This chapter covers the following subjects:

- Configuring access and translation rules using CiscoWorks Management Center for Firewalls (Firewall MC)
- Reporting, tool use, and administration using Firewall MC
- Introduction to the Auto Update Server (AUS)
- Cisco PIX Firewall and AUS communication settings using AUS
- Devices, images, and assignments in AUS
- Reporting and administration through AUS

It also covers the following supplemental topics:

- Firewall MC installation
- Key features and concepts of Firewall MC
- Importing devices into Firewall MC
- Device management and groups in Firewall MC
- Multiple firewall management in Firewall MC

CHAPTER 14

CiscoWorks Management Center for Firewalls (PIX MC)

Configuring your Cisco PIX Firewalls with a graphical interface enables you to manage their operation efficiently. Chapter 13, "PIX Device Manager," explains how to use the PIX Device Manager (PDM) to configure a single PIX system. This graphical interface is very effective to administer just a few PIX systems, but if you manage a larger number of PIX devices, you need a different application. The CiscoWorks Management Center for Firewalls (Firewall MC) enables you to manage multiple PIX devices easily from a single graphical interface. This chapter explains in detail the major features of Firewall MC and how you can use that functionality to manage multiple PIX devices across your network.

To manage the configuration of multiple firewalls effectively, you must also maintain current software images. The Auto Update Server (AUS) enables you to maintain and deploy up-to-date software images on your managed firewalls. This chapter explains how you can use the AUS to manage the images on your managed firewalls.

How to Best Use This Chapter

This chapter provides an overview of both the Firewall MC and the AUS. Unlike the PDM, the Firewall MC provides a graphical user environment suited to managing large numbers of firewalls, and the AUS enables you to maintain current images and configurations efficiently on a large number of firewalls. Understanding these applications is vital if you manage a large number of firewalls. If you are at all familiar with these applications, you will probably find this chapter very easy. Test yourself with the "Do I Know This Already?" quiz.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide if you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The ten-question quiz, derived from the major sections in the "Foundation and Supplemental Topics" portion of the chapter, helps you determine how to spend your limited study time.

Table 14-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 14-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Supplemental or Foundations Topics Section	Questions Covered in This Section	Score
CiscoWorks Management Center for Firewalls Overview	6	
CiscoWorks	5	
Firewall MC Interface	4	
Basic User Task Flow		
Device Management	8	
Configuration Tasks	1, 2, 10	
Reports	3	
Administration Tasks	7	
CiscoWorks Auto Update Server (AUS)	9	

CAUTION The goal of self assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of the self assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following are types of building blocks? (Choose two.)
   a. Network objects
   b. Address translation pools
   c. Access rules
   d. Static translation rules
   e. Dynamic translation rules

2. What are the three types of access rules?

   a. Firewall rules
   b. Static translation rules
   c. AAA rules
   d. Dynamic translation rules
   e. Filter rules

3. What are the three reports supported by Firewall MC?

   a. Device Report
   b. Activity Report
   c. Configuration Differences report
   d. Device Setting Report
   e. Deployment reports

4. When making changes to device configurations in Firewall MC, the changes can apply to which firewalls?

   a. A single firewall
   b. The firewalls in a group
   c. All of the managed firewalls
   d. Firewalls belonging to multiple groups
   e. Answers a, b, and c

5. Which software manages login access to the Firewall MC?

   a. CiscoWorks
   b. Firewall MC
   c. Windows OS
   d. Auto Update Server
   e. None of the above

6. Firewall MC groups comprise which items? (Choose two.)
   a. Configuration lists
   b. Devices
   c. Subgroups
   d. Software images
   e. Access lists

7. What are the three steps involved in updating device configurations when workflow is enabled?
   a. Define, deploy, review
   b. Define, test, evaluate
   c. Create, test, review
   d. Define, approve, deploy
   e. None of the above

8. Which of the following is not an option when importing devices into Firewall MC?
   a. Import configuration file for a device
   b. Import configuration file for multiple devices
   c. Import configuration from PDM
   d. Create firewall device
   e. Import configuration from device

9. Which of the following is not a configuration tab in AUS?
   a. Devices
   b. Deployment
   c. Images
   d. Assignments
   e. Admin

