Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **NetSec Analyst**

Title : Palo Alto Networks Network Security Analyst

Version : DEMO

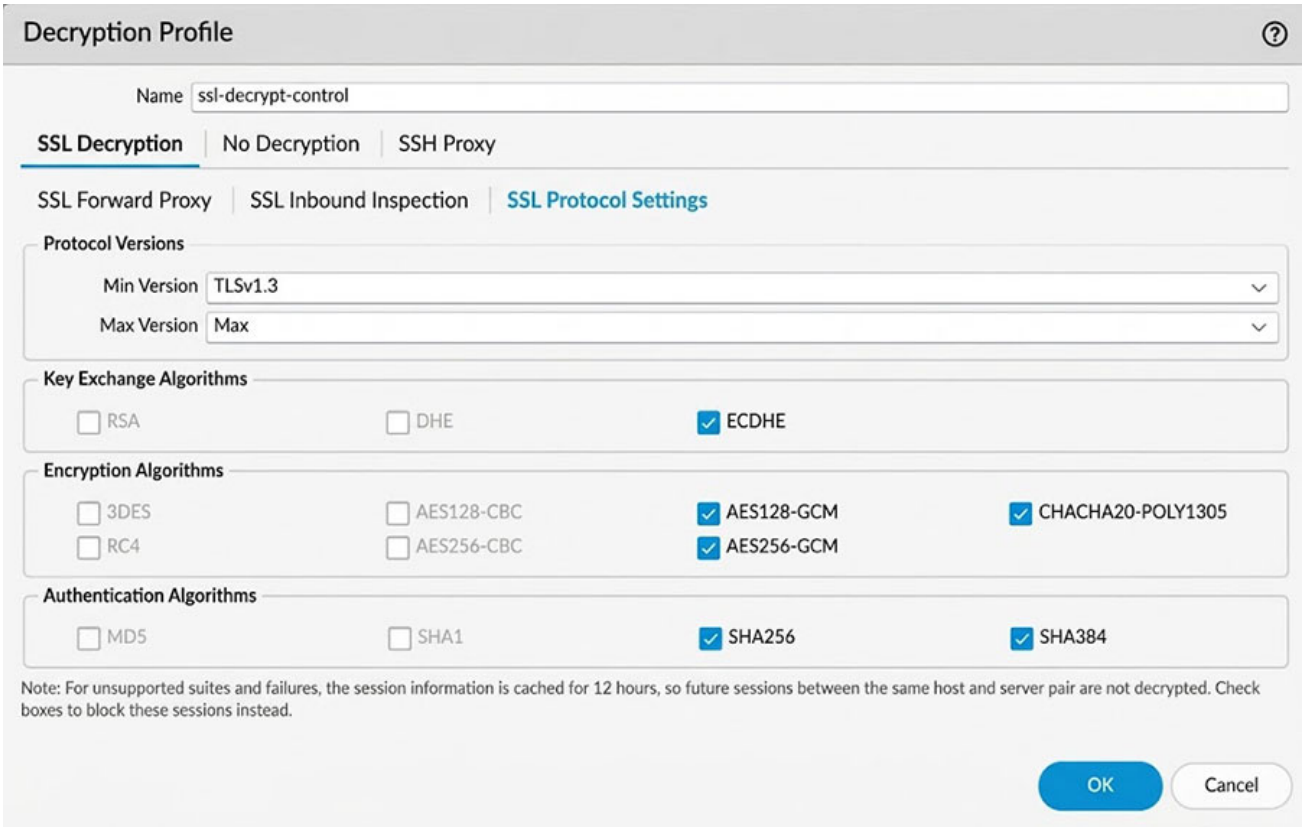
1.A security administrator is creating an internet of things (IoT) Security policy and needs to select behaviors for the traffic.

Characteristic
Evasive
Excessive Bandwidth Use
Used by Malware
Capable of File Transfer
Known Vulnerabilities
Tunnels Other Apps
Prone to Misuse
Pervasive

Which characteristic has the greatest effect on the risk level of applications?
A. Used by Malware
B. Pervasive
C. Tunnels Other Apps
D. Known Vulnerabilities
Answer: A
Explanation:
Traffic that is commonly used by malware directly increases the likelihood of compromise because attackers actively leverage it for command-and-control, data exfiltration, and lateral movement. This makes it an immediate and practical threat vector, giving it the highest impact on overall application risk compared to general prevalence or structural characteristics.

2.DNS rewrite can only be configured on a NAT rule with which type of destination address translation?
A. Dynamic IP and Port (DIPP)
B. Dynamic IP (with session distribution)
C. Static IP
D. Dynamic IP
Answer: C
Explanation:
DNS rewrite requires a one-to-one, predictable mapping between the original and translated destination address so the firewall can consistently modify DNS responses. Static IP translation provides this fixed mapping, enabling accurate DNS record rewriting for inbound traffic.

3.Based on the image below, what is a risk associated with this configuration?



A. Min Version setting of TLSvl 3 can cause compatibility issues with legacy applications or clients.
B. Authentication algorithm selections can significantly increase resource consumption and cause performance degradation.
C. Encryption algorithms 3DES and RC4 being disabled decreases security posture.
D. Max Version setting of "Max" enables the use of Perfect Forward Secrecy (PFS) and cannot be decrypted.

Answer: A

Explanation:

Setting the minimum TLS version to TLS 1.3 restricts connections to only the newest protocol, which many legacy clients, devices, or older applications may not support. This can prevent those systems from establishing secure sessions, creating compatibility and connectivity issues.

4.Which action ensures that sensitive information such as medical records, financial transactions, and legal communications are not decrypted and that they maintain strong security?

A. Create a log forwarding filter to exclude sensitive information.
B. Disable decryption globally to avoid exposing sensitive data.
C. Create an SSL Inbound Inspection policy to identify users sending sensitive information.
D. Create a no-decrypt policy for traffic matching specific URL categories.

Answer: D

Explanation:

A no-decrypt policy selectively exempts traffic that matches sensitive URL categories from SSL decryption, ensuring private data such as medical, financial, or legal communications remains encrypted end-to-end while still allowing decryption for other traffic, maintaining both privacy and overall security.

5.An alert indicates that multiple internal endpoints are communicating with a known malicious IP address, and the analyst needs to identify the scope of this activity by using Log Viewer.
What is the first step in identifying which internal hosts have communicated with the malicious IP address and determining the extent of the communication?
A. Filter the traffic logs by the known endpoint IP addresses.
B. Filter the traffic logs by the DNS Server's IP address.
C. Filter the traffic logs by the NGFWs IP addresses.
D. Filter the traffic logs by the malicious IP address.
Answer: D
Explanation:
Filtering the traffic logs by the malicious IP address immediately isolates all sessions involving that threat indicator, allowing the analyst to see every internal host that communicated with it and assess the full scope and extent of the activity.