



# 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

When Identity Access is enabled, policy decision and enforcement is handled by which two processes on the Security Gateway?

- A. LDAP Account Unit and Identity Collector.
- B. Identity Check Service (ICS) and Authorization Granting Service (AGS).
- C. Policy Distribution Point (PDP) and Packet Enforcement Policy (PEP)
- D. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)

**Answer:** D

### NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

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 9

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 10

What is the effect of enabling ??Shared Layer?? in an Inline Layer?

- A. It enables NAT translation
- B. It disables the layer in other policies
- C. It restricts access to the layer
- D. It allows the layer to be used in multiple rules and policies

**Answer:** D

#### Explanation:

The correct answer is D. A shared layer allows a policy layer to be reused rather than recreated separately in every rule or policy package. In R82, layer properties include a sharing option that lets administrators share a layer with other policies. Official guidance also states that a new policy layer can be configured directly in a specific policy or as a shared policy layer for several policies, and that an Inline Layer can be configured within a specific rule while an Ordered Layer exists as a separate dedicated layer. This supports modular policy design: common controls can be centralized and reused, which improves consistency and reduces administrative duplication. Option A is wrong because NAT translation is configured through NAT rules and NAT settings, not by enabling a shared layer. Option B is the opposite of the real function; sharing increases reuse rather than disabling the layer elsewhere. Option C is also wrong because permissions can restrict who edits a layer, but the ??Shared Layer?? function itself is about reuse across rules or policies. Reference topics: Policy Layers, Inline Layers, Ordered Layers, Shared Layers, SmartConsole Layer Properties.

#### NEW QUESTION 10

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 12

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 20

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 24

You are using a rule to block traffic to a specific https site. However, traffic is not blocked as expected during the first attempts to the site. It will be blocked later. What is the most likely reason?

- A. Categorization is in fail close mode and the requests are not allowed until the categorization is complete.
- B. Categorization is in hold mode and the requests are not allowed until the categorization is complete.
- C. Categorization is in Background mode and the requests are allowed until the categorization is complete.
- D. Categorization is in fail open mode and the requests are allowed until the categorization is complete.

**Answer:** C

#### NEW QUESTION 28

How does Application Control blade identify and control the usage of applications?

- A. By using signatures to determine applications from the traffic flow
- B. by using port and protocol, to determine the application from the traffic flow
- C. by using protocol and encryption, to determine the application from the traffic flow
- D. by using port, protocol and encryption, to determine the application from the traffic flow

**Answer:** A

#### Explanation:

The correct answer is A. Application Control identifies applications using application signatures and classification logic rather than relying only on ports and protocols. Modern applications frequently use common ports such as TCP 80 and 443, dynamic cloud endpoints, encrypted sessions, and evasive behavior. Port-based matching alone cannot reliably distinguish Facebook, YouTube, file-sharing services, chat applications, business SaaS platforms, or application subfunctions. Option B is wrong because port/protocol matching is the traditional firewall service model, not full application identification. Option C and D are also insufficient because protocol and encryption status do not identify application behavior by themselves. Check Point??s Application Control uses the Application Database and signatures to identify traffic from the flow and apply policy based on application or category. HTTPS Inspection can improve visibility into encrypted application traffic, but the blade??s core identification method is signature-based application recognition. Reference topics: Application Control, application signatures, Application Database, Access Control Policy.

#### NEW QUESTION 29

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 34

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 39

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 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

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 49

What is the purpose of the Gaia Clish shell?

- A. To manage objects and policies
- B. To inspect inbound and outbound traffic

- C. To provide a graphical interface
- D. For initial system configuration and ongoing management

**Answer:** D

**Explanation:**

The correct answer is D. Gaia Clish is the default role-based command-line shell used for initial system configuration and ongoing Gaia operating-system management. Administrators use it for platform tasks such as configuring interfaces, routes, DNS, host access, administrators, backups, snapshots, and other OS-level settings. Option A is wrong because objects and security policies are primarily managed in SmartConsole, not Gaia Clish. Option B is wrong because traffic inspection is performed by the Security Gateway enforcement engine according to installed policy, not by the shell itself. Option C is wrong because Gaia Clish is a command-line interface; Gaia Portal provides the web-based graphical interface. The key CCSA distinction is platform versus security-management administration: Gaia Clish manages the operating system/platform, while SmartConsole manages the security policy and objects on the Security Management Server. Reference topics: Gaia Clish, Gaia OS, Expert Mode, initial configuration and ongoing management.

