



CheckPoint

Exam Questions 156-215.82

Check Point Certified Security Administrator - R82

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

What is the primary benefit of HTTPS Inspection in a security environment?

- A. It enables inspection of encrypted traffic for threats
- B. It replaces SSL/TLS with a proprietary protocol
- C. It blocks all HTTPS traffic by default
- D. It accelerates encrypted traffic

Answer: A

Explanation:

The correct answer is A. The primary benefit of HTTPS Inspection is that it enables the Security Gateway to inspect encrypted HTTPS traffic for threats, policy violations, malicious content, inappropriate websites, and application behavior. Without HTTPS Inspection, many security blades can see only limited metadata for encrypted sessions, reducing visibility into modern web traffic. Option B is false because Check Point does not replace SSL/TLS with a proprietary protocol; it intercepts and re-encrypts traffic using certificate-based inspection where configured. Option C is wrong because HTTPS Inspection does not block all HTTPS traffic by default; policy defines what is inspected, bypassed, allowed, or blocked. Option D is wrong because traffic acceleration belongs to performance technologies such as SecureXL, not HTTPS Inspection. The technical model is controlled TLS interception using an outbound CA certificate for client-initiated HTTPS or inbound certificate/private key handling for protected servers. Reference topics: HTTPS Inspection, encrypted traffic inspection, outbound policy, inbound policy, Threat Prevention with HTTPS.

NEW QUESTION 2

Where is it possible to view SmartConsole locked account?

- A. Administrators list under Permissions & administrators
- B. View Sessions in Gaia portal
- C. View Sessions in SmartConsole
- D. cpview in ssh

Answer: A

Explanation:

The correct verified answer is A. The uploaded answer key shows C, but that is not the correct administrative location for a locked SmartConsole administrator account. Check Point documentation for unlocking administrator accounts states that an administrator with Manage Administrators permission can go to the Manage&Settings view, right-click the locked administrator, and select Unlock Administrator. That points directly to the administrator list under Permissions&Administrators, not the View Sessions page. View Sessions in SmartConsole is for active or saved administrative sessions and session ownership, not primarily for unlocking an administrator account locked by login restrictions. Gaia Portal sessions are Gaia OS sessions, not SmartConsole account lock status. CPView is a monitoring/performance utility, not an administrator account unlock interface. This is an important correction because confusing sessions with administrator-account lockout leads to wrong operational action during a real lockout incident. Reference topics: Administrator Account Management, locked administrators, Manage&Settings, Permissions and Administrators, Unlock Administrator.

NEW QUESTION 3

What is the purpose of Audit logs?

- A. Audit Logs record administrative actions, such as configuration of static routes in CLISH or adding an OS administrator password.
- B. Audit Logs record administrative actions, such as policy modifications, user logins, and configuration changes.
- C. Audit Logs is to check the validity of the IPS, Anti-Bot, Anti-Virus, URL Filtering, Application Control subscription license from the Check Point ThreatCloud repository.
- D. Audit Log is to comply with the Regulations, such as FIPS, HIPAA or PCI-DSS.

Answer: B

Explanation:

The correct answer is B. Audit logs record administrative activity in the security-management environment, including administrator logins, policy modifications, object changes, publishing, installation operations, and other configuration changes. Option A is too narrow and Gaia-specific; Gaia administrative actions can be logged, but the best general definition for Audit Logs in this CCSA context is broader management accountability across policy and configuration activity. Option C is wrong because license/subscription validation is not the purpose of audit logs. Option D identifies a possible compliance benefit, but audit logs are not ??for?? one specific regulation; their direct purpose is recording administrative actions so changes can be traced to administrators and sessions. This matters operationally because audit logs answer ??who changed what and when,?? while security logs answer ??what traffic or security event occurred.?? Reference topics: Security Operations Monitoring, Audit Logs, administrator accountability, policy and configuration change tracking.

NEW QUESTION 4

In HTTPS Inspection, what is the role of Categorization Mode?

