PassQueen
a.k.a dumpsqueen.com

Check Point Certified Security Administrator R81.20

Checkpoint 156-215.81

Version Demo

Total Demo Questions: 38

Total Premium Questions: 389

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, System Management	153
Topic 2, Security Policies	87
Topic 3, Security Gateway	83
Topic 4, Traffic Visibility	22
Topic 5, Threat Prevention	24
Topic 6, VPN	20
Total	389

QUESTION NO: 1

You have enabled "Extended Log" as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

A. Identity Awareness is not enabled.

B. Log Trimming is enabled.

C. Logging has disk space issues

D. Content Awareness is not enabled.

ANSWER: D

Explanation:

Content Awareness is not enabled. Extended Log tracking instructs the Security Gateway to produce a richer log record, but it does not itself inspect content or identify data types. Data-type details are generated by the Content Awareness Software Blade, which examines traffic according to configured Content Awareness rules and recognizes defined data types, such as files, documents, or custom data patterns. Therefore, enabling Extended Log alone cannot populate a log entry with data-type information.

To obtain these details, Content Awareness must be enabled on the applicable Security Gateway and a policy must inspect the relevant traffic with the required data types selected. The rule must also be logged so that the inspection result is sent to the Log Server/SmartConsole. Once content inspection is active and matching traffic is processed, Extended Log can display the additional fields associated with that inspection, including identified data-type information where applicable. Check Point describes Content Awareness as the blade responsible for controlling and inspecting content according to data types and related rules. See the Check Point R81 Content Awareness documentation and the R81 tracking-options documentation.

QUESTION NO: 2

Which actions are required to make a new Threat Prevention rule effective on a Security Gateway? (Select two.)

A. Publish the SmartConsole session.

B. Install the Threat Prevention policy on the target gateway.

C. Run `save config` in Gaia CLISH.

D. Reboot the Security Gateway.

ANSWER: A B

Explanation:

After adding or modifying a Threat Prevention rule, the administrator must publish the SmartConsole session so that the changes become part of the shared management database. The applicable Threat Prevention policy must then be installed on the target Security Gateway for enforcement to change.

Saving the Gaia configuration is unrelated to SmartConsole policy changes. Restarting the gateway is not normally required after a Threat Prevention policy installation.

See the Check Point R81 Threat Prevention Policy documentation.

QUESTION NO: 3

In SmartEvent, a correlation unit (CU) is used to do what?

A. Collect security gateway logs, Index the logs and then compress the logs.

B. Receive firewall and other software blade logs in a region and forward them to the primary log server.

C. Analyze log entries and identify events.

D. Send SAM block rules to the firewalls during a DOS attack.

ANSWER: C

Explanation:

“Analyze log entries and identify events.” is correct because the SmartEvent Correlation Unit is the SmartEvent component that processes incoming log data and applies correlation logic to it. Rather than simply retaining individual records, it examines related log entries to recognize patterns, consolidate relevant activity, and generate meaningful security events. This lets administrators investigate potentially significant activity as an event instead of manually reviewing large volumes of separate gateway and Software Blade logs.

In a SmartEvent deployment, the Correlation Unit receives log information from Log Servers, analyzes the logs according to SmartEvent’s event definitions and correlation rules, and sends the resulting event information to the SmartEvent Server. The SmartEvent Server then stores and presents those events through SmartConsole views, reports, and monitoring tools. This correlation process is central to SmartEvent’s purpose: turning raw operational and security logs into actionable event data that can be prioritized and investigated efficiently.

Check Point describes the Correlation Unit’s role in its SmartEvent Correlation Unit documentation. Additional SmartEvent architecture and administration context is available in the R81.20 Logging and Monitoring Administration Guide.

QUESTION NO: 4

Which path below is available only when CoreXL is enabled?

