

Chapter

Introduction to Endpoint Security

1

This chapter provides an overview of Endpoint Security features and concepts. Planning security policies is covered based on enterprise requirements and user needs. This chapter does not cover all available features in detail as provided by Endpoint Security. Refer to the Check Point Endpoint Security manual for more information.

Objectives:

- Using fundamental Endpoint Security architecture and concepts, confirm communication between the server and clients.
- Understand Endpoint Security communications, modes and views.
- Manage Catalogs and groups to organize Endpoint Security users into units.
- Understand Endpoint Security policy types and the major features for providing security through policy administration.
- Select your client and policy types, and your security model to plan a pilot installation before implementing in an enterprise environment.
- Considering recommended administrative workflow, install Check Point Endpoint Security Management Server on a Windows 2003 environment.

Key Terms:

- Endpoint Security Server
- Endpoint Security clients
- Endpoint Security Agent
- Endpoint Security Flex
- Firewall Rules
- Zone Rules
- Program Control
- Trusted Zone
- Blocked Zone
- Internet Zone
- Program Observation
- Enforcement
- Single Domain Mode
- Multi Domain Mode
- Simple View
- Advanced View
- User Catalogs
- IP Catalogs
- Connected Enterprise Policies
- Disconnected Enterprise Policies

Endpoint Security Overview

Any organization concerned about information security would discover that endpoints are the universal Achilles heel of risk. Endpoints bring three significant new risks. First, attacks are often directed to endpoints and the enterprise network through a variety of methods including interaction with malicious Web sites. Second, since endpoints are often mobile, they may be used both inside and outside the controlled network. Lastly, endpoints are a logistical challenge to IT staff who often must manage deployment of policies and controls for multiple security agents on each device.

Given that endpoints are considered especially vulnerable, a way to prevent exploitation of endpoints is to deploy a comprehensive layer of endpoint security on each PC. Endpoint Security is a new strategy that unifies functionality on each PC that is centrally deployed and managed by IT security specialists on a single console. For a unified endpoint security system to be effective, the following requirements should be considered:

- Detect and block malware
- Secure data
- Enforce policy compliance
- Ensure secure remote access
- Streamline management
- Minimize end-user impact

Each of these functions relate to specific Check Point products, and the goal of Endpoint Security is to permit managing these products from a central location for all of your security.

The Endpoint Security features include:

- **Firewall Rules** – Provides same level of security as standard perimeter firewalls by restricting or allowing network activity based on connection information.
- **Access Zones and Zone Rules** – Provides network security through creating groups of locations to which you assign network permissions.
- **Program Control** – Restricts network access on a per-application basis.
- **SmartDefense Program Advisor Service** – Automates application control management.
- **Program Enforcement** – Ensures that every Endpoint computer meets application and version requirements before it connects to the network. For example, using Program Enforcement, you can require that Endpoint computers have a certain version of Antivirus protection.
- **Cooperative Enforcement®** – Restricts or disconnects noncompliant users at the network access/authorization level. For a complete list of devices that are compatible with Endpoint Security, see the Endpoint Security Systems Requirements Guide.
- **Check Point Antispyware** – Protects your company's data by detecting and removing spyware.
- **Check Point Antivirus** - Provides centrally-managed antivirus protection to your Endpoint users.

System Architecture

The Endpoint Security system consists of two basic components:

- **Endpoint Security Server**
- **Endpoint Security clients**

You can also optionally include other items in your system, such as gateways, RADIUS servers and LDAP servers. All Endpoint Security installations include SmartPortal, which provides some of Endpoint Security's reporting functionality.

