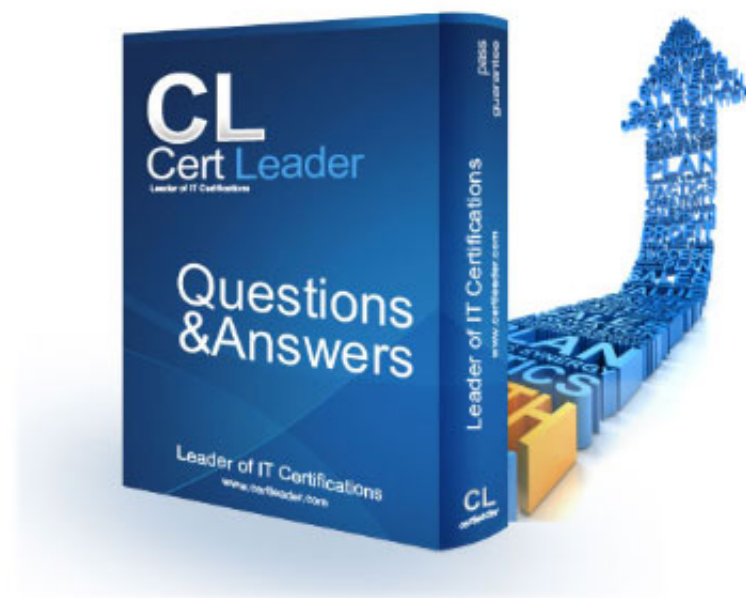


156-215.82 Dumps

Check Point Certified Security Administrator - R82

<https://www.certleader.com/156-215.82-dumps.html>



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

What is true of the URL Filtering Software Blade?

- A. It's part of HTTPS Inspection Policy
- B. It's part of URL Filtering policy
- C. It's part of the Access Control Policy
- D. It's part of Threat Prevention Policy

Answer: C

NEW QUESTION 3

After enabling and configuring Outbound HTTPS inspection on Security Gateway, you need to prevent users from getting warnings about the generated CA certificates that HTTPS Inspection uses.

In which certificate store do you need to add exported HTTPS Inspection certificate to client computer?

- A. Third-party Root Certification Authorities certificate store - (Local Computer)
- B. Trusted Root Certification Authorities certificate store - (Local computer)
- C. Third-party Root Certification Authorities certificate store - (Current User)
- D. Trusted Root Certification Authorities certificate store - (Current user)

Answer: B

NEW QUESTION 4

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 5

What is the recommended service for web browsing in Application Control?

- A. DNS
- B. HTTP
- C. FTP
- D. SMTP

Answer: B

NEW QUESTION 6

Select the correct order of Enforcement for Ordered Layers.

- A. When a packet arrives at the Security Gateway if Action of the matching rule is Accept, the Security Gateway stops matching against later rules and accepts the

- packet.
- B. When a packet arrives at the Security Gateway if Action of the matching rule is Drop, the Security Gateway stops matching against later rules in current Layer and continues to check rules in the next Ordered Layer
- C. When a packet arrives at the Security Gateway if Action of the matching rule is Drop, the Security Gateway stops matching against later rules in the Policy Rule Base and drops the packet
- D. When a packet arrives at the Security Gateway if Action of the matching rule is Accept, the Security Gateway stops matching against later rules in current Layer and continues to check rules in the previous Ordered Layer

Answer: C

Explanation:

The correct answer is C. In Ordered Layer enforcement, if a packet matches a rule with the Drop action, the Security Gateway stops further rule matching and drops the packet. Drop is terminating. Option A is wrong because in a layered policy, an Accept in one Ordered Layer can allow evaluation to continue into later Ordered Layers before final acceptance. Option B is wrong because a Drop action does not continue to the next Ordered Layer. Option D is nonsense because enforcement never continues to a ??previous?? ordered layer. The correct mental model is: layers are evaluated in sequence; rules inside each layer are evaluated top-down; Drop stops processing and drops traffic; Accept may pass the connection to additional ordered layers depending on policy structure. This is essential for troubleshooting layered policy behavior. Reference topics: Ordered Layers, rulebase enforcement, Drop action, Access Control Policy.

NEW QUESTION 7

An administrator wants to simulate threat prevention without impacting traffic. Which profile should be used?

- A. Monitor
- B. Internal Network
- C. Guests Network
- D. Strict Security

Answer: A

NEW QUESTION 8

How could you benefit from exporting a SmartConsole object to a CSV file?

