FreeCram

FreeCram

Instant Download | 365 Days Free Updates | Money Back Guarantee | Security & Privacy

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

We're not the only ones **happy** about FreeCram Practice Material ...

12514+ customers in 100+ countries use FreeCram Test Engine. Meet our customers.

https://www.freecram.com

Free Exam/Cram Practice Materials.

Exam : **156-215.81**

Title : Check Point Certified Security Administrator R81

Vendor : CheckPoint

Version : DEMO

NO.1 By default, which port does the WebUI listen on?

A. 8080

B. 80

C. 4434

D. 443

Answer: B

Explanation:

By default, the WebUI listens on port 80. The WebUI is a web-based interface that allows administrators to configure and monitor Gaia OS settings and features from a web browser. The WebUI uses the HTTP protocol to communicate with the Gaia machine, which by default uses port 80 as the standard port number.

The other port numbers are not used by the WebUI by default, but they can be changed by modifying the Gaia configuration file or using CLISH commands.

NO.2 Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the

_____ algorithm.

A. SHA-256

B. SHA-200

C. MD5

D. SHA-128

Answer: A

Explanation:

By default, the SIC certificates issued by R80 Management Server are based on the SHA-256 algorithm1.

SHA-256 is a secure hash algorithm that produces a 256-bit digest. SHA-200, MD5, and SHA-128 are not valid algorithms for SIC certificates. References: SHA-1 and SHA-256 certificates in Check Point Internal CA (ICA)

NO.3 Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs

B. Capsule Cloud

C. Capsule Enterprise

D. Capsule Workspace

Answer: C

Explanation:

The components of Check Point Capsule are Capsule Docs, Capsule Cloud, and Capsule Workspace123.

There is no Capsule Enterprise component. Capsule Docs protects business documents everywhere they go.

Capsule Cloud protects mobile users outside the enterprise security perimeter. Capsule Workspace creates a secure business environment on mobile devices. References: Check Point Capsule Datasheet, Check Point Capsule Workspace Datasheet, Mobile Secure Workspace with Capsule

NO.4 What does it mean if Deyra sees the gateway status:

Choose the BEST answer.

A. SmartCenter Server cannot reach this Security Gateway

B. There is a blade reporting a problem

C. VPN software blade is reporting a malfunction

D. Security Gateway's MGNT NIC card is disconnected.

Answer: B

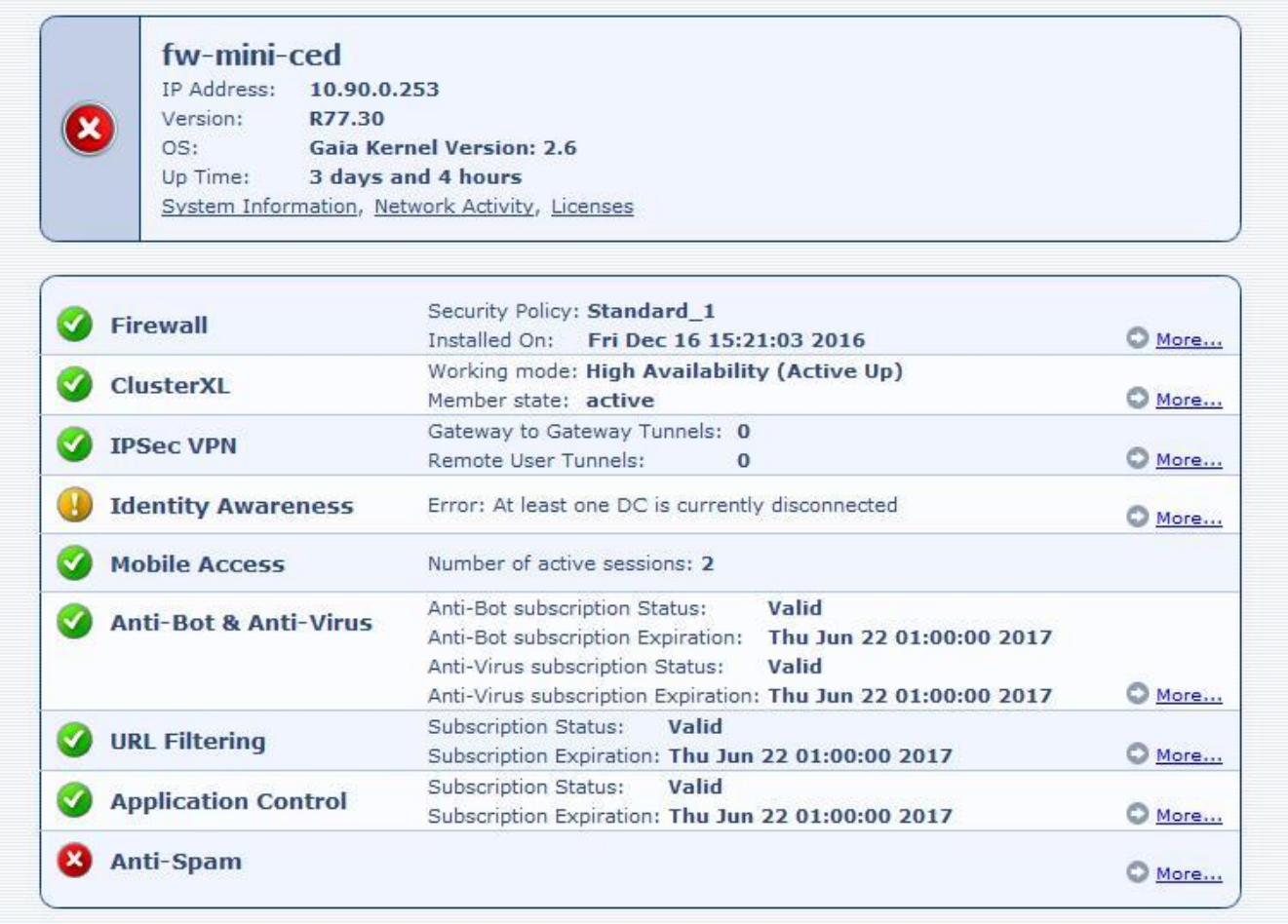
Explanation:

If Deyra sees the gateway status as shown in the image, it means that there is a blade reporting a problem.

The red "X" in the status column indicates that one or more blades on the Security Gateway have a problem that requires attention. The other options are not correct, as they do not match the status shown in the image.

If the SmartCenter Server cannot reach this Security Gateway, the status column would show a yellow triangle with an exclamation mark. If the VPN software blade is reporting a malfunction, the blades column would show a red "X" on the VPN icon. If the Security Gateway's MGNT NIC card is disconnected, the IP column would show "N/A" instead of the IP address.

References: Remote Access VPN R81 Administration Guide, Check Point R81.10



NO.5 Which of the following is an authentication method used for Identity Awareness?

A. SSL

B. Captive Portal

C. PKI

D. RSA

Answer: B

Explanation:

Captive Portal is an authentication method used for Identity Awareness4. Captive Portal is a web-based authentication method that redirects users to a browser-based login page when they try to access the network.

Users must provide their credentials to access the network resources. Captive Portal can be used for guest users or users who are not identified by other methods4. SSL, PKI, and RSA are not authentication methods used for Identity Awareness, but rather encryption or certificate technologies. References: Identity Awareness Reference Architecture and Best Practices

NO.6 What are the three main components of Check Point security management architecture?

A. SmartConsole, Security Management, and Security Gateway

B. Smart Console, Standalone, and Security Management

C. SmartConsole, Security policy, and Logs & Monitoring

D. GUI-Client, Security Management, and Security Gateway

Answer: A

Explanation:
The three main components of Check Point security management architecture are SmartConsole, Security Management, and Security Gateway5. SmartConsole is the graphical user interface that allows administrators to manage and monitor Check Point products. Security Management is the server that stores the security policy and configuration data. Security Gateway is the device that enforces the security policy on the network traffic. References: Check Point R81 Security Management Administration Guide

NO.7 A security zone is a group of one or more network interfaces from different centrally managed gateways.
What is considered part of the zone?
A. The zone is based on the network topology and determined according to where the interface leads to.
B. Security Zones are not supported by Check Point firewalls.
C. The firewall rule can be configured to include one or more subnets in a zone.
D. The local directly connected subnet defined by the subnet IP and subnet mask.
Answer: A
Explanation:
A security zone is a group of one or more network interfaces from different centrally managed gateways that have the same security requirements. The zone is based on the network topology and determined according to where the interface leads to. For example, a zone can be defined as internal, external, DMZ, VPN, etc.
Security zones are supported by Check Point firewalls and can be used to simplify security policies and network segmentation. The firewall rule can be configured to include one or more zones as source or destination objects. The local directly connected subnet defined by the subnet IP and subnet mask is not considered part of the zone, but rather a property of the interface.References: [Security Zones], [Security Zones Best Practices]

NO.8 Security Gateway software blades must be attached to what?
A. Security Gateway
B. Security Gateway container
C. Management server
D. Management container
Answer: B
Explanation:
Security Gateway software blades must be attached to a Security Gateway container. A Security Gateway container is a logical object that represents a physical or virtual machine that runs the Security Gateway software. A software blade is a modular security feature that can be enabled or disabled eway container. A software blade can provide functions such as firewall, VPN, IPS, anti-virus, anti-bot, application control, URL filtering, etc.References: [Security Gateway Containers], [Software Blades]

NO.9 Tom has connected to the Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward.

