CheckPoint 156-215.81 CCSA Practice Questions

Shared by Gregory on 24-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What are the software components used by Autonomous Threat Prevention Profiles in R8I.20 and higher?

Options:

A- Sandbox, ThreatCloud, Zero Phishing, Sanitization, C&C Protection, JPS, File and URL Reputation
B- IPS, Threat Emulation and Threat Extraction
C- Sandbox, ThreatCloud, Sanitization, C&C Protection, IPS
D- IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction

Answer:

D

Explanation:

This answer is correct because these are the software components that are used by the pre-defined Autonomous Threat Prevention Profiles in R81.20 and higher1.These profiles provide zero-maintenance protection from zero-day threats and continuously and autonomously ensure that your protection is up-to-date with the latest cyber threats and prevention technologies2.

The other answers are not correct because they either include software components that are not part of the Autonomous Threat Prevention Profiles, such as Sandbox, ThreatCloud, Zero Phishing, Sanitization, C&C Protection, JPS, File and URL Reputation, or they omit some of the software components that are part of the Autonomous Threat Prevention Profiles, such as Anti-Bot, Anti-Virus, and Macro Extraction.

Autonomous Threat Prevention Management - Check Point Software

Check Point Quantum R81.20 (Titan) Release

Threat Prevention R81.20 Best Practices - Check Point Software

Check Point R81

Question 2

Question Type: MultipleChoice

Fill in the blank: An identity server uses a_____to trust a Terminal Server Identity Agent.

Options:

A- One-time password
B- Shared secret
C- Certificate
D- Token

Answer:

B

Question 3

Question Type: MultipleChoice

When a gateway requires user information for authentication, what order does it query servers for user information?

Options:

A- First - Internal user database, then LDAP servers in order of priority, finally the generic external user profile
B- First the Internal user database, then generic external user profile, finally LDAP servers in order of priority.
C- First the highest priority LDAP server, then the internal user database, then lower priority LDAP servers, finally the generic external profile
D- The external generic profile, then the internal user database finally the LDAP servers in order of priority.

Answer:

B

Explanation:

When a gateway requires user information for authentication, it queries servers for user information in the following order: first the internal user database, then the generic external user profile, and finally LDAP servers in order of priority. The internal user database is a local

database that stores user information on the Security Gateway or Security Management Server. The generic external user profile is a predefined profile that allows users to authenticate with any external server that supports RADIUS or TACACS protocols. LDAP servers are external servers that use the Lightweight Directory Access Protocol to store and retrieve user information. The gateway queries LDAP servers according to the priority that is defined in the LDAP Account Unit object properties.

Question 4

Question Type: MultipleChoice

Log query results can be exported to what file format?

Options:

A- Word Document (docx)
B- Comma Separated Value (csv)
C- Portable Document Format (pdf)
D- Text (txt)

Answer:

B

Explanation:

Log query results can be exported to Comma Separated Value (csv) file format. CSV is a file format that stores tabular data in plain text. It is compatible with various applications, such as Excel, Google Sheets, etc. The other options are not valid file formats for exporting log query results.

Question 5

Question Type: MultipleChoice

When enabling tracking on a rule, what is the default option?

Options:

A- Accounting Log
B- Extended Log
C- Log
D- Detailed Log

Answer:

C

Explanation:

When enabling tracking on a rule, the default option is Log. This option generates a log entry for each connection that matches the rule. The log entry contains information such as the source, destination, service, action, and time of the connection. Reference: [Logging and Monitoring R81], [Logging and Monitoring]

Question 6

Question Type: MultipleChoice

Why is a Central License the preferred and recommended method of licensing?

Options:

A- Central Licensing is actually not supported with Gaia.
B- Central Licensing is the only option when deploying Gaia
C- Central Licensing ties to the IP address of a gateway and can be changed to any gateway if needed.
D- Central Licensing ties to the IP address of the management server and is not dependent on the IP of any gateway in the event it changes.