- A. To integrate object into Third Party Security Systems such as FortiManager.
- B. You can use it in a scrip
- C. For example, batch import to a different Quantum Security environment.
- D. To get RADIUS Accounting information based on the utilization of those objects.
- E. For saving the information as inventory information.

Answer: B

NEW QUESTION 9

Identity Awareness is configured with which tool and where would the policy be enabled?

- A. It is configured using SmartDashboard and is enabled on the Security Gateway.
- B. It is configured using SmartConsole and is enabled on the Security Gateway.
- C. Is configured using SmartDashboard and is enabled on the Security Management Server
- D. Is configure using SmartConsole and is enabled on the SmartEvent Correlation Unit.

Answer: B

NEW QUESTION 10

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 10

What is the purpose of Dynamic Objects in SmartConsole?

- A. To change IP addresses dynamically
- B. To provide default security settings
- C. To represent external services
- D. To manage user accounts

Answer: A

NEW QUESTION 12

What is the main purpose of SecureXL?

- A. Provides software-based solution Security Management Performance.
- B. The gateway accesses the central ThreatCloud information to get the verdict of specific files prior to sending it to the intended destination.

- C. This is a solution to offer SSL Offloading to minimize the performance impact of the servers located in the Web Server farm.
- D. Provides software-based solution for Security Gateway Performance.

Answer: D

Explanation:

The correct answer is D. SecureXL is a Check Point acceleration technology used on Security Gateways to improve traffic-processing performance. Official R82 Performance Tuning documentation describes SecureXL as a product on a Security Gateway that accelerates IPv4 and IPv6 traffic passing through the gateway. Option A is wrong because SecureXL is not for Security Management Server performance; it is gateway-side acceleration. Option B describes a Threat Prevention or ThreatCloud-style lookup concept, not SecureXL. Option C is incorrect because SecureXL is not an SSL offload feature for web server farms. Its purpose is packet and connection acceleration, reducing load on deeper inspection paths where traffic is eligible for acceleration. In CCSA terms, SecureXL belongs to gateway performance and traffic acceleration, not policy authoring, logging, or cloud verdict lookup. Administrators should understand SecureXL as part of the Security Gateway's performance architecture, especially when troubleshooting throughput, acceleration state, and packet processing path. Reference topics: Introduction to Quantum Security, Security Gateway performance, SecureXL, Performance Tuning.

NEW QUESTION 14

What are some of the common tasks that the SmartConsole is used for?

- A. Create and manage policies, Monitor logs, Maintain licenses and contracts
- B. Create and manage license
- C. Monitor policies, Maintain performance
- D. Manage all devices on the corporate network, including firewalls, security gateway, switches, routers and load balancers.
- E. Redeploy the management server and gateways during troubleshooting

Answer: A

NEW QUESTION 16

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 17

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 21

A permission profile is a predefined set of Security Management Server and SmartConsole administrative permissions that you can assign to administrators. What are the three default profiles?

- A. Read Only All, Read Write All, and Super User
- B. Read Only, Read & Write, and Super User
- C. Access Control All, Threat Prevention All, and Super User
- D. RO, RW, and Universal admin

Answer: A

Explanation:

The correct answer is A. The three default permission profiles are Read Only All, Read Write All, and Super User. Read Only All permits viewing without modification. Read Write All allows broad modification access but does not necessarily equal the full administrative authority of Super User. Super User has full read/write permissions, including sensitive permissions such as managing administrators and sessions. Option B uses informal labels rather than the official profile names. Option C invents blade-specific default profiles that are not the three standard predefined profiles in this question. Option D uses shorthand and ??Universal admin,?? which is not the official Check Point default profile terminology. Correct permission profile assignment is a major administrative-control topic because overusing Super User breaks least privilege, while underprivileged accounts can prevent administrators from performing required operational tasks. Reference topics: Permission Profiles, Read Only All, Read Write All, Super User, SmartConsole administrator permissions.

NEW QUESTION 26

Inline Layers are evaluated against the rules; if none of the rules match _____ is applied.