What will happen to the changes already made?

A. Tom will have to reboot his SmartConsole computer, clear the cache, and restore changes.

B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.

C. Tom's changes will be lost since he lost connectivity and he will have to start again.

D. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.

Answer: D

Explanation:

Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work. This is because SmartConsole uses a session mechanism that allows users to work offline and save their changes locally until they are ready to publish them to the Management13. If Tom loses connectivity, he can resume his session when he reconnects and continue working on his Rule Base changes. He does not need to reboot his SmartConsole computer, clear the cache, or restore changes. His changes will not be lost since he lost connectivity. References: Check Point R81 Security Management Administration Guide, Check Point CCSA - R81: Practice Test & Explanation | Udemy

NO.10 One of major features in R80.x SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?

A. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.

B. AdminA and AdminB are editing the same rule at the same time.

C. AdminB sees a pencil icon next the rule that AdminB is currently editing.

D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Answer: B

Explanation:

One of the major features in R80.x SmartConsole is concurrent administration, which allows multiple administrators to work on the same Security Policy at the same time12. However, only one administrator can edit a rule at a time. If AdminA and AdminB are editing the same rule at the same time, it will cause a conflict and prevent them from saving their changes12. Therefore, the correct answer is B. AdminA and AdminB are editing the same rule at the same time.

NO.11 Bob and Joe both have Administrator Roles on their Gaia Platform. Bob logs in on the WebUI and then Joe logs in through CLI. Choose what BEST describes the following scenario, where Bob and Joe are both logged in:

A. Since they both are logged in on different interfaces, they will both be able to make changes.

B. When Joe logs in. Bob will be logged out automatically.

C. The database will be locked by Bob and Joe will not be able to make any changes.

D. Bob will receive a prompt that Joe has logged in.

Answer: A

Explanation:

Since Bob and Joe both have Administrator Roles on their Gaia Platform and they both are logged in

on different interfaces, they will both be able to make changes. Gaia allows multiple administrators to log in simultaneously and perform different tasks without locking the database or logging out each other. References: Gaia R81.20 Administration Guide, page 18.

NO.12 Fill in the blank: Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is _____.

A. Stored on the Security Management Server.

B. Stored on the Certificate Revocation List.

C. Sent to the Internal Certificate Authority.

D. Sent to the Security Administrator.

Answer: B

Explanation:

When a certificate is revoked from a Security Gateway, the information is stored on the Certificate Revocation List (CRL). The CRL is maintained by the Internal Certificate Authority (ICA) and is checked during certificate validation processes.

* Option A (Incorrect): The Security Management Server maintains certificate information but does not store revoked certificates permanently.

* Option C (Incorrect): The Internal Certificate Authority manages certificate issuance but does not store revoked certificates-it publishes a CRL instead.

* Option D (Incorrect): The Security Administrator does not receive direct notifications of revoked certificates.

Thus, the correct answer is B. Stored on the Certificate Revocation List.

NO.13 Which software blade enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine?

A. Application Control

B. Data Awareness

C. Identity Awareness

D. Threat Emulation

Answer: A

Explanation:

Application Control is the software blade that enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine. Application Control allows you to define granular rules for applications, web sites, web categories, web content types, and users. You can also use Application Control to monitor and block risky applications and web usage. References: [Application Control Administration Guide R80.40]

NO.14 Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers? (Choose the best answer.)