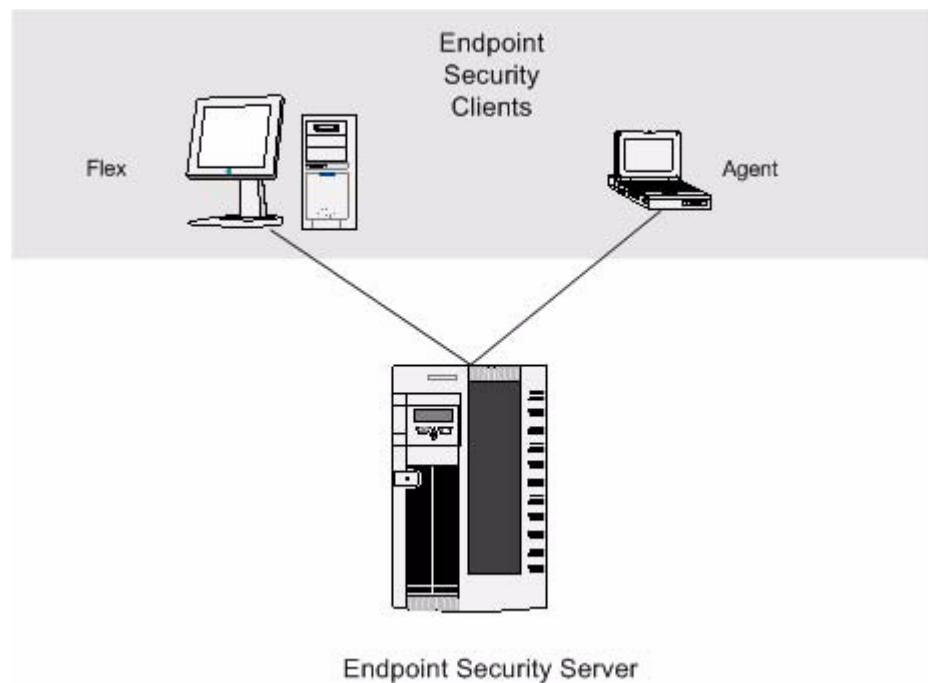


Figure 1-1: Basic Endpoint Security Architecture

Integrated Check Point Components

Endpoint Security installations include some other Check Point components that function in the background to create an integrated security solution. Notable integration elements include:

- **Installation Options** – There are a variety of installation options for Endpoint Security with other Check Point products. These options include:
 - Single Server – You can now install Endpoint Security on the same server as SmartCenter and Provider-1. This reduces your resource costs.
 - Multi-Server – You can install SmartCenter and Endpoint Security on separate servers. You can also choose to have logging on another server.
- **Licensing** – Licensing is performed on the server side so you do not need to update your Endpoint Security clients with a new license when adding features. You can manage your licenses using Check Point license management tools:
 - SmartUpdate
 - The **cplic** command
 - Check Point Configuration Tool (for local licenses only)
- **Gateway Integration** – Endpoint Security provides Cooperative Enforcement in conjunction with the following Check Point devices and software:
 - Check Point VPN-1 for remote access users
 - Check Point VPN-1 UTM/Power
 - Check Point VPN-1® SecureClient™ with Application Intelligence
 - Check Point Interspect Gateway

- **Unified Logging, Reporting, and Monitoring** – Endpoint Security logs are stored in a format that makes them readable by third-party and Check Point Products, such as SmartView Tracker, Eventia Reporter and Eventia Analyzer. This has the following advantages:
 - Logs use a file system instead of a database, which allows you to archive and rotate the logs in the same way as other Check Point logs.
 - Log info is stored locally if the remote logging server is unavailable.
 - Perimeter, internal, and Web security events are all logged in one place.
 - Using Eventia Reporter, you can schedule reports to run during periods of low system use. You can also e-mail reports to other people, and upload reports to a Web site.
 - Using SmartView Tracker, you can view logs in real time using a client application that provides easy log navigation and filtering.
 - Certain reports in SmartPortal are available from the Endpoint Security Administrator console. See “Monitoring Client Security,” on page 200. This allows you to view the detailed reports that interest you directly from the Endpoint Security Administrator Console.
 - SmartView Monitor displays real time Endpoint Security statistics, along with all other Check Point events.
- **Shared Administrator Logins** – You can use the same login for Endpoint Security as you do for other Check Point products. SmartDashboard automatically creates an Integrity object upon

installation and grants Endpoint Security access to all administrators with SmartDashboard access.