- A. the Accept action
- B. the Implicit Cleanup Rule
- C. the Drop action
- D. the Explicit Cleanup Rule if exists

Answer: B

Explanation:

The correct answer is B. Every policy layer has an implicit cleanup action. When traffic enters an Inline Layer and none of the rules inside that layer match, the layer's Implicit Cleanup Rule is applied. Option D is not the best answer because the question asks what happens if none of the rules match, and the baseline layer behavior is the implicit cleanup rule; an explicit cleanup rule is an administrator-created final rule and would itself be one of the rules evaluated before falling to the implicit action. Option A is wrong because unmatched traffic is not automatically accepted. Option C is too simplistic because while the default implicit cleanup action is commonly Drop in many layers, the technical mechanism is the Implicit Cleanup Rule. This distinction matters because administrators should add explicit cleanup rules for visibility and logging, but the system still has implicit behavior if they do not. Reference topics: Policy Layers, Inline Layers, Implicit Cleanup Rule, Access Control rulebase evaluation.

NEW QUESTION 27

Which type of object represents Office365?

- A. Updatable object
- B. server
- C. host
- D. logical object

Answer: A

NEW QUESTION 32

You have been tasked with determining how much resources will be consumed by a potential HTTPS inspection deployment. Which of the following tools can you use?

- A. listening mode
- B. Learning mode
- C. inbound HTTPS inspection only
- D. Full Deployment

Answer: B

NEW QUESTION 35

What is a common use case for Application Control and URL Filtering rules?

- A. Block Applications and Inform Users
- B. To create and manage security policies
- C. To install policies
- D. Monitor Applications

Answer: A

NEW QUESTION 36

A company wants to monitor VPN tunnel status and gateway performance in real time. Which tool should they use?

- A. SmartConsole Logs View
- B. SmartUpdate
- C. SmartView Monitor
- D. SmartEvent

Answer: C

Explanation:

The correct answer is C. SmartView Monitor is used for real-time monitoring of gateway status, performance, VPN tunnels, users, traffic counters, and related operational indicators. Official R82 monitoring documentation describes SmartView Monitor as the tool for monitoring device status and traffic/system counters, and VPN documentation points administrators to SmartView Monitor for viewing tunnel status. Option A is wrong because SmartConsole Logs View is used for log search and investigation, not real-time gateway performance and tunnel status monitoring. Option B is incorrect because SmartUpdate is associated with updates/licenses in older management workflows, not live monitoring. Option D is wrong because SmartEvent focuses on event correlation, analysis, and reporting rather than direct real-time tunnel and gateway status views. The operational distinction is clean: logs for historical events, SmartEvent for correlation/reporting, SmartView Monitor for live health/performance/tunnel monitoring. Reference topics: SmartView Monitor, gateway status, VPN tunnel monitoring, traffic and system counters.

NEW QUESTION 41

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 42

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 47

Select the most correct statement about policy types.

- A. IPS Threat Cloud Protections are included in Access Control Polic
- B. Anti-Virus, Anti-Bot and SandBlast are included in the Threat Prevention Policy
- C. Access Control Policy includes features like Firewall, Application Control and URL Filtering, IPS Threat Cloud Protections
- D. NAT policy is a subset of Access Control Policy
- E. Application Control is included in Access Control Polic
- F. URL Filtering is included in the Threat Prevention Policy

Answer: B

Explanation:

The intended answer is B, but the wording is not perfect. Officially, an Access Control layer supports blades such as Firewall, Application and URL Filtering, Content Awareness, and Mobile Access. The Security Policies view separates Access Control management from Threat Prevention management, where IPS, Anti-Bot, Anti-Virus, and Threat Emulation are handled as threat-prevention capabilities. Therefore, the phrase ??IPS Threat Cloud Protections?? inside option B is technically imprecise if read strictly. However, among the available choices, B is still the best exam answer because it correctly places Firewall and Application Control/URL Filtering under Access Control, while the other choices create stronger architectural errors. Option C is wrong because NAT is not simply a subset of Access Control; NAT is a related policy/rulebase function but not the same as Access Control rules. Option D is wrong because URL Filtering belongs with Application Control in Access Control, not Threat Prevention. Option A also incorrectly places IPS in Access Control. Reference topics: Security Policy Management, Access Control Policy, Threat Prevention Policy, Policy Layers.

NEW QUESTION 51

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 54

Some use cases for Application Control and URL Filtering rules are:

- A. Monitor Applications, Allow Applications and Inform Users, Block malicious files
- B. limit Applications traffic, Allow Applications and Inform Users, Block malicious files
- C. limit Applications traffic, Block Applications and Inform Users, Block malicious files
- D. Monitor Applications, Block Applications and Inform Users, Block Sites

Answer: D

NEW QUESTION 55

Which of the following are 2 possible types of policy layers?