A. Slow path

B. Firewall path

C. Medium path

D. Accelerated path

ANSWER: C

Explanation:

Medium path is available only when CoreXL is enabled. CoreXL distributes firewall processing across multiple CPU cores by assigning traffic handling to Firewall Worker instances. The medium path is the processing route used for connections that cannot remain fully accelerated by SecureXL but can still benefit from CoreXL’s multicore Firewall Worker processing. This enables traffic to be inspected by the Firewall in a more scalable way than a single-core processing model while retaining the required security checks and connection-state handling.

In Check Point’s acceleration architecture, a connection can be handled through different processing paths according to its characteristics and whether it is eligible for acceleration. The medium path specifically depends on the CoreXL architecture because its purpose is to pass traffic to the applicable CoreXL Firewall Worker for processing. Therefore, it does not exist as an available path when CoreXL is disabled. Administrators can use performance-monitoring and diagnostic tools to observe acceleration and CoreXL behavior when validating gateway throughput and tuning a deployment.

See Check Point’s Medium Path documentation and the CoreXL documentation.

QUESTION NO: 5

Which statements about a user-defined service object in SmartConsole are correct? (Select two.)

A. It can define a TCP or UDP destination port or port range.

B. It can be reused in multiple Access Control rules.

C. Creating it automatically permits the service through all gateways.

D. It assigns an IP address to a network object.

ANSWER: A B

Explanation:

A user-defined service object represents a protocol and port or port range that can be used in policy rules. For a TCP or UDP service, the service object specifies the applicable protocol and destination port information. Service objects can then be reused in Access Control rules, which improves consistency and simplifies administration.

Creating a service object alone does not open a port on the gateway; the object must be used in an installed policy rule. A service object also does not assign an IP address to a host or gateway interface.

See the Check Point R81 Services and Applications documentation.

QUESTION NO: 6

You are going to perform a major upgrade. Which back up solution should you use to ensure your database can be restored on that device?

A. backup

B. logswitch

C. Database Revision

D. snapshot

ANSWER: D

Explanation:

snapshot is the appropriate backup solution when preparing a device for a major upgrade and needing a reliable restore point on that device. A Gaia snapshot creates a binary image of the system's root disk partition, including the installed Check Point software, Gaia operating-system components, and the current configuration. This provides a complete rollback mechanism: if the upgrade does not complete as expected, the administrator can restore the snapshot and return the appliance to the captured pre-upgrade state.

Snapshots are particularly useful for upgrade planning because they preserve substantially more than policy or management-database content. They capture the appliance system state required to restore the environment as it existed when the snapshot was taken. Check Point supports exporting and importing snapshots between machines of the same type, subject to the applicable version and platform requirements. Administrators should account for the fact that the log partition is not part of a snapshot, so locally stored logs require separate retention if they are needed after recovery. See Check Point's Gaia Administration Guide: Managing Snapshots and the R81 Installation and Upgrade Guide.

QUESTION NO: 7

DLP and Geo Policy are examples of what type of Policy?

A. Inspection Policies

B. Shared Policies

C. Unified Policies

D. Standard Policies

ANSWER: B

Explanation:

DLP and Geo Policy are examples of **Shared Policies** in Check Point SmartConsole. A shared policy is designed to hold rules that can be reused and applied consistently where the same inspection or enforcement requirements are needed. This approach centralizes administration: an administrator maintains the common policy logic in one place rather than duplicating equivalent controls throughout separate policy configurations.

Data Loss Prevention is a clear use case for a shared policy because its rules define how sensitive information is detected and handled across protected traffic. Geo Policy likewise represents reusable geographic controls, allowing administrators to consistently enforce location-based restrictions. By treating these as shared policies, SmartConsole supports modular policy design and helps ensure that common protections are managed uniformly across the relevant security configuration.

Check Point's Security Gateway documentation discusses policy configuration and the policy components available for inspection and enforcement. See the official Check Point Next Generation Security Gateway Guide and the Check Point documentation portal for product documentation.

QUESTION NO: 8

Before enabling HTTPS Inspection for outbound traffic, which items should an administrator plan or configure? (Select three.)

