Check Point technology is designed to address network exploitation, administrative flexibility and critical accessibility. This chapter introduces the basic concepts of network security and management based on Check Point’s three-tier structure, and provides the foundation for technologies involved in the Check Point Software Blade Architecture, as discussed in the introduction. This course is lab-intensive, and in this chapter, you will begin your hands-on approach with a first-time installation using standalone and distributed topologies.

Topics:

- Learn basic security administrator functions in order to ensure network access control.
- Learn what is a firewall, and how is Check Point’s firewall unique.
- Learn what are some useful gateway deployment strategies in a corporate network.
- Learn about Check Point’s key security policy management features in SmartConsole.
Chapter 1: Check Point Technology Overview

Key Terms:

- Firewall
- Security Gateway
- OSI model
- Network Address Translation
- Packet filtering
- Stateful Inspection
- INSPECT Engine
- Application Intelligence
- Bridge mode
- Inspection Module
- Rule Base
- Security Management Architecture (SMART)
- SmartConsole
- Security Policy
- Management Server
- Stand-alone deployment
- Distributed deployment
- Secure Internal Communications (SIC)
- Internal Certificate Authority (ICA)
- Central license
- Local license
Network Access Control

Network administrators need the means to securely control access to resources such as networks, hosts, network services and protocols. Determining how and what resources can be accessed is the responsibility of authorization, or Access Control. Determining who can access these resources is the responsibility of User Authentication.

A Check Point Security Gateway at the network boundary inspects and provides access control for all gateway traffic. Traffic that does not pass through the gateway is not controlled.

Figure 1-1: A Gateway-Controlled Network

A security administrator is responsible for implementing company security policy. Check Point Security Gateway allows administrators to enforce security policies consistently across multiple gateways. To do this, the administrator defines a company-wide security policy Rule Base using SmartDashboard and installs it to the Security Management server.
SmartDashboard is a SmartConsole client application that administrators use to define and apply security policies to gateways. Granular security policy control is possible by applying specific rules to specific gateways.

Check Point Security Gateway provides secure access control because of its granular understanding of all underlying services and applications traveling on the network. Stateful Inspection technology provides full application level awareness and comprehensive access control for more than 150 predefined applications, services and protocols as well as the ability to specify and define custom services.

Stateful Inspection extracts state-related information required for security decisions from all application levels and maintains this information in dynamic state tables that are used to evaluate subsequent connection attempts. For additional technical information on Stateful Inspection, refer to the Check Point Technical Note at:


The Security Gateway System delivers a unified security architecture for perimeter, internal, Web and endpoint security.
The Check Point Firewall

To understand the capabilities of the basic firewall, it is useful to examine the aspects of the Open Systems Interconnect (OSI) model. It is meant to represent network communication between computer systems and network devices. For discussion purposes only, an illustration of the OSI model in Figure 1-2 below shows a stack of networking layers. (This is not meant to imply a structural relationship.)

Figure 1-2: OSI Communication Stack

- **Layer 1**: Represents physical-communication hardware or media required, such as Ethernet cards, cables and hubs.

- **Layer 2**: Represents where network traffic is delivered to the local area networks (LAN); this is where identification of a single specific machine takes place. Media Access Control (MAC) addresses are assigned to network interfaces by the manufacturers. An Ethernet address belonging to an Ethernet card is a layer 2 MAC address. An example of a physical device performing in this layer would be a switch.

- **Layer 3**: Represents where delivery of network traffic on Wide Area Networks (WANs) or more commonly, the Internet, takes place; addressing in this layer is referred to as Internet Protocol.
Check Point Technology Overview

Chapter 1: Check Point Technology Overview

(IP) addressing, and creates unique addresses, except when Network Address Translation (NAT) is employed. Network Address Translation makes it possible to address multiple physical systems by a single layer 3 IP address. An example of a physical device performing in this layer would be a router.

- **Layer 4**: Represents where specific network applications and communication sessions are identified; multiple layer 4 sessions may occur simultaneously on any given system with other systems on the same network. This layer introduces the concept of ports, or endpoints, for sessions. The session on an originating system is identified by the source-port number, and similarly for the destination system.

- **Layers 5, 6 and 7**: Represent end-user applications and systems; the application layer is not the actual end-user software application, but a set of services that allow the software application to communicate through the network. Distinctions among layers 5, 6, and 7 are not always clear, and some competing models combine these layers, as does this handbook.