- A. Top / Bottom
- B. Application / Compliance
- C. Ordered / Inline
- D. Firewall / Application

Answer: C

NEW QUESTION 58

How is an Autonomous Threat Prevention Policy created?

- A. Automatically by AI
- B. Automatically downloaded from the Threat Cloud Repository.
- C. Manually downloaded from the Threat Cloud
- D. Automatically, but the date and time of the updates must be added to a cron job.

Answer: B

Explanation:

The correct answer is B as the best available option. Autonomous Threat Prevention relies on Check Point cloud-delivered threat intelligence and predefined profiles that are kept updated automatically. The phrase ??downloaded from the Threat Cloud Repository?? is not ideal wording, but it captures the correct principle: policy recommendations and protection updates are cloud-delivered and maintained by Check Point rather than manually built protection by protection. Option A is too vague and marketing-heavy; the policy is not simply ??created by AI?? as an administrator-facing technical mechanism. Option C is wrong because the point is automation, not manual download. Option D is wrong because administrators do not configure cron jobs for Autonomous Threat Prevention updates. The operational model is profile selection plus automatic updates, which reduces administrative burden while keeping protections aligned with Check Point??s current intelligence. Reference topics: Autonomous Threat Prevention, ThreatCloud-delivered updates, predefined profiles, automatic configuration updates.

NEW QUESTION 62

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 63

Which HTTPS Inspection setting allows bypassing connections to software update services?

- A. Fail Mode
- B. Categorization Mode
- C. Bypass Allow List
- D. Certificate Blocking

Answer: C

NEW QUESTION 66

During a routine audit, an administrator needs to review which users made changes to the security policy. Which log type should be reviewed?

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

Answer: B

Explanation:

The correct answer is B. To determine which users made changes to the security policy, the administrator must review Audit Logs. Audit Logs track administrative activity, including policy edits, publishing, installation, administrator logins, object modifications, and other configuration changes. Option A is wrong because Security Logs record enforcement and security events such as firewall traffic, VPN events, Threat Prevention detections, and application/site activity. Option C is wrong because Traffic Logs are traffic-related records, not administrator change records. Option D is wrong because Compliance Logs relate to compliance checks or reporting, not identifying which administrator changed policy. This is a basic audit-control concept: policy-change accountability comes from audit logs, while network activity comes from security/traffic logs. For any regulated or mature environment, reviewing Audit Logs is mandatory when investigating unauthorized, unexpected, or undocumented policy changes. Reference topics: Audit Logs, administrator activity tracking, policy modification audit, Logging and Monitoring.

NEW QUESTION 68

What management solution does Check Point offer as a service to deliver unified management for self-hosted Security Gateways, and ensures secure multifactor authentication access?

- A. CloudGuard SaaS
- B. CloudGuard Network Security
- C. Smart-1 Cloud
- D. SMS Cloud Extension Hotfix (SCEH)

Answer: C

Explanation:

The correct answer is C. Smart-1 Cloud is Check Point??s management-as-a-service offering for managing self-hosted Security Gateways from the cloud. It provides centralized security management without requiring the customer to deploy and maintain a local Security Management Server for that function. Smart-1 Cloud supports gateway onboarding, device monitoring, software updates, and cloud-based management operations, with secure access controls such as multifactor authentication through the Infinity Portal environment. Option A, CloudGuard SaaS, relates to SaaS application protection, not gateway security management. Option B, CloudGuard Network Security, is primarily cloud network security enforcement for public/private cloud environments, not the management service named in the question. Option D is not the official management product name; ??SMS Cloud Extension Hotfix?? is not the Check Point as-a-service management solution being tested. The key distinction is that Smart-1 Cloud is a Security Management Server service model, while CloudGuard products focus on cloud security enforcement and posture areas. Reference topics: Smart-1 Cloud, Security Management as a Service, Security Gateway onboarding, unified management.

NEW QUESTION 73

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 75

Which feature / blade can be used on both Check Point servers; the Security Management server for monitoring and on Security Gateway for enforcing Access Control Policy rules?

- A. Application Control and URL Filtering
- B. Identity Awareness
- C. Layer 8
- D. NAC

Answer: B

NEW QUESTION 79

What best describes the capability of the anti-bot blade?

- A. Protection against infections from undiscovered exploits
- B. Pre-infection detection
- C. Comprehensive protection against malicious and unwanted network traffic
- D. Post-infection detection

Answer: D

NEW QUESTION 82

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 85

When Accounting is enabled what is the time interval the logs are being updated?

