CHAPTER 5

Deploying Secure Internet Connectivity

This chapter is a step-by-step procedure explaining how to use the ASDM Startup Wizard to set up the initial configuration for your ASA/PIX Security Appliance.

These steps are intended to show you how to achieve secure connectivity to the Internet. After completing these steps, you will have access to the Internet. In addition, you will be protected from both Internet-sourced attacks against the hosts on the inside of your network and denial-of-service (DoS) attacks against your firewall.

Chapter 6, "Deploying Web and Mail Services," covers how to configure ASDM to advertise and secure public services such as web servers and e-mail.

Introducing the ASDM Startup Wizard

The ASDM Startup Wizard is an easy-to-use tool that steps you through the procedures necessary to get your firewall functional. It provides the configurations necessary for both Internet connectivity and protection for your network resources. The wizard queries you for all items pertinent to the configuration of your firewall, including the following:

- Inside IP addresses
- Outside IP addresses
- Default gateway
- Domain name
- Public services
- Network address translations
- Firewall name
- Access passwords
- Interface options
- Inside addressing options (DHCP)

Before you begin, take a look at Table 5-1, which defines the network terms used in the preceding list.

Table 5-1 *Networking Terminology*

Terminology	Definition
Inside IP address	The IP address of the inside interface of your firewall, which connects to your internal network.
Outside IP address	The IP address of the outside interface of your firewall, which connects to your service provider for Internet connectivity. This address is provided by your service provider.
Default gateway	The next-hop IP address of your firewall outside interface. This is provided by your service provider.
Domain name	This is optional. If you are providing public services, you need to identify a domain name for those services. Either your ISP or a web registration service provides your domain name.
Public services	These are services that you are providing to other people over the Internet. Common public services are web servers, mail servers, or DNS servers. You can elect not to manage your own services and have your ISP manage the services for you.
Network address translation	This feature enables you to use private addresses inside your network and still obtain Internet access.
Access passwords	This password allows you privileged access to your firewall.
Inside addressing options (DHCP, static)	These are IP addresses that you assign to devices on the inside of your firewall. You have two options for configuring your inside hosts with IP addresses: You can manually set up each address on each PC, or you can use DHCP on the ASA/PIX Security Appliance to assign addresses for you.

Basic Network Topology

This chapter provides a common and basic network topology as an example for the ASDM Startup Wizard procedure. The topology is such a standard template that, unless you have a unusual circumstance, you can follow these steps verbatim and have secure Internet connectivity upon completion.

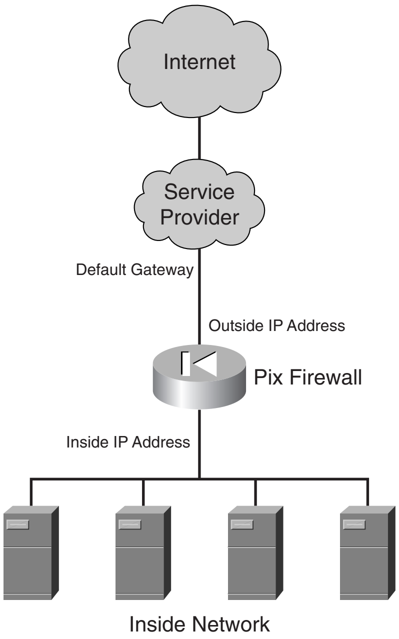
Figure 5-1 shows the topology you will use for your ASDM Startup Wizard procedure.

It's important to understand the basic elements and terminology used in this topology:

- Internet
- Service provider
- Default gateway
- IP address and subnet masks
- Inside address

- Inside network
- Internet server addresses

Figure 5-1 *Basic Network to Internet Topology*



Understanding the Elements of Your Network

Before you begin, let's review some basic Internet terminology to ensure that we are all on the same page.

The Internet

The *Internet*, which of course everyone is familiar with, is millions of networks and hosts that reach all over the globe. Most companies want to be connected to the Internet to either tap into this vast array of information, communicate with others who have Internet access, or provide services or advertisement to other Internet users.

The Internet Service Provider

The *Internet service provider* (ISP) is your entry point into the Internet. There are many different providers throughout the world. Your first step to connect to the Internet is to select a local ISP. Your local ISP might be a local telephone company or a small company that focuses on providing Internet coverage in small target areas. It is beyond the scope of this book to recommend ISPs. It is recommended, however, that you talk to other companies or use the web to find out who provides the best service in your area.

The ISP provides you with a physical point of entry into its network. This is usually a networking device such as a DSL/cable modem or a router. The outside of your ASA/PIX Security Appliance plugs into this device.

Default Gateway

Your ISP will provide an IP address called a *default gateway address*. This is the address of a router that the ISP owns that will be the next hop toward the Internet from your ASA/PIX Security Appliance.

Internet IP Address and Subnet Mask

Along with a default gateway, the ISP will provide you with an *IP address* and a *subnet mask*. The IP address and subnet mask are applied to the outside of your firewall. The IP address always has four octets and might look something like 199.200.2.4. The address and mask work together to form a network number and a host number. You don't have to worry about this for now; suffice it to say that if you correctly enter your IP address and mask, you will be properly connected to the Internet.

NOTE A new addressing scheme called *IPv6* will be used in the Internet a few years from now. The format of the v6 address will be different. However, the IPv6-style addresses will be designed so that they work seamlessly with IPv4 addresses. Therefore, no changes will need to be made to your configuration when IPv6 comes of age. It is also important to note that the ASA/PIX Security Appliance supports IPv6 in the version 7 release.

Inside Addresses

The concept of *inside addresses* could get complex if you let it. Don't let it! It can also be simple. Addresses on the inside of your network are usually defined as private or reserved addresses.