The more layers a firewall is capable of covering, the more thorough and effective the firewall. Advanced applications and protocols can be accommodated more efficiently with additional layer coverage. In addition, more advanced firewalls, such as Check Point’s Security Gateways, can provide services that are specifically oriented to the user, such as authentication techniques and logging events to specific users.

**Mechanisms for Controlling Network Traffic**

Any firewall must deny or permit traffic based on explicitly defined rules. Check Point utilizes the following technologies to grant or deny network traffic:

- Packet filtering
- Stateful Inspection
- Application Intelligence
Packet Filtering
Fundamentally, messages are divided into packets that include the destination address and data. Packets are transmitted individually and often by different routes. Once the packets reach their destination, they are recompiled into the original message.

Packet filtering is a firewall in its most basic form. Primarily, the purpose is to control access to specific network segments as directed by a pre configured set of rules, or rule base, which defines the traffic permitted access. Packet filters usually function at layers 3 (network) and 4 (transport) of the OSI model. In general, a typical rule base will include the following elements:

- Source address
- Destination address
- Source port
- Destination port
- Protocol

Packet-filter firewalls are the least secure type of firewall, because they cannot understand the context of a given communication, making them easier for intruders to attack.
Stateful Inspection

**Stateful Inspection**, a technology developed and patented by Check Point, incorporates layer 4 awareness into the standard packet-filter firewall architecture. Stateful Inspection differs from static packet filtering, in that it examines a packet not only in its header, but also the contents of the packet up through the application layer, to determine more about the packet than just information about its source and destination. The state of the connection is monitored and a state table is created to compile the information. As a result, filtering includes context that has been established by previous packets passed through the firewall. For example, stateful-inspection firewalls provide a security measure against port scanning, by closing all ports until the specific port is requested.

There are many state tables that hold useful information in regards to monitoring performance through a Security Gateway. State tables are used to keep state information needed to correctly inspect packets. The tables are key components of Check Point Stateful Inspection technology.
To see a list of the state tables on the Security Gateway, from the command line, type `fw tab -s` for the list in the short format.

For example:

```
[ExpertESSngnt1#] fw tab -s
HOST NAME ID # BURES #PEAK #SLINKS
localhost webgui_clients_list 0 1 1 0
localhost netso_forward_ip 7674 0 0 0
localhost netso_forward_cona 7675 0 0 0
localhost uas_dynamic_session_data 7676 0 0 0
localhost uag_groups_hash 7677 0 0 0
localhost uag_groups_array 7678 0 0 0
localhost netsrv_logon 7679 0 0 0
localhost sam_l2_requests 8888 0 0 0
localhost sam_blocked_ips_v2 8888 0 0 0
localhost sam_requests_v2 8888 0 0 0
localhost sam_ahd 8889 0 0 0
localhost sam_l2_src_dst_requests 8888 0 0 0
localhost mif_sync_table 8892 0 0 0
localhost closed_coams 8894 0 0 0
localhost fiverr_argp_table 8897 0 0 0
```

Figure 1-4: Short State Table List

For more information about state tables, see the Check Point Security Expert (CCSE) Courseware.
Chapter 1: Check Point Technology Overview

Check Point’s **INSPECT Engine** is the mechanism used for extracting the state-related information from all application layers, and maintains this information in these dynamic state tables needed for evaluating subsequent connections. The **INSPECT** Engine enforces Security Policies on the Security Gateway on which they reside.

Figure 1-5: Stateful Inspection Technology

**Application Intelligence**

A growing number of attacks attempt to exploit vulnerabilities in network applications, rather than targeting firewalls directly. **Application Intelligence** is a set of advanced capabilities, integrated into the firewall and IPS, which detect and prevent application-level attacks. This section describes how to protect against application-level attacks for each application protocol.
Application Intelligence works primarily with application-layer defenses. In practice however, many attacks aimed at network applications actually target the network and transport layers.

Security Gateway Inspection Architecture
The Security Gateway integrates both network-level and application-level protection by combining Stateful Inspection and Application Intelligence. All inbound traffic is routed through the Security Gateway, as this is the logical place for active defenses to reside.

