

CheckPoint

Exam Questions 156-215.82

Check Point Certified Security Administrator - R82



NEW QUESTION 1

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 2

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

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

Answer: B

NEW QUESTION 3

Which Identity Source provides identity information through Captive Portal login or Transparent Kerberos Authentication?

- A. Browser-Based Authentication
- B. Identity Agents
- C. RADIUS Accounting
- D. AD Query

Answer: A

NEW QUESTION 4

What is a Security Policy?

- A. A collection of rules and settings that control network traffic and enforce the organization guidelines for data protection.
- B. This is stored on the Security Gateway and enforced by the Security Management Server.
- C. This is a written policy which has to conform with the Regulatory Compliance standards.
- D. This is stored on the Security Management Server and enforced by the log server.

Answer: A

Explanation:

The correct answer is A. In Check Point R82, a Security Policy is the rule-based configuration that controls traffic and enforces organizational security requirements, including access to resources and data protection. The official glossary describes a Security Policy as a collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection. Option B reverses the architecture: the policy is configured and managed on the Security Management Server, then installed on Security Gateways for enforcement. The Security Management Server does not enforce production traffic. Option C describes a governance document, which may influence technical policy design, but it is not what SmartConsole calls a Security Policy. Option D is also wrong because a Log Server stores and processes logs; it does not enforce policy. The Security Gateway is the enforcement component. In CCSA terms, this is foundational: administrators define rules, publish changes, and install the policy to gateways, where traffic is actually inspected and acted upon. Reference topics: Security Policy Management, Access Control Policy, Security Gateway enforcement, SmartConsole policy configuration.

NEW QUESTION 5

Which of the following is the default role-based shell on Gaia?

- A. Expert
- B. AdvancedCLI
- C. Supermode
- D. Clish

Answer: D

NEW QUESTION 6

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 7

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

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

Answer: D

Explanation:

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

NEW QUESTION 8

Select the correct description of the Identity Collector.

- A. Acquires identities using Identity Agents installed on user endpoint computer
- B. Acquires identities using Identity Agents installed on Active Directory Domain Controllers, Cisco Identity Services Engine Servers or NetIQ eDirectory Servers
- C. Acquire identities from Identity Agents installed on a Windows-based application server that hosts Terminal Servers, Citrix XenAp
- D. and Citrix XenDesktop services
- E. Acquires identities seamlessly from Microsoft Active Directory

Answer: B

NEW QUESTION 9

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 10

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 10

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

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

Answer: A

NEW QUESTION 15

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 19

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 24

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 28

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 33

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 37

Select the correct policy layer type.

- A. Shared Layer
- B. Inner Layer
- C. Inline Layer
- D. Nested Layer

Answer: C

Explanation:

The correct answer is C. Check Point Access Control policy supports two main layer types: Ordered Layers and Inline Layers. An Inline Layer is attached to a parent rule and is evaluated only when the parent rule matches. This lets administrators create sub-rulebases for more granular inspection after a broad parent condition is satisfied. Option A, Shared Layer, is not a layer type in the same sense; sharing is a property that allows a layer to be reused across rules or policies. Option B, Inner Layer, is not the official Check Point policy-layer type. Option D, Nested Layer, is generic wording and not the official R82 terminology. This distinction is common in CCSA: ordered layers are evaluated sequentially as separate layers, while inline layers are conditional sub-layers inside a matching rule. Reference topics: Policy Layers, Ordered Layers, Inline Layers, Access Control Policy structure.

NEW QUESTION 42

Which tool should be used to display real-time and historical graphical views of traffic and block suspicious network activity while you investigate the traffic?

- A. SmartView Tracker
- B. SmartEvent
- C. SmartView Monitor
- D. SmartView Web Application

Answer: C

Explanation:

The correct answer is C. SmartView Monitor provides real-time and historical graphical views of traffic, system counters, gateway status, and activity. It also supports operational response actions such as blocking specified suspicious traffic while the administrator investigates. Option A, SmartView Tracker, is legacy terminology and not the correct R82 answer for this monitoring function. Option B, SmartEvent, is used for event analysis, correlation, and reporting, but the specific combination of traffic monitoring and immediate blocking during investigation points to SmartView Monitor. Option D, SmartView Web Application, is used for web-based log/report views, not this real-time monitoring and blocking function. The key phrase in the question is ??real-time and historical graphical views of traffic?? combined with ??block suspicious network activity,?? which maps directly to SmartView Monitor??s monitoring and response capabilities. Reference topics: SmartView Monitor, traffic counters, real-time monitoring, blocking specified traffic during investigation.