Don't be intimidated if you don't understand IP addressing. If you enter the addresses correctly from your ISP and follow the procedures in this book, the details of IP addressing are insignificant. The most commonly used private addresses are the following:

- **Class A**: 10.0.0.0 through 10.255.255.255 (subnet mask: 255.0.0.0)
- **Class B**: 172.16.0.0 through 172.31.255.255 (subnet mask: 255.255.0.0)
- **Class C**: 192.168.0.0 through 192.168.255.255 (subnet mask: 255.255.255.0)

It doesn't matter which of these addresses you elect to use because they all function in exactly the same manner. In this book, you use 192.168.1.x and a subnet mask of 255.255.255.0 as your private inside network addresses.

Network Address Translation

One thing you must understand about private inside addresses is that they are not routable on the Internet. This means that if you were to send traffic out from a host that has a private address to http://www.cisco.com, the packet would make it out to the Internet. However, because it's a private nonroutable Internet address, it cannot be returned to the host that originated the request. Therefore, your web request would never be returned and your connection would time out.

The ASA/PIX Security Appliance handles this situation by using a concept called *network address translation* (NAT). When NAT is applied on the firewall, it uses the following process to ensure that the traffic is both delivered to the destination address and then returned back to the host that has the private address:

1. Looks at the address of the host requesting Internet access
2. Stores the original private address in its NAT lookup table
3. Replaces the private address with either the outside interface IP address of your ASA/PIX Security Appliance or another address provided by your service provider
4. Accepts the return packet, looks up the host that made the original request in its NAT table, and replaces the private address
5. Routes the return packet back to the correct host

Inside Network

The *inside network* refers to the hosts that will be behind your firewall. Normally, these hosts are connected to a switch or a series of switches and routers, depending on the complexity of your network. Because this book is a beginner's guide, you are going to use the topology shown in Figure 5-1, which is a flat network, which means that the inside of your firewall and all of your hosts will be connected to a single switch comprising your inside network.

Your inside network addresses *must* be in the same subnet as the inside interface of your ASA/PIX Security Appliance. You could manually configure the IP addresses of each of your inside hosts so that they are in the same subnet. However, the security appliance can also do this for you. You will use a function of the ASA/PIX Security Appliance called *Dynamic Host Configuration Protocol* (DHCP) to automatically assign IP addresses to your inside host. This protocol will save you many hours of initial labor and ongoing maintenance.

Public Servers: Mail DNS, Web Servers

Public servers provide services that you plan to allow Internet users to access. The most common of these are web servers, mail servers, and DNS servers. If you plan to offer public services, you must request an IP address for each of the servers from your ISP. Also, remember from earlier reading, that if you are going to offer public services, you need to have a firewall (such as a PIX 515E) that has more than two interfaces. This way, you can put your servers on an interface separate from your inside users. This setup ensures that if hackers do compromise one of your public servers, your inside network is still isolated from the hackers. Chapter 6 covers the deployment of these servers.

Using the ASDM Startup Wizard

It’s time to start with ASDM. At the end of this section, you will have a secure connection established to the Internet.

You complete the following tasks in this section:

- Connect to the ASA/PIX Security Appliance with ASDM.
- Configure the ASA/PIX Security Appliance host name and domain name and enable password.
- Configure the outside interface information.
- Configure other interface characteristics.
- Configure NAT.

Connecting to the ASA/PIX Security Appliance with ASDM

If you haven’t completed the steps from Chapter 3, “Getting Started with the ASA/PIX Security Appliance,” to install ASA/PIX version 7 and ASDM, you cannot proceed. You must complete the configuration portion of that chapter before you can do any of the step-by step portions of this section.

You need to complete three steps before you can connect to the ASA/PIX Security Appliance using ASDM:

Step 1 Configure an interface port.

Step 2 Allow ASDM access to the box.

Step 3 Ensure you have the appropriate Java Runtime Environment on your host that will be running ASDM.

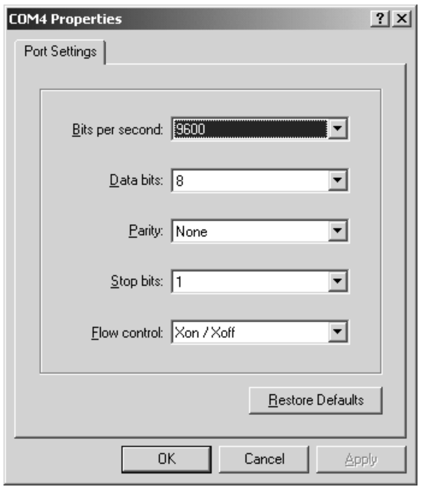
Configure an Interface Port

These steps assume that there is currently no configuration on your ASA/PIX Security Appliance. If it is the first time you boot your ASA/PIX Security Appliance, it will prompt you with a question asking whether you want to configure the device. Enter **No**. All of your configuration steps are outlined in the following steps.

If you already configured your security appliance as described in Chapter 3, you can skip to the section titled “Configure Your PC to Access the ASA/PIX Security Appliance.”

Step 1 Plug your PC serial port into the console of the ASA/PIX Security Appliance using the serial cable. Using HyperTerminal or any terminal emulator application, set your parameters to match those in Figure 5-2. These setting show speed at 9600 bps, 8 data bits, no parity checking, and 1 stop bit.

Figure 5-2 *HyperTerminal Parameter Setup*



COM4 Properties

Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: Xon / Xoff

Step 2 Power on the ASA/PIX Security Appliance. The Security Appliance will go through its boot sequence and you will be presented with a pixfirewall> prompt.

