

CheckPoint

Exam Questions 156-215.82

Check Point Certified Security Administrator - R82



NEW QUESTION 1

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

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

Answer: A

Explanation:

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

NEW QUESTION 2

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

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

Answer: D

NEW QUESTION 3

Where is it possible to view SmartConsole locked account?

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

Answer: A

Explanation:

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

NEW QUESTION 4

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

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

Answer: B

NEW QUESTION 5

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 6

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

- A. Identity Agent for a User Endpoint Computer

- B. Identity Agent for a Terminal Server v2
- C. Identity Agent for a Terminal Server
- D. Identity Collector

Answer: D

NEW QUESTION 7

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 8

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

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

Answer: A

NEW QUESTION 9

What is the purpose of Dynamic Objects in SmartConsole?

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

Answer: A

NEW QUESTION 10

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

What are the default zone objects?

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

Answer: A

NEW QUESTION 14

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 16

What is the most appropriate statement about methods of managing objects in SmartConsole?

- A. Objects can be managed by various methods like New Menu in Gateways & Servers, Objects Menu, Object Explorer, or, Rules in the Security Policy
- B. Only Gateway and Management Objects are managed from the New Menu in Gateways and Server
- C. All other objects can be managed from Objects Menu or Object Explore
- D. Objects can only be selected in the Rules in Security Policy
- E. Objects can only be managed from the Object Explorer, however they can be viewed in the Rules in Security Policy
- F. Objects can be management either from Objects Menu or from Object Explore
- G. All other methods including the Rules in Security Policy are for view only

Answer: A

NEW QUESTION 21

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 24

What of the following is NOT an Identity Source supported by the Check Point Identity Awareness Blade?

- A. Remote Access and Terminal Servers.
- B. Identity Connector and TACACS
- C. Browser-Based Authentication and AD Query.
- D. RADIUS Accounting, Identity Collector.

Answer: B

NEW QUESTION 25

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 29

Which type of object represents Office365?

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

Answer: A

NEW QUESTION 31

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 33

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 38

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 39

Which profile is optimized for protecting east-west traffic in cloud and on-premises data centers?

- A. Cloud/Data Center
- B. Internal Network
- C. Guests Network
- D. Perimeter

Answer: A

NEW QUESTION 41

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

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

Answer: C

Explanation:

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

NEW QUESTION 44

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 47

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 50

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

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

Answer: C

NEW QUESTION 51

Primary capabilities of Autonomous Threat Prevention include the following

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

Answer: A

Explanation:

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

NEW QUESTION 54

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 60

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 65

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

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

Answer: A

Explanation:

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

SmartConsole connection. Reference topics: SmartConsole sessions, Publish, Discard, administrator logout, session workflow.

NEW QUESTION 66

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

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

Answer: C

NEW QUESTION 69

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 71

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

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

Answer: A

NEW QUESTION 76

What are the capabilities integrated into a Threat Prevention Policy?

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

Answer: B

NEW QUESTION 77

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 79

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 82

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 84

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 87

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 88

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 92

What is the primary purpose of SmartConsole Objects?

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

Answer: D

Explanation:

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

NEW QUESTION 97

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

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

Answer: D

NEW QUESTION 101

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 105

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 106

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 110

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 111

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

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

Answer: B

NEW QUESTION 115

What provides the trusted client option in SmartConsole?

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

D. IP address(es) allowed to connect to the Security Gateway(s)

Answer: B

Explanation:

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

NEW QUESTION 120

What is the purpose of the Explicit Default Cleanup Rule?

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

Answer: C

NEW QUESTION 123

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 128

What is the correct default permission profile?

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

Answer: D

NEW QUESTION 132

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

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

Answer: A

NEW QUESTION 135

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

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

Answer: C

NEW QUESTION 136

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 141

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 142

What is one main purpose of URL Filtering?

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

Answer: D

NEW QUESTION 147

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 148

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 151

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 155

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

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

Answer: B

NEW QUESTION 158

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 160

What is a recommended best practice after deploying Autonomous Threat Prevention?

- A. Regularly monitor logs and reports for unusual activity
- B. Use the same profile for all network segments
- C. Disable logging to improve performance
- D. Avoid customizing any profiles

Answer: A

NEW QUESTION 165

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

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

Answer: B

NEW QUESTION 166

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

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

Answer: D

Explanation:

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

NEW QUESTION 167

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 172

What are the predefined Autonomous Threat Prevention Profiles?

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

Answer: B

NEW QUESTION 177

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

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

Answer: C

NEW QUESTION 178

With URL Filtering you can:

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

Answer: B

NEW QUESTION 181

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 182

Which statement best describes Trusted Clients?

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

Answer: B

NEW QUESTION 185

Which tool is used to create and manage Security Policies?

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

Answer: A

NEW QUESTION 187

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 189

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

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

Answer: A

Explanation:

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

NEW QUESTION 190

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

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

Answer: B

NEW QUESTION 192

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 194

Select one of the Common Types of Policies.

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

Answer: D

NEW QUESTION 196

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 197

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 200

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 202

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 205

Select the correct description of the Outbound HTTPS Inspection.

- A. It protects internal servers by Man in the Middle style interception

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

Answer: B

Explanation:

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

NEW QUESTION 206

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

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

Answer: C

NEW QUESTION 209

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

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

Answer: C

Explanation:

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

NEW QUESTION 214

.....

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](#)