System resources and processing time are saved by processing packets in an operating system's kernel. Applications and processes in the kernel layer suffer little, if any, performance degradation, and can support data-throughput rates ranging in the multi gigabits. The Security Gateway kernel is placed between NICs and the TCP/IP stack, solving the problem of protecting the TCP/IP stack itself.

Packet Flow Through the INSPECT Engine
If packets pass inspection, the Security Gateway passes the packets through the TCP/IP stack and to their destination. Packets pass through the NIC, to the Inspection Module, and up through the network stack. Some packets are destined for an operating system's local processes.
this case, the **Inspection Module** inspects the packets and passes them through the TCP/IP stack. If packets do not pass inspection, they are rejected or dropped and logged, according to rules set in the Check Point Rule Base. (The **Rule Base** is a collection of individual rules that determine your Security Policy.)

Packets are not processed by higher protocol-stack layers, unless the Security Gateway verifies that they comply with Security Policies.
Figure 1-6 presents a sample flow of a new inbound packet initiating a TCP/IP session through the Inspection Module, at the kernel level:

Figure 1-6: Inspection Module Flow
Deployment Strategies

As a brief introduction to Gateway deployments, consider the network topology. The network topology represents the internal network (both the local access network (LAN) and the demilitarized zone (DMZ)) protected by the Gateway. The Gateway must be aware of the layout of the network topology to:

• Correctly enforce the Security Policy.
• Ensure the validity of IP addresses for inbound and outbound traffic.
• Configure a special domain for Virtual Private Networks.

Each component in the network topology is distinguished on the network by its IP address and net mask. The combination of objects and their respective IP information make up the topology. For example:

• The IP address of the LAN is 10.111.254.0 with Net Mask 255.255.255.0.
• A Security Gateway on this network has an external interface with the IP address 192.168.1.1, and an internal interface with 10.111.254.254.

In this case, there is one simple internal network.

In more complicated scenarios, the LAN is composed of many different networks, as in the Figure 1-17.
The internal network is composed of the following:

- The IP address of the first is 10.11.254.0 with Net Mask 255.255.255.0.
- The IP address of the second is 10.112.117.0 with Net Mask 255.255.255.0.
- A Security Gateway that protects this network has an external interface with IP address 192.168.1.1, and an internal interface with 10.111.254.254.

It is important to take into consideration your existing corporate network when deciding the best deployment strategy for your Security Gateway. Installing a new Gateway in an existing network often requires
reconfiguration of the routing scheme. However, in more complex deployments, you may find that the reconfiguration necessary to enable a new routing scheme is prohibitive. In this case, Bridge mode may be your best option. (See the discussion below.)

It may also be necessary to consider adding a cluster to your security network. A cluster environment provides reliability through high availability, and enhanced reliability and performance through load sharing. Clustering is discussed in more detail in the Check Point Security Administrator course.

The DMZ

If you have servers that are externally accessible from the Internet, it is recommended to create a demilitarized zone (DMZ). The DMZ isolates all servers that are accessible from untrusted sources, such as the Internet, so that if one of those servers is compromised, the intruder only has limited access to other externally accessible servers. Servers in the DMZ are accessible from any network, and all externally accessible servers should be located in the DMZ. Servers in the DMZ should be as secure as possible. Do not allow the DMZ to initiate connections into the internal network, other than for specific applications such as UserAuthority. See Figure 1-8.
Bridge Mode

**Bridge mode** allows for the placement of a Security Gateway without changing the existing IP routing.

A Security Gateway in Bridge mode operates as a firewall, inspecting traffic and dropping or blocking unauthorized or unsafe traffic. A Gateway in Bridge mode is invisible to all layer 3 traffic. When authorized traffic arrives at the Gateway, it is passed from one interface to another through a procedure known as bridging. Bridging creates a layer 2 relationship between two or more interfaces, where any traffic that enters one interface always exits the other. This way, the firewall can inspect and forward traffic without interfering with the original IP routing. Bridge mode is supported on the operating system Check Point SecurePlatform.

Figure 1-8: Sample Network with a DMZ
**Bridge Mode and STP**

Bridge mode allows a transparent deployment of a Check Point Security Gateway. The figure below illustrates how a Security Gateway in Bridge mode does not alter the IP routing of an existing network.

In the figure, the subnet’s network address is 192.168.1.0 and objects labeled S-\* are switches.