Step 3 You must now configure the inside interface of the ASA/PIX Security Appliance with a valid inside address so that you can access it using ASDM. At the prompt, enter the commands in the following example that are in bold text. Comment lines have been added to indicate what each command does. Comment lines are preceded with an exclamation point (!):

```
pixfirewall> enable
! en - puts you in Enable (Privileged) mode.
Password:<CR>
! <CR> - is the default password for the PIX.
pixfirewall# configure terminal
! conf t - specifies that the following commands will be configuration
   commands.
pixfirewall(Config)# interface ethernet
! int e1 – specifies that the commands following will be applied to the
   Ethernet 1 interface.
pixfirewall(Config-if)# nameif inside
! nameif inside – defines Ethernet 1 as the inside or protected
   interface.
INFO: Security level for "inside" set to 100 by default.
pixfirewall(Config-if)# ip address 192.168.1.1 255.255.255.0
```

```
! ip add 192.168.1.1 255.255.255.0 – sets the IP address and subnet mask
   for the inside interface.
pixfirewall(Config-if)# no shut
! no shut – enables the interface for operating.
pixfirewall(Config-if)#
```

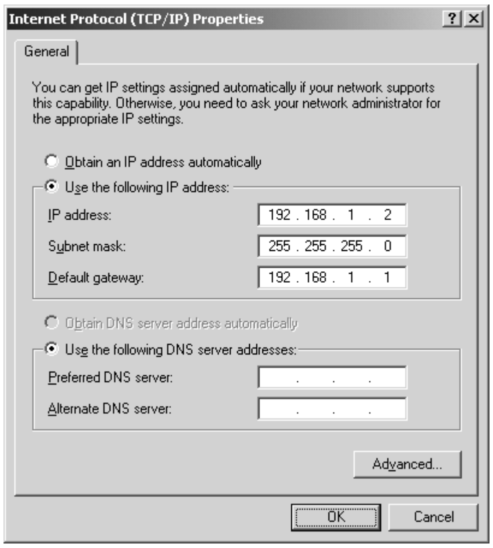
In this book, this is the only time you use the native ASA/PIX Security Appliance command-line interface (CLI) to enable the security appliance to accept ASDM connections.

Configure Your PC to Access the ASA/PIX Security Appliance

Because you will be accessing ASDM with your PC on the inside interface of the ASA/PIX Security Appliance, you must configure your PC with an inside IP address. You will use 192.168.1.2 with a subnet mask of 255.255.255.0 (same as the security appliance subnet mask). The gateway is the next-hop address; so in this case, it is the address you gave to the inside of the security appliance: 192.168.1.1.

Figure 5-3 illustrates how your Network Control Panel should look when configured if you are using Windows 2000.

Figure 5-3 *PC Network Configuration*



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

You can connect the PC to the ASA/PIX Security Appliance in one of two ways. You can directly connect to the interface labeled Ethernet 1 using a crossover cable, or you can plug the PC and Security Appliance Ethernet 1 into a switch using straight-through Ethernet cables. You should now be able to ping the firewall from your PC using the command **ping 192.168.1.1**. If your pings are not successful, recheck your addressing and cabling. Make sure that the PC Ethernet card and Ethernet 1 on the security appliance are enabled. You should see link lights on the security appliance interface and the network card of your PC when properly configured.

Allow ASDM Access to the ASA/PIX Security Appliance

You must now tell the ASA/PIX Security Appliance that you are enabling it to run ASDM. You are also defining what IP address can access the security appliance with the ASDM application.

Follow these steps:

Step 1 The first thing you need to do is tell the PIX the name of the ASDM file. Enter the following command on the PIX: **asdm image flash:/asdm.bin**.

Step 2 Now, you must enable the ASA/PIX Security Appliance to start its secure web server. Enter the command **http server enable**.

Step 3 After the ASA/PIX Security Appliance web server is enabled, you must tell the security appliance who can access ASDM and where they are located. To accomplish this, enter the address of your PC and tell the security appliance you are located on the inside interface. Enter the command **http 192.168.1.2 255.255.255.255 inside**.

Caution You can enable ASDM on the outside interface of the ASA/PIX Security Appliance, but it is not recommended. If you do, you open yourself to the possibility that someone can guess your username and password and gain full access to your firewall.

Step 4 Enter the command **show running http** on the ASA/PIX Security Appliance and ensure that the output matches the following output:

```
pixfirewall(Config)# show running http
http server enabled
http 192.168.1.2 255.255.255.255 inside
pixfirewall(Config)#
```

At this point, you should have full connectivity to your ASA/PIX Security Appliance via ASDM.

Launching ASDM

The instructions in this section show you how to launch ASDM. Just follow these steps:

Step 1 Open the browser on your PC and enter **https://192.168.1.1/admin**.

This action downloads the ASDM applet to your PC. The first time you do this, it might take a minute to load. However, in subsequent connections, ASDM will start in just a few seconds.

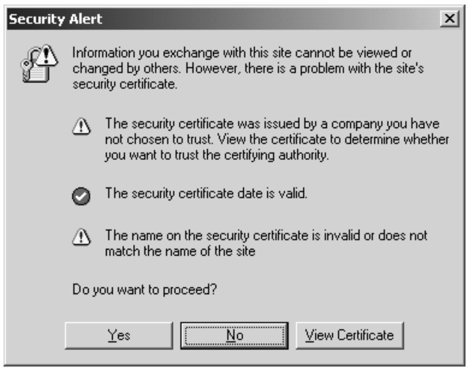
ASDM will also present you with an option to download a utility called the *ASDM Launcher*. This launcher is an application that functions exactly the same as the Java applet. Using this application will eliminate the need to launch a browser to access the ASA/PIX Security Appliance.

The browser-based ASDM applet requires Java 1.4.2 or 1.5.0. If you don't have one of these Java versions installed on your PC, you will get the following message and you must download the required software: "Your browser does not have the required Java Plug-in. ASDM requires Java Plug-in version 1.4.2 or higher." We will point you to a web page from which you can download the correct Java version to your PC.

Because ASDM is using a connection secured by SSL, you will see the various security warnings as described in the following steps.

Step 2 The first pop-up (Figure 5-4) is a message that lets you know that the secure connection has a valid certificate, but that the certificate is from an untrusted source. This certificate is a self-generated certificate by the ASA/PIX Security Appliance. You must click **Yes** to continue.