Administrator accounts created in SmartCenter can launch Endpoint Security using the same read/write privileges assigned to them in SmartCenter. However, these administrators are not able to create administrator accounts in Endpoint Security. Also, you cannot create administrator accounts in SmartCenter using the roles and role permissions available in Endpoint Security, i.e., an account with the ability to assign policy but not edit policies, or an account with only the ability to run reports. To create these types of accounts you must log directly into Endpoint Security using the masteradmin login.

Endpoint Security Server

The Server allows you to centrally configure your policies. Endpoint Security uses its own embedded datastore to store administrator, configuration, and security policy information.

The Administrator Console

Most administrative functions are performed using the Endpoint Security Administrator Console. The Console is a Web-based graphical user interface (GUI) and is available at:

`https://<Endpoint Security IP Address>/signon.do`

You use the Console to create the Security Policies and deploy them to clients. In addition, the Console can be used to pre-package Endpoint Security client executables with configuration settings and policies before you deliver them to your users.

Endpoint Security Clients

As part of the Endpoint Security system, you will be installing Endpoint Security clients on your endpoint computers. These clients monitor your endpoints and enforce your Security Policies. The Endpoint Security system includes **Endpoint Security Agent** and **Endpoint Security Flex**. It also includes versions of each that contain VPN capabilities.

- **Endpoint Security Agent** - Use Endpoint Security Agent when you want to centrally manage security at all times. It has a limited interface and does not allow the user to control security settings. If you use the version of Agent that also has VPN capability, the users are provided with an interface to configure their VPN. It also provides an interface to manage some anti-virus and anti-spyware functions. Generally, use Agent for your less advanced users and for computers that belong to your organization. Since Agent provides a simpler user interface and fewer messages to the user, it is less confusing. Agent is available in both Windows and Linux.
- **Endpoint Security Flex** - Use Flex when you want the endpoint user to control his or her security settings some of the time. Flex has a full user interface that allows the user to control security settings under certain conditions. Generally, use Flex for expert users who are familiar with security issues. Flex is useful when you do not own the endpoint computers or wish to reduce management requirements, particularly for disconnected policies.

Major Security Features

Endpoint Security uses three major features to provide security:

- **Firewall Rules** - Control traffic using packet data
- **Zone Rules** - Allow or deny traffic based on security locations defined by the Administrator
- **Program Control** - Protects your network by controlling program access

Firewall Rules

Implementing Firewall Rules achieves the same level of security as standard perimeter firewalls by restricting or allowing network activity based on connection information, such as IP addresses, ports, and protocols, regardless of which program sends or receives the packet. You can also specify firewall rules within Program Rules to restrict

access to and from programs or within Enforcement Rules, to restrict a non-compliant user to a particular area of your network.

Firewall Rules block or allow network traffic based on the attributes of communication packets, such as:

- Source and/or destination locations
- Protocol and/or port
- Time

Zones

In addition to Firewall Rules, you can also control network traffic through the use of Access Zones and Zone Rules. Access Zones are groups of locations to which you assign the same network permissions.

For example, refer to the following image:

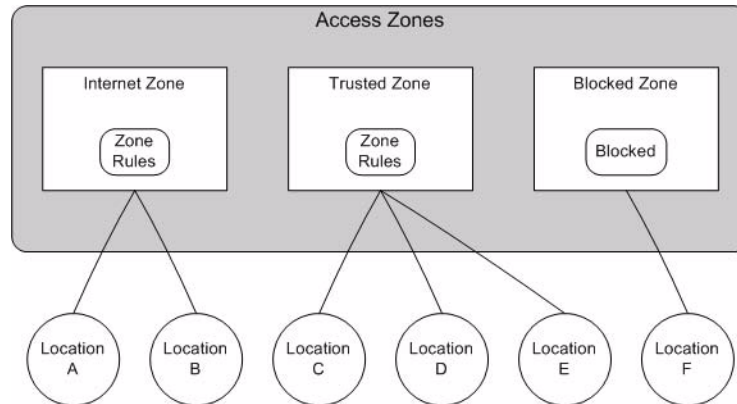


Figure 1-2: Locations, Zones and Zone Rules

Locations - Locations refer to network locations that are defined by the administrator using any of the following options:

- host
- Site

- IP address
- IP range
- IP subnet and mask

Access Zones - Access Zones are groups of locations. There are three types of Access Zones:

- **Trusted** - Trusted zones are believed to be safe and to which more permissive network access is provided, such as the Domain Name Server, Mail Server, Domain Controller, file sharing servers, print servers, gateways, etc.
- **Blocked** - Blocked zones include restricted locations such as human resources (HR) servers from non-HR personnel.
- **Internet** - The Internet zone includes all the areas not explicitly defined in the Trusted or Blocked zones. This zone does not need to be defined.

Program Control

Program rules restrict network access on a per-program basis. Program Control allows you to restrict network access between a particular program and either your Trusted or Internet Zone. You can also further refine program rules by adding firewall rules.

When planning your program control, consider both your security goals and your endpoint users' needs in order to achieve the most cost effective balance. For instance, by configuring program control to block all programs except those you explicitly allow, you achieve a high level of security at the expense of endpoint user productivity. But, by configuring program control to allow all programs except those you explicitly forbid, you achieve a lower level of security, but cause less disruption to your endpoint users.

Enforcement

In contrast to Program Control, another security feature provided by Endpoint Security is **Enforcement**. It controls which computers may access your network based on the software loaded on the endpoint computer when connecting to the network.

Enforcement rules are designed to require or prohibit software. If a user does not comply with the Enforcement rules specified, they can be warned about the noncompliance before permitting access to the network, or restricted to a particular area on the network.

Communications, Modes and Views

Endpoint Security operations are implemented by separate Endpoint Security services. An Apache **httpd** server proxies requests to these services from entities external to Endpoint Security, such as Endpoint Security clients or administrators logging on to Endpoint Security from remote computers. The Apache **httpd** server acts as a single point of entry, managing requests using SSL, file caching, UDP, and/or TCP socket off-loading functionality.

Ports

By default, Endpoint Security uses the ports listed below to communicate with Endpoint Security Clients. It is recommended to ensure that these ports are all available on the Endpoint Security Server:

- TCP/80 HTTP
- TCP/443 HTTPS
- TCP/2100 HTTPS (for 7.0 and later clients)
- UDP/6054 (alternate heartbeat port, and for endpoints with client versions less than 7.0)

Modes and Views

There are two modes used for Endpoint Security:

- **Single Domain**
- **Multi Domain**

The domain mode is chosen during the Endpoint Security installation. Having multiple domains is useful for Internet Service Providers and large companies that want local administration for locations and business units.

Single Domain Mode

Single Domain Mode has two views:

- **Simple view**
- **Advanced view**

Simple View

Simple view offers a simplified user interface and feature set intended to account for situations where only the core Endpoint Security features are required. When selecting Single Domain mode during installation, the Simple view is the default.

Simple view can be useful under the following circumstances:

- Demonstrations - When it is necessary to show core Endpoint Security functionality.
- Getting Started - When learning core functionality.
- Simple Installations - When the advanced features of Endpoint Security are not needed for the network environment. You may choose to remain permanently in Simple view.

Advanced View

Advanced view in Single Domain mode provides access to all the Endpoint Security features, which include those not included in Simple view, such as:

- Domains
- Catalogs
- Policy assignment
- Policy creation from templates or files
- Manually-added reference sources for programs
- Server settings

Switching Views

During the Endpoint Security installation, if you choose to install the Single Domain mode, it automatically starts in Simple view. After installation, you can switch between Advanced and Simple views using the Administrator Console. Then you can optionally choose to change to Advanced view and back to Simple view at any time, provided you have not used any of the features that are not included in Simple view.