- A. It disables inspection for trusted sites
- B. It decrypts all HTTPS traffic by default
- C. It blocks all encrypted traffic
- D. It categorizes traffic based on domain and certificate without decryption

Answer: D

Explanation:

The correct answer is D. Categorization Mode in HTTPS-related handling allows the gateway to make a category decision using information available before full decryption, such as the destination domain, SNI/certificate attributes, and reputation/category lookup. The purpose is classification, not full content inspection. Option A is incomplete because trusted-site bypass is handled with bypass rules, bypass lists, or policy exceptions, not by Categorization Mode alone. Option B is wrong because categorization does not mean decrypting all HTTPS traffic by default. Option C is also wrong because the mode is not a blanket block action against encrypted traffic. This distinction matters because Application Control and URL Filtering frequently need to decide whether a site should be allowed, blocked, or bypassed before content is inspected. Full HTTPS Inspection decrypts traffic for supported blades, whereas categorization can classify traffic based on metadata and certificate/domain details. Reference topics: HTTPS Inspection, URL Filtering categorization, certificate/domain-based HTTPS handling, encrypted

traffic policy decisions.

NEW QUESTION 5

Which Identity Awareness Client can collect identities from not only Active Directory Domain Controllers, but also from Cisco Identity Services Engine Servers or NetIQ eDirectory Servers?

- A. Identity Agent for a User Endpoint Computer
- B. Identity Agent for a Terminal Server v2
- C. Identity Agent for a Terminal Server
- D. Identity Collector

Answer: D

NEW QUESTION 6

Which of these Autonomous Threat Prevention profiles mainly focuses on providing extensive protection against server attacks and east-west traffic?

- A. Cloud/Data Center
- B. Guest Network
- C. Perimeter
- D. Strict Security

Answer: A

NEW QUESTION 7

When a packet arrives at the Security Gateway, the Security Gateway checks it against the rules in the Ordered Layers. Where does the implied Policy (Implied rules) get checked and enforced?

- A. Implied rules First Rules apply to the first Ordered Layer in the Access Control polic
- B. Implied rules Before last and Last are applied only to the last Ordered Layer in the list.
- C. Implied rules apply to each layer in the Access Control policy.
- D. Implied rules apply only to the first Ordered Layer only in the Access Control policy.
- E. Implied rules apply only to the first Ordered Layer in the Access Control policy but if there is an Inline Layer then the Implied rules are checked again if the parent rule is matched and before the Inline Layer is checked.

Answer: A

NEW QUESTION 8

What is the main benefit of Identity Awareness?

- A. It allows you to configure security policy based on the source or destination network and user agent.
- B. It allows you to configure security policy based user or machine identity.
- C. It allows you to configure security policy based on password length
- D. RADIUS group membership and the source operating system.
- E. It allows you to configure security policy based on source network, destination network
- F. LDAP Group membership and source operating system.

Answer: B

NEW QUESTION 9

What are the default zone objects?

- A. InternalZone, ExternalZone, DMZZone
- B. InternalZone, PublicZone, DMZZone
- C. InternalZone, WanZone, DMZZone
- D. InternalZone, Internetzone, DMZZone

Answer: A

NEW QUESTION 10

Which type of Control Model is used in Application Control & URL Filtering and Content Awareness Policy?

- A. Permissive Control Model (also known as Whitelist Model)
- B. Restrictive Control Model (also known as Blacklist Model)
- C. Positive Control Model (also known as Whitelist Model)
- D. Negative Control Model (also known as Blacklist Model)

Answer: D

NEW QUESTION 10

What type of logs capture security-related events such as firewall activity and VPN connections?

- A. Audit Logs
- B. Security Logs
- C. Compliance Logs
- D. Traffic Logs

Answer: B

NEW QUESTION 13

Select the correct description of the Explicit Rules.

- A. Explicit rules are created by the administrator
- B. Explicit rules are created in Security Policies by the Security Management Server
- C. Explicit rules are created by the Security Gateway
- D. Explicit rules are created in the Global Properties on the Security Management Server

Answer: A

NEW QUESTION 16

How do you match a user or a computer identity in the security policy?

- A. Use identity awareness objects in source or destination columns.
- B. Use the AD Query Object in source or destination column.
- C. Use a user or a user group object in source or destination column.
- D. Use Access Role Objects in source or destination columns.