NEW QUESTION 43

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 47

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

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

Answer: B

NEW QUESTION 49

What control is available in SmartConsole GUI Main Window?

- A. Objects Manager
- B. Objects Explorer
- C. Objects Selector
- D. Objects Menu

Answer: D

Explanation:

The correct answer is D. In the SmartConsole GUI, the Objects menu is one of the available controls used for creating and managing objects. It provides access to object-management capabilities and is part of the administrator??s normal SmartConsole workflow. Option A, ??Objects Manager,?? is not the official SmartConsole control name in this context. Option B is close but imprecise: Object Explorer is a separate object-management tool/window that can be opened for comprehensive object management, but the question asks which control is available in the SmartConsole GUI main window. Option C, ??Objects Selector,?? is not the standard named control being tested. The distinction is important because SmartConsole provides multiple ways to work with objects: the Objects menu, Object Explorer, creation options from Gateways&Servers, and object selection inside rule columns. For this item, the main-window control terminology points to the Objects menu. Reference topics: Object Management, SmartConsole main window, Objects menu, Object Explorer.

NEW QUESTION 53

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 58

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 63

What is the primary benefit of Autonomous Threat Prevention?

- A. It blocks all HTTPS traffic by default
- B. It replaces SSL/TLS with a proprietary protocol
- C. It accelerates encrypted traffic
- D. It simplifies and enhances cybersecurity management by automating the configuration and updating of security policies

Answer: D

NEW QUESTION 64

What is the purpose of the Change Log in SmartConsole?

- A. To install security policies
- B. To manage user sessions
- C. To keep a record of changes made to objects
- D. To monitor network traffic

Answer: C

NEW QUESTION 69

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 71

Which of these is one of the components of Check Point's three-tier architecture?

- A. Security Gateway
- B. Gaia Portal
- C. Firewall Router
- D. CloudGuard Controller

Answer: A

NEW QUESTION 75

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 78

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 80

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 85

What is a best practice for managing SmartConsole administrator accounts?

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

Answer: B

NEW QUESTION 86

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 88

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 90

How should you exit Expert Mode?

- A. by typing the "bye" command
- B. By pressing the and CTRL Keys
- C. by typing the "quit" command
- D. by typing the "exit" command

Answer: D

Explanation:

The correct answer is D. To leave Expert Mode and return to Gaia Clish, the administrator types the exit command. Official R82 Gaia documentation explicitly states that to move from the Expert shell back to Gaia Clish, run exit in Expert Mode. Option A is wrong because bye is not the Gaia Expert Mode exit command being tested. Option B is not a proper or reliable administrative command; keyboard interrupts are not the documented method for leaving Expert Mode. Option C is misleading because quit exits Gaia Clish, while exit exits the current shell context and is the documented way to return from Expert Mode to Gaia Clish. The broader point is that Expert Mode is a privileged shell and should be used carefully. If a task can be done in Gaia Clish, Check Point guidance generally favors Clish because it is role-based and records configuration changes more cleanly. Reference topics: Gaia Clish, Expert Mode, moving between shells.

NEW QUESTION 93

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 98

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 102

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 106

What is one benefit of using the Object Explorer in SmartConsole?

- A. It disables editing of custom objects
- B. It limits access to only default objects
- C. It only supports network objects

D. It allows exporting objects to a CSV file

Answer: D

NEW QUESTION 110

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 114

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

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

Answer: A

NEW QUESTION 118

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 123

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 127

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 129

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

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

Answer: D

Explanation:

The correct answer is D. Sharing layers with other policy packages is a best practice when the same set of controls should be reused consistently across multiple

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

NEW QUESTION 132

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 137

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 140

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 143

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 146

A company wants to allow access to social media sites but block file uploads through those platforms. Which combination of features best supports this requirement?