- A. The log is updated in 10-minute intervals.
- B. The log update interval has to be specified as a firewall kernel parameter.
- C. The log is updated in 10-minute intervals or if 20 MB of log data is collected.
- D. The log update interval varies upon the queued user mode processes on the Management Servers, such as FWD, CPD, CPM.

Answer: A

Explanation:

The correct answer is A. In Check Point R82 tracking options, Accounting is used when the administrator wants traffic-volume information in the log record, including upload bytes, download bytes, and browse time. The official R82 Logging and Monitoring Administration Guide states that Accounting updates the log at 10-minute intervals to show how much data has passed in the connection. This is not a firewall kernel parameter that the administrator normally defines per rule, so option B is wrong. Option C adds a 20 MB threshold that is not the official Accounting interval behavior in the R82 guide. Option D is also incorrect because the Accounting update timing is not described as dependent on management-side user mode processes such as FWD, CPD, or CPM. The purpose of Accounting is operational visibility: it gives administrators more detail than a basic accept/drop log by showing the volume and duration characteristics of the connection. This is especially useful for Application Control, URL Filtering, and user-activity analysis. Reference topics: Security Operations Monitoring, Tracking Options, Accounting logs, SmartConsole Logs&Events.

NEW QUESTION 89

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 94

How does Application Control identify applications on the network?

- A. By decrypting all HTTPS traffic
- B. By matching IP addresses to known services
- C. By analyzing DNS queries
- D. By using traffic signatures regardless of port or protocol

Answer: D

Explanation:

The correct answer is D. Application Control identifies applications using application signatures and traffic classification rather than relying only on fixed ports or protocols. This is necessary because modern applications often use common ports such as 80 and 443, cloud-hosted endpoints, dynamic infrastructure, and encrypted traffic. Option A is wrong because HTTPS Inspection can improve visibility into encrypted traffic, but Application Control does not simply decrypt all HTTPS traffic as its identification method. Option B is wrong because IP-to-service matching is too brittle for modern applications and SaaS platforms. Option C is incomplete because DNS queries may provide useful context, but DNS analysis alone does not identify application behavior reliably. The correct principle is signature-based recognition from traffic flow, allowing policy to control applications even when they do not use traditional or predictable ports. Reference topics: Application Control, application signatures, Application and URL Filtering, Access Control Policy.

NEW QUESTION 96

What information does the Accounting option in Logs provide?

- A. The Accounting option records the number of times the same type of connection has been made in the last 24 hours (configurable) by default
- B. Enabling the Accounting option shows the amount of data passed in the connection including upload bytes, download bytes and browse time
- C. The Accounting option provides user accountability by associating a user identity with every log record
- D. The Accounting option tracks the amount of time required by the Firewall to process and pass the connection

Answer: B

NEW QUESTION 98

Primary log types are .

- A. Access Logs and Audit Logs
- B. Security Logs and compliance Logs
- C. Security Logs and Audit Logs
- D. Security Logs and Threat Prevention Logs

Answer: C

NEW QUESTION 100

Which tool is primarily used for managing Quantum Security policies?

- A. SmartEvent
- B. SmartView Monitor
- C. SmartConsole
- D. SmartUpdate

Answer: C

NEW QUESTION 104

What is the default Implicit Cleanup Action in both Ordered and Inline Layers?

- A. Log
- B. Reject
- C. Drop
- D. Accept

Answer: C

NEW QUESTION 105

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 109

What are the valid types of Administrator Accounts?

- A. Gaia account, Operating system account, SmartConsole account
- B. System account, Security Management Server account, SmartConsole account
- C. Gaia account, Security Management Server account, SmartConsole account
- D. Expert account, Security Management Server account, SmartConsole account

Answer: C

Explanation:

The correct answer is C. The valid administrator account types in this context are Gaia account, Security Management Server account, and SmartConsole account. A Gaia account is used for platform administration through Gaia Portal or Gaia Clish. A Security Management Server administrator account controls access to the management database and management functions. A SmartConsole administrator account is used to log in through SmartConsole and perform tasks according to assigned permission profiles. Option A is redundant and less precise because ??Operating system account?? overlaps Gaia but does not name the Security Management Server account type. Option B omits Gaia and uses vague ??System account?? wording. Option D is wrong because Expert is a shell/mode, not a standalone administrator account type. This separation matters because a person may have SmartConsole permissions without Gaia OS access, or Gaia OS access without permission to modify security policies in SmartConsole. Reference topics: Administrator Account Management, Gaia accounts, Security Management Server administrators, SmartConsole administrators.

