DUMPSBOSS.

Check Point Certified Security Administrator R82

Checkpoint 156-215.82

Version Demo

Total Demo Questions: 19

Total Premium Questions: 195

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Management	69
Topic 2, Security Policies	54
Topic 3, Monitoring Traffic and Connections	15
Topic 4, Network Address Translation	5
Topic 5, User Management and Authentication	1
Topic 6, Identity Awareness	21
Topic 7, Mobile Access	1
Topic 8, Threat Prevention	29
Total	195

QUESTION NO: 1

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 rules. The Negative Control Model is what firewalls use and they require explicit rules to allow and route traffic.

B. The Positive Control Model allows specific, approved actions or traffic and blocks everything else. The Negative Control Model begins by blocking specific, known threats, or unwanted actions and allows everything else.

C. The Positive Control Model begins by blocking specific, known threats, or unwanted actions and allows everything else. The Negative Control Model allows specific, approved actions or traffic and blocks everything else.

D. The Positive Control Model aims to keep administrators in a positive mind set. The Negative Control Model results in administrators having a negative mind set.

ANSWER: B

Explanation:

The Positive Control Model allows specific, approved actions or traffic and blocks everything else. The Negative Control Model begins by blocking specific, known threats, or unwanted actions and allows everything else. This accurately distinguishes an allow-list approach from a block-list approach. In a positive-control design, access is granted only when policy explicitly authorizes it. For a Check Point Access Control policy, this is implemented by placing rules that permit required, validated communications above a cleanup rule that drops traffic not matched by an earlier rule. The result is a default-deny security posture: new, unrecognized, or unintended traffic does not gain access merely because no rule mentions it. This approach reduces exposure and gives administrators precise control over permitted network services and connections. A negative-control design instead focuses on identifying and denying known undesirable items while traffic that is not identified by those restrictions can proceed. Check Point policy administration supports explicit ordered rules and a cleanup rule, which are fundamental to building a positive-control Access Control policy. See Check Point's R82 Security Management Administration Guide: Access Control Policy and the Check Point firewall overview.

QUESTION NO: 2

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 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:

It performs a Man in the Middle style interception on outbound HTTPS connections initiated by internal users is correct because Outbound HTTPS Inspection applies when a client on the internal network initiates an HTTPS session to an external web server. The Security Gateway acts as a controlled proxy between the internal client and the requested site. It establishes a secure connection to the external server, presents a substitute certificate for the requested site to the client, decrypts the HTTPS content, and then allows supported Security Gateway protections to inspect that content according to the configured HTTPS Inspection policy. The gateway re-encrypts traffic as required for each side of the session, rather than merely observing encrypted packets.

For this process to work transparently, client devices must trust the outbound HTTPS Inspection CA certificate generated or imported on the Security Management Server and deployed to the clients' trusted certificate stores. This trusted CA relationship is essential because the gateway dynamically signs the certificate presented during inspection. Administrators can configure inspection rules and exceptions for destinations or categories that should not be decrypted, while applying inspection to appropriate outbound traffic. Check Point documents HTTPS Inspection as a mechanism for inspecting

encrypted connections passing through the gateway: Check Point R82 HTTPS Inspection documentation. See also Check Point's HTTPS Inspection deployment guidance.

QUESTION NO: 3

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

Explanation:

The *It provides aggressive protection for north-south traffic* profile is correct. In Check Point Autonomous Threat Prevention, the Perimeter profile is designed for gateways that protect an organization's external boundary, where north-south traffic enters from or leaves for untrusted networks such as the Internet. This location is exposed to a broad range of attack attempts and unknown sources, so the profile applies a more stringent prevention posture to identify and block threats before they reach internal assets. Its purpose is to provide strong automated threat prevention at the network edge while using the characteristics of perimeter traffic to tune protections appropriately. Check Point describes Autonomous Threat Prevention as a capability that automatically adapts threat-prevention policy based on gateway role and traffic context, reducing the administrative effort required to maintain an effective security posture. The Perimeter profile therefore aligns with an Internet-facing enforcement point rather than a passive observation-only deployment. For Check Point's overview of threat prevention and the protections available on Security Gateways, see Check Point Threat Prevention. Additional product and administration documentation is available through the Check Point Documentation Portal.