Answer:

D

Explanation:

Central License is the preferred and recommended method of licensing because it ties to the IP address of the management server and is not dependent on the IP of any gateway in the event it

changes. Central License allows administrators to manage licenses for all Security Gateways from one central location. If the IP address of a gateway changes, the license remains valid as long as it is connected to the same management server. Central Licensing is supported with Gaia and is not the only option when deploying Gaia. Central Licensing does not tie to the IP address of a gateway and can not be changed to any gateway if needed.

Question 7

Question Type: MultipleChoice

What are the Threat Prevention software components available on the Check Point Security Gateway?

Options:

A- IPS, Threat Emulation and Threat Extraction
B- IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction
C- IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction
D- IDS, Forensics, Anti-Virus, Sandboxing

Answer:

C

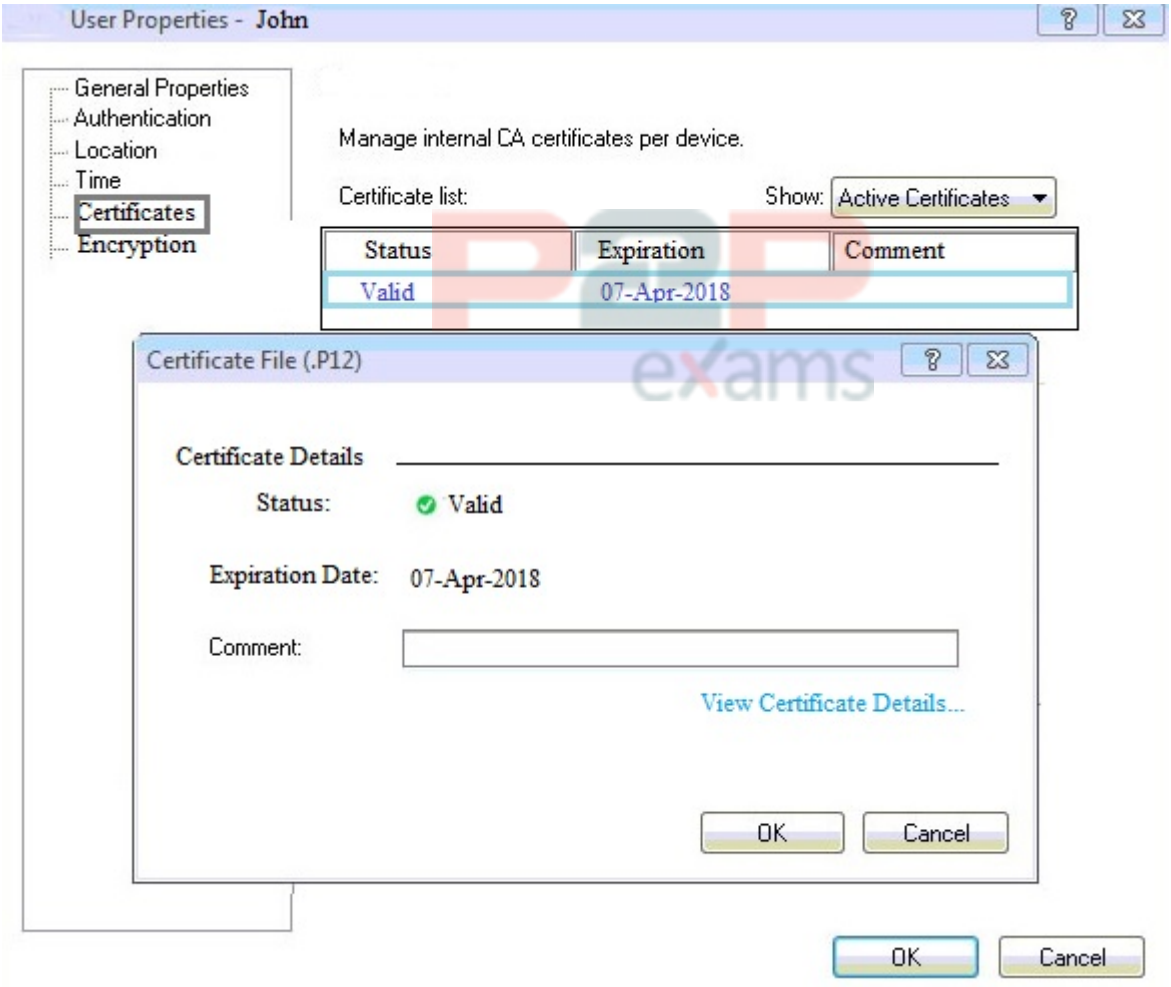
Explanation:

Threat Prevention is a comprehensive solution that protects networks from malicious attacks by using multiple security blades, such as Anti-Bot, Anti-Virus, IPS, Threat Emulation, and Threat Extraction. These are the Threat Prevention software components available on the Check Point Security Gateway. IPS (Intrusion Prevention System) is a blade that detects and prevents network attacks by using signatures and behavioral patterns. Anti-Bot is a blade that detects and blocks botnet communications by using reputation services and heuristics. Anti-Virus is a blade that scans files and web content for malware by using signatures and emulation. Threat Emulation is a blade that analyzes suspicious files in a sandbox environment and blocks malicious files from entering the network.Threat Extraction is a blade that removes exploitable content from files and delivers clean files to users2. Reference:Check Point R81 Threat Prevention Administration Guide

Question 8

Question Type: MultipleChoice

You can see the following graphic:



What is presented on it?

Options:

A- Properties of personal. p12 certificate file issued for user John.
B- Shared secret properties of John's password.
C- VPN certificate properties of the John's gateway.
D- Expired. p12 certificate properties for user John.

Answer:

A

Explanation:

The answer is A because the graphic shows the properties of a personal .p12 certificate file issued for user John. A .p12 file is a file format that contains a user's private key and public key certificate. The graphic shows that the certificate file is valid and has an expiration date of 07-Apr-2018. The graphic also shows that the certificate file is issued by an internal CA, which is a Check Point component that manages certificates for users and gateways. Reference: Check Point R81 Certificate Management, Check Point R81 Internal CA

Question 9

Question Type: MultipleChoice

When URL Filtering is set, what identifying data gets sent to the Check Point Online Web Service?

Options:

A- The URL and server certificate are sent to the Check Point Online Web Service
B- The full URL, including page data, is sent to the Check Point Online Web Service
C- The host part of the URL is sent to the Check Point Online Web Service
D- The URL and IP address are sent to the Check Point Online Web Service

Answer:

C

Explanation:

When URL Filtering is set, only the host part of the URL is sent to the Check Point Online Web Service for analysis. The host part is the part of the URL that identifies the web server, such as www.example.com. The Check Point Online Web Service uses this information to categorize the URL and return the appropriate action to the Security Gateway. The other options are not sent to the Check Point Online Web Service for analysis, as they may contain sensitive or irrelevant data.

Question 10

Question Type: MultipleChoice

In order to modify Security Policies, the administrator can use Which option best tools? (Select the best answer.)

Options:

A- SmartConsole and WebUI on the Security Management Server.
B- SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed.
C- Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.
D- mgmt_cli (API) or WebUI on Security Gateway and SmartConsole on the Security Management Server.

Answer:

B

Explanation:

In order to modify Security Policies, the administrator can use SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed. SmartConsole is a graphical tool that allows the administrator to create, edit, and manage security policies using a web browser. mgmt_cli (API) is a command-line tool that allows the administrator to perform the same tasks using commands and scripts. Both tools can connect to the Security Management Server remotely from any computer that has SmartConsole installed. Reference: [SmartConsole Overview], [mgmt_cli (API)]