A. An HTTPS Inspection certificate for the gateway.

B. Distribution of the trusted CA certificate to inspected clients.

C. HTTPS Inspection policy rules.

D. A separate ClusterXL synchronization interface.

E. Conversion of all outbound HTTPS services to TCP port 80.

ANSWER: A B C

Explanation:

HTTPS Inspection decrypts applicable TLS sessions so that enabled security blades can inspect the traffic. The gateway needs an HTTPS Inspection certificate, and endpoint browsers must trust the issuing CA certificate to avoid certificate warnings. The HTTPS Inspection policy must also define the traffic to inspect, bypass, or block. Administrators should carefully define bypass rules for traffic that should not be decrypted, based on organizational and legal requirements.

See HTTPS Inspection in the R81 Security Management Administration Guide.

QUESTION NO: 9

To enforce the Security Policy correctly, a Security Gateway requires:

A. a routing table

B. awareness of the network topology

C. a Demilitarized Zone

D. a Security Policy install

ANSWER: B

Explanation:

Awareness of the network topology is required because the Security Gateway must know which networks and hosts are considered internal, external, or located in a DMZ in relation to each of its interfaces. Check Point uses the gateway topology definition to apply anti-spoofing protections. These protections validate that the source address of traffic arriving on an interface is plausible for that interface and is not claiming to originate from a network that should be reachable through another interface. This contextual understanding allows the gateway to enforce access-control decisions with the intended network boundaries and to identify traffic that attempts to impersonate trusted internal addresses.

In SmartConsole, administrators define the topology of gateway interfaces and the networks behind them. The resulting information is part of the gateway configuration used when policy is installed and evaluated. Accurate topology is particularly important where a gateway protects multiple internal segments, such as LAN and DMZ networks, because it establishes the trusted address ranges and expected traffic direction for each interface. Check Point documents interface topology and anti-spoofing configuration in its Security Management Administration Guide and provides general product documentation through the Check Point Documentation Portal.

QUESTION NO: 10

What is UserCheck?

A. Messaging tool user to verify a user's credentials

B. Communication tool used to inform a user about a website or application they are trying to access

C. Administrator tool used to monitor users on their network

D. Communication tool used to notify an administrator when a new user is created

ANSWER: B

Explanation:

UserCheck is a Check Point communication mechanism that provides immediate, contextual information to an end user when a Security Gateway policy affects the user's attempt to access a website or application. It can display a customizable message explaining the relevant policy, such as an organization's acceptable-use requirements, and can give the user a way to continue only after acknowledging the message where the configured policy permits this. UserCheck is therefore intended to make security-policy enforcement visible and understandable at the point of access, rather than merely blocking traffic without feedback.

The message can be presented through a web browser for web traffic or through the UserCheck client for supported non-web applications. In R81, UserCheck is associated with access-control and application-control policy actions, allowing administrators to educate users and communicate the reason for access restrictions or required acknowledgement. This behavior matches "Communication tool used to inform a user about a website or application they are trying to access." Check Point's R81 Next Generation Security Gateway Administration Guide describes UserCheck and its use in policy enforcement: Check Point R81 UserCheck documentation.

QUESTION NO: 11

Which of the following situations would not require a new license to be generated and installed?

A. The Security Gateway is upgraded.

B. The existing license expires.

C. The license is upgraded.

D. The IP address of the Security Management or Security Gateway has changed.

ANSWER: A

Explanation:

The Security Gateway is upgraded. A Check Point software upgrade changes the gateway software version but does not, by itself, change the licensing identity or invalidate the license already installed on the gateway. Check Point licenses are entitlement-based and are installed on the applicable management server or gateway; moving to a later supported software release normally preserves the existing license, provided that the underlying licensed product, appliance, and applicable support or subscription entitlement remain valid. Administrators should confirm upgrade compatibility and make the usual upgrade backups, but generating and installing a replacement license is not a standard requirement solely because the Security Gateway is upgraded. This behavior supports normal lifecycle maintenance: an organization can upgrade a gateway to a newer Check Point release without treating the software upgrade as a licensing rehost event. Check Point's licensing resources describe license management and entitlement handling, while the Security Gateway administration documentation covers standard upgrade procedures. See the Check Point Licensing page and the R81.20 Installation and Upgrade Guide.