In terms of IP routing, the Gateway is transparently inserted into the existing network, leaving the 192.168.1.0 subnet on both sides of the Gateway. Internal traffic is inspected and authorized by the Gateway, without changes to the IP routing scheme. Traffic that is accepted by the Gateway is forwarded from one interface to the other through MAC addresses.

**Bridge Mode Restrictions**

- A bridge must be configured with a pair of interfaces.
- Cluster configurations are not supported.
- Network Address Translation (NAT) is not supported.
- In order to manage a Gateway in Bridge mode, an interface with an IP address is required. It is important to install a separate, routed interface for this purpose.
STP Protocol
A Security Gateway in Bridge mode supports the spanning tree protocol (STP). STP is a link-management protocol that provides path redundancy and prevents undesirable loops between switches. STP runs the length of the network, monitors for device failure, and controls which switches the traffic passes through. Check Point supports the following STP types:

- STP (the original protocol)
- RSTP (rapid STP)
- PVSTP (per-VLAN STP)

A Security Gateway in Bridge mode directs traffic on layer 2 between the switches on either side of the Gateway, and transparently supports network-linking decisions forwarded by the STP.

Configuring Bridge Mode
To bridge two interfaces:

1. Connect to the management interface of the Security Gateway using the WebUI.
2. Select Network > Connections > New > Bridge.
3. Select the interfaces to comprise the bridge, and click Add.
4. Enter the IP Address and Netmask of the bridge interface (not the physical interface).

![Check Point Security Administrator R70](image)

Although the bridge can function without an IP address, an IP address on the relevant subnet is required for certain SmartDefense protections in SmartDashboard.

5. Select Apply.
Displaying Bridge Configuration via Command

The `brctl show` command displays the status of the bridge configuration. The following is an example of a `brctl show` report:

```
[Expert@GW-1]# brctl show
bridge        bridge id       STP enabled interfaces
br0           8000.000423b93e56 no           eth0 eth1 e56
```

The `brctl show` command report displays the following results:

- **bridge name**: The name given to the bridge
- **bridge id**: The unique identifier of the bridge
- **Interfaces**: The names of the two interfaces in the bridge

The MAC address of the bridge is inherited from one of the physical interfaces.
Security Policy Management

Check Point provides for security across the four most critical layers of network security: the network perimeter, the network core, the Web, and the endpoints. This unified security architecture centralizes Policy configuration, monitoring, logging, analysis and reporting within a single control center.

This system provides many advantages to the Administrator, namely with regard to command-line usage. This centralized-management capability that does not require command-line interaction on a device-by-device basis can save hours of time. One security architecture runs through one management console, and eliminates the need for separate management logins, servers, and reports.

Because all Check Point applications and devices are linked to the same system, the Security Gateway offers increased visibility for real-time detection of security problems and anomalies. With the appropriate license, an integrated IPS tab enables network Administrators to update Check Point enforcement points (Gateways) globally, download updates, and apply defenses for new protocols, applications, and threats, without service interruptions.

A single application, SmartConsole, is used to provide all necessary elements to complete the unified approach.

SmartConsole Components

SmartConsole is comprised of several software modules and blades used to manage Security Gateway components. These include the following:

- SmartDashboard
- SmartMap
- SmartView Tracker
- SmartView Monitor
- Eventia Reporter
- Eventia Analyzer
- SmartProvisioning
- SmartUpdate
- Manage Endpoint Security Server
**SmartDashboard**

SmartDashboard is a single, comprehensive user interface for defining and managing multiple elements of a Security Policy: firewall security, Virtual Private Networks (VPNs), Network Address Translation, Web content and access security (i.e., URL Filtering and SSL VPN), desktop security, antivirus security, IPS threat-defense protections, QoS, and VPN client security. The Check Point SmartDashboard allows you to define Security Policies and rules in terms of network objects (hosts, networks, gateways, etc.). All such object definitions are shared among all applications for efficient Policy creation and security management.

Figure 1-10: Check Point SmartDashboard
Nine types of tabs are available to define, configure or manage Check Point networks:

1. **Firewall Policy** — Provides parameters useful to define the Rule Base for your network; here, you specify how connections are allowed or disallowed, authenticated and encrypted.