Answer: D

NEW QUESTION 21

What happens when disk space on the Log Server drops below 5000 MBytes by default?

- A. A popup alert is triggered
- B. Files begin to be deleted
- C. Logging stops immediately
- D. A script is executed

Answer: B

NEW QUESTION 24

When looking at the Ordered Access Control Layers in the SmartConsole they are organized sequentially. How does the security gateway enforce the rules?

- A. All ordered layers are analyzed in parallel
- B. If there is a matched drop rule in any layer then the traffic is allowed.
- C. After checking each layer the firewall engages the relevant blades and starts to evaluate again one at a time while working with the other access control blades.
- D. Each layer is evaluated independently.
- E. All ordered layers are analyzed in parallel
- F. If there is a matched accept rule in any layer then the traffic is allowed.

Answer: C

NEW QUESTION 28

What is the primary purpose of the Security Policy Management solution?

- A. To provide out-of-the-box threat prevention
- B. To manage network traffic
- C. To simplify and enhance cybersecurity management
- D. To monitor user activity

Answer: C

Explanation:

The correct answer is C. Security Policy Management in Check Point R82 is designed to simplify and enhance cybersecurity management by giving administrators a centralized model for defining objects, policies, rulebases, NAT behavior, policy packages, layers, and installation targets. Option A is too narrow because out-of-the-box threat prevention is only one area of security configuration and belongs more specifically to Threat Prevention profiles and protections. Option B is incomplete because the Security Gateway manages and enforces traffic, while Security Policy Management defines the control logic and administrative structure used to govern traffic. Option D is also incomplete because monitoring user activity is handled through logging, Identity Awareness, SmartView, and related monitoring tools. Security Policy Management's value is broader: it provides the central administrative framework for translating business and security requirements into enforceable gateway policy. Reference topics: Security Policy Management, Access Control Policy, Policy Packages, SmartConsole management workflow.

NEW QUESTION 32

What is a best practice for managing SmartConsole administrator accounts?

- A. Allow unlimited concurrent sessions
- B. Limit the use of Super User accounts
- C. Use simple passwords
- D. Assign roles based on maximum privilege

Answer: B

NEW QUESTION 33

Which component is the source of the Logs sent to the Log Server?

- A. The SmartReporter along with the Eventia Reporter.
- B. The SmartEvent Correlation Unit
- C. The SmartEvent Server
- D. Security Gateway

Answer: D

NEW QUESTION 35

Automatic NAT rules can be enabled inside the .

- A. Domain Object
- B. Network Group Object
- C. Service Object
- D. Host Object

Answer: D

NEW QUESTION 38

Which component is essential for enabling HTTPS Inspection on a Security Gateway?

- A. URL Filtering blade
- B. DNS Resolver
- C. Certificate Authority (CA) certificate
- D. Static NAT rule

Answer: C

NEW QUESTION 43

What is the primary function of the ??Trusted Clients?? feature in SmartConsole?

- A. To restrict access to the management server
- B. To manage user accounts
- C. To configure network settings
- D. To install security policies

Answer: A

NEW QUESTION 45

What is the primary purpose of SecureXL?

- A. Provides software-based solution for Security Gateway performance
- B. Encrypts and decrypts traffic to and from Security Gateways
- C. Protect sensitive data from being lost, stolen, or accessed by unauthorized users
- D. Identifies and controls sensitive data within network

Answer: A

Explanation:

The correct answer is A. SecureXL is a Security Gateway performance acceleration technology. It improves packet and connection handling by accelerating eligible traffic through optimized processing paths. Official R82 Performance Tuning documentation identifies SecureXL as the Security Gateway component that accelerates IPv4 and IPv6 traffic passing through the gateway. Option B describes VPN/IPsec or encryption/decryption functionality, not SecureXL??s primary purpose. Option C describes a broad data-protection outcome and is closer to DLP or security policy objectives. Option D is specifically associated with Content Awareness or Data Loss Prevention-type capabilities, not SecureXL. SecureXL is not a content inspection blade and does not classify sensitive data; it exists to improve gateway throughput and reduce processing overhead where traffic can be accelerated safely. In real administration, SecureXL becomes relevant when analyzing traffic paths, throughput, acceleration status, performance tuning, and packet-processing behavior on a gateway. Reference topics: SecureXL, Security Gateway performance, Performance Tuning, traffic acceleration.