NEW QUESTION 114

What is the role of Policy Decision Point (PDP) in Identity Awareness?

- A. The PDP receives identity data from identity sources
- B. The PDP receives identity data from the identity sources and enforces network access restrictions on traffic based on the identity of a user
- C. The PDP is an object to configure specifies users, computers, and network locations as one object
- D. The PDP enforces network access restrictions on traffic based on the identity of a user

Answer: A

NEW QUESTION 117

One of the key component of the Three-Tier Architecture of Check Point R82 is:

- A. SmartDashboard
- B. SmartProvisioning
- C. SmartUpdate
- D. SmartConsole

Answer: D

NEW QUESTION 121

When is a new Revision created?

- A. by executing "set revision" command
- B. during database installation
- C. during publish
- D. during installation

Answer: C

NEW QUESTION 125

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 126

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 130

What is the role of the "Perimeter" profile in Autonomous Threat Prevention?

- A. It provides aggressive protection for north-south traffic
- B. To simulate protection without enforcement
- C. It is a default profile for any security deployment

D. It is used to monitor traffic without enforcement

Answer: A

NEW QUESTION 131

What is the purpose of the 'Compare Revisions' feature in SmartConsole?

- A. Manage security policies
- B. View and manage session changes
- C. View connected administrator sessions
- D. Compare selected revisions

Answer: D

NEW QUESTION 133

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 135

Which of the following is a best practice for URL Filtering?

- A. Disable HTTPS Inspection to reduce complexity
- B. Use outdated URL databases for stability
- C. Combine both in a single rule for simplicity
- D. Create custom URL categories for specific needs

Answer: D

NEW QUESTION 137

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 141

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 144

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 145

SmartConsole objects can represent .

- A. server, virtual, or cloud components
- B. networks, virtual, or cloud components
- C. physical, virtual, or logical network components
- D. networks, virtual, or logical network components

Answer: C

NEW QUESTION 150

What is the benefit to use Log Indexing?

- A. It allows faster queries
- B. The logs will consume less disk space
- C. By indexing the log entries, you can get the whole time line of an infection of end entities
- D. Log entries are checked for duplicates, which are then deleted due to space constraints

Answer: A

NEW QUESTION 153

What are the predefined Autonomous Threat Prevention Profiles?

- A. Perimeter, Strict, DMZ, guest
- B. Perimeter, Strict, Internal, Guest
- C. Perimeter, Strict, External, Guest
- D. Perimeter, Strict, Internet, Guest

Answer: B

NEW QUESTION 154

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 156

Select the correct predefined profile of the Autonomous Threat Prevention.

- A. Hardened
- B. Monitor
- C. Recommended
- D. Optimized

Answer: B

NEW QUESTION 158

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 163

Which of these is one of the Identity Sources used by the Identity Awareness Blade?

- A. Identity Proxy API
- B. LDAP Authentication
- C. RADIUS Accounting
- D. Certificate Enrolment Service (CES)

Answer: C

NEW QUESTION 166

With URL Filtering you can:

- A. Control employee application access
- B. Control employee Internet access to inappropriate and illicit websites
- C. Control employee intranet access to internal web sites
- D. Control employee file access

Answer: B

NEW QUESTION 169

Application Control and URL Filtering can be combined with which of the Security measures?

- A. HTTPS Inspection and Content Awareness.
- B. Integration with an OPSEC-certified AAA Server

- C. HTTPS Inspection and Data Integrity Checking.
- D. OPSEC-certified Reporting Server using LEA and ELA interfaces for bidirectional communication with the Management Server.

Answer: A

NEW QUESTION 172

Which statement best describes Trusted Clients?

- A. These are trusted administrators allowed to connect to the Security Management Server using SmartConsole
- B. These are specific devices or IP addresses allowed to connect to the Security Management Server using SmartConsole
- C. These are Security Gateways allowed to connect to the Security Management Server using SmartConsole
- D. These are trusted users allowed to connect to the Security Management Server using SmartConsole

Answer: B

NEW QUESTION 173

What happens to packets if Explicit Default Rule is missing?

- A. The Implicit Cleanup Rule is applied.
- B. It depends on the Post NAT Rule.
- C. It depends on the matching feature located after the Access Control policy.
- D. Nothing happens as there is no matching rule.

Answer: A

NEW QUESTION 178

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 181

What is the main purpose of objects in SmartConsole?

