Free Questions for PCNSE by certscare

Shared by Doyle on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

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

Options:

A- Set the passive link state to shutdown'.

B- Disable config sync.

C- Disable the HA2 link.

D- Disable HA.

Answer:

B

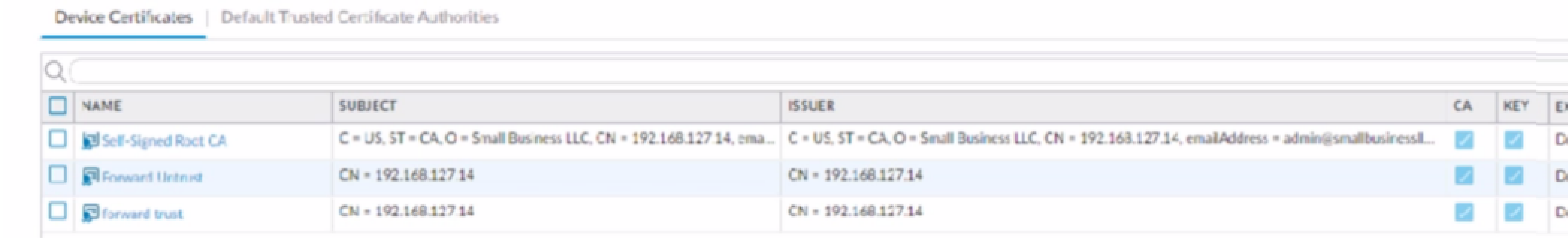
Explanation:

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.Reference:Migrate a Firewall HA Pair to Panorama Management, PCNSE Study Guide (page 50)

Question 2

Question Type: MultipleChoice

Review the screenshot of the Certificates page.



Device Certificates | Default Trusted Certificate Authorities

□	NAME	SUBJECT	ISSUER	CA	KEY	E
□	Self-Signed Root CA	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.14, ema...	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.14, emailAddress = admin@smallbusinessl...	☑	☑	D
□	Forward Untrust	CN = 192.168.127.14	CN = 192.168.127.14	☑	☑	D
□	forward trust	CN = 192.168.127.14	CN = 192.168.127.14	☑	☑	D

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?

Options:

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.Reference:Keys and Certificates for Decryption Policies,How to Configure SSL Decryption

Question 3

Question Type: **MultipleChoice**

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?

Options:

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.Reference:Configure a Syslog Listener for User Mapping,User-ID Agent Deployment Guide, PCNSE Study Guide (page 48)

Question 4

Question Type: MultipleChoice

An engineer is monitoring an active/active high availability (HA) firewall pair.

Which HA firewall state describes the firewall that is currently processing traffic?

Options:

A- Initial

B- Passive

C- Active

D- Active-primary

Answer:

C

Explanation:

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

Question 5

Question Type: MultipleChoice

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.)

Options:

A- Log Forwarding profile

B- SSL decryption exclusion

C- Email scheduler

D- Login banner

E- Dynamic updates

Answer:

B, D, E

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.Reference:Manage Templates and Template Stacks, PCNSE Study Guide (page 50)

Question 6

Question Type: MultipleChoice

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?

Options:

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.Reference:Panorama Plugins Upgrade/Downgrade Considerations,Troubleshoot Your Panorama Upgrade, PCNSE Study Guide (page 54)

Question 7

Question Type: MultipleChoice

What must be configured to apply tags automatically based on User-ID logs?

Options:

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.Reference:Use Auto-Tagging to Automate Security Actions, PCNSE Study Guide (page 49)

Question 8

Question Type: **MultipleChoice**

You are auditing the work of a co-worker and need to verify that they have matched the Palo Alto Networks Best Practices for Anti-Spyware Profiles.

For which three severity levels should single-packet captures be enabled to meet the Best Practice standard? (Choose three.)

Options:

A- Low

B- High

C- Critical

D- Informational

E- Medium

Answer:

B, C, E

Explanation:

https://docs.paloaltonetworks.com/best-practices/10-2/data-center-best-practices/data-center-best-practice-security-policy/how-to-create-data-center-best-practice-security-profiles/create-the-data-center-best-practice-anti-spyware-profile

The Palo Alto Networks Best Practices for Anti-Spyware Profiles recommend enabling single-packet captures (PCAP) for medium, high, and critical severity threats. This allows for capturing the first packet of the malicious traffic for further analysis and investigation.PCAP should not be enabled for low and informational severity threats, as they generate a relatively high volume of traffic and are not particularly useful compared to potential threats2.Reference:Create the Data Center Best Practice Anti-Spyware Profile,Security Profile: Anti-Spyware, PCNSE Study Guide (page 57)

Question 9

Question Type: MultipleChoice

An engineer is designing a deployment of multi-vsys firewalls.

What must be taken into consideration when designing the device group structure?

Options:

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.Reference:Device Group Push to a Multi-VSYS Firewall,Configure Virtual Systems, PCNSE Study Guide (page 50)

Question 10

Question Type: **MultipleChoice**

An engineer is monitoring an active/active high availability (HA) firewall pair.

Which HA firewall state describes the firewall that is experiencing a failure of a monitored path?

Options:

A- Initial

B- Tentative

C- Passive

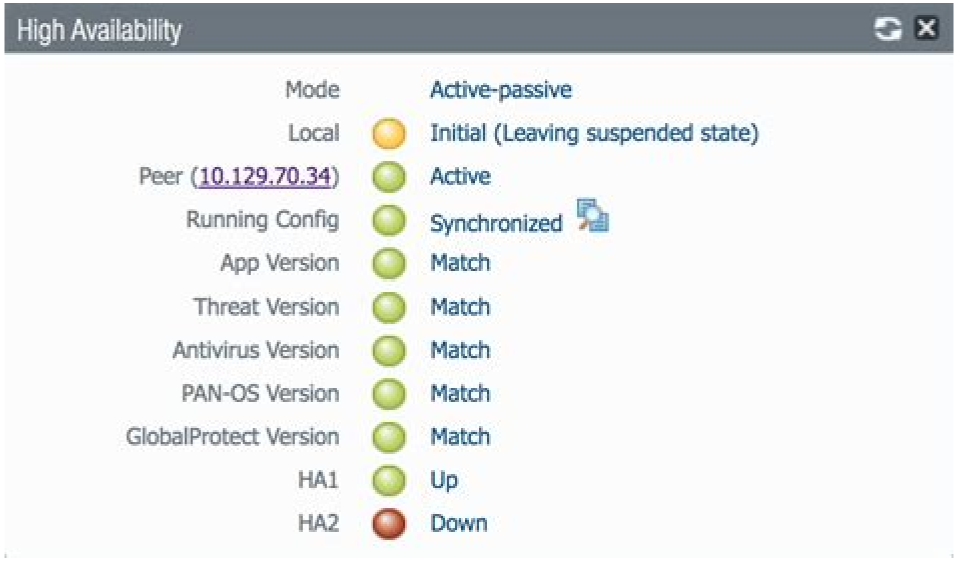
D- Active-secondary

Answer:

B

Explanation:

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



High Availability

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

20%
DISCOUNT