2. **Network Address Translation Policy** — Specifies how reserved internal IP addresses will be translated to valid, external IP addresses.

3. **Intrusion Prevention System** — Gets an overview of various attacks and their corresponding mechanisms of protection; configures network security, Application Intelligence and Web Intelligence; and creates and assigns profiles for different Gateways.

4. **Anti Spam and Mail** — Configures integrated antivirus scanning, secure messaging and appropriate Web filtering parameters.

5. **Anti-Virus & URL Filtering** — Automatic or manual updates the Anti-Virus scanning and URL filtering Database with the latest defense signatures from Check Point.

6. **SSL VPN** — Applies to all connected Connectra Gateways; users and applications can be defined and configured, and Integrity Clientless Security (ICS) and SmartDefense measures can be activated on those particular Gateways.

7. **IPSec VPN Policy** — Used to manage VPN Communities.

8. **Quality of Service (QoS) Policy** — Specifies the allocation of bandwidth resources among connections, maximizing throughput.

9. **Desktop Security Policy** — Used to control access to desktops, both those within a local network and those connecting remotely.

**SmartMap**

SmartMap is a Security Policy visualization tool that provides a detailed, graphical map of an organization’s security deployment. SmartMap provides greater control, improved security and ease of use, by allowing...
Administrators to validate the integrity of their Security Policies before deployment.

**SmartView Tracker**
SmartView Tracker is used for managing and tracking logs and alerts. It provides real-time historical and visual tracking, monitoring, and accounting information for all logged connections. Additionally, SmartView Tracker logs Administrator actions, such as changes to object definitions or rules, which can dramatically reduce the time needed to troubleshoot configuration errors. Security Administrators can filter or perform searches on log records, to quickly locate and track events of interest. In the case of an attack or otherwise suspicious network activity, Security Administrators can use SmartView Tracker to temporarily or permanently terminate connections from specific IP addresses.

Figure 1-11: Sample SmartView Tracker Display
1. **Network & Endpoint tab** — displays entries for security-related events for different Check Point products, as well as Check Point's OPSEC partners

2. **Active tab** — shows active connections in the SmartView Tracker, i.e., to connections currently open through any Security Gateway components logging to the currently active log file

3. **Management tab** — tracks changes made to objects in the Rule Base, as well as general SmartDashboard use

4. **Records pane** — displays the list of records in the log file; the columns that appear depend on which query is open.

*SmartPortal*
SmartPortal enables Web based administration of the SmartCenter Server. SmartPortal is included on the NGX R65 CD-ROM and can be installed on its own machine, or on the SmartCenter Server machine. SSL encrypted connections are used to access the SmartPortal Web interface.

*User Directory*
For user management, you can make a choice between managing customers on the internal-user database or implementing an external server.

LDAP is an open industry standard for user management that is used by multiple vendors. It is widely accepted as the directory-access method of the Internet. One of the reasons that it is the obvious choice for so many vendors is because of its cross-platform compliance. LDAP is automatically installed on different operating systems (e.g., Microsoft Active Directory) and servers (such as Novell, Netscape, etc.).

When integrated with Check Point's SmartCenter, LDAP is referred to as “SmartDirectory”.

Check Point Security Administrator R70
**SmartView Monitor**

Based on SMART technology, SmartView Monitor provides a single, central interface for monitoring network activity and performance of Check Point applications.

SmartView Monitor allows Administrators to easily configure and monitor different aspects of network activities. Graphical views can easily be viewed from an integrated, intuitive GUI.

SmartView Monitor is used to monitor and generate reports for traffic on different Check Point components. The SmartView Monitor is a VPN performance-analysis solution that presents users with graphical views of end-to-end VPN tunnel-performance metrics, such as bandwidth, round-trip time, and packet loss. In addition, SmartView Monitor compares actual VPN performance to service-level agreements.

![Sample SmartView Monitor Display](image)

Figure 1-12: Sample SmartView Monitor Display
The following list describes the key features of SmartView Monitor and how it is employed:

1. **Gateway Status** — SmartView Monitor enables information about the status of all Gateways in the system to be collected from these Gateways. This information is gathered by the SmartCenter Server and can be viewed in an easy-to-use SmartConsole. The views can be customized, so that details about the Gateway(s) can be shown in a manner that best meets the Administrator’s needs.