- A. They are essential for defining security policies, network topologies, and other network configurations.
- B. The objects represent potential targets of a DoS attack.
- C. The objects serve as a target of an Access Control Policy.
- D. The objects are items which has to be placed in the Track column of a security policy.

Answer: A

NEW QUESTION 182

What is the purpose of the Objects menu in SmartConsole?

- A. To monitor network traffic
- B. To configure system settings
- C. To install policies
- D. To create and manage objects

Answer: D

Explanation:

The correct answer is D. The Objects menu in SmartConsole is used to create and manage objects. Objects can represent hosts, networks, groups, services, applications, zones, access roles, gateways, and other reusable policy elements. Option A is wrong because traffic monitoring is performed through Logs&Events, SmartView Monitor, SmartEvent, and related tools. Option B is wrong because system settings are usually handled through Gaia Portal/Clish or management settings depending on the setting type. Option C is wrong because policy installation is performed through Security Policies workflows, not the Objects menu. The Objects menu is a practical entry point for object creation and management, while Object Explorer provides a more comprehensive object-management window. Good object management is essential because clean, reusable, accurately named objects make policies easier to maintain and reduce configuration errors. Reference topics: SmartConsole Objects menu, Object Management, Object Explorer, reusable policy objects.

NEW QUESTION 183

What methods could be used with Custom Queries for querying logs?

- A. The syntax consists of Boolean operators, wildcards, fields and ranges.
- B. The syntax is referred to as PCRE which stands for Perl compatible Regular Expression.
- C. The syntax has to be converted into BASE64 format to randomize some security- relevant parameters.
- D. The syntax is the same as used in fw monitor or tcpdump.

Answer: A

NEW QUESTION 187

What is a best practice when naming a session in SmartConsole?

- A. Use complex passwords
- B. Limit the use of Super User accounts
- C. Assign roles based on least privilege
- D. Give the session a name and brief description

Answer: D

NEW QUESTION 192

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 194

A security administrator wants to integrate a third-party system with Check Point to send identity data using a REST API. Which identity source should be used?

- A. Identity Web API
- B. Identity Collector
- C. RADIUS Accounting
- D. AD Query

Answer: A

Explanation:

The correct answer is A. Identity Web API is the Identity Awareness method used when a third-party system needs to create or send identity data to Check Point using a web/API-based method. It gives flexible identity integration for systems that are not covered cleanly by AD Query, RADIUS Accounting, or Identity Collector. Option B is wrong because Identity Collector collects identities from supported infrastructure sources such as Active Directory domain controllers, Cisco ISE, NetIQ eDirectory, and Syslog sources. Option C is wrong because RADIUS Accounting consumes RADIUS accounting messages from network access infrastructure. Option D is wrong because AD Query learns identity information from Microsoft Active Directory events. The phrase ??REST API?? is decisive: API-based identity creation points to Identity Web API. Reference topics: Identity Awareness sources, Identity Web API, third-party identity integration, REST/API-based identity data.

NEW QUESTION 199

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 204

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 205

What is the purpose of the ??Advanced?? window in SmartConsole session management?

- A. To define session requirements
- B. To compare selected revisions
- C. To manage security policies
- D. To view connected administrator sessions

Answer: A

NEW QUESTION 207

What are the different types of Policy Layers supported in an Access Control Policy?

- A. Ordered Layers - Inline Layers
- B. Static Policy Layers - Updateable Policy Layers

- C. Global Access Layers - Exception Layers
- D. Firewall Layers - Application Layers - Content Layers

Answer: A

NEW QUESTION 210

What is the purpose of Security Zones in rulebase creation?

- A. To simplify rulebase creation
- B. To enforce user policies
- C. To provide threat prevention
- D. To monitor network traffic

Answer: A

NEW QUESTION 214

What is the difference between generating logs per connection or per session?

- A. Per Session is only available for URL Filtering, whereas the Connection could be applied to URL Filtering as well as Application Control.
- B. Per connection means that a log is generated for each connection in the session while per session means that only one log per session is generated.
- C. Per Session means that you will get the name of application in Application Control, although the applications were not specified in the rule bas
- D. Per Connections means that you will get the whole list of content in the Content Awareness blade.
- E. Per session means that a log is collected for each session in a connection while per connection means that only one log is collected per session.

Answer: B

NEW QUESTION 219

Which menu in SmartConsole provides the most comprehensive object management capabilities?

