Free Questions for PCNSE

Shared by Sutton on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

During the process of developing a decryption strategy and evaluating which websites are required for corporate users to access, several sites have been identified that cannot be decrypted due to technical reasons. In this case, the technical reason is unsupported ciphers Traffic to these sites will therefore be blocked if decrypted.

How should the engineer proceed?

Options:

A- Install the unsupported cipher into the firewall to allow the sites to be decrypted
B- Allow the firewall to block the sites to improve the security posture.
C- Add the sites to the SSL Decryption Exclusion list to exempt them from decryption.
D- Create a Security policy to allow access to those sites.

Answer:

C

Explanation:

If some sites cannot be decrypted due to technical reasons, such as unsupported ciphers, and blocking them is not an option, then the engineer should add the sites to the SSL Decryption Exclusion list to exempt them from decryption. The SSL Decryption Exclusion list is a predefined list of sites that are not subject to SSL decryption by the firewall. The list includes sites that use certificate pinning, mutual authentication, or unsupported cipher suites.The engineer can also add custom sites to the list if they have a valid business reason or technical limitation for not decrypting them34. Adding the sites to the SSL Decryption Exclusion list will allow the traffic to pass through without being decrypted or blocked by the firewall.Reference:SSL Decryption Exclusion,Troubleshoot Unsupported Cipher Suites

Question 2

Question Type: MultipleChoice

A root cause analysis investigation into a recent security incident reveals that several decryption rules have been disabled. The security team wants to generate email alerts when decryption rules are changed.

How should email log forwarding be configured to achieve this goal?

Options:

A- With the relevant configuration log filter inside Device > Log Settings
B- With the relevant system log filter inside Objects > Log Forwarding
C- With the relevant system log filter inside Device > Log Settings
D- With the relevant configuration log filter inside Objects > Log Forwarding

Answer:

C

Explanation:

To generate email alerts when decryption rules are changed in a Palo Alto Networks firewall, you would configure email log forwarding based on specific system logs that capture changes to decryption policies. This is done by setting up log forwarding profiles with filters that match events related to decryption rule modifications. These profiles are then applied to the relevant log types within the firewall's log settings.

To specifically monitor for changes to decryption rules, you would navigate to the Device > Log Settings section of the firewall's web interface. Here, you can configure log forwarding for system logs, which capture configuration changes among other system-level events. By creating a filter that looks for logs associated with decryption rule changes, and associating this filter with an email server profile, the firewall can automatically send out email alerts whenever a decryption rule is modified.

This setup ensures that the security team is promptly notified of any changes to the decryption policies, allowing for quick review and action if the changes were unauthorized or unintended. It is an essential part of maintaining the security posture of the network and ensuring compliance with organizational policies on encrypted traffic inspection.

Question 3

Question Type: MultipleChoice

Where is Palo Alto Networks Device Telemetry data stored on a firewall with a device certificate installed?

Options:

A- On Palo Alto Networks Update Servers
B- M600 Log Collectors
C- Cortex Data Lake
D- Panorama

Answer:

