."

[https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=en\\_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=en_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail)

<https://help.aryaka.com/display/public/KNOW/Palo+Alto+Networks+NFV+Technical+Brief>

#### Question No : 28

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: B,D**

**Explanation:** When deploying SSL Forward Proxy decryption, a forward trust certificate must have a subject alternative name (SAN) and be a server certificate. SAN is an extension to the X.509 standard that allows multiple domain names to be protected by a single SSL/TLS certificate. It is used to identify the domain names or IP addresses that the certificate should be valid for. A private key is also required but it is not mentioned in the options. A certificate authority (CA) certificate is not required as the forward trust certificate