2. **Traffic/System Counters** — SmartView Monitor provides a solution for monitoring and analyzing network traffic and network usage. You can generate fully detailed or summarized graphs and charts for all connections when monitoring traffic, and for numerous rates and figures when counting usage throughout the network. The Traffic view also enables filtering according to categories (services, IP addresses, interfaces, security rules, etc.).

3. **Tunnels** — SmartView Monitor enables Administrators to monitor connectivity among Gateways. By showing real-time information about active tunnels (i.e., information about their state and activities, volume of traffic, which hosts are most active, etc.), Administrators can verify whether the tunnels are working properly and verify privacy, authentication and integrity.

4. **Remote Users** — The Remote User Monitor is an administrative feature allowing you to keep track of VPN remote users currently logged in (i.e., SecuRemote, SecureClient and SSL Network Extender, and in general any IPSec client connecting to the Gateway). It provides you with a comprehensive set of filters, which enables you to easily navigate through the obtained results.

5. **Cooperative Enforcement** — This is a feature that works in conjunction with the Integrity Server. This feature utilizes the Integrity Server compliance capability to verify connections arriving from the various hosts across the internal network. The Security Gateway generates logs for unauthorized hosts. The logs generated for both authorized and unauthorized hosts can be viewed.
**Eventia Reporter**

To manage networks effectively and to make informed decisions, Security Administrators need to gather information about network-traffic patterns. Eventia Reporter is a user-friendly solution for monitoring and auditing traffic. You can generate detailed or summarized reports in the format of your choice (list, vertical bar, pie chart, etc.) for all events logged by Power-1, SecureClient and SmartDefense.

![Image: Sample Eventia Reporter](image_url)

Figure 1-13: Sample Eventia Reporter
Eventia Analyzer

Eventia Analyzer provides centralized, real-time event correlation and management of log data for all Check Point products, such as Power-1, InterSpect, and Connectra, as well as third-party firewalls, routers and switches, intrusion detection systems, operating systems, applications and Web servers. Eventia Analyzer automatically prioritizes security events, and by automating the aggregation and correlation of raw log data, minimizes the amount of data needing review and isolates and prioritizes the real security threats. These threats may not have been otherwise detected when viewed in isolation per device, but pattern anomalies appear when data is correlated over time. Therefore, the network-security team need not comb through the massive amount of data generated by the devices in a network. Instead, the team can focus on deploying resources on the threats that pose the greatest risk to the team’s business.

![Sample Eventia Analyzer](image)

Figure 1-14: Sample Eventia Analyzer
SmartProvisioning

SmartProvisioning provides centralized administration and provisioning of Check Point security devices via a single management console.

Check Point SmartProvisioning enables you to manage thousands of Gateways from a single Security Management Server or Provider-1 CMA, with features to define, manage, and provision large-scale deployments of Check Point Gateways.

The SmartProvisioning management concept is based on profiles; a definitive set of Gateway properties and when relevant, a Check Point Security Policy. Each profile may be assigned to multiple Gateways and defines most of the Gateway properties per profile object instead of per physical Gateway, reducing the administrative overhead.

Figure 1-15: Sample SmartProvisioning
SmartUpdate
SmartUpdate is used to manage and maintain a license repository, as well as to facilitate upgrading Check Point software. SmartUpdate is a component that automatically distributes software applications and updates for Check Point and OPSEC certified products, and manages product licenses. SmartUpdate provides a centralized means to guarantee that Internet security throughout an enterprise network is always up-to-date.

Figure 1-16: SmartUpdate
SmartCenter Server

The **SmartCenter Server** is used by the Administrator to manage the Security Policy. The organization's databases and Security Policies are stored on the SmartCenter Server and downloaded to the Gateway(s). The SmartCenter Server also maintains the Security Gateway databases, including object definitions, Security Policies, and log files for all Gateways. Policies are defined using SmartDashboard, and saved on the SmartCenter Server. To make the most of Check Point products and to best use their capabilities and features, it is helpful to review some basic concepts and components.

**Basic Concepts and Terminology**

- **Administrators** — The designated managers of SmartConsole; they are assigned different levels of access permissions, which define their ability to view and/or modify data using the SmartConsole. At least one Administrator must have full Read/Write permissions, so that he can manage the Security Policy.