QUESTION NO: 4

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

Explanation:

Files begin to be deleted is correct. In the Log Server disk-space management settings, 5000 MB is the default free-space threshold used to protect the system from exhausting its available storage. When the available disk space falls below that threshold, the default automatic action is to remove older log files, thereby reclaiming space so that the Log Server can continue accepting and processing new log data. This behavior is important because log collection depends on adequate free disk capacity for new log files, indexing, and related management operations. Administrators can review and modify log-file storage and disk-space handling in SmartConsole to suit their organization's retention requirements, but the out-of-box behavior associated with this threshold is deletion of old log files. Check Point documents Log Server log-file management and storage behavior in the R82 Security Management Administration Guide. General R82 management documentation is also available through the Security Management Administration Guide introduction.

QUESTION NO: 5

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

Explanation:

Identity Awareness is configured in SmartConsole and enabled on the applicable Security Gateway or Security Gateway cluster because the gateway is the enforcement point for identity-based access control. In SmartConsole, an administrator opens the gateway object and enables the Identity Awareness blade, then configures the required identity-acquisition methods, such as Active Directory integration, Identity Collector, Captive Portal, or Terminal Servers. Identity information learned by the gateway is associated with users, groups, and machines, allowing administrators to define Access Roles that can be used as sources in Access Control policy rules. After the policy is published and installed, the Security Gateway evaluates connections against those identity-aware rules and permits or blocks traffic as defined by policy. This placement is fundamental: the management components define and distribute configuration, while the Security Gateway applies the resulting policy to live traffic. Check Point's Identity Awareness Administration Guide describes enabling Identity Awareness in the Security Gateway object through SmartConsole and using Access Roles in the policy. See the Check Point R82 Identity Awareness Administration Guide and the R82 Security Management Administration Guide.

QUESTION NO: 6

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

Explanation:

Automatic configuration updates is correct because Autonomous Threat Prevention is designed to reduce the administrative effort required to maintain an effective Threat Prevention posture. Check Point provides predefined protection profiles for common organizational segments and continuously maintains the protection logic behind those profiles. Automatic updates allow the configured Autonomous Threat Prevention profiles to receive current Check Point recommendations and protection settings as threat conditions, intelligence, and product capabilities evolve. Consequently, an organization can adopt current protections without an administrator having to manually review and alter each individual prevention setting or profile parameter. This automation supports more consistent security across protected environments while allowing administrators to retain visibility into policy behavior, events, and profile assignments. The feature is especially valuable when new threats emerge or when Check Point refines recommended protection coverage, because the operational profile can remain aligned with those updates without routine manual configuration work. Check Point's Security Management documentation describes Threat Prevention profile management and automation capabilities, while its Network Security information provides broader context for the prevention technologies used by Quantum Security Gateways. See the Check Point R82 Security Management Administration Guide and Check Point Quantum Network Security.

QUESTION NO: 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 policy. Implied rules Before last and Last are applied only to the last Ordered Layer in the list.

B. Implied rules apply to each layer in the Access Control policy.

C. Implied rules apply only to the first Ordered Layer only in the Access Control policy.

D. 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

Explanation:

Implied rules First Rules apply to the first Ordered Layer in the Access Control policy. Implied rules Before last and Last are applied only to the last Ordered Layer in the list. This is the documented enforcement model for an Access Control policy that contains Ordered Layers. The gateway evaluates the ordered layers as a unified policy flow, while the placement configured for implied rules determines where those system-generated controls are inserted. “First” implied rules are evaluated at the beginning of that flow, so Check Point applies them with the first Ordered Layer. The “Before Last” and “Last” implied-rule groups are evaluated at the end of the ordered-layer flow and therefore apply with the final Ordered Layer. This placement is important because implied rules provide essential platform and management connectivity, such as traffic required for gateway control and policy-management functions, while still allowing the administrator’s explicit Access Control rules to be evaluated at the appropriate point in the rulebase. Check Point documents that, for ordered layers, First implied rules belong to the first layer and Before Last/Last implied rules belong to the last layer. See the Check Point R82 Security Management Administration Guide: Implied Rules and the Access Control Layers documentation.