A. IPS

B. Anti-Virus

C. Anti-Malware

D. Content Awareness

Answer: B

Explanation:

The Threat Prevention Software Blade that provides protection from malicious software that can infect your network computers is Anti-Virus. Anti-Virus is a software blade that scans files and traffic for viruses, worms, trojans, spyware, and other malware. Anti-Virus can block or clean infected files and prevent malware outbreaks. IPS is a software blade that provides protection from network attacks and exploits. Anti-Malware is not a software blade, but rather a term that refers to any software that can detect and remove malware.
Content Awareness is a software blade that provides visibility and control over data that enters or leaves the network based on file types, data types, and keywords.
References: [Anti-Virus Software Blade], [IPS Software Blade], [What is Anti-Malware?], [Content Awareness Software Blade]

NO.15 Which product correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

A. SmartDashboard

B. SmartEvent

C. SmartView Monitor

D. SmartUpdate

Answer: B

Explanation:
The product that correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices is SmartEvent. SmartEvent is a software blade that analyzes logs from various sources such as Security Gateways, Endpoint Security Servers, Identity Awareness Servers, etc.
and generates security events based on predefined or custom rules. SmartEvent provides a graphical interface for viewing and managing security events in real-time or historical mode. References: [Check Point R81 SmartEvent Administration Guide]

NO.16 Which back up method uses the command line to create an image of the OS?

A. System backup

B. Save Configuration

C. Migrate

D. snapshot

Answer: D

Explanation:
According to the Hewlett Packard Enterprise Support Center3, the snapshot command uses the command line to create an image of the OS. A snapshot is a point-in-time copy of a disk partition that can be used to restore the system in case of a failure or corruption. References: Hewlett Packard Enterprise Support Center

NO.17 AdminA and AdminB are both logged into SmartConsole. What does it mean if AdminB sees a lock icon on a rule? Choose the BEST answer.

A. Rule is locked by AdminA and will be made available if the session is published.

B. Rule is locked by AdminA and if the session is saved, the rule will be made available.

C. Rule is locked by AdminB because the save button has not been pressed.

D. Rule is locked by AdminB because the rule is currently being edited.

Answer: A
Explanation:
In Check Point SmartConsole, when multiple administrators work on security policies, a lock icon appears on rules or objects that are being modified.
* If AdminB sees a lock, it means that AdminA is currently editing the rule, and it is locked for others.
* Once AdminA publishes the session, the rule becomes available to other administrators.
* Option B (incorrect): Saving a session does not release the lock; it must be published.
* Option C (incorrect): The lock is not caused by AdminB but by another user (AdminA).
* Option D (incorrect): A lock appears when another user (AdminA) is editing, not the current user.
Thus, the correct answer is A. Rule is locked by AdminA and will be made available if the session is published.

NO.18 What is a reason for manual creation of a NAT rule?
A. In R80 all Network Address Translation is done automatically and there is no need for manually defined NAT-rules.
B. Network Address Translation of RFC1918-compliant networks is needed to access the Internet.
C. Network Address Translation is desired for some services, but not for others.
D. The public IP-address is different from the gateway's external IP
Answer: D
Explanation:
A reason for manual creation of a NAT rule is when the public IP-address is different from the gateway's external IP. This can happen when the gateway is behind another NAT device or firewall3 .
References: Check Point R81 Security Gateway Administration Guide, Check Point CCSA - R81: Practice Test & Explanation

NO.19 What is the BEST method to deploy Identity Awareness for roaming users?
A. Use Office Mode
B. Use identity agents
C. Share user identities between gateways
D. Use captive portal
Answer: B
Explanation:
The BEST method to deploy Identity Awareness for roaming users is to use identity agents, which are software components installed on endpoints that provide user and machine identity information to the Security Gateway45. Identity agents are more secure and reliable than other methods, as they do not require network changes or user interaction4. Office Mode, sharing user identities between gateways, and using captive portal are not methods to deploy Identity Awareness, but rather features or options that can be used with Identity Awareness46.
References: Identity Awareness Reference Architecture and Best Practices, Identity Awareness PDP Broker, Identity Awareness Datasheet

NO.20 In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?
A. SND is a feature to accelerate multiple SSL VPN connections
B. SND is an alternative to IPSec Main Mode, using only 3 packets
C. SND is used to distribute packets among Firewall instances

D. SND is a feature of fw monitor to capture accelerated packets

Answer: C

Explanation:

The Secure Network Distributor (SND) is a feature of the Security Gateway that is used to distribute packets among Firewall instances . It improves the performance and scalability of the Firewall by utilizing multiple CPU cores. The other options are not related to SND. References: [Check Point Security Gateway Architecture and Packet Flow], [Free Check Point CCSA Sample Questions and Study Guide]

NO.21 What default layers are included when creating a new policy layer?

