



# Installing and Setting Up the PIX 515E Security Appliance

---

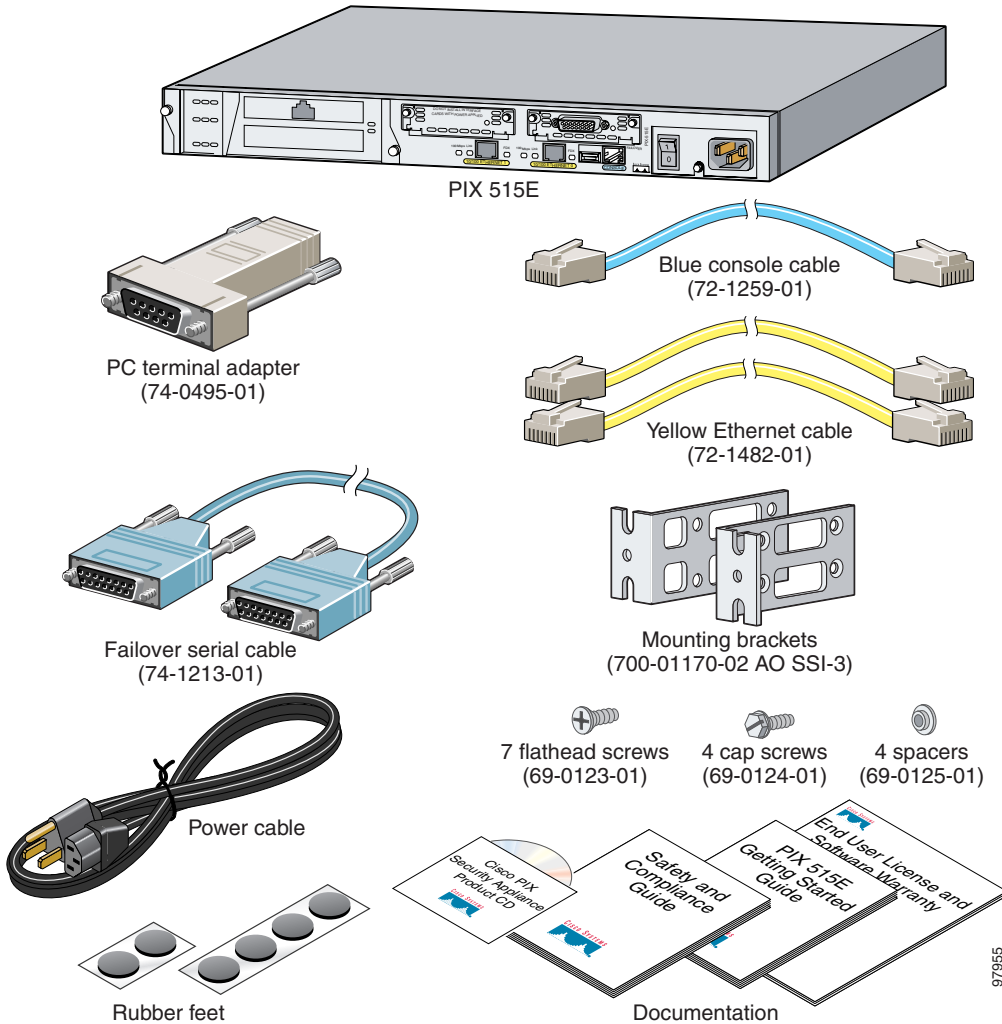
This chapter describes how to install and perform the initial configuration of the security appliance. This chapter includes the following sections:

- [Verifying the Package Contents, page 1-2](#)
- [Installing the PIX 515E Security Appliance, page 1-3](#)
- [Front and Back Panel Components, page 1-4](#)
- [Setting Up the Security Appliance, page 1-5](#)
- [What to Do Next, page 1-9](#)

# Verifying the Package Contents

Verify the contents of the packing box, shown in [Figure 1-1](#), to ensure that you have received all items necessary to install your PIX 515E security appliance.

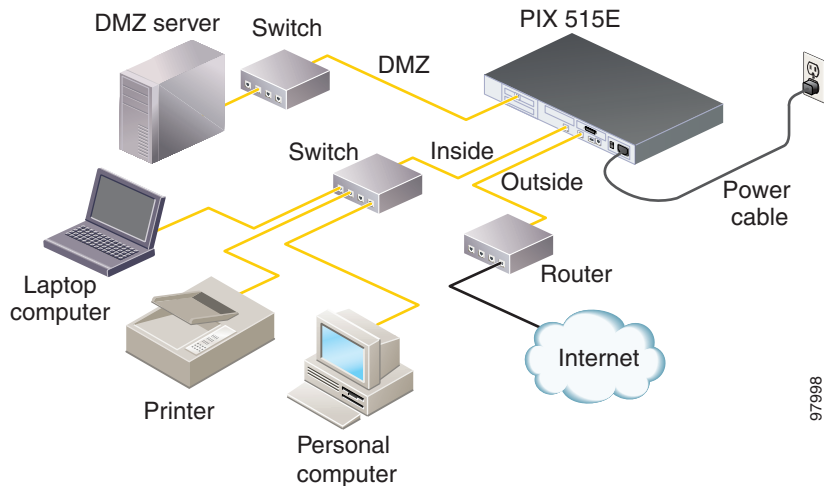
**Figure 1-1** Contents of PIX 515E Package



# Installing the PIX 515E Security Appliance

This section describes how to install your PIX 515E security appliance into your own network, which might resemble the example network in [Figure 1-2](#).

**Figure 1-2** Sample Network Layout



To install the PIX 515E security appliance, complete these steps:

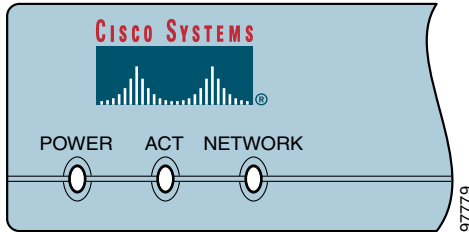
- 
- Step 1** Mount the chassis in a rack by performing the following steps:
- a. Attach the brackets to the chassis with the supplied screws. The brackets attach to the holes near the front of the chassis.
  - b. Attach the chassis to the equipment rack.
- Step 2** Use one of the provided yellow Ethernet cables to connect the outside 10/100 Ethernet interface, Ethernet 0, to a DSL modem, cable modem, router, or switch.
- Step 3** Use the other provided yellow Ethernet cable to connect the inside 10/100 Ethernet interface, Ethernet 1, to a switch or hub.
- Step 4** Connect one end of the power cable to the rear of the PIX 515E security appliance and the other end to a power outlet.

- Step 5** Power up the PIX 515E security appliance. The power switch is located at the rear of the chassis.

## Front and Back Panel Components

Figure 1-3 illustrates the LEDs on the front panel of the PIX515E Security Appliance.

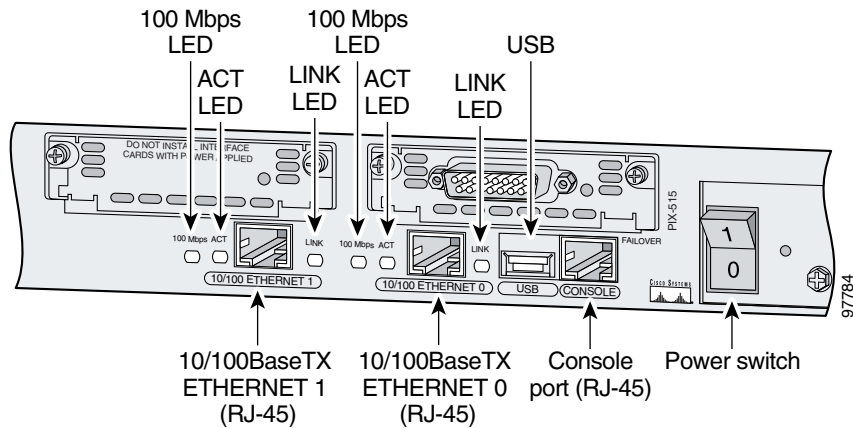
**Figure 1-3** PIX515E Security Appliance Front Panel LEDs



LED	Color	State	Description
POWER	Green	On	On when the unit has power.
ACT	Green	On	If part of a failover pair, the light is on when the unit is the active unit.
		Off	If part of a failover pair, the light is off when the unit is in standby mode.
NETWORK	Green	Flashing	Flashing when at least one network interface is passing traffic.

Figure 1-4 illustrates the back panel components.

Figure 1-4 PIX 515E Security Appliance Back Panel



## Setting Up the Security Appliance

This section describes the initial configuration of the security appliance. You can perform the configuration steps using either the browser-based Cisco Adaptive Security Device Manager (ASDM) or the command-line interface (CLI). However, the procedures in this chapter refer to the method using ASDM.



### Note

To use ASDM, you must have a DES license or a 3DES-AES license. For more information, see [Appendix A, “Obtaining a DES License or a 3DES-AES License.”](#)

This section includes the following topics:

- [About the Factory-Default Configuration, page 1-6](#)
- [About the Adaptive Security Device Manager, page 1-6](#)
- [Using the Startup Wizard, page 1-7](#)

## About the Factory-Default Configuration

Cisco security appliances are shipped with a factory-default configuration that enables quick startup. The factory-default configuration automatically configures an interface for management so you can quickly connect to the device and use ASDM to complete your configuration.

By default, the security appliance management interface is configured with a default DHCP address pool. This configuration enables a client on the inside network to obtain a DHCP address from the security appliance to connect to the appliance. Administrators can then configure and manage the security appliance using ASDM.

## About the Adaptive Security Device Manager



The Adaptive Security Device Manager (ASDM) is a feature-rich graphical interface that enables you to manage and monitor the security appliance. Its web-based design provides secure access so that you can connect to and manage the security appliance from any location by using a web browser.

In addition to its complete configuration and management capability, ASDM features intelligent wizards to simplify and accelerate the deployment of the security appliance.

In addition to the ASDM web configuration tool, you can configure the security appliance by using the command-line interface. For more information, see the [Cisco Security Appliance Command Line Configuration Guide](#) and the [Cisco Security Appliance Command Reference](#).

## Using the Startup Wizard

ASDM includes a Startup Wizard to simplify the initial configuration of your security appliance. With a few steps, the Startup Wizard enables you to configure the security appliance so that it allows packets to flow securely between the inside network and the outside network.

This section describes how to use the Startup Wizard to set basic configuration parameters. This section includes the following topics:

- [Before Launching the Startup Wizard, page 1-7](#)
- [Running the Startup Wizard, page 1-8](#)

## Before Launching the Startup Wizard

Before you launch the Startup Wizard, perform the following steps:

---

**Step 1** Obtain a DES license or a 3DES-AES license.

To run ASDM, you must have a DES license or a 3DES-AES license. If you did not purchase one of these licenses with the security appliance, see [Appendix A, “Obtaining a DES License or a 3DES-AES License”](#) for information about how to obtain and activate one.

**Step 2** Enable Java and Javascript in your web browser.

- Step 3** Gather the following information:
- A unique hostname to identify the security appliance on your network.
  - The IP addresses of your outside interface, inside interface, and any other interfaces to be configured.
  - The IP addresses to use for Network Address Translation (NAT) or Port Address Translation (PAT) configuration.
  - The IP address range for the DHCP server.
- 

## Running the Startup Wizard

To use the Startup Wizard to set up a basic configuration for the security appliance, perform the following steps:

- Step 1** Use an Ethernet cable to connect your PC to the inside port (Ethernet 1) on the rear panel of the PIX 515E.
- Step 2** Configure your PC to use DHCP (to receive an IP address automatically from the PIX 515E).

Alternatively, you can assign a static IP address to your PC. If you use a static IP address, use any address from the 192.168.1.0 range except 192.168.1.1. This IP address is assigned to the inside interface of the PIX 515E.

- Step 3** Start ASDM.
- a. On the PC connected to the inside port of the PIX 515E, start an Internet browser.
  - b. In the address field of the browser, enter this URL:  
**https://192.168.1.1/admin.**



**Note**

The security appliance ships with a default IP address of 192.168.1.1. Remember to add the “s” in “**https**” or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the security appliance.

---

- c. In the window that requires you to choose the method you want to use to run the ASDM software, choose either to download the ASDM launcher or to run the ASDM software as a Java applet.
- Step 4** In the dialog box that requires a username and password, leave both fields empty. Press **Enter**.
- Step 5** Click **Yes** to accept the certificates. Click **Yes** for all subsequent authentication and certificate dialog boxes.
- ASDM starts.
- Step 6** From the Wizards menu, choose Startup Wizard.
- Step 7** Follow the instructions in the Startup Wizard to set up your security appliance.
- For information about any field in the Startup Wizard, click **Help** at the bottom of the window.

**Note**

Based on your network security policy, you should also consider configuring the security appliance to deny all ICMP traffic through the outside interface or any other interface that is necessary. You can configure this access control policy using the **icmp** command. For more information about the **icmp** command, see the [Cisco Security Appliance Command Reference](#).

## What to Do Next

Next, configure the security appliance for your deployment using one or more of the following chapters:

To Do This ...	See ...
Configure the security appliance to protect a DMZ web server	<a href="#">Chapter 2, “Scenario: DMZ Configuration”</a>
Configure the security appliance for remote-access VPN	<a href="#">Chapter 3, “Scenario: IPsec Remote-Access VPN Configuration”</a>
Configure the security appliance for Site-to-Site VPN	<a href="#">Chapter 4, “Scenario: Site-to-Site VPN Configuration”</a>

■ What to Do Next