- **Configuration** — The process by which Power-1 and UTM-1 is configured using the Check Point Configuration Tool; this tool runs immediately after the initial stages of installation are complete. During the configuration process, the major attributes of the installed product are defined, such as the definition of Administrators, the fingerprint (for first-time SmartCenter Server identity verification), as well as features such as Management High Availability.

- **Security Gateway** — Available in two editions:
  - Power-1 provides a comprehensive security solution for large-enterprise environments.
  - UTM-1 provides next-generation unified threat management, including antivirus, spyware and Web application protection for small- and medium-sized deployments.
Chapter 1: Check Point Technology Overview — Basic Concepts and Terminology

- **Installation** — The process by which Security Gateway components are installed on a computer. A typical Check Point deployment is composed of a Security Gateway, the SmartCenter Server and a SmartConsole (usually SmartDashboard). There are different ways to deploy these components. In all deployments, SmartConsole can be installed on any machine, unless stated otherwise.
  - A **stand-alone deployment** is the simplest deployment, where the SmartCenter Server and the Gateway are installed on the same machine.
  - A **distributed deployment** is a more complex deployment, where the Gateway and SmartCenter Server are deployed on different machines.

- **Licenses** — Required to use certain Check Point products and features; Check Point recommends using SmartUpdate for license management.

- **Login** — The process by which the Administrator connects to the SmartCenter Server using a SmartConsole; the recommended method to log in to the SmartCenter Server is by using a Certificate.

- **Objects** — Defined and managed in SmartDashboard to represent actual network components, such as users, gateways, servers and networks.

- **Policy Package** — A set of Policies that are enforced on selected Gateways; these Policies may include different types of Policies, such as a Security Policy or QoS Policy.

- **Security Policy** — Defines the rules and conditions that govern which communication is permitted to enter and to leave the organization.
Managing Users in SmartDashboard

- **Log Server** — The repository for log entries generated on Gateways; that is, the Gateways send their log entries to the log server. A log server is often installed on the same machine as the SmartCenter Server.

- **SmartDashboard** — The SmartConsole used to create, edit and install Policies.

- **Users** — The people defined in SmartDashboard as the users of an organization.

**Managing Users in SmartDashboard**

Your network can be accessed and managed by multiple users and administrators. A secure network is efficiently managed by centrally controlled user and administrator accounts. SmartDashboard manages users, administrators and their groups as objects using the standard object administration tools; i.e., the Objects Tree pane and the Users and Administrators window. See Figure 1-10.

![Figure 1-17: Users and Administrators Tab and Window](image)
The user’s definition includes access permissions to and from specific machines at specific times of the day. The user definition can be used in the Rule Base’s Authentication Rules and in Remote Access VPN.

SmartDashboard further facilitates user management by allowing you to define user and administrator templates. Templates serve as prototypes of standard user account properties that are common to many users. Any user you create based on a template inherits all of the template’s properties, including membership in groups.

**Users Database**

The users defined in SmartDashboard (as well as their authentication schemes and encryption keys) are saved to the proprietary Check Point Internal Users Database on the Security Management Server.

The Users Database is automatically downloaded to Check Point hosts with installed Management Software Blades as part of the Policy installation process. Alternatively, you can manually install the Users Database by selecting **Policy > Install Database...** from the menu. Security Gateways that do not include a Management Software Blade do not receive the Users Database.

The Users Database does not contain information about users defined externally to the Security Management Server (such as users in external SmartDirectory (LDAP) groups), but it does contain information about the external groups themselves.

**User and Administrator Types**

SmartDashboard allows you to manage a variety of user and administrator types:

**Administrators** — Login to Check Point SmartConsole (i.e., SmartDashboard, SmartUpdate, etc.) with either Read Only or Read/Write permissions, to view or manage (respectively) the network’s various databases and policies.
Administrator Groups — Consist of administrators and administrator sub-groups. Administrator groups are used to specify which administrators have permissions to install Policies on a specific Gateway.

External User Profiles — Profiles of externally defined users who are not defined in the internal users database or on an LDAP server. External user profiles are used to avoid the burden of maintaining multiple Users Databases, by defining a single, generic profile for all external users. External users are authenticated based on either their name or their domain.

Groups — User groups consist of users and of user sub-groups. Including users in groups is required for performing a variety of operations, such as defining user access rules or remote access communities.