A. Application Control, URL Filtering and Threat Prevention

B. Access Control, Threat Prevention and HTTPS Inspection

C. Firewall, Application Control and IPSec VPN

D. Firewall, Application Control and IPS

Answer: B

Explanation:

The default layers that are included when creating a new policy layer are Access Control, Threat Prevention, and HTTPS Inspection. Access Control is the layer that defines the basic firewall rules. Threat Prevention is the layer that enables the protection against various types of attacks, such as IPS, Anti-Virus, Anti-Bot, etc. HTTPS Inspection is the layer that allows the inspection of encrypted traffic1. The other options are not the default layers that are included when creating a new policy layer.

NO.22 What is the main difference between Static NAT and Hide NAT?

A. Static NAT only allows incoming connections to protect your network.

B. Static NAT allow incoming and outgoing connections. Hide NAT only allows outgoing connections.

C. Static NAT only allows outgoing connections. Hide NAT allows incoming and outgoing connections.

D. Hide NAT only allows incoming connections to protect your network.

Answer: B

Explanation:

The main difference between Static NAT and Hide NAT is that Static NAT allows incoming and outgoing connections, while Hide NAT only allows outgoing connections4. Static NAT translates a single IP address to another single IP address, while Hide NAT translates a group of IP addresses to a single IP address. Static NAT is used to expose internal servers to external networks, while Hide NAT is used to hide internal hosts from external networks. References: Check Point R81 Firewall Administration Guide

NO.23 To enforce the Security Policy correctly, a Security Gateway requires:

A. a routing table

B. awareness of the network topology

C. a Demilitarized Zone

D. a Security Policy install

Answer: B

Explanation:

To enforce the Security Policy correctly, a Security Gateway requires awareness of the network topology.
This means that the gateway knows which networks and interfaces are internal and external, and how to route packets between them . References: [Check Point R81 Security Gateway Technical Administration Guide], Check Point CCSA - R81: Practice Test & Explanation

NO.24 Which of the following is NOT an identity source used for Identity Awareness?
A. Remote Access
B. UserCheck
C. AD Query
D. RADIUS
Answer: B
Explanation:
UserCheck is not an identity source used for Identity Awareness. UserCheck is a feature that allows you to interact with users when they trigger Data Loss Prevention or Threat Prevention incidents2. Identity Awareness uses different methods to acquire identities, such as AD Query, Identity Agent, Browser-Based Authentication, Terminal Servers, Captive Portal, and RADIUS3 . Therefore, the correct answer is B: UserCheck.

NO.25 When dealing with rule base layers, what two layer types can be utilized?
A. Ordered Layers and Inline Layers
B. Inbound Layers and Outbound Layers
C. R81.10 does not support Layers
D. Structured Layers and Overlap Layers
Answer: A
Explanation:
When dealing with rule base layers, two layer types can be utilized: Ordered Layers and Inline Layers5.
Ordered Layers are executed sequentially according to their order in the policy. Inline Layers are embedded in a parent layer and are executed only if the parent rule matches. References: Check Point R81 Firewall Administration Guide, [Check Point R81 Security Management Administration Guide]

NO.26 Core Protections are installed as part of what Policy?
A. Access Control Policy.
B. Desktop Firewall Policy
C. Mobile Access Policy.
D. Threat Prevention Policy.
Answer: D
Explanation:
Core Protections are installed as part of the Threat Prevention Policy. Core Protections are a set of IPS protections that are essential for securing your network against malicious traffic4. The other policies do not include Core Protections.
References: 1: Check Point CLI Reference Card 2: Anti-Spoofing 3: SmartView Tracker 4: Core Protections

NO.27 What is the most complete definition of the difference between the Install Policy button on the SmartConsole' s tab, and the Install Policy within a specific policy?

A. The Global one also saves and published the session before installation.

B. The Global one can install multiple selected policies at the same time.

C. The local one does not install the Anti-Malware policy along with the Network policy.

D. The second one pre-select the installation for only the current policy and for the applicable gateways.

Answer: D

Explanation:

The difference between the Install Policy button on the SmartConsole's tab and the Install Policy within a specific policy is that the former installs all the policies that are selected in the Install Policy window, while the latter pre-selects the installation for only the current policy and for the applicable gateways5 . The other options are not accurate differences. References: Installing Policies, [Check Point CCSA - R81: Practice Test
& Explanation]

NO.28 Gaia has two default user accounts that cannot be deleted. What are those user accounts?

A. Admin and Default

B. Expert and Clish

C. Control and Monitor

D. Admin and Monitor

Answer: D

Explanation:

Gaia has two default user accounts that cannot be deleted. They are Admin and Monitor. Admin is the user account that has full administrative privileges and can access both WebUI and CLI. Monitor is the user account that has read-only privileges and can access only WebUI2. The other options are not default user accounts in Gaia.