QUESTION NO: 8

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 administrator, Security Management Server administrator, SmartConsole administrator

ANSWER: D

Explanation:

Gaia administrator, Security Management Server administrator, SmartConsole administrator is correct because Check Point separates administration according to the component and management plane being administered. A Gaia administrator is an account on a Security Gateway or management server that administers the Gaia operating system, typically through the Gaia Portal or the command-line interface (Clish). This includes platform-level tasks such as network configuration, system settings, and operating-system administration.

A Security Management Server administrator is defined in the Security Management environment and is granted permissions to manage the security-management infrastructure and its configuration. A SmartConsole administrator is also a Security Management administrator account, but the term identifies the administrator’s use of SmartConsole to authenticate to the management server and perform authorized security-policy and object-management tasks. The permissions available in SmartConsole are controlled through the administrator’s assigned permission profile, supporting role-based access control and separation of duties. Together, these terms accurately represent the platform, Security Management Server, and SmartConsole administrative contexts used in a Quantum Security deployment. See Check Point’s R82 Security Management Administration Guide and R82 Gaia Administration Guide.

QUESTION NO: 9

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

Explanation:

Identity Collector is the correct choice because it is Check Point's centralized Identity Awareness data-collection component for obtaining user-to-IP address mappings from supported external identity sources. In addition to Microsoft Active Directory Domain Controllers, Identity Collector can integrate with Cisco Identity Services Engine and NetIQ eDirectory. This allows an administrator to use identity information already maintained by those infrastructure platforms when enforcing Identity Awareness-based Access Control policies on Check Point Security Gateways.

Identity Collector is particularly useful where identity events need to be collected at scale or where the organization's directory and network-access-control environment is not limited to Windows domain-controller log data. It receives and processes authentication or session information from the configured sources, then supplies the resulting identity associations to the Check Point management and enforcement environment. Policies can consequently use Access Roles based on users, groups, and machines rather than relying only on source IP addresses. Check Point documents Identity Collector as an Identity Awareness acquisition method and describes its support for directory and identity-service integrations in the R82 Identity Awareness Administration Guide: Identity Collector and Identity Sources.

QUESTION NO: 10

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

Explanation:

HTTPS Inspection and Content Awareness. is correct because Application Control and URL Filtering can use these capabilities together to provide visibility and policy enforcement beyond basic URL categorization. HTTPS Inspection decrypts eligible TLS-encrypted traffic for inspection, allowing the Security Gateway to identify applications and URLs that would otherwise be hidden inside encrypted sessions. This is essential for applying Application Control and URL Filtering policy accurately to modern web traffic. Content Awareness adds data-centric inspection, enabling the gateway to recognize sensitive content and apply rules based on the data being transferred, such as files or information matching configured data types. Combining these protections gives administrators layered control: identifying the application or destination, inspecting encrypted sessions where permitted, and evaluating content against organizational data-protection requirements. Policy configuration must account for privacy, legal, and operational requirements before decrypting traffic, including appropriate exceptions for traffic that should not be inspected. Check Point documents HTTPS Inspection as a mechanism for inspecting encrypted traffic and documents Content Awareness as the blade used to identify and control sensitive data. See the Check Point R82 HTTPS Inspection documentation and the Check Point R82 Content Awareness documentation.

QUESTION NO: 11

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

Explanation:

“Perimeter, Cloud/Data Center, Internal Network, Guest Network” is correct because Check Point Autonomous Threat Prevention provides predefined deployment profiles that tune threat-prevention behavior to the security context of the protected environment. A perimeter deployment is intended for traffic entering or leaving the organization, where inspection typically addresses exposure to external threats. The Cloud/Data Center profile is designed for server and cloud workloads, where protection must account for application-centric traffic and data-center architectures. The Internal Network profile supports protection of enterprise users and internal segments, helping detect and prevent threats that could spread inside the organization. The Guest Network profile is intended for less-trusted visitor or unmanaged-device access, where a more restrictive security posture is generally appropriate. Selecting one of these profiles lets administrators apply recommended threat-prevention settings without having to manually construct every policy and profile parameter from scratch, while retaining the ability to customize settings as operational requirements evolve. Check Point describes its threat-prevention architecture and the role of security profiles in its administration documentation and product materials. See the Check Point R82 Threat Prevention Administration Guide and Check Point Threat Prevention overview.