Figure 5-4 *Valid Certificate Alert*



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

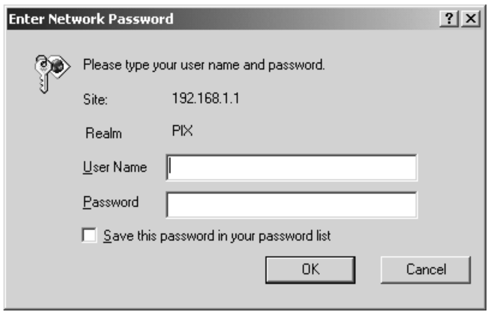
⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Step 3 When you get the prompt for the ASA/PIX Security Appliance username and password (Figure 5-5), leave the fields empty and click **OK**. You haven't set a password yet, so no input is required.

Step 4 Figure 5-6 informs you that the certificate is going to be used as a key to encrypt data but that the issuer isn't trusted. You must click **Yes** to continue. Don't be concerned when you see these messages that say that certificates are not trusted. Trust is a technical concept in public certificate authentication related to the prior knowledge of a certificate.

Figure 5-5 *ASA/PIX Security Appliance Username and Password Prompt*



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

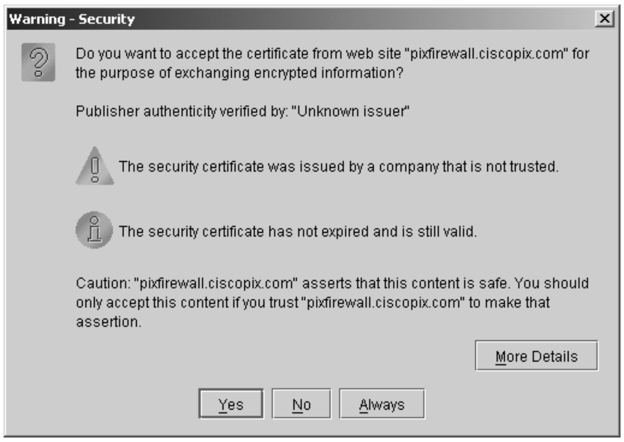
Realm PIX

User Name

Password

□ Save this password in your password list

Figure 5-6 *Valid Certificate Alert*



Warning - Security

Do you want to accept the certificate from web site "pixfirewall.ciscopix.com" for the purpose of exchanging encrypted information?

Publisher authenticity verified by: "Unknown issuer"

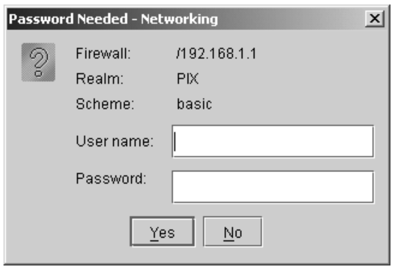
The security certificate was issued by a company that is not trusted.

The security certificate has not expired and is still valid.

Caution: "pixfirewall.ciscopix.com" asserts that this content is safe. You should only accept this content if you trust "pixfirewall.ciscopix.com" to make that assertion.

Step 5 Figure 5-7 prompts you again for username and password because the Java applet is now running. Again, because you haven't set passwords at this point, you should click **Yes**. If you are using the ASDM Launcher application rather than the web browser, you won't get this prompt.

Figure 5-7 *Network Password Access*



Password Needed - Networking

Firewall: /192.168.1.1

Realm: PIX

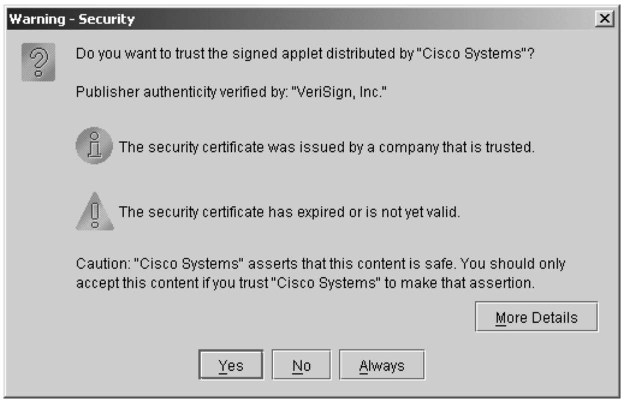
Scheme: basic

User name:

Password:

Step 6 Figure 5-8 is a certificate that needs to be approved to download the ASDM applet to your PC. Click **Yes** to continue.

Figure 5-8 *Certificate to Download ASDM*



Warning - Security

Do you want to trust the signed applet distributed by "Cisco Systems"?

Publisher authenticity verified by: "VeriSign, Inc."