QUESTION NO: 12

What are the three main components of Check Point security management architecture?

A. SmartConsole, Security Management Server, and Security Gateway

B. Smart Console, Standalone, and Security Management

C. SmartConsole, Security policy, and Logs & Monitoring

D. GUI-Client, Security Management, and Security Gateway

ANSWER: A

Explanation:

SmartConsole, Security Management Server, and Security Gateway are the three principal components in the Check Point security management architecture. SmartConsole is the administrator's graphical client application. It is used to define and manage objects, configure access-control and threat-prevention policies, install policy, and review monitoring information. The Security Management Server is the central management component: it maintains the management database, including policies, objects, administrators, and configuration information, and distributes the applicable policy to managed gateways. The Security Gateway is the enforcement point deployed at the network boundary or within protected network segments. It receives the installed policy from the Security Management Server and inspects traffic to enforce the configured security controls. This separation of administration, centralized policy management, and traffic enforcement is fundamental to the distributed Check Point architecture and enables consistent security policy across one or many gateways. Check Point's Security Management Administration Guide describes the roles of the Security Management Server and Security Gateways, while the SmartConsole documentation covers the client used to administer them. See the Check Point Security Management Administration Guide and SmartConsole Administration Guide.

QUESTION NO: 13

Which statements about an inline layer in an R81 Access Control policy are correct? (Select two.)

A. It is evaluated after traffic matches its parent rule.

B. Its rules are evaluated from top to bottom.

C. It is always evaluated before every ordered policy layer.

D. A matching parent rule automatically accepts the connection.

ANSWER: A B

Explanation:

An inline layer is attached to a parent rule and is evaluated only when traffic matches that parent rule. Within the inline layer, rules are evaluated from top to bottom. This lets administrators place detailed exceptions or additional controls under a broader parent rule while keeping the primary policy layer organized.

An inline layer is not evaluated independently as a separate top-level layer, and a match in the parent rule does not automatically mean the traffic is accepted; the action in the matching inline-layer rule determines the result.

See Check Point R81 Policy Layers documentation.

QUESTION NO: 14

Which statements describe the purpose of Check Point SIC? (Select two.)

A. It authenticates communication between Check Point management components and gateways.

B. It uses certificates issued by the Internal Certificate Authority.

C. It encrypts all user traffic passing through the Security Gateway.

D. It replaces the need for an administrator account in SmartConsole.

E. It uses the activation password as the permanent tunnel key.

ANSWER: A B

Explanation:

Secure Internal Communication (SIC) establishes a trusted and authenticated communication channel between Check Point components, such as a Security Management Server and a Security Gateway. SIC uses certificates issued through the Internal Certificate Authority and is required for management operations such as policy installation. The one-time activation password is used when establishing SIC; it is not used as the ongoing communication credential.

See Secure Internal Communication in the R81 Security Management Administration Guide.

QUESTION NO: 15

Which of the following is NOT a tracking option? (Select three)

A. Partial log

B. Log

C. Network log

D. Full log

ANSWER: A C D

Explanation:

In an R81 Security Policy rule, the Track column controls what Check Point does when traffic matches the rule, including whether it creates a log entry or initiates a configured notification or accounting action. **Partial log**, **Network log**, and **Full log** are not named Track options in SmartConsole and therefore are correctly selected as items that are not tracking options. Check Point logging does not use a partial-versus-full or network-log classification as selectable values in the rule's Track field.