QUESTION NO: 12

What happens to packets if Explicit Default Rule is missing?

A. The Implicit Cleanup Rule is applied.

B. It depends on the Post NAT Rule.

C. It depends on the matching feature located after the Access Control policy.

D. Nothing happens as there is no matching rule.

ANSWER: A

Explanation:

The Implicit Cleanup Rule is applied. In a Check Point Access Control policy layer, traffic is evaluated against the rules in order. When a packet does not match any administrator-defined rule, Check Point does not leave that packet unprocessed. Instead, it reaches the layer’s implicit cleanup behavior, which is the built-in default handling for unmatched traffic. An explicit default rule (also commonly called an explicit cleanup rule) is an administrator-created rule placed at the end of the rule base to make the intended final action, such as Drop and Log, visible and configurable in the policy. If that explicit rule is absent, the implicit cleanup rule supplies the final match. Its configured action determines whether unmatched traffic is accepted or dropped, and its logging behavior determines whether that traffic is recorded. This preserves deterministic policy processing and ensures every packet reaching the Access Control layer receives an outcome. Check Point documents the policy-layer cleanup mechanism and the distinction between explicit and implicit cleanup actions in its Security Management Administration Guide. See the Check Point R82 Access Control Policy documentation and the Policy Layers documentation.

QUESTION NO: 13

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:

IP address(es) allowed to connect to the Security Management Server using SmartConsole is correct because Check Point GUI Clients, also called trusted clients, are the source hosts authorized to establish SmartConsole management connections to a Security Management Server. This setting is an initial network-based restriction on access to the management server: before an administrator can authenticate and perform management tasks, the SmartConsole workstation must originate from an address permitted in the GUI Clients configuration. Administrators can define individual IPv4 or IPv6 addresses, networks, or address ranges as appropriate for their authorized management workstations. The setting therefore helps limit the exposure of the Check Point management interface to approved administrative endpoints and is separate from the administrator account and permission profile used after connecting. GUI Client configuration is managed in SmartConsole through the management-server properties and is specifically intended to control SmartConsole client connectivity to that management server. Check Point documents the GUI Clients setting in its Security Management administration guidance and identifies it as the list of client IP addresses from which SmartConsole connections are accepted. See Check Point R82 Security Management Administration Guide: GUI Clients and Managing the Security Management Server.

QUESTION NO: 14

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

Explanation:

Security Zones are used to simplify rulebase creation by grouping network interfaces according to their security role or network location, such as internal, external, or a demilitarized network. Rather than writing and maintaining rules that individually identify every relevant interface, an administrator can use a zone as the source or destination in an Access Control rule. The Security Management Server then applies the rule according to the interfaces assigned to that zone on the Security Gateway. This creates a more readable and scalable policy, especially when gateways have multiple interfaces or when interface assignments change over time. Zone-based objects also make the intended trust boundaries clearer during policy review: a rule can express traffic allowed from an internal zone to an external zone without depending on a particular interface name. Check Point documents Security Zones as a method for defining rules based on groups of interfaces, helping administrators manage network access controls more efficiently. See the Check Point R82 Security Zones documentation and the R82 Access Control Policy documentation.

QUESTION NO: 15

A ClusterXL deployment protects an internal application. When the active member fails over to the standby member, existing user connections must continue without requiring users to establish new sessions.

Which configuration is required to support this behavior?

A. Configure State Synchronization between the cluster members

B. Install a separate Access Control policy on each member

C. Configure a different Cluster Virtual IP address for each member

D. Enable automatic Hide NAT for the application server

ANSWER: A

Explanation:

Configure State Synchronization between the cluster members is correct. ClusterXL uses State Synchronization to share connection-state information between members. When a failover occurs, the standby member can continue processing synchronized connections rather than treating them as unknown new sessions.

Policy installation ensures that members enforce the intended rules, but it does not synchronize active connection state. A Cluster Virtual IP address provides a common gateway address, while the synchronization network provides the state-sharing capability needed for connection continuity.