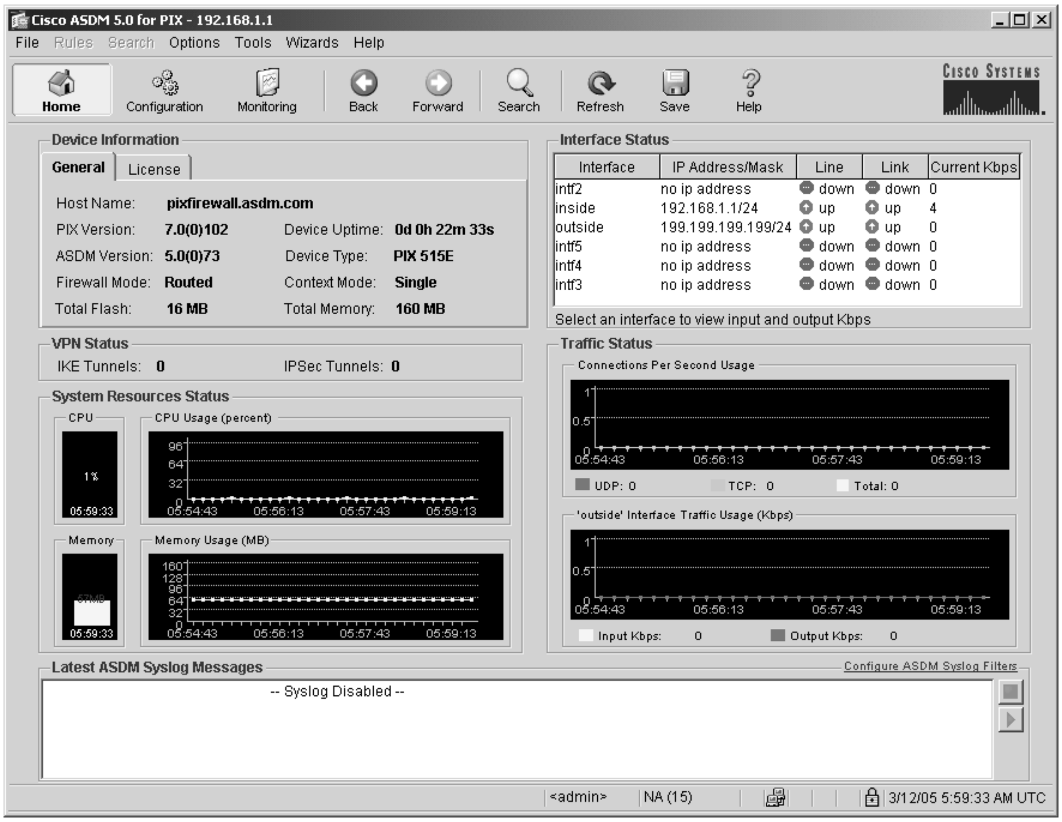
The security certificate was issued by a company that is trusted.

The security certificate has expired or is not yet valid.

Caution: "Cisco Systems" asserts that this content is safe. You should only accept this content if you trust "Cisco Systems" to make that assertion.

You are now presented with Figure 5-9, which is the ASDM Welcome screen.

Figure 5-9 *ASDM Welcome Screen*



Cisco ASDM 5.0 for PIX - 192.168.1.1

Device Information

Host Name: pixfirewall.asdm.com

PIX Version: 7.0(0)102 Device Uptime: 0d 0h 22m 33s

ASDM Version: 5.0(0)73 Device Type: PIX 515E

Firewall Mode: Routed Context Mode: Single

Total Flash: 16 MB Total Memory: 160 MB

Interface Status

Interface	IP Address/Mask	Line	Link	Current Kbps
intf2	no ip address	down	down	0
inside	192.168.1.1/24	up	up	4
outside	199.199.199.199/24	up	up	0
intf5	no ip address	down	down	0
intf4	no ip address	down	down	0
intf3	no ip address	down	down	0

Select an interface to view input and output Kbps

VPN Status

IKE Tunnels: 0 IPSec Tunnels: 0

System Resources Status

Traffic Status

UDP: 0 TCP: 0 Total: 0

Input Kbps: 0 Output Kbps: 0

Latest ASDM Syslog Messages

-- Syslog Disabled --

<admin> NA (15) 3/12/05 5:59:33 AM UTC

You are now logged on to your ASA/PIX Security Appliance using ASDM.

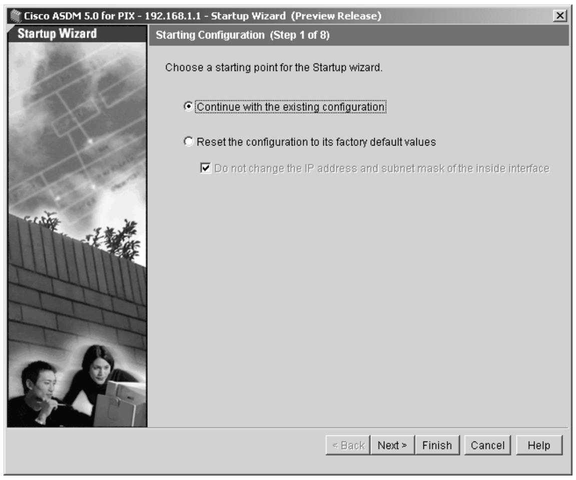
Using the ASDM Startup Wizard to Configure the ASA/PIX Security Appliance

Now, you are ready to begin entering configuration information into ASDM. Just follow these steps:

Step 1 To start the wizard, click the **Wizard** pull-down menu item or the click the **Wizard** option on the navigation panel to the far left of the ASDM home screen and choose **Startup Wizard**.

Step 2 You will first be asked whether you want to use the existing configuration. The only existing configuration should be your IP address and the command that allows ASDM to communicate with your browser. Click **Continue with Existing Configuration**, and then click **Next**. (See Figure 5-10.)

Figure 5-10 *ASDM Starting Configuration*



Cisco ASDM 5.0 for PIX - 192.168.1.1 - Startup Wizard (Preview Release)

Startup Wizard

Starting Configuration (Step 1 of 8)

Choose a starting point for the Startup wizard.

● Continue with the existing configuration

○ Reset the configuration to its factory default values

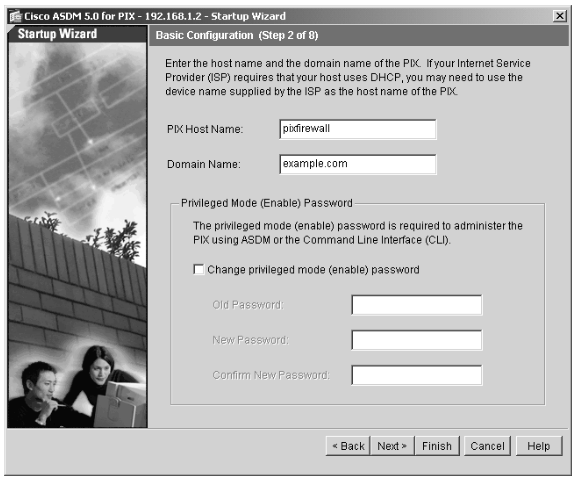
☑ Do not change the IP address and subnet mask of the inside interface

Step 3 You are than prompted for the basic configuration (see Figure 5-11).

