

CheckPoint

Exam Questions 156-215.82

Check Point Certified Security Administrator - R82



NEW QUESTION 1

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

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

Answer: B

NEW QUESTION 2

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 3

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 4

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 5

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 6

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

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

Answer: B

NEW QUESTION 7

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

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

Answer: A

NEW QUESTION 8

What is the 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 9

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 10

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 10

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 15

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 18

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 23

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 28

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

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

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

Answer: A

NEW QUESTION 39

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 44

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 45

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 49

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 52

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 53

What is the command line to verify the backup was created?

- A. show backup last-successful
- B. show backup list-successful

- C. show backup successful
- D. show backups

Answer: D

NEW QUESTION 57

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

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

Answer: D

NEW QUESTION 59

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 64

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 66

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 70

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 73

Identify the default username and password for a newly installed Check Point appliance.

- A. admin/password
- B. admin/Chkp1234
- C. cadmin/cadmin
- D. admin/admin

Answer: D

NEW QUESTION 75

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 79

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 81

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 84

When should you enable log indexing on a Standalone Deployment?

- A. Log indexing is enabled by default on all deployments
- B. only when the standalone computer CPU has 8 or more cores
- C. Log indexing is disabled by default only on Bridge mode deployments
- D. only when the standalone computer CPU has 4 or more cores

Answer: D

Explanation:

The correct answer is D. Official R82 Logging and Monitoring documentation states that in a standalone deployment, log indexing is disabled by default and should be enabled only if the standalone server CPU has 4 or more cores. Option A is false because standalone is the explicit exception to default-enabled log indexing. Option B is too strict; the official threshold is four cores, not eight. Option C is wrong because Bridge mode is not the deployment category for this log-indexing default. Log indexing improves log query speed, but it consumes CPU and disk resources. In a standalone deployment, the same machine acts as management/log server and Security Gateway, so enabling indexing without adequate resources can hurt gateway performance. The practical exam takeaway is direct: distributed management/logging normally supports indexing by default; standalone requires a resource check before enabling indexing. Reference topics: Log Indexing, Standalone deployment, log query performance, CPU requirements.

NEW QUESTION 86

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 90

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 92

When is a new Revision created?

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

Answer: C

NEW QUESTION 95

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 97

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 99

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 103

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 104

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 109

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 111

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 112

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 116

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 119

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 124

Select the correct predefined profile of the Autonomous Threat Prevention.

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

Answer: B

NEW QUESTION 128

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 133

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 135

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

- A. HTTPS Inspection and Content Awareness.
- B. Integration with an OPSEC-certified AAA Server
- C. HTTPS Inspection and Data Integrity Checking.
- D. OPSEC-certified Reporting Server using LEA and ELA interfaces for bidirectional communication with the Management Server.

Answer: A

NEW QUESTION 140

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 142

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 143

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 146

Which tool is used to create and manage Security Policies?

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

Answer: A

NEW QUESTION 149

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

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

Answer: A

NEW QUESTION 154

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 157

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 159

Select one of the Common Types of Policies.

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

Answer: D

NEW QUESTION 162

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 164

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 168

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

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

Answer: B

Explanation:

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

NEW QUESTION 172

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 175

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 180

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

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

Answer: A

NEW QUESTION 183

What is the primary purpose of the Access Control Policy?

- A. To control access to network resources
- B. To monitor network traffic
- C. To provide threat prevention
- D. To manage user accounts

Answer: A

NEW QUESTION 188

.....

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](#)