LDAP Groups — An LDAP group specifies certain LDAP user characteristics. All LDAP users defined on the LDAP server that match these characteristics are included in the LDAP group. LDAP groups are required for performing a variety of operations, such as defining LDAP user access rules or LDAP remote access communities. For detailed information on LDAP groups, see chapter, “User Management and Authentication”.

Templates — User templates facilitate the user definition process and prevent mistakes, by allowing you to create a new user based on the appropriate template and change only a few relevant properties as needed.

Users — These are either local clients or remote clients, who access your network and its resources.
Securing Channels of Communication

The SmartCenter Server must be able to communicate with all components and partner-OPSEC applications that it manages, even though they may be installed on different machines. The interaction must take place to ensure that the components receive all necessary information from the SmartCenter Server (such as the Security Policy). While information must be allowed to pass freely, it also has to pass securely.

This means that:

- The communication must be encrypted so that an imposter cannot send, receive or intercept communication meant for someone else.
- The communication must be authenticated; there can be no doubt as to the identity of the communicating peers.
- The transmitted communication should have data integrity; that is, the communication must not be altered or distorted in any form.
- The SIC setup process allowing the intercommunication to take place must be user-friendly.

If these criteria are met, secure channels of communication between intercommunicating components of the system can be set up and enforced, to protect the free and secure flow of information.
Secure Internal Communications (SIC) is the Check Point feature that ensures components, such as Security Gateways, SmartCenter Servers, etc., can communicate freely and securely using a simple communication-initialization process.

The following security measures are taken to ensure the safety of SIC:

- Certificates for authentication
- Standards-based SSL for the creation of the secure channel
- 3DES for encryption

The Internal Certificate Authority (ICA)

The Internal Certificate Authority (ICA) is created during the SmartCenter Server installation process. It is responsible for issuing Certificates for:

- **SIC** — Certificates issued for the SmartCenter Server, its components, OPSEC components, and product Administrators, to enable secure communication for all Check Point-related operations (such as Policy installation on components, logging, SmartConsole-SmartCenter Server connectivity, etc.)

- **Virtual Private Network (VPN) Certificates for gateways** — To enable efficient and seamless strong authentication in VPN tunnel creation.

- **Users** — To enable strong authentication between remote-access users and Gateways, as well as other features, such as clientless VPN.

ICA Clients

ICA operations are performed using the following clients:

- Check Point configuration tool or `cpconfig` on the command line. Using this tool, the ICA is created and a SIC Certificate is issued for the SmartCenter Server.

- SmartDashboard. This SmartConsole is used to manage:
- SIC Certificates for the various components, as well as for Administrators.

- VPN Certificates.

- User Certificates managed in the internal database.

- ICA management tool. This tool is used to manage VPN Certificates for users that are either managed on the internal database or on an LDAP server, and to perform ICA management operations. The ICA generates audit logs when ICA operations are performed. These logs can be viewed in the SmartView Tracker.
SIC Among SmartCenter Servers and Components
The following graphic illustrates the SIC process in a distributed environment:

Figure 1-18: Distributed Configuration Showing Components with Certificates

1. The ICA creates a Certificate for the SmartCenter Server during the SmartCenter Server installation. The ICA is created automatically during the installation procedure.

2. Certificates for the Security Gateways, and any other communicating components, are created via a simple initialization from the SmartConsole. Upon initialization, the ICA creates, signs, and delivers a Certificate to the communication component. Every component can then verify the Certificate for authenticity.
Communication between a SmartCenter Server and its components depends on a Security Policy specified in a Policy file on each machine. Communication using Certificates will take place, provided that the communicating components are of the appropriate version, and agree on the authentication and encryption methods. The SmartCenter Server and its components are identified by their SIC name, also known as the Distinguished Name.

Administrative Login Using SIC
The login process, in which Administrators connect to the SmartCenter Server, is common to all Check Point SmartConsole components (SmartDashboard, SmartUpdate, etc.). This process consists of a bidirectional operation, in which the Administrator and the SmartCenter Server authenticate each other and create a secure channel of communication between them using SIC. Once both the Administrator and the SmartCenter Server have been successfully authenticated, SmartCenter launches the selected SmartConsole.
Figure 1-19: Sample SmartDashboard Login