Enter the name you want to call your ASA/PIX Security Appliance. Enter the domain, if you have one. You can enter anything you want in these fields; Figure 5-11 shows pixfirewall and example.com entered in these fields. The default domain name is default.domain.invalid until you enter your own domain name into this field.

Step 4 You need to enter an enable password (privileged) for the firewall. Because no password is yet configured, leave the old password blank. According to security best practices, you should enter a password at least eight characters long, using numerals, special characters, and containing uppercase and lowercase characters. Following this rule will significantly reduce the chances of an attacker being able to run a brute-force or guessing attack against your firewall to get the password and gain full access. Click **Next**.

Figure 5-11 *ASDM Basic Configuration*



Cisco ASDM 5.0 for PIX - 192.168.1.2 - Startup Wizard

Startup Wizard

Basic Configuration (Step 2 of 8)

Enter the host name and the domain name of the PIX. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to use the device name supplied by the ISP as the host name of the PIX.

PIX Host Name: pixfirewall

Domain Name: example.com

Privileged Mode (Enable) Password

The privileged mode (enable) password is required to administer the PIX using ASDM or the Command Line Interface (CLI).

☐ Change privileged mode (enable) password

Old Password:

New Password:

Confirm New Password:

Step 5 The next step is to configure the connectivity to the Internet. This consists of the following:

— The name of your firewall's outside interface

— The outside IP address of your firewall provided to you by your ISP

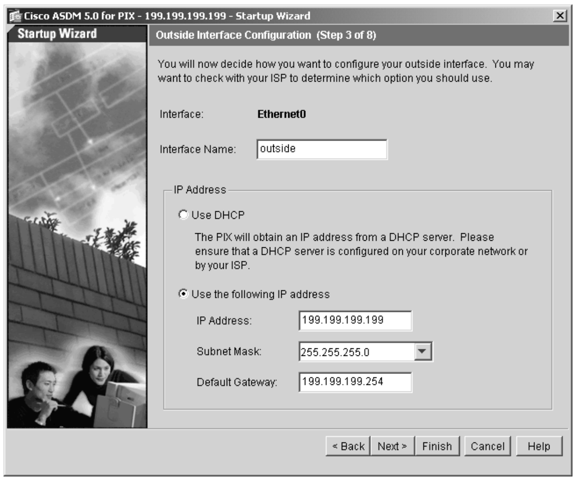
— The subnet mask provided by your ISP

— The default gateway provided by your ISP

In Figure 5-12, you can see that outside is entered as the name the interface, 199.199.199.199 as the IP address, 255.255.255.0 as the subnet mask, and 199.199.199.254 as the default gateway. A default security level will be set to 0 on your outside interface. These addresses were randomly chosen for the step-by-step procedures in this book. The address you actually enter will be provided by your ISP. Although not addressed in this book, your ISP might ask you to accept a DHCP address on the outside interface. To do this, you just click the **Use DHCP** option button.

Security level is important. In the ASA/PIX Security Appliance, traffic will flow unimpeded from a high-security level to a low-security level. Conversely, traffic from a low-security level to a higher-security level will be blocked by default. Later when you configure access lists, you will allow traffic from low to high.

Figure 5-12 *Outside Interface Configuration*



Cisco ASDM 5.0 for PIX - 199.199.199.199 - Startup Wizard

Startup Wizard

Outside Interface Configuration (Step 3 of 8)

You will now decide how you want to configure your outside interface. You may want to check with your ISP to determine which option you should use.

Interface: **Ethernet0**

Interface Name: outside

IP Address

○ Use DHCP

The PIX will obtain an IP address from a DHCP server. Please ensure that a DHCP server is configured on your corporate network or by your ISP.

● Use the following IP address

IP Address: 199.199.199.199

Subnet Mask: 255.255.255.0

Default Gateway: 199.199.199.254

By default on the ASA/PIX Security Appliance, because the inside interface has a security level of 100 and the outside has a default of 0, traffic originating from the inside is allowed to pass to the outside interface. Because the ASA/PIX Security Appliance is a stateful device, this means that all traffic going through the firewall will also be allowed to return. The default security appliance behavior blocks traffic sourced from the Internet, effectively mitigating against thousands of possible attacks that can be launched against your network from the Internet.

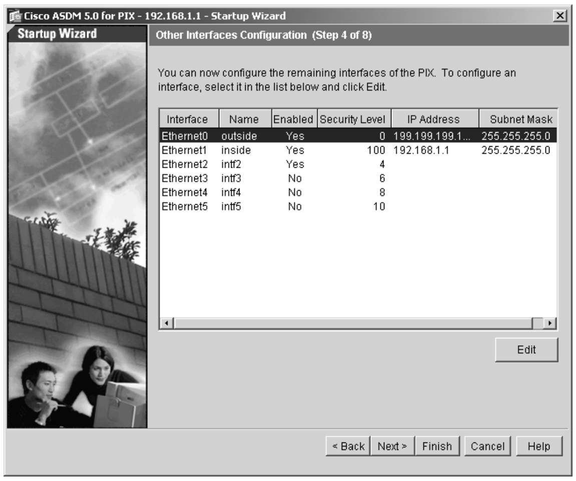
The IP addresses for the outside interface listed are only an example and will not work for your network deployment. You must use the values provided by your ISP.

Your service provider might not give you an IP address for the outside interface of your security appliance; they might require you to run DHCP and automatically configure your outside address using its DHCP server.

The next screen is titled Other Interface Configuration. (See Figure 5-13.) In this chapter, you do not make any changes to other interfaces. In Chapter 6, you add another interface if you plan to host a web or mail server.

Step 6 You shouldn't need to make any changes to this screen. Click **Next** to proceed.