- A. Rule menu
- B. Object Explorer
- C. Objects menu
- D. New menu

Answer: B

Explanation:

The correct answer is B. Object Explorer provides the most comprehensive object-management capability in SmartConsole. While the Objects menu can create many object types and the New menu under Gateways&Servers is useful for infrastructure objects, Object Explorer is the broader management interface for searching, filtering, viewing, editing, importing, exporting, and organizing objects. Option A is wrong because the Rule menu is tied to rulebase operations, not full object lifecycle management. Option C is useful but less comprehensive than Object Explorer because it is primarily a menu-based creation and access point. Option D is too limited; ??New?? creates objects in a specific context but does not provide the full object inventory and management window. For larger CCSA/R82 environments, Object Explorer is the correct tool when the administrator needs a central view of object categories, object relationships, and object-management actions. Reference topics: Object Management, Object Explorer, SmartConsole object lifecycle, CSV import/export.

NEW QUESTION 223

How many predefined Security Zones as a starting point are available in a newly installed Security Management Server?

- A. 5
- B. 4
- C. 3
- D. 6

Answer: B

NEW QUESTION 224

Which authentication method is the simplest for SmartConsole admin accounts?

- A. Check Point Password
- B. SecurID
- C. RADIUS
- D. OS Password

Answer: A

NEW QUESTION 225

What is the role of real-time updates in Application Control and URL Filtering?

- A. They ensure accurate categorization of applications and websites
- B. They encrypt traffic between gateways
- C. They manage user authentication
- D. They reduce the need for HTTPS Inspection

Answer: A

NEW QUESTION 230

Which type of administrator account is used to log in to the Gaia Portal or Gaia Clish command line?

- A. Primary Security Management Server admin account
- B. Gaia admin account
- C. API admin account
- D. SmartConsole admin account

Answer: B

Explanation:

The correct answer is B. Login to the Gaia Portal or Gaia Clish uses a Gaia administrator account, not a SmartConsole administrator account. Gaia accounts are operating-system/platform administration accounts used to configure and manage the Gaia OS, including interfaces, routes, DNS, host access, system backups, user roles, SNMP, and other appliance/server-level settings. Option A is wrong because a primary Security Management Server administrator account is used for management-server administration through SmartConsole or management tools, not automatically for Gaia OS login. Option C is wrong because API administrators are used for management API access according to permissions and authentication method. Option D is wrong because SmartConsole admin accounts authenticate to the Security Management Server through SmartConsole; they are not the same thing as Gaia OS accounts unless separately configured. This separation is critical: one account type controls the Check Point security-management database; the other controls the underlying platform. Reference topics: Gaia administrator accounts, Gaia Portal, Gaia Clish, SmartConsole administrators.

NEW QUESTION 234

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 238

There are 2 ordered layers in a policy with 20 rules each. A connection matches rule number 5 in the first layer and the action for that rule is Drop. What will the firewall do now?

- A. Both layers are checked simultaneously and the strictest action is taken, hence the Firewall will wait for the matching results of the second layer before taking an action
- B. The Firewall will check if any rules in the second layer match with the connection and take action accordingly
- C. The Firewall will drop the connection and stop further inspection for it
- D. The Firewall will check if there is an Inline Layer attached to the rule 5 and will continue inspection if found

Answer: C

NEW QUESTION 240

Which tool provides a graphical interface for centralized management of the Check Point Security environment?

- A. Gaia Portal
- B. Security Management Server
- C. SmartConsole
- D. SmartEvent

Answer: C

NEW QUESTION 244

In addition to the ability to add New objects, the Object Explorer lets you:

- A. Export one or more objects to the JSON file
- B. Import one or more objects from the JSON file
- C. Import/Export one or more objects from the CSV file
- D. Export one or more objects to the CSV file

Answer: C

Explanation:

The correct answer is C. Object Explorer supports importing and exporting objects using CSV files. This capability is useful for bulk object administration, object inventory review, object migration preparation, and consistency checks across environments. Option A is incomplete and uses JSON rather than the tested CSV capability. Option B is also JSON-based and therefore incorrect for this question. Option D is partially correct because export to CSV is supported, but the more complete answer is import/export from CSV. In real administration, CSV import/export is valuable when many hosts, networks, or service objects must be reviewed or moved in a controlled way. It is not a substitute for understanding policy dependencies, but it is a powerful object-management feature. Reference topics: Object Explorer, CSV import/export, SmartConsole object management, bulk object administration.

NEW QUESTION 245

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 156-215.82 Exam with Our Prep Materials Via below:

<https://www.certleader.com/156-215.82-dumps.html>