The valid logging-related Track choice is **Log**. Additional supported choices can include logging variants such as Extended Log or Detailed Log, accounting, alerting, SNMP traps, and user-defined alert actions, depending on the configuration and installed components. These options determine the type of event handling performed after the rule match; they are not arbitrary labels for different log completeness levels. Check Point's Security Management Administration Guide describes configuring rule tracking through the Track column and the available log, alert, and accounting actions. See the Check Point R81 Tracking documentation and the Access Control Policy documentation.

QUESTION NO: 16

When an Admin logs into SmartConsole and sees a lock icon on a gateway object and cannot edit that object, what does that indicate?

A. The gateway is not powered on.

B. Incorrect routing to reach the gateway.

C. The Admin would need to login to Read-Only mode

D. Another Admin has made an edit to that object and has yet to publish the change.

ANSWER: D

Explanation:

Another Admin has made an edit to that object and has yet to publish the change. SmartConsole uses sessions to allow multiple administrators to work on the Security Management Server at the same time without unintentionally overwriting one another's work. When an administrator modifies an object, such as a gateway object, that object is locked for editing by other administrators for the duration of the first administrator's active session. The lock icon communicates that the object has pending changes owned by another session, so its configuration cannot be changed from the current administrator's session.

The administrator who owns the session can continue editing and then publish the session to commit the changes to the management database, or discard the session to remove the pending changes. Once the changes are published or discarded, the object is no longer held by that session and other authorized administrators can edit it. This behavior is part of SmartConsole's session-management and concurrent-administration controls; it is unrelated to the gateway's power state, connectivity, or routing. Check Point documents the session workflow, including publishing and discarding changes, in its Security Management Administration Guide: Session Management. Additional SmartConsole administration guidance is available from the Check Point Documentation Portal.

QUESTION NO: 17

Which firewall daemon is responsible for the FW CLI commands?

A. fwd

B. fwm

C. cpm

D. cpd

ANSWER: A

Explanation:

fwd is the Firewall Daemon and is responsible for processing Firewall-related command-line operations, including the `fw` CLI command family. On a Security Gateway, it operates as a core component of the enforcement infrastructure and communicates with the kernel-level firewall processes to obtain status, connections, policy-related information, and other operational data requested by administrative commands. Commands such as `fw stat`, `fw monitor`, and `fw tab` rely on the Firewall Daemon to interact with the running Check Point security services and return their results.

The daemon is normally started automatically as part of the Check Point services on the gateway. Administrators can inspect its state with Check Point process-status commands, such as `cpwd_admin list`, when troubleshooting command execution or gateway-service availability. Check Point documents the Firewall Daemon as a principal Security Gateway process and describes the `fw` command as the command-line utility for firewall and Security Gateway operations. See the Check Point Processes documentation and the FW Firewall Commands reference.

QUESTION NO: 18

An administrator can use section titles to more easily navigate between large rule bases. Which of these statements is FALSE?

A. Section titles are not sent to the gateway side.

B. These sections are simple visual divisions of the Rule Base and do not hinder the order of rule enforcement.

C. A Sectional Title can be used to disable multiple rules by disabling only the sectional title.

D. Sectional Titles do not need to be created in the SmartConsole.

ANSWER: D

Explanation:

“Sectional Titles do not need to be created in the SmartConsole.” is the false statement. In the standard SmartConsole policy-management workflow, an administrator creates a section directly in the Access Control Rule Base by adding a section title and then placing rules within that section. The section title is therefore a Rule Base organizational item that is configured from SmartConsole; it is not an independently discovered or automatically created policy element on the Security Gateway.

Sections help administrators manage large policies by grouping related rules under a meaningful heading. SmartConsole can collapse or expand these groups for easier navigation, and section-level administrative actions can be applied to the rules grouped beneath the title. The section remains part of the management-side presentation and policy-editing experience, while the gateway receives the resulting rule policy when it is installed. Check Point’s Security Management Administration Guide describes the SmartConsole Rule Base workflow and the use of sections to organize rules. See Check Point R81 Security Management Administration Guide: Access Control Rules and Check Point SmartConsole overview.