NEW QUESTION 48

Which of the following is a best practice for policy layers?

- A. Avoid sharing layers across policies
- B. Use only one layer per policy
- C. Disable implicit cleanup rules
- D. Share layers with other policy packages

Answer: D

Explanation:

The correct answer is D. Sharing layers with other policy packages is a best practice when the same set of controls should be reused consistently across multiple policies. Shared layers reduce duplication, support common policy modules, and make governance easier because updates to a shared layer can be maintained centrally. Option A is the opposite of the intended best practice where reuse is appropriate. Option B is too restrictive; one of the benefits of the Check Point layered policy model is the ability to separate network, application, content, or identity logic into manageable layers. Option C is wrong because implicit cleanup behavior exists as part of layer processing; administrators should add explicit cleanup rules for visibility, not try to disable the implicit mechanism. The proper design is modular but controlled: use shared layers where consistency is needed, use ordered and inline layers appropriately, and keep cleanup behavior explicit and logged where possible. Reference topics: Policy Layers, Shared Layers, Ordered Layers, Inline Layers, Access Control policy design.

NEW QUESTION 52

What are Trusted Clients?

- A. This is a list of Check Point customers considered trustworthy (such as Microsoft, Adobe, Apple, Amazon and others).
- B. This is a definition of Client IP addresses allowed to connect to the Security Management server using SmartConsole.
- C. This is a list of partners of Check Point also known as OPSEC companies.
- D. This is a group of RemoteAccess Users with User Certificates not yet expired nor revoked.

Answer: B

NEW QUESTION 57

Which process receives identity data from identity sources and organizes the data into tables, before forwarding the data to the other process on Security Gateway?

- A. CPD
- B. PDP
- C. CPM
- D. PEP

Answer: B

NEW QUESTION 60

What is the difference between the Positive Control Model and the Negative Control Model?

- A. The Positive Control Model allows is what routers use and simply route traffic with no security rule
- B. The Negative Control Model is what firewalls use and they require explicit rules to allow and route traffic.
- C. The Positive Control Model allows specific, approved actions or traffic and blocks everything els
- D. The Negative Control Model begins by blocking specific, known threats, or unwanted actions and allows everything else.
- E. The Positive Control Model begins by blocking specific, known threats, or unwanted actions and allows everything els
- F. The Negative Control Model allows specific, approved actions or traffic and blocks everything else.
- G. The Positive Control Model aims to keep administrators in a positive mind se
- H. The Negative Control Model results in administrators having a negative mind set.

Answer: B

NEW QUESTION 61

What provides the trusted client option in SmartConsole?

- A. IP address(es) allowed to connect to the Gaia Portal
- B. IP address(es) allowed to connect to the Security Management Server using SmartConsole
- C. IP address(es) allowed to connect to the Security Management Server using ssh
- D. IP address(es) allowed to connect to the Security Gateway(s)

Answer: B

Explanation:

The correct answer is B. In Check Point administration, ??trusted clients?? or GUI Clients define which computers are allowed to connect to the Security Management Server using SmartConsole. This is an administrative access-control mechanism for management connectivity, not traffic inspection. The trusted client definition can be a specific IP address, network, address range, or unrestricted ??Any?? setting, depending on how the administrator configures GUI Clients. Option A is wrong because Gaia Portal access is controlled by Gaia OS access and user settings, not SmartConsole trusted clients. Option C is wrong because SSH access is command-line access to Gaia, not SmartConsole GUI access. Option D is wrong because SmartConsole does not normally connect directly to gateways for policy administration; it connects to the management server, which then manages gateways. This feature is important because it reduces the management attack surface by preventing unauthorized administrator workstations from even attempting SmartConsole login to the Security Management Server. Reference topics: Administrator Account Management, GUI Clients, Trusted Clients, SmartConsole management access.

NEW QUESTION 64

What is the role of the Security Gateway in the Check Point environment?