**NEW QUESTION 52**

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 54**

Primary capabilities of Autonomous Threat Prevention include the following

- A. Automatic configuration updates
- B. Manual configuration updates
- C. Complex configuration and deployment
- D. no customization

**Answer:** A

**Explanation:**

The correct answer is A. A central capability of Autonomous Threat Prevention is automatic configuration updates. Instead of requiring administrators to manually tune every individual IPS, Anti-Bot, Anti-Virus, Threat Emulation, and file-protection behavior, Autonomous Threat Prevention uses predefined profiles and Check Point-maintained recommendations that can update as threat intelligence evolves. Option B is the opposite of the intended feature. Option C is wrong because the purpose of Autonomous Threat Prevention is to simplify deployment and reduce operational complexity, not increase it. Option D is also false because administrators can still view profile protections and override recommended file protections where required. The exam concept is automation with controlled administrator choice: select the correct profile for the network segment, monitor logs and reports, and customize only where business requirements justify it. Reference topics: Autonomous Threat Prevention, automatic configuration updates, file protections, profile customization.

**NEW QUESTION 58**

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 62**

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 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 67**

What is the last step involved in the high-level session workflow for administrators?

- A. SmartConsole Logout
- B. Removing the Session ID or take over a session from another administrator
- C. SmartConsole typing password for the specified administrator account
- D. Session Discard or Publish

**Answer:** A

**Explanation:**

The correct answer is A. In the high-level SmartConsole administrator session workflow, the administrator logs in, makes changes inside a session, then publishes or discards those changes, and finally logs out of SmartConsole. Option D is a critical step, but it is not the last step because the administrator still exits the management client after finishing the session. Option C happens at login, not at the end. Option B refers to exceptional session handling, such as taking over or dealing with another administrator's session, and is not the normal final step. This workflow is important because Check Point R82 uses a session-based model: changes are not committed to the published database until the administrator publishes. Discard removes session changes. Logout ends the administrator's SmartConsole connection. Reference topics: SmartConsole sessions, Publish, Discard, administrator logout, session workflow.

**NEW QUESTION 68**

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 73**

By default, alerts about specific security events are sent by which method?

- A. pop-ups
- B. log
- C. SNMP
- D. mail

**Answer:** A

**NEW QUESTION 76**

What are the capabilities integrated into a Threat Prevention Policy?

- A. IPS Anti-Bot, Anti-Virus, Content Awareness, URL Filtering
- B. IPS, Anti-Bot, Anti-Virus, SandBlast
- C. IPS, Anti-Bot, Application Control, URL Filtering
- D. Application Control, URL Filtering, Content Awareness, IPS

**Answer:** B

**NEW QUESTION 80**

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 84**

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 89**

How are objects organized in the SmartConsole?

- A. These objects are organized by type in SmartConsole.
- B. These objects are organized by priority in SmartConsole.
- C. These objects are organized by category in SmartConsole.
- D. These objects are organized alphabetically in SmartConsole.

**Answer:** C

**NEW QUESTION 92**

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 96**

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 100**

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 104**

What is the primary purpose of SmartConsole Objects?

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

**Answer:** D

**Explanation:**

The correct answer is D. SmartConsole objects simplify and enhance cybersecurity management by allowing administrators to define reusable representations of assets, networks, users, services, applications, zones, and other entities. Instead of manually entering IP addresses, networks, or services repeatedly in every rule, administrators create objects and reference them throughout the policy. This improves consistency, reduces configuration errors, and makes later changes easier. Option A is wrong because out-of-the-box threat prevention is provided through Threat Prevention blades, protections, profiles, and ThreatCloud updates, not by SmartConsole objects alone. Option B is wrong because monitoring user activity is handled through logging, Identity Awareness, SmartView, and audit/security logs. Option C is too generic; the Security Gateway enforces traffic handling, while objects are management abstractions used to construct policy. The official R82 documentation states SmartConsole is used to configure required objects and policies, and the glossary defines network objects as logical representations used by administrators in Security Policies. That is why the best answer is the broad management value of objects, not enforcement or monitoring by themselves. Reference topics: Object Management, SmartConsole Objects, Managing Objects, Security Policy object reuse.

#### NEW QUESTION 108

Which type of Control Model is used in Check Point Access Control Firewall Policy?

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

**Answer:** A

#### NEW QUESTION 112

What shells are offered by the Gaia Operating Systems?

- A. Gaia Clish and C-Shell
- B. Command Line and CLISH
- C. C-Shell, -Shell and Bourne Shell (bsh)
- D. Gaia Clish and Expert Mode

**Answer:** D

#### NEW QUESTION 114

Which statement is a best practice concerning a Cleanup rule?