QUESTION NO: 19

Which statements about the implied rules in an R81 Access Control policy are correct? (Select two.)

A. They support required Check Point control and management communications.

B. Relevant settings are configured in Global Properties.

C. They can be edited directly as standard rules in the Access Control rule base.

D. They are created only after an administrator enables Identity Awareness.

ANSWER: A B

Explanation:

Implied rules are automatically generated rules that enable required Check Point services and management functions, such as communication between Security Gateways and the Security Management Server. Administrators configure relevant implied-rule settings in the Global Properties of SmartConsole.

Implied rules are not ordinary administrator-created rules in the visible policy rule base. Their placement and behavior depend on the specific implied rule and its configured setting; they should be reviewed carefully because they can affect traffic that is not explicitly represented by a visible rule.

See Check Point R81 Global Properties documentation.

QUESTION NO: 20

What is NOT an advantage of Stateful Inspection?

A. High Performance

B. Good Security

C. No Screening above Network layer

D. Transparency

ANSWER: C

Explanation:

No Screening above Network layer is not an advantage of Stateful Inspection. Check Point Stateful Inspection evaluates traffic in context rather than making a decision from an isolated packet header. The Security Gateway maintains connection state in its state table and can determine whether a packet belongs to a valid, permitted session. This lets policy enforcement consider protocol behavior and traffic information beyond only basic network-layer addressing and routing details.

In practical terms, Stateful Inspection is designed to apply security controls to connections and services while tracking session establishment, continuation, and termination. The ability to inspect and enforce policy for traffic at and above the network layer is a core reason stateful firewalls provide more meaningful access control than devices limited to simple network-layer packet filtering. Therefore, an absence of screening above the network layer describes a limitation, not a benefit, of the technology.

Check Point describes Access Control as the policy mechanism that inspects and controls traffic through Security Gateways, while its Stateful Inspection technology provides context-aware enforcement for connections. See the Check Point R81 Security Management Administration Guide and Check Point Next-Generation Firewall overview.

QUESTION NO: 21

What is the default tracking option of a rule?

A. Tracking

B. Log

C. None

D. Alert

ANSWER: B

Explanation:

The default tracking option for a newly created Access Control rule is **Log**. In Check Point SmartConsole, the Track column determines whether traffic that matches a rule generates a log entry. With the default Log setting, the Security Gateway records relevant connection and rule-match information, making the activity available for investigation in the Logs & Monitor view. This default supports operational visibility from the outset: administrators can confirm that a rule is being matched, review source and destination details, identify the applicable service, and correlate events during troubleshooting or security analysis.

Tracking is configured per rule in the Access Control policy and is enforced when the policy is installed on the Security Gateway. Administrators can subsequently tailor the tracking behavior to their operational needs, but a standard new rule begins with Log selected. Check Point documents the available rule tracking settings and their behavior in its R81 Logging and Monitoring Administration Guide: Tracking Options. Additional context on configuring rules and their Track settings is available in the R81 Security Management Administration Guide: Access Control Policy.

QUESTION NO: 22

Which statements about an Access Role in an Access Control policy are correct? (Select two.)

A. It can include users or user groups.

B. It can be used in the Source column of an Access Control rule.

C. It replaces the need to enable Identity Awareness on the gateway.

D. It can be used only in Threat Prevention rules.

E. It assigns an IP address to an authenticated user.

ANSWER: A B

Explanation:

An Access Role is an object that can combine identity-related criteria, such as users, groups, machines, and network locations. An administrator can use an Access Role in the Source column of an Access Control rule to apply policy based on identity rather than only on an IP address. Identity Awareness must be enabled and an applicable identity source must identify users or computers for identity-based matching to occur.

See Access Roles in the R81 Identity Awareness Administration Guide.

QUESTION NO: 23

What default layers are included when creating a new policy layer?