QUESTION NO: 16

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

Explanation:

The packet is dropped and no further rules are checked is correct. An Ordered Layer is evaluated sequentially, from the first rule downward, until the Security Gateway finds a rule whose matching criteria apply to the packet. When that matching rule has the Drop action, the gateway immediately discards the packet. This is a terminal enforcement result: the packet is not permitted to proceed through the gateway, and policy evaluation for that packet stops rather than continuing to rules below the matched rule or to subsequent ordered layers.

This behavior is essential to the intended design of Access Control policies. Administrators can place specific blocking rules above broader allow rules, knowing that traffic matching the blocking rule will be denied immediately. A Drop action can also be configured with tracking, so the gateway may create a log entry or other tracking event according to the rule's Track setting; however, tracking does not change the enforcement result. The packet remains discarded and is never forwarded. Check Point's Security Management Administration Guide describes ordered-layer rule processing and the terminal behavior of Drop actions in the Access Control policy. See the R82 Ordered Layers documentation and the R82 Access Control Policy documentation.

QUESTION NO: 17

Select the correct description of the Explicit Rules.

A. Explicit rules are created by the administrator

B. Explicit rules are created in Security Policies by the Security Management Server

C. Explicit rules are created by the Security Gateway

D. Explicit rules are created in the Global Properties on the Security Management Server

ANSWER: A

Explanation:

Explicit rules are created by the administrator. In a Check Point Access Control policy, these are the rules that an administrator deliberately adds and configures in the rulebase through SmartConsole to express the organization's security requirements. An explicit rule contains administrator-selected match criteria, such as source, destination, services and applications, VPN community, content settings, time, and the action to apply. It can also include tracking and installation-target settings. After the administrator publishes and installs the policy, the Security Gateway evaluates traffic against the installed policy and enforces the result; the gateway does not originate the administrator's rule definitions.

This distinction is important when reviewing policy behavior. The visible rules that represent intended access-control decisions are explicit rules, which makes them the primary place to document, audit, and maintain permitted or blocked traffic flows. Check Point separately uses implied rules for system-required connectivity and blade-related behavior that can be generated by product settings rather than entered as ordinary rulebase entries. Check Point's Security Management documentation describes creating and managing Access Control rules in SmartConsole and installing the resulting policy on gateways. See the R82 Security Management Administration Guide: Access Control Policy and the R82 documentation on implied rules.

QUESTION NO: 18

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

Explanation:

Clone default objects and edit the clone is the recommended practice because it preserves the original, vendor-supplied object while providing a starting configuration that already contains suitable settings. Check Point default objects can be referenced by policies, features, and predefined configurations, so retaining them unchanged makes the environment easier to support, audit, and troubleshoot. A cloned object can be given a meaningful, consistent name and then tailored to the organization's specific address, service, protocol, or other requirements without changing the baseline definition. This approach also improves change control: administrators can readily distinguish customized objects from built-in objects, document the purpose of the customization, and revert to or compare against the original when needed. SmartConsole is designed to manage objects centrally and reuse them in policy rules, so creating a clearly named custom clone supports safe, maintainable policy administration as the rule base grows. Check Point's Security Management guidance describes managing network and service objects in SmartConsole, while its best-practices guidance emphasizes maintaining an organized and manageable security-policy environment. See the Check Point R82 Security Management Administration Guide and Check Point Best Practices resources.

QUESTION NO: 19

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

Explanation:

Use the Install Policy button in the active policy (in the SECURITY POLICIES view). This is the recommended SmartConsole workflow because it starts the installation process from the policy package currently being viewed and edited. The administrator can then confirm the relevant installation targets, such as the intended Security Gateways or clusters, before deployment. Keeping installation within the active policy context helps ensure that the correct policy package is selected and provides a clear operational sequence: make and review policy changes, publish the SmartConsole session, select Install Policy from the active policy, confirm targets, and monitor the installation result. Check Point describes policy installation as the process of deploying the policy package to the selected gateway targets, with SmartConsole presenting the installation dialog and status information. This context-driven approach is especially appropriate for routine administrator operations and reduces the risk of deploying an unintended package to an incorrect target. See the Check Point Security Management Administration Guide: Installing Policy and the Check Point Technical Services portal.