- A. Application Control and Content Awareness
- B. URL Filtering and NAT features
- C. Identity Awareness and VPN
- D. HTTPS Inspection and Threat Emulation

Answer: A

Explanation:

The correct answer is A. Allowing social media access while blocking file uploads requires two types of control: application/site recognition and content/action awareness. Application Control identifies and controls access to social media applications and services. Content Awareness can match data/content characteristics and help enforce restrictions on what is transferred, such as files or sensitive content. Option B is wrong because NAT changes addresses and ports; it does not control social media upload behavior. Option C is unrelated to the upload-control requirement: Identity Awareness can restrict access by user or group, and VPN secures remote/site connectivity, but they do not directly block uploads on social platforms. Option D is also not the best answer: HTTPS Inspection may be needed to see encrypted upload traffic, and Threat Emulation can inspect suspicious files, but the core policy combination is Application Control plus Content Awareness. Reference topics: Application Control, Content Awareness, Access Control Policy, application/site and content-based enforcement.

NEW QUESTION 150

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 154

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 159

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 161

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 163

What is the correct default permission profile?

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

Answer: D

NEW QUESTION 166

What is the advantage of Autonomous Threat Prevention?

- A. cheaper licenses than classis threat prevention
- B. less resource consumption than classis 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 167

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 170

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 174

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 179

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

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

Answer: C

NEW QUESTION 183

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 188

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

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

Answer: C

NEW QUESTION 191

What is the purpose of the Cleanup Rule in a security policy?

- A. To accept all unmatched traffic
- B. To log all security events
- C. To block all known malicious traffic
- D. To drop or reject all traffic that does not match any rule in the rulebase

Answer: D

Explanation:

The correct answer is D. A Cleanup Rule is placed at the bottom of a rulebase or layer to handle traffic that did not match any earlier explicit rule. In a secure Access Control Policy, its usual purpose is to drop or reject all unmatched traffic and, as a best practice, log that traffic for investigation. Option A is the opposite of a secure cleanup rule because accepting unmatched traffic defeats positive-control policy design. Option B is incomplete: cleanup rules can log unmatched traffic, but logging is not the primary enforcement action. Option C is wrong because ??known malicious traffic?? is handled primarily by Threat Prevention protections; the cleanup rule deals with unmatched traffic, whether malicious or simply unauthorized. The cleanup rule is important because it makes the default-deny posture visible and auditable rather than relying silently on an implicit cleanup rule. Reference topics: Cleanup Rule, Explicit Cleanup Rule, Access Control Policy, positive-control firewall model.

NEW QUESTION 195

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 198

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 201

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 205

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 206

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 207

Session Management Controls include:

- A. Session Comments
- B. Session Import/Export
- C. Session Save
- D. Session Name

Answer: A

NEW QUESTION 212

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 217

What is the best practice for installing the security policy?

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

Answer: C

NEW QUESTION 218

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

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

Answer: C

NEW QUESTION 219

Which Identity Awareness client is used in high-volume environments that use Microsoft Active Directory, Cisco Identity Services, NetIQ eDirectory, or Syslog?

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

Answer: B

NEW QUESTION 223

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 226

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 229

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 230

Which tool is used to create and manage Security Policies?

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

Answer: A

NEW QUESTION 235

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 240

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 245

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

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

Answer: A

NEW QUESTION 249

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

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

Answer: B

NEW QUESTION 251

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 253

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 256

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 257

What should be added at the end of each Ordered Layer?

- A. Implicit Cleanup Rule
- B. Explicit Cleanup Rule
- C. Logging Rule
- D. NAT Rule

Answer: B

NEW QUESTION 258

Select one of the Common Types of Policies.

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

Answer: D

NEW QUESTION 260

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 265

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 267

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 271

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 276

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

156-215.82 Practice Exam Features:

- * 156-215.82 Questions and Answers Updated Frequently
- * 156-215.82 Practice Questions Verified by Expert Senior Certified Staff
- * 156-215.82 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 156-215.82 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 156-215.82 Practice Test Here](#)