A. Application Control, URL Filtering and Threat Prevention

B. Access Control, Threat Prevention and HTTPS Inspection

C. Firewall, Application Control and IPSec VPN

D. Firewall, Application Control and IPS

ANSWER: B

Explanation:

Access Control, Threat Prevention and HTTPS Inspection are the default policy layers provided for a newly created policy package in SmartConsole. Together, these layers establish the standard structure for defining and enforcing Security Gateway protections. The Access Control layer is used to define permitted and blocked traffic according to network objects, services, users, applications, URLs, and other matching criteria. The Threat Prevention layer supplies the policy framework for the enabled threat-prevention protections, such as IPS, Anti-Bot, Anti-Virus, Threat Emulation, and Threat Extraction. The HTTPS Inspection layer provides rules governing whether encrypted HTTPS traffic is inspected, enabling applicable security protections to evaluate traffic after decryption when inspection is configured. These distinct layers support ordered and organized policy evaluation while allowing administrators to manage connectivity controls, threat controls, and encrypted-traffic inspection separately. Check Point describes policy layers and their ordered evaluation in the R81 Security Management Administration Guide. HTTPS inspection policy configuration is documented in the R81 Threat Prevention Administration Guide.

QUESTION NO: 24

Log query results can be exported to what file format?

A. Word Document (docx)

B. Comma Separated Value (csv)

C. Portable Document Format (pdf)

D. Text (txt)

ANSWER: B

Explanation:

Comma Separated Value (csv) is the correct export format for log query results in Check Point SmartConsole. After an administrator runs a query in the Logs & Monitor view, the displayed results can be exported for use outside SmartConsole. CSV is a structured, plain-text tabular format: each log entry can be represented as a row, while selected log fields are represented as comma-delimited columns. This makes the exported data practical for review, filtering, reporting, archival, or import into spreadsheet and analysis tools such as Microsoft Excel. The export is intended to preserve query-result data in a portable format rather than to create a formatted document or report. Check Point describes log viewing, querying, and result handling in its Security Management administration documentation; see the R81.20 Security Management Administration Guide: Logs. SmartConsole's central role in reviewing and managing log information is also documented in the R81.20 SmartConsole Administration Guide: Logs. Therefore, exporting queried log results as CSV is the supported and appropriate format.

QUESTION NO: 25

Which statements about a Check Point Security Management Server backup created with `backup` are correct? (Select two.)

A. It includes Gaia operating-system configuration.

B. It includes Check Point product configuration.

C. It is the preferred method for importing a management database into a newer major release.

D. It can be installed directly as a policy package on a Security Gateway.

ANSWER: A B

Explanation:

The `backup` utility creates a backup of both the Check Point configuration and the Gaia operating-system configuration. It is intended to restore a server to the same or compatible platform and release context, rather than to perform a cross-version management migration.

For moving management data to another server or release, the migration export/import workflow is normally used. A `backup` archive is not simply a policy package that can be installed on a gateway.

See the Check Point R81 Backup and Restore documentation.

QUESTION NO: 26

Which actions are appropriate when a Security Gateway cannot establish SIC with its Security Management Server? (Select two.)

A. Verify IP connectivity between the gateway and Management Server.

B. Verify the SIC activation password used during initialization.

C. Reset SIC and initialize it again when rebuilding trust is required.

D. Disable the Access Control policy permanently.

E. Reinstall Gaia before checking connectivity.

ANSWER: A B C

Explanation:

First verify basic IP connectivity and name resolution, where DNS names are used, between the gateway and the management server. Also verify that the SIC activation password entered during initialization matches the password configured for the gateway object. If SIC was previously established and must be rebuilt, reset SIC in SmartConsole and

initialize SIC again on the gateway using a newly defined activation password. Reinstalling the operating system is not a normal SIC troubleshooting step.

See Secure Internal Communication in the R81 Security Management Administration Guide.

QUESTION NO: 27

URL Filtering employs a technology, which educates users on web usage policy in real time. What is the name of that technology?