10. Which translation rules define a permanent mapping between an internal IP address and a public IP address?

    a. Dynamic translation rules
    b. AAA rules
    c. Web filter rules
    d. Static translation rules
    e. None of the above

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. This includes the "Foundation and Supplemental Topics," "Foundation Summary," and "Q&A" sections.
- **9 or 10 overall score**—If you want more review of these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation and Supplemental Topics

CiscoWorks Management Center for Firewalls Overview

The CiscoWorks Management Center for Firewalls (Firewall MC) enables you to manage the configuration of multiple PIX Firewall devices deployed throughout your network. Firewall MC is a Web-based application that provides centralized management for devices on your network and accelerates the deployment of firewalls to protect your network. Some features of Firewall MC are as follows:

- Web-based interface for configuring and managing multiple firewalls
- Configuration hierarchy and user interface to facilitate configuration of firewall settings
- Support for PIX Firewall Version 6.0 and later
- Ability to import configurations from existing firewalls
- Ability to support dynamically addressed PIX Firewalls
- Support for up to 1000 PIX Firewalls
- Secure Sockets Layer (SSL) protocol support for client communications to CiscoWorks
- Support for Workflow and audit trails

To obtain maximum functionality from Firewall MC, you need to understand the following items:

- Key concepts
- Supported devices
- Installation

Key Concepts

To use Firewall MC effectively to manage and configure the PIX Firewalls on your network, you need to understand certain key concepts. These concepts fall into the following three categories:

- Configuration hierarchy
- Configuration elements
- Workflow process

Configuration Hierarchy

All devices managed by Firewall MC are grouped in a hierarchical structure beneath a global group. By placing managed devices in different groups and subgroups, you can simplify your configuration and management tasks because each group can include devices with similar attributes, such as similar access rules and configuration settings.

Each device managed by Firewall MC can be a member of only one specific group. A group is composed of one or more of the following items:

- Subgroups
- Devices

Devices inherit properties either from a specific group or individually from a specific device. Inheritance of properties allows your configuration changes to apply to multiple managed devices using less administrative effort.

Configuration Elements

Through Firewall MC, you can configure various characteristics of the managed firewalls deployed throughout your network. These characteristics fall into the following four major categories:

- Device settings
- Access rules
- Translation rules
- Building blocks

Device settings control specific configuration parameters on your PIX Firewalls, such as interface and routing properties. Access rules regulate network traffic and fall into the two categories shown in Table 14-2. Translation rules define the address translations that your firewalls will perform on network traffic. Building blocks associate names with specific objects, such as subnets, that you can then use when defining rules. All of the configuration elements are explained in detail later in this chapter.

Table 14-2 *Access Rule Types*

Access Rule Type	Description
Mandatory	Rules that apply to an enclosed group and that are ordered down to the devices in the group. These rules cannot be overwritten.
Default	Rules that apply to all of the devices in a group. These rules can be overwritten.

Workflow Process

The workflow process divides configuration changes made using Firewall MC into the following three steps:

Step 1 Define configuration.

Step 2 Implement configuration (approve).

Step 3 Deploy configuration.

A collection of configuration changes made for a specific purpose is called an *activity*. After you submit an activity to be deployed, it is converted into a set of configuration files known as a *job*. Finally, the job is scheduled for deployment on the network. A different person can approve each of these steps. Activities and job management are explained in detail later in the chapter.

Supported Devices

Firewall MC Version 1.2.1 supports PIX Firewall Versions 6.0, 6.1, 6.2, and 6.3.*x* along with the Firewall Service Module (FWSM) Version 1.1.*x*.

NOTE Not all PIX command-line interface (CLI) commands are configurable by using Firewall MC. For a complete list of Firewall MC[en]supported commands and devices refer to http://www.cisco.com/en/US/products/sw/cscowork/ps3992/products-device-support-tables-list.html.

The following PIX hardware models are supported by Firewall MC Version 1.2.1:

- PIX 501
- PIX 506/506E
- PIX 515/515E
- PIX 525
- PIX 535
- FWSM

Installation

Firewall MC requires CiscoWorks Common Services to run. Therefore, before you can install Firewall MC, you must install CiscoWorks Common Services (Version 2.2). Common Services provides services for the following:

- Interacting with the CiscoWorks desktop

- Setting up the CiscoWorks server
- Administering