NO.29 What is a role of Publishing?

A. The Publish operation sends the modifications made via SmartConsole in the private session and makes them public

B. The Security Management Server installs the updated policy and the entire database on Security Gateways

C. The Security Management Server installs the updated session and the entire Rule Base on Security Gateways

D. Modifies network objects, such as servers, users, services, or IPS profiles, but not the Rule Base

Answer: A

Explanation:

The Publish operation sends the modifications made via SmartConsole in the private session and makes them public is the correct answer. This is because publishing is the process of saving your changes to the database and making them available to other administrators. Publishing also allows you to install policies on Security Gateways. References: [Publishing Changes]

NO.30 When should you generate new licenses?

A. Before installing contract files.
B. After an RMA procedure when the MAC address or serial number of the appliance changes.
C. When the existing license expires, license is upgraded or the IP-address where the license is tied changes.
D. Only when the license is upgraded.
Answer: C
Explanation:
You should generate new licenses when the existing license expires, license is upgraded or the IP-address where the license is tied changes13. These scenarios require a new license to be generated and activated on the Security Gateway or Management Server13. Therefore, the correct answer is C. When the existing license expires, license is upgraded or the IP-address where the license is tied changes

NO.31 What is the difference between SSL VPN and IPSec VPN?
A. IPSec VPN does not require installation of a resident VPN client
B. SSL VPN requires installation of a resident VPN client
C. SSL VPN and IPSec VPN are the same
D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser
Answer: D
Explanation:
The difference between SSL VPN and IPSec VPN is that IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed browser5 . IPSec VPN uses a pre-shared key or certificates to authenticate the endpoints and encrypts the data at the network layer. SSL VPN uses SSL/TLS protocols to authenticate the endpoints and encrypts the data at the application layer. References: Check Point Remote Access VPN Administration Guide R81, [Free Check Point CCSA Sample Questions and Study Guide]

NO.32 What are the three deployment considerations for a secure network?
A. Distributed, Bridge Mode, and Remote
B. Bridge Mode, Remote, and Standalone
C. Remote, Standalone, and Distributed
D. Standalone, Distributed, and Bridge Mode
Answer: C
Explanation:
The three deployment considerations for a secure network are Remote, Standalone, and Distributed3. Remote deployment means that the Security Management Server and Security Gateway are installed on different machines. Standalone deployment means that the Security Management Server and Security Gateway are installed on the same machine. Distributed deployment means that there are multiple Security Gateways managed by one or more Security Management Servers3. Therefore, the correct answer is C. Remote, Standalone, and Distributed.

NO.33 You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet connected to the company Wireless. The Wireless system goes through

the Check Point Gateway. How do you review the logs to see what the problem may be?

A. Open SmartLog and connect remotely to the IP of the wireless controller

B. Open SmartView Tracker and filter the logs for the IP address of the tablet

C. Open SmartView Tracker and check all the IP logs for the tablet

D. Open SmartLog and query for the IP address of the Manager's tablet

Answer: D

Explanation:

SmartLog is a unified log viewer that provides fast and easy access to logs from all Check Point components3. It allows the administrator to query for any log field, such as the IP address of the tablet, and filter the results by time, severity, blade, action, and more4. SmartView Tracker is a legacy tool that displays network activity logs from Security Gateways and other Check Point devices. It does not support remote connection to the wireless controller or querying for specific IP addresses.

References: SmartLog, SmartLog Queries, [SmartView Tracker]

NO.34 Which Check Point Software Wade provides visibility of users, groups and machines while also providing access control through identity-based policies?

A. Firewall

B. Identity Awareness

C. Application Control

D. URL Filtering

Answer: B

Explanation:

Identity Awareness is the Check Point software blade that provides visibility of users, groups and machines while also providing access control through identity-based policies. Identity Awareness enables administrators to define granular access rules based on user or machine identity, rather than just IP addresses. Identity Awareness also allows administrators to monitor user activity and generate reports based on user or machine identity.

NO.35 Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

A. Application Control

B. Threat Emulation

C. Anti-Virus

D. Advanced Networking Blade

Answer: D

Explanation:

The Advanced Networking Blade is NOT subscription-based and therefore does not have to be renewed on a regular basis1011. The Advanced Networking Blade provides advanced routing capabilities such as BGP, OSPF, VRRP, and multicast routing10. The other blades are subscription-based and require annual renewal to receive updates and support from Check Point1012.

References: Check Point License Guide, IPS Software Blade contracts, Product Catalog