- A. To act as a centralized management server
- B. To provide a web-based interface
- C. To inspect inbound and outbound traffic
- D. To manage objects and policies

Answer: C

NEW QUESTION 68

SmartView Web Application is accessed from a web browser with which URL?

- A. <https:// /smartconsole/>
- B. <https:// /smartlog/>
- C. <https://>
- D. <https:// /smartview/>

Answer: D

NEW QUESTION 70

What is one main purpose of URL Filtering?

- A. Automatic translation of foreign web sites into your preferred language.
- B. Specify the application which should be blocked during business hours, such as Facebook-Game, Indeed-Chat, among others.
- C. Synchronizing verdicts on URL Categories for better hit rates.
- D. Use URL Categories to block access to malicious or non-work-related websites.

Answer: D

NEW QUESTION 71

What is the purpose of the Command Line button in SmartConsole?

- A. Open a console session on SmartUpdate
- B. Open an SSH connection to the Management
- C. Open an SSH connection to the Gateway
- D. Open API session on Management Server

Answer: C

NEW QUESTION 72

Which feature of Autonomous Threat Prevention ensures that organizations benefit from the latest protections without manual configuration?

- A. Threat Emulation
- B. Manual policy tuning
- C. Automatic configuration updates
- D. Static NAT enforcement

Answer: C

NEW QUESTION 74

What is the purpose of the "Fail Mode" setting in HTTPS Inspection?

- A. To enforce strict NAT policies
- B. To define how the gateway handles inspection failures
- C. To disable inspection for internal traffic
- D. To allow only HTTP traffic

Answer: B

NEW QUESTION 76

What is the purpose of the Policy Enforcement Point (PEP) in Identity Awareness?

- A. To receive identity data from identity sources
- B. To organize identity data
- C. To store logs of user activity
- D. To enforce network access restrictions based on identity

Answer: D

NEW QUESTION 77

What does URL Filtering primarily focus on?

- A. Managing user credentials
- B. Blocking all HTTP traffic
- C. Controlling access to websites based on their URLs
- D. Encrypting web traffic

Answer: C

NEW QUESTION 82

Which of the following is a key advantage of using predefined Autonomous Threat Prevention profiles?

- A. They are only available in R77 and earlier
- B. They allow instant protection tailored to network segments
- C. They require manual updates for each new threat
- D. They eliminate the need for any monitoring

Answer: B

NEW QUESTION 87

The Access Control Policy includes which of these features?

- A. Firewall, Application & URL Filtering, Content Awareness, IPsec VPN and Mobile Access, Identity Awareness
- B. Firewall, Application & URL Filtering, Data Loss Prevention, IPsec VPN and Mobile Access, Identity Awareness
- C. Firewall, Application & URL Filtering, antivirus, IPsec VPN and Mobile Access, Identity Awareness

D. Firewall, Application & URL Filtering, file content analysis, IPsec VPN and Mobile Access, Identity Awareness

Answer: A

NEW QUESTION 88

What are the two main processes of the Identity Awareness blade?

- A. Identity Decision Process (IDP) Identity Direction and Accounting Process (IDAP)
- B. Pre-Deployment Process (PDP) Pre-Enforcement Process (PEP)
- C. Policy Decision Point (PDP) Policy Enforcement Point (PEP)
- D. Inter-Process Communication (IPC) Remote-Process Communication (RPC)

Answer: C

Explanation:

The correct answer is C. Check Point Identity Awareness relies on two key functional roles: Policy Decision Point (PDP) and Policy Enforcement Point (PEP). The PDP is responsible for acquiring identity information from configured identity sources and sharing identity data as required. The PEP is responsible for enforcing network access restrictions based on identity information. This architecture lets Check Point map users, computers, and groups to network activity, then use that identity context inside Access Control rules. Option A invents process names that are not official Identity Awareness process names. Option B incorrectly expands PDP and PEP as ??Pre-Deployment?? and ??Pre-Enforcement??; those are not Check Point terms. Option D refers to generic communication concepts and not the Identity Awareness blade?s main decision/enforcement model. This question is foundational because Identity Awareness is not merely authentication; it is the bridge between identity acquisition and firewall enforcement. Reference topics: Identity Awareness, Policy Decision Point, Policy Enforcement Point, identity-based enforcement.