C

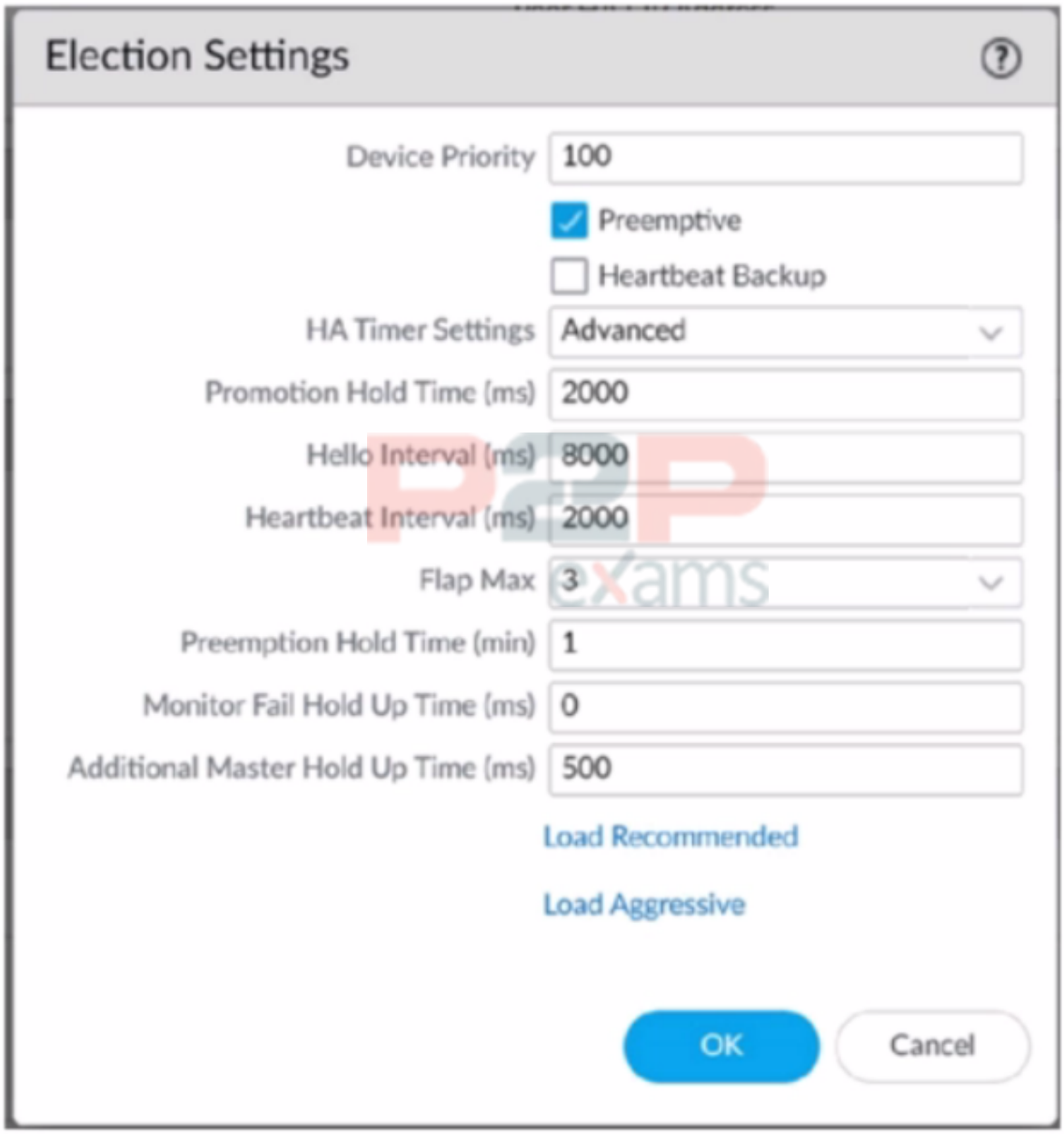
Explanation:

Palo Alto Networks Device Telemetry data, collected from firewalls with a device certificate installed, is stored on Palo Alto Networks Update Servers. This telemetry data includes information about threats, device health, and other operational metrics that are crucial for the continuous improvement of security services and threat intelligence. The collected data is anonymized and securely transmitted to Palo Alto Networks, where it is used to enhance the overall effectiveness of threat identification and prevention capabilities across all deployed devices. This collaborative approach helps in keeping the security ecosystem updated and resilient against emerging threats.

Question 4

Question Type: MultipleChoice

An engineer is reviewing the following high availability (HA) settings to understand a recent HAfailover event.



Which timer determines the frequency between packets sent to verify that the HA functionality on the other HA firewall is operational?

Options:

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.Reference:HA Timers,Layer 3 High Availability with Optimal Failover Times Best Practices

Question 5

Question Type: MultipleChoice

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

Options:

A- ECDSA
B- ECDHE
C- RSA
D- DHE

Answer:

B, D

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.Reference:Key Exchange Algorithms,Best Practices for Enabling SSL Decryption, PCNSE Study Guide (page 60)

Question 6

Question Type: MultipleChoice

An administrator is required to create an application-based Security policy rule to allow Evernote. The Evernote application implicitly uses SSL and web browsing.

What is the minimum the administrator needs to configure in the Security rule to allow only Evernote?

Options:

A- Add the Evernote application to the Security policy rule, then add a second Security policy rule containing both HTTP and SSL.
B- Create an Application Override using TCP ports 443 and 80.
C- Add the HTTP. SSL. and Evernote applications to the same Security policy.
D- Add only the Evernote application to the Security policy rule.

Answer:

D

Explanation:

https://live.paloaltonetworks.com/t5/blogs/what-is-application-dependency/ba-p/344330

To create an application-based Security policy rule to allow Evernote, the administrator only needs to add the Evernote application to the Security policy rule. The Evernote application is a predefined App-ID that identifies the traffic generated by the Evernote client or web interface. The Evernote application implicitly uses SSL and web browsing as dependencies, which means that the firewall automatically allows these applications when the Evernote application is allowed. Therefore, there is no need to add HTTP, SSL, or web browsing applications to the same Security policy rule.Adding these applications would broaden the scope of the rule and potentially allow unwanted traffic12.Reference:App-ID Overview,Create a Security Policy Rule