- A. A Cleanup rule should be placed at the bottom of the rulebase.
- B. A Cleanup rule is optional and not considered Best Practice.
- C. A Cleanup rule could be used to terminate VPN tunnels on purpose.
- D. A Cleanup rule should be placed at the top of the rulebase to increase security and performance alike.

**Answer:** A

#### NEW QUESTION 119

Which of the following can be installed on a Windows Server to acquire identities?

- A. Identity Acquisition
- B. AD Collaboration
- C. Identity query tool
- D. Identity collector

**Answer:** D

#### Explanation:

The correct answer is D. Identity Collector can be installed on a Windows Server to acquire identities from supported identity sources and share those identities with the Identity Awareness Gateway. Official Check Point Identity Collector documentation states that Identity Collector must be installed on a Windows server and integrated with sources such as Active Directory, Cisco ISE, Syslog, and/or NetIQ eDirectory. Option A is a generic phrase and not the product/component name. Option B, ??AD Collaboration,?? is not a Check Point Identity Awareness component. Option C, ??Identity query tool,?? is also not the correct installable component in this context. In practice, Identity Collector is valuable where the organization needs scalable identity acquisition beyond a simple AD Query deployment. It supports enterprise identity visibility so Access Control rules can use user, group, computer, and network-location context through Access Role objects. Reference topics: Identity Awareness, Identity Collector installation, Windows Server deployment, identity acquisition sources.

#### NEW QUESTION 120

Which tool is primarily used for managing Quantum Security policies?

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

**Answer:** C

#### NEW QUESTION 125

What is the purpose of the Explicit Default Cleanup Rule?

- A. To forward unmatched traffic
- B. To accept unmatched traffic
- C. To drop unmatched traffic
- D. To encrypt unmatched traffic

**Answer:** C

#### NEW QUESTION 129

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 133

What is the correct default permission profile?

- A. Super Admin
- B. Super Profile
- C. Super Permission
- D. Super User

**Answer:** D

#### NEW QUESTION 134

What is the advantage of Autonomous Threat Prevention?

- A. cheaper licenses than classic threat prevention
- B. less resource consumption than classic Threat Prevention
- C. Single-Click configuration
- D. better protection than manual threat prevention

**Answer:** C

#### Explanation:

The correct answer is C. The practical advantage of Autonomous Threat Prevention is simplified, profile-based, single-click-style configuration. Administrators select an appropriate Autonomous profile rather than manually assembling and tuning large sets of protections. Option A is unsupported because licensing cost is not the technical advantage being tested. Option B is also unsupported; simplified configuration does not automatically mean lower resource consumption than classic Threat Prevention. Option D is too absolute because the protection quality depends on the deployment, profile, traffic visibility, updates, and policy design. The correct exam framing is operational simplification: Autonomous Threat Prevention gives fast deployment and Check Point-maintained protection recommendations while still allowing administrators to review, monitor, and customize where necessary. This makes it useful for organizations that want strong baseline prevention without maintaining every IPS/protection setting manually. Reference topics: Autonomous Threat Prevention, profile-based deployment, simplified configuration, automatic updates.

#### NEW QUESTION 135

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 138

What is a best practice when creating custom objects in SmartConsole?

- A. Use inconsistent naming conventions
- B. Edit default objects directly
- C. Clone default objects and edit the clone
- D. Avoid using groups

**Answer:** C

#### NEW QUESTION 142

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 144

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 146

With Autonomous Threat-Prevention, you can choose a profile that best fits your needs. What are the available options?

- A. Perimeter, Cloud North-West, East-West, Lateral Movement, External Network.
- B. Perimeter, Cloud/Data Center, Internal Network, Guest Network
- C. Perimeter, Cloud/Data Center, East-West-Traffic, Guest Network
- D. Perimeter, Fully Overlapping Encryption Domain, Partially Overlapping Encryption Domain, Proper Subset.

**Answer:** B

#### NEW QUESTION 147

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 151

What is the primary purpose of Check Point Identity Awareness?

- A. To manage network traffic
- B. To provide out-of-the-box threat prevention
- C. To enforce access and audit data based on identity
- D. To monitor user activity

**Answer:** C

#### NEW QUESTION 154

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 155

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 159

Which of the following groups represents valid administrator types in the Quantum Security environment?