NEW QUESTION 91

What is the best practice for installing the security policy?

- A. Use the Install Policy button in the Global toolbar at the top of the SmartConsole
- B. Use the API command install-policy policy-package
- C. Use the Install Policy button in the active policy (in the SECURITY POLICIES view)
- D. Right click on the word Policy in the SECURITY POLICIES view and choose Install Policy

Answer: C

NEW QUESTION 95

What condition needs to be matched for an Inline Layer to be used?

- A. The Inline Layer Software blade must be enabled first
- B. A Dynamic Layer must be added before the Inline Layer and then the policy should be installed.
- C. The Inline Layer must be installed after the Ordered Layer.
- D. A parent rule is matched

Answer: D

NEW QUESTION 96

What are types of Policy Layers?

- A. Access Control Layer and Content Awareness Layer
- B. Access Control layer, QoS Layer, Desktop Security Layer and Threat Prevention Layer
- C. Ordered Layers and Inline Layers
- D. Access Control Layer and Threat Prevention Layer

Answer: C

NEW QUESTION 101

The Security Gateway uses Implied and Explicit rules to determine whether connections are allowed or denied. Where can the administrator view the Implied rules?

- A. SmartConsole > MANAGE & SETTINGS > Blades > Firewall > Implied rules
- B. Use the command fw stat --implied-rules or the CLISH command show security-gateway implied-rules
- C. SmartConsole > SECURITY POLICIES > Actions > Implied rules
- D. The Implied rules cannot be viewed in the SmartConsole
- E. They are hidden and are there to allow Control Connections, including policy installation and log traffic.

Answer: C

NEW QUESTION 103

What happens when a rule in an Ordered Layer matches a packet and the action is Drop?

- A. The packet is encrypted
- B. The packet is dropped and no further rules are checked
- C. The packet is logged and forwarded
- D. The packet is sent to the next layer

Answer: B

NEW QUESTION 105

Which feature enhances security by restricting access to the Management Server to only those SmartConsole clients that are explicitly permitted?

- A. Gaia Admin Roles
- B. Permission Profiles
- C. allowed-gui-ips.conf file in \$CPDIR/conf
- D. Trusted Clients

Answer: D

Explanation:

The correct answer is D. Trusted Clients are the SmartConsole/GUI client restrictions that define which systems may connect to the Security Management Server. This feature enhances management-plane security because even if an attacker has valid credentials, the login attempt should fail if it comes from a client that is not permitted. Option A is wrong because Gaia Admin Roles control permissions inside Gaia OS, not SmartConsole client source restrictions to the management server. Option B is related to what an authenticated administrator is allowed to do inside SmartConsole, not which client workstation can connect. Option C references a file path-style concept, but the official administrator-facing feature name is Trusted Clients/GUI Clients, and the exam is asking for the feature rather than a file. Trusted Clients are configured as specific IP addresses, ranges, hostnames, or ??Any,?? although ??Any?? is weaker and generally less secure. Reference topics: Trusted Clients, GUI Clients, Security Management Server access control, SmartConsole access hardening.

NEW QUESTION 108

The Objects menu provides more management capabilities than the GATEWAYS & SERVERS New menu. It lets you add all types of custom objects. What other object management tool can the administrator use to manage objects in a separate window?

- A. The Objects Pane
- B. The Categories Explorer
- C. The Object Explorer
- D. The More object types menu

Answer: C

NEW QUESTION 111

What are the key components that make up the Check Point Three-Tier Architecture?

- A. Gaia WebUI Portal, Security Management and Security Gateway installed together on same server
- B. Security Dashboard, Management Database Server, Firewall
- C. Web Security Console, Log Server, Firewall
- D. SmartConsole, Security Management Server, Security Gateway

Answer: D

NEW QUESTION 115

What is a benefit of https inspection?