To switch between views:

1. Click **Change View** from the main menu of the Endpoint Security Administrator Console.
2. From the **Confirm Change View** window, click **Change View**.

Activating Policies

In simple mode, you cannot assign policies. Instead, you can choose which policies to activate as your connected, disconnected, and gateway policies. Disconnected policies apply to users that are not connected to the Endpoint Security server. VPN Policies apply to users who connect through a gateway. Any other policies you have created remain inactive, and do not affect your endpoint users.

Managing Catalogs and Groups

Endpoint Security uses catalogs and groups to organize endpoint users into units. This permits assigning policies to a number of endpoint users at once.

Catalogs can contain any number of groups. These groups can be imported from existing third-party user directories, or if using a custom catalog, it is possible to create groups manually.

There are two basic types of catalogs used by Endpoint Security:

- **User Catalogs**
- **IP Catalogs**

The use of either catalog type is entirely dependent on the enterprise security needs and your existing network infrastructure.

Authenticating Users

Endpoint Security imports user directory information from LDAP, NT Domain and RADIUS servers, allowing endpoint users to be authenticated against those directories.

Authentication is performed using:

- **Native authentication** - If the authentication system uses NT Domain, Novell NDS LDAP or Microsoft Active Directory, those endpoint users are automatically recognized.
- **Proxy login** - Use if the authentication system is RADIUS or LDAP (other than Novell NDS and Microsoft Active Directory). When an endpoint connects to the enterprise network, a proxy login window displays requiring the user's authentication credentials. Then the user's credentials are checked against the external user directory, and if successful, assigns the appropriate security policy.

User Catalogs

User catalogs organize users according to the information imported from third-party user directories. A good way to apply User Catalogs is when assigning policies according to the department or location of the endpoint users.

The following are types of User Catalogs:

- Custom Catalogs
- LDAP Catalogs
- NT Domain Catalogs
- RADIUS Catalogs
- IP Catalogs

Custom Catalogs

Use custom catalogs in conjunction with the User ID field in the client packager to create your own catalogs in the administrator console. Once the custom catalog is created, client packages can be created and deployed to the assigned users. The workstation will always be defined as the custom catalog user regardless of the person logging into the workstation.

LDAP Catalogs

Use LDAP catalogs to organize your users according to the directory groups in your existing LDAP (Lightweight Directory Access Protocol) server.

Endpoint Security supports RFC 1777-compliant LDAP servers versions 2 and 3. Endpoint Security provides the configuration filters for Novell eDirectory for Windows, Netscape Directory Server for Windows 2000, and Windows Active Directory Service (native/mixed mode). If you are using any other LDAP server, you must have the user and group filter information to import the directories. For more information, see your LDAP provider's documentation.

NT Domain Catalogs

Use NT Domain catalogs to organize your users according to the directory groups in your existing NT Domain.



NT Domain catalogs are not available in SecurePlatform installations.

RADIUS Catalogs

If you are going to assign policies only at the RADIUS directory level and not at the individual user level, you do not need to import the RADIUS catalogs. Endpoint Security adds users when they are successfully authenticated during proxy login, and it assigns the RADIUS catalog-level policy automatically if you use the **Auto Add** feature. Endpoint Security supports RFC 2865-compliant RADIUS software.

IP Catalogs

Use IP Catalogs if your users are organized by IP range. This will allow you to assign policies based on the location of the workstation regardless of the user logged in.

Planning

Carefully planning the Endpoint Security installation can avoid potential problems, and make best use of the Endpoint Security features.

Check Point recommends that a pilot or test environment is developed before attempting to set up the Endpoint Security system for production.

Prerequisites

Before beginning the installation, ensure that the system designated as the Endpoint Security server, as well as pilot endpoints meets the following prerequisites:

- Hardware, Software and Operating System

Please see the Endpoint Security System Requirements document for a list of supported operating systems and hardware requirements.

- Network Connectivity

Ensure that the network is configured and operating normally. Have at least two endpoint computers connected to the network. They will serve as the Endpoint Security clients and pilot endpoint computers.

Choosing Client Type

Decide whether the clients will be Flex or Agent (see page 9 for definitions). In a production environment, it is best to choose Agent unless the users are very experienced with security issues and will want to create their own personal security policies. However, for a pilot

installation, it may be preferred to use Flex so that the deployment results can be easily viewed.



The Agent does not solicit users to make security choices. Therefore, by default it adds new networks to the Trusted Zone and allows newly detected programs. This could be less secure when the personal policy is active. However, you can maintain security on remote users using Agent if implementing both disconnected and connected policies in a policy package.

Choosing Enterprise Policy Types

Endpoint Security enforces your security rules by means of enterprise policies. By using different types of enterprise policies, different levels of security to your endpoint users can be provided depending on their situation.

Connected Enterprise Policies — These policies are enforced when the endpoint computer is connected to the Endpoint Security server. Generally, the connected policies are the strictest policies.

Disconnected Enterprise Policies — These policies are enforced when the endpoint user is not connected to the Endpoint Security server. These policies are usually more permissive than connected policies.

A policy package can be used to assign connected and disconnected policies to the same users. If an endpoint user has also created a personal policy using Flex, Endpoint Security will forbid any traffic that violates either policy. It is possible to configure the enterprise policy to override the personal policy. If using a VPN, create a connected enterprise policy and assign it to the VPN. This is the policy that will apply when the users of that VPN gateway use it to connect to the network.

Choosing the Security Model

A Security Model is based on assigning policies or policy packages to groups of users according to their security needs. There are two options:

- IP - Assigning policies to IP ranges
- User - Assigning policies to groups created through catalogs

While you can configure Endpoint Security to arbitrate between security models, it is easier to begin with only one security model. Choose the security model that best fits the way the company network is organized and gather either the IP or catalog information for the system.

For example, there are several options for catalog types, but if LDAP using Microsoft Active Directory is selected, the following information is needed:

- Primary Host
- User Filter
- Group Filter
- User-ID Attribute
- Server Port
- Base DN
- Admin Name
- Admin Password

General Administrative Workflow

Although some administrative tasks can be performed in any order, Check Point recommends that you use a general workflow as a guideline when working with the Endpoint Security system. Use the workflow to understand what tasks should be performed when, and to understand what resources are available for assistance. Each of these steps is covered in some detail in this book.

1. Plan the installation.

These steps are essential, and all should be performed before attempting to install or configure the Endpoint Security Server.

- a Obtain all up-to-date documentation.
 - b Read the Release Notes to prevent unexpected results.
 - c Check system requirements to verify the hardware and software are supported.
 - d Perform the pilot configuration steps as outlined in the Check Point Endpoint Security Implementation Guide for assistance in planning policies and helpdesk training.
 - e If using Gateways or Microsoft GPO, ensure these are correctly configured and working properly before continuing.
2. Install and license the Endpoint Security Server.
 - a Obtain the licenses which are based on the number of client seats permitted. Add-on features such as SmartDefense are additional licenses.
 - b Install the Endpoint Security Server as shown in Lab 1-Installing Endpoint Security Server.
 3. Configure the system, which may include setting database backup options.
 4. Configure gateways and create user catalogs.

5. Create roles and administrator accounts.
6. Configure global settings for Program Control that apply to the entire organization and used in the policies by default.
7. Create and assign policies using Zone and firewall rules, Program Control and Program Advisor, Enforcement rules, Check Point Anti-virus, Mailsafe, SmartDefense and Check Point Anti-spyware.
8. Deploy clients using client packages or third-party distribution methods.
9. Monitor and improve policies as needed using reports.