- A. Quantum global admin, Quantum local admin, Quantum cloud admin
- B. CloudGuard admin, Harmony admin, Infinity admin
- C. Firewall admin, Management admin, OS admin
- D. Gaia admin, Primary SMS admin, SmartConsole admin

**Answer:** D

#### Explanation:

The correct answer is D. In a Check Point Quantum Security environment, administrators must distinguish between different administrative scopes. A Gaia admin manages the Gaia operating system through Gaia Portal or Gaia Clish. A Security Management Server administrator manages the security-management database and administrative access. A SmartConsole administrator logs in through SmartConsole to manage objects, policies, gateways, logs, and related security configuration according to permission profile. Option A invents generic ??Quantum global/local/cloud?? labels and is not the official administrator grouping for this CCSA context. Option B mixes Check Point product pillars and portal-level terminology, but it does not describe the core R82 administrator account types in the local Quantum Security environment. Option C is too generic and not official enough; ??firewall admin?? or ??OS admin?? may describe job functions, but not the account categories tested here. The key concept is separation of platform administration from security-management administration. Reference topics: Administrator Account Management, Gaia administrators, Security Management Server administrators, SmartConsole administrator access.

#### NEW QUESTION 163

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 164

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 169

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 171

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 176

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 177

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 178

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 180

What type of logs record administrative actions and changes within the security management, such as policy modifications, user logins, and configuration changes, essential for tracking administrative activities and ensuring accountability?

- A. Administration Logs
- B. Audit Logs
- C. Security Event Logs
- D. Compliance Detailed Logs

**Answer: B**

#### NEW QUESTION 182

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 184

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 188

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 189

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 192

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 194

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 198

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 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 203

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 204

What is the purpose of the Security Policies menu in SmartConsole?

- A. To create and manage security policies
- B. To monitor security logs
- C. To install policies
- D. To configure system settings

**Answer:** A

#### Explanation:

The correct answer is A. The Security Policies view/menu in SmartConsole is primarily used to create, edit, organize, and manage security policies, including Access Control and Threat Prevention policy components. Administrators work with rulebases, layers, policy packages, NAT rules, HTTPS Inspection policy, and related security-policy settings from this area. Option B is incorrect because logs are primarily reviewed in the Logs&Events view, not the Security Policies menu. Option C is partially related because policy installation can be launched from the Security Policies view after policy changes are complete, but installation is not the broader purpose of the menu. Option D is wrong because system settings are handled through Gaia Portal/Clish or Manage&Settings depending on the setting type. The exact exam distinction is between policy authoring and other administrative functions: Security Policies is where the administrator defines the logic that gateways will enforce after installation. Reference topics: Security Policy Management, Access Control Policy, Threat Prevention Policy, SmartConsole Security Policies view.

#### NEW QUESTION 208

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 213

Select one of the Common Types of Policies.

- A. Content Awareness
- B. Application & URL Filtering
- C. Firewall
- D. Access Control

**Answer:** D

#### NEW QUESTION 214

In Check Point Security Management, what is the term for a logical grouping of one or more policy types? (For example: Access Control, QoS, Desktop Security, Threat Prevention)

- A. Unified Policy
- B. Global Policy
- C. Group Policy Object (GPO)
- D. Policy Package

**Answer:** D

#### NEW QUESTION 219

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 220

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 224

Select the correct description of the SmartView Monitor.

- A. Used to view collected logs, monitor health, performance, and regulatory compliance of Check Point components
- B. Used to view collected logs and query for information
- C. Used to monitor health, performance, and regulatory compliance of Check Point components using web browser
- D. Used to monitor health, performance, and regulatory compliance of Check Point components

**Answer:** D

#### NEW QUESTION 228

Within SmartConsole, administrators work in sessions. What is the best description of a session?

- A. Sessions are working environments where administrators can make changes without immediately affecting the live environment.
- B. Sessions are only used by managers when reviewing candidate changes submitted by administrator
- C. Managers can Publish the administrators changes.
- D. Sessions are working environments where administrators can not make changes without immediately affecting the live environment.
- E. Sessions are Read Only working environments by default and administrators can view the live environment configuration and logs.

**Answer:** A

#### Explanation:

The correct answer is A. In SmartConsole, a session is a working environment where administrators can make changes without immediately committing them to the published management database or affecting the live enforcement state. Changes remain in the administrator's session until they are published or discarded. Publishing commits changes and creates a revision; installing policy then pushes the published policy to selected gateways. Option B is wrong because sessions are not only for managers, and ordinary administrators work inside sessions depending on their permissions. Option C is the opposite of the real model; sessions specifically prevent every edit from immediately affecting the published configuration. Option D is wrong because sessions are not read-only by default; permissions determine whether the administrator can make changes. This session model is critical in multi-administrator environments because it supports change isolation, review, accountability, publishing, revision comparison, and controlled installation. Reference topics: SmartConsole sessions, Publish, Discard, revisions,

administrator workflow.

#### NEW QUESTION 233

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 238

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 240

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 244

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 245

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 250

.....

## 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/>