- A. Blocking sites
- B. Filtering malicious content
- C. Controlling bandwidth
- D. Monitoring applications

Answer: B

Explanation:

The correct answer is B. A direct security benefit of HTTPS Inspection is filtering malicious content inside encrypted traffic. Modern malware delivery, phishing, command-and-control activity, and file downloads often use HTTPS. If the gateway cannot inspect encrypted content, Threat Prevention, Anti-Virus, Threat Emulation, URL Filtering, and Application Control may have reduced visibility. Option A is partially related because URL Filtering can block sites, but site blocking is not the main technical benefit of HTTPS Inspection itself. Option C is wrong because bandwidth control is not the purpose of HTTPS Inspection. Option D is also only partially related: inspection can improve application visibility, but the stronger security answer is malicious-content filtering. HTTPS Inspection enables deeper inspection by decrypting traffic according to policy, applying security blades, and then re-encrypting traffic. Reference topics: HTTPS Inspection, Threat Prevention with HTTPS traffic, malicious content filtering, encrypted traffic visibility.

NEW QUESTION 116

Which of the following best describes how Access Role objects enhance identity-based policies in SmartConsole?

- A. They store logs of user activity for auditing
- B. They replace the need for traditional firewall rules
- C. They allow grouping of users, computers, and networks into a single rule condition
- D. They authenticate users before granting access

Answer: C

NEW QUESTION 119

Select the correct option available in Tops in SmartConsole Logs view.

- A. Top Users
- B. Top Hosts
- C. Top Gateways
- D. Top Locations

Answer:

A

NEW QUESTION 120

What is the role of the Security Management Server in the Check Point environment?

- A. To act as the first line of defense against cyberattacks
- B. To manage objects and policies
- C. To inspect inbound and outbound traffic
- D. To provide a web-based interface

Answer: B

NEW QUESTION 123

Which of the following is an example of a physical or virtual component in Smartconsole?

- A. Network Groups
- B. Security Gateways
- C. dns
- D. Adobe Acrobat

Answer: B

NEW QUESTION 127

What is a primary benefit of NAT?

- A. Changing your source IP address hitting internet web servers randomly to hide your real identity for security reasons.
- B. Security - Hides internal IP addresses behind a public IP address which prevents the internal hosts from being exposed to the internet.
- C. Business Continuity - If only a small amount of IP addresses were allowed to access a particular resource, you can change your source IP address to overcome this limitation.
- D. Accessibility - In a IPSec VPN environment, you can access resources with private IP addresses by assigning respective public IP addresses.

Answer: B

NEW QUESTION 129

Select the correct description of the Outbound HTTPS Inspection.

- A. It protects internal servers by Man in the Middle style interception
- B. It performs a Man in the Middle style interception on outbound HTTPS connections initiated by an internal users
- C. It performs a Man in the Middle style interception on outbound HTTPS connections initiated by both internal users and hosts on the Internet
- D. It performs a Man in the Middle style interception on outbound HTTPS connections initiated by hosts on the Internet

Answer: B

Explanation:

The correct answer is B. Outbound HTTPS Inspection applies to HTTPS connections initiated by internal users or internal clients toward external HTTPS servers. The Security Gateway performs controlled man-in-the-middle inspection: it represents the requested site to the client using a trusted inspection CA certificate, decrypts the traffic for inspection by supported blades, and creates a separate encrypted connection to the real external server. Option A describes inbound HTTPS Inspection more closely because inbound inspection protects internal servers from external clients. Option C is wrong because outbound inspection is not initiated by both internal users and internet hosts; the direction is internal-to-external. Option D is also inbound-style wording and not outbound inspection. The key production requirement is trust: internal clients must trust the gateway's outbound HTTPS Inspection CA certificate to avoid certificate warnings. Reference topics: HTTPS Inspection, Outbound HTTPS Inspection, CA certificate, encrypted traffic inspection.

NEW QUESTION 130

Which SmartConsole feature allows to filter logs using predefined or custom queries?

- A. Log Catalog
- B. Query Search
- C. Alert Configuration
- D. Track Options

Answer: B

NEW QUESTION 131

.....

Relate Links

100% Pass Your 156-215.82 Exam with Exambible Prep Materials

<https://www.exambible.com/156-215.82-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>