Figure 5-13 *Other Interface Configuration*



Cisco ASDM 5.0 for PIX - 192.168.1.1 - Startup Wizard

Other Interfaces Configuration (Step 4 of 8)

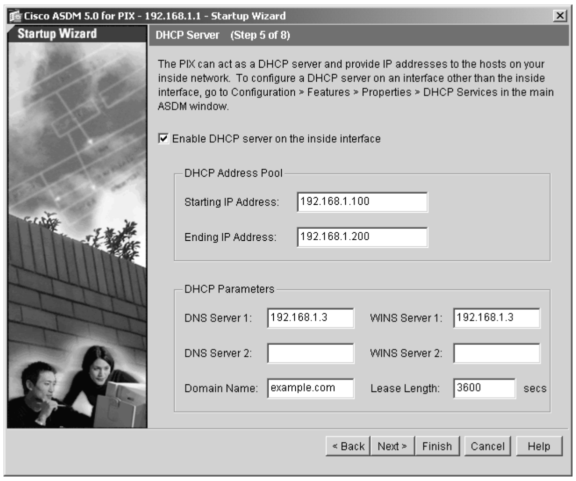
You can now configure the remaining interfaces of the PIX. To configure an interface, select it in the list below and click Edit.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask
Ethernet0	outside	Yes	0	199.199.199.1...	255.255.255.0
Ethernet1	inside	Yes	100	192.168.1.1	255.255.255.0
Ethernet2	intf2	Yes	4		
Ethernet3	intf3	No	6		
Ethernet4	intf4	No	8		
Ethernet5	intf5	No	10		

Step 7 The next screen, DHCP Server, allows you to automatically configure the IP addresses of your inside hosts. (See Figure 5-14.) As mentioned earlier in this chapter, the most expeditious way to deliver addresses to the inside is to use DHCP. If you use DHCP, the ASA/PIX Security Appliance assigns an address to each host on your inside network when the host boots up.

To activate DHCP, click the box next to **Enable the DHCP Server on the Inside Interface**.

Figure 5-14 *DHCP Server Configuration*



Cisco ASDM 5.0 for PIX - 192.168.1.1 - Startup Wizard

DHCP Server (Step 5 of 8)

The PIX can act as a DHCP server and provide IP addresses to the hosts on your inside network. To configure a DHCP server on an interface other than the inside interface, go to Configuration > Features > Properties > DHCP Services in the main ASDM window.

☑ Enable DHCP server on the inside interface

DHCP Address Pool

Starting IP Address: 192.168.1.100

Ending IP Address: 192.168.1.200

DHCP Parameters

DNS Server 1:	192.168.1.3	WINS Server 1:	192.168.1.3
DNS Server 2:		WINS Server 2:	
Domain Name:	example.com	Lease Length:	3600 secs

Step 8 Enter a range of IP addresses that will be allocated by DHCP for your hosts. Make sure you allow enough IP addresses for all of your hosts. Use a starting address of **192.168.1.100** and an ending address of **192.168.1.200**. You need to make sure that the range you use does not overlap with any other IP addresses, such as the inside interface of your security appliance (192.168.1.1) or the static address of your PC (192.168.1.2).

Step 9 You now need to enter the DNS and WINS address that you want automatically configured on your inside hosts. If you don't have your own DNS server, the address will be given to you by your ISP. A WINS server is required if you plan to use Microsoft File or Print Sharing on your network. You need to consult with Microsoft on how to enable this on your system. You can leave this field blank. In the example, the same address as my DNS and WINS server is used.

Step 10 To enable your PCs to accept DHCP addresses from your ASA/PIX Security Appliance, you need to go to the Network Control Panel, choose **Properties**, highlight **Internet Protocol**, choose **Properties**, check **Obtain an IP Address Dynamically**, check **Obtain a DNS Server Address Dynamically**, and then click **OK**.

After the wizard has completed and the PCs have been configured, addresses are automatically allocated when a PC is started and connected to the inside network.

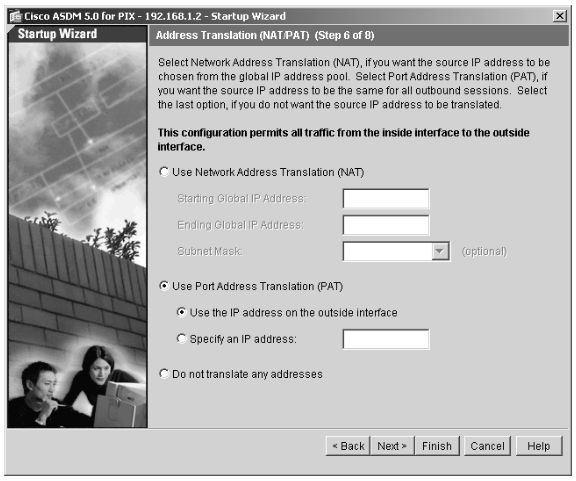
Step 11 If you have a domain name given to you by your ISP, enter it into the Domain Name field. This is an optional field.

Step 12 After you have filled in the values, click **Next** to proceed.

Step 13 The next screen is the Address Translation screen. (See Figure 5-15.) As mentioned previously in this chapter, private inside addresses are not routable on the Internet. Therefore, you must use NAT to translate the private addresses and allow them access to and from the Internet. In your case, you are going to use something called *port address translation* (PAT), which uses a combination of something called a port and the outside address of the ASA/PIX Security Appliance. Using PAT simplifies the configuration steps for address translation; in addition, because you are using an existing address, you don't need to purchase additional addresses from you ISP.

Click the **Use Port Address Translation** option button, click the **Use Port on the Outside Interface** option button, and then click **Next** to continue.

Figure 5-15 *Address Translation*



Address Translation (NAT/PAT) (Step 6 of 8)

Select Network Address Translation (NAT), if you want the source IP address to be chosen from the global IP address pool. Select Port Address Translation (PAT), if you want the source IP address to be the same for all outbound sessions. Select the last option, if you do not want the source IP address to be translated.