A. WebCheck

B. UserCheck

C. Harmony Endpoint

D. URL categorization

ANSWER: B

Explanation:

UserCheck is the Check Point technology that provides real-time user education and interaction when a user attempts to access content governed by a Security Management policy, including URL Filtering rules. Rather than silently allowing or denying the request, UserCheck displays a browser-based notification page before the requested web page is loaded. The message can tell the user that the site is blocked or restricted by organizational policy, identify the applicable category or reason, and—in configurations that permit it—let the user acknowledge the notification or submit a request for access. This immediate feedback helps users understand acceptable web-use requirements at the point of decision, while the Security Gateway continues to enforce the configured access-control policy. Check Point documents UserCheck as an awareness and notification capability integrated with Content Awareness and related Software Blades, including URL Filtering. Administrators can customize the UserCheck message and configure its behavior through the applicable security policy and gateway settings. For Check Point's description of URL Filtering and its user-awareness capabilities, see Check Point URL Filtering documentation. Additional configuration details are available in the Check Point UserCheck documentation.

QUESTION NO: 28

Security Zones do no work with what type of defined rule?

A. Application Control rule

B. Manual NAT rule

C. IPS bypass rule

D. Firewall rule

ANSWER: B

Explanation:

Manual NAT rule is correct. In Check Point Security Management, security zones provide a logical way to group interfaces and use those zones as source or destination objects in the Access Control policy. This allows policy rules to be written according to the traffic direction between zones rather than requiring each individual interface or network to be specified.

Manual NAT rules, however, require concrete source, destination, and translated-object definitions that can be resolved for the NAT policy. A security zone is an access-control abstraction based on gateway interfaces, not an object that manual NAT can use to determine the necessary original and translated addressing. Therefore, zones cannot be used directly in manually defined NAT rules. When an environment uses security zones, administrators should instead define the appropriate network, host, or gateway objects in the manual NAT rule while retaining zones for the access-control policy where applicable.

Check Point's Security Management guidance describes security zones as interface-based groupings for policy use. Check Point community documentation also specifically addresses the limitation and workaround for manual NAT with security zones: Security Zones documentation and Manual NAT and security zones workaround.

QUESTION NO: 29

Which statements about Check Point NAT are correct? (Select two.)

A. Manual NAT rules are evaluated before automatic NAT rules.

B. Automatic NAT can be configured in an object's NAT settings.

C. NAT rules are enforced without installing policy.

D. Automatic NAT can be configured only for user objects.

E. Manual NAT rules cannot perform Hide NAT.

ANSWER: A B

Explanation:

Automatic NAT is configured in the properties of a host, network, or gateway object and is generated automatically during policy installation. Manual NAT rules are configured in the NAT Rule Base and are processed before automatic NAT rules. NAT behavior should be designed together with routing, proxy ARP requirements, and the applicable Access Control policy.

See NAT in the R81 Security Management Administration Guide.

QUESTION NO: 30

To view statistics on detected threats, which Threat Tool would an administrator use?

A. Protections

B. IPS Protections

C. Profiles

D. ThreatWiki

ANSWER: D

Explanation:

ThreatWiki is the Threat Prevention tool used to research detected threats and view related threat information and statistics. In SmartConsole, it provides an integrated interface to Check Point's ThreatCloud intelligence, allowing an administrator to investigate a threat by its name, identifier, or protection and obtain contextual data about its prevalence, behavior, severity, and associated protections. This makes it useful during monitoring and incident investigation, when the administrator needs to move from a detection event to intelligence about the threat behind it.

ThreatWiki is backed by Check Point ThreatCloud, the threat-intelligence service that continuously correlates threat data from global telemetry, research, and security services. The displayed intelligence helps administrators understand the significance of detections and make informed decisions about threat-prevention policy and protection configuration. Check Point describes ThreatCloud and its threat-research capabilities at Check Point ThreatCloud. Additional threat research and threat-specific intelligence is available through Check Point ThreatWiki.