This configuration permits all traffic from the inside interface to the outside interface.

○ Use Network Address Translation (NAT)

Starting Global IP Address:

Ending Global IP Address:

Subnet Mask: (optional)

● Use Port Address Translation (PAT)

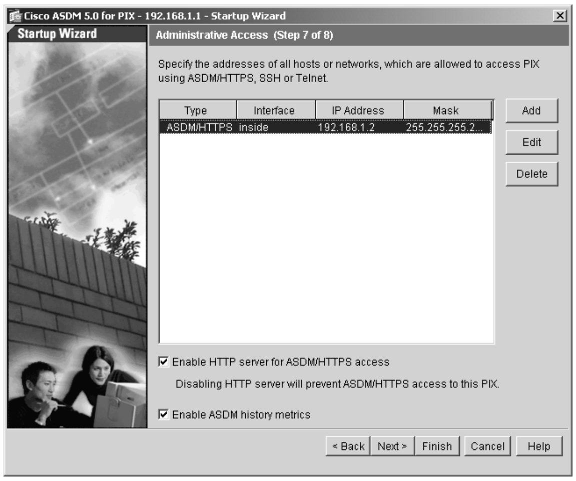
● Use the IP address on the outside interface

○ Specify an IP address:

○ Do not translate any addresses

Step 14 Now, you must select which IP addresses are allowed to have administrative access to your ASA/PIX Security Appliance. This specification should already be set or you wouldn't have access to ASDM. If you need to add additional authorized IP addresses, choose an interface and click **Add**. Then, enter the data for the PC for which you need to allow access. Click **Next**. This value should already be set from when you used the CLI to configure the security appliance to allow access from 192.168.1.2. (See Figure 5-16.)

Figure 5-16 *ASDM Configuration Panel*



Administrative Access (Step 7 of 8)

Specify the addresses of all hosts or networks, which are allowed to access PIX using ASDM/HTTPS, SSH or Telnet.

Type	Interface	IP Address	Mask
ASDM/HTTPS	inside	192.168.1.2	255.255.255.2...

☑ Enable HTTP server for ASDM/HTTPS access

Disabling HTTP server will prevent ASDM/HTTPS access to this PIX.

☑ Enable ASDM history metrics

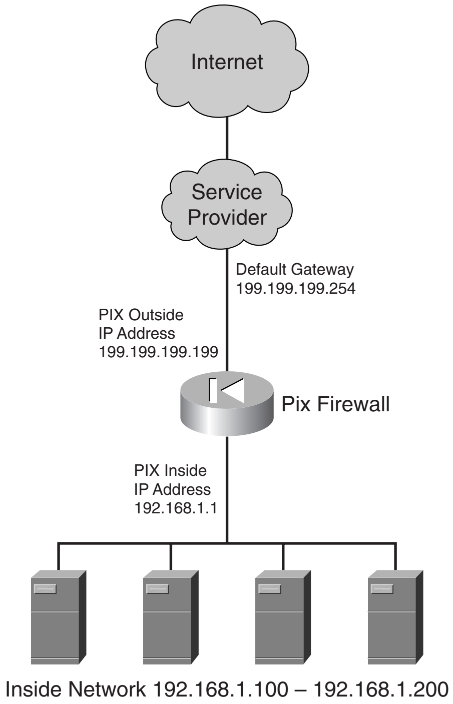
Step 15 Click **Finish**.

The ASA/PIX Security Appliance then automatically generates and sends commands to the security appliance according to the selections that you made during the wizard configuration process.

Congratulations! You now have a secure, working connection to the Internet.

When the Startup Wizard has completed, the resulting addresses of your network display, as shown in Figure 5-17.

Figure 5-17 *Server Topology*


Internet
Service Provider
Default Gateway 199.199.199.254
PIX Outside IP Address 199.199.199.199
Pix Firewall
PIX Inside IP Address 192.168.1.1
Inside Network 192.168.1.100 – 192.168.1.200

You are now protected from several hundred attacks that can originate from the Internet because traffic is allowed only from the inside out. In addition, by default, many processes are running on your firewall to help protect it from DoS attacks. You are still susceptible to many other attacks, such as mail- and web-based viruses, but in subsequent chapters, you are instructed on how to mitigate these threats.

Summary

In this chapter, you used ASDM to configure the ASA/PIX Security Appliance to enable the users inside your business or enterprise to securely access the World Wide Web.

In this chapter, you did the following:

- Gained an understanding of basic networking terminology
- Defined a network topology
- Assigned IP addresses to the network devices
- Configured connectivity between the ASA/PIX Security Appliance and the PC running ASDM
- Used the ASDM Startup Wizard to configure your network

Table 5-2 provides a summary of the network terminology defined in this chapter.

Table 5-2 *Network Terminology Summary*

Terminology	Definition
Inside IP address	The IP address of the inside interface of your firewall.
Outside IP address	The IP address of the outside interface of your firewall. This is provided by your service provider.
Default gateway	The next-hop IP address of your firewall outside interface. This is provided by your service provider.
Domain name	This is optional. If you are providing public services, you need to identify a domain name for those services. Either your ISP or a web registration service provides the domain name.
Public services	The public services include mail, web, or DNS servers. The intent of a public server is to share or exchange data with other Internet users. You may elect not to manage your own services and have your ISP manage the services for you.
Network address translation	This protocol enables you to use private addresses inside your network and still obtain Internet access.
Access passwords	These passwords allow privileged access to your firewall.
Inside addressing options (DHCP)	These are IP addresses that need to be assigned to devices on the inside of your firewall.
Internet	Several thousands of networks and hosts interconnected that reach all over the globe.
Service provider	The Internet service provider is a company that provides you with your access point into the Internet.

You then defined a topology that described your Internet connection in relation to your firewall and your protected users. The firewall outside interface, Ethernet 0, was plugged into a network connection provided by your ISP. Your inside users were connected to the inside of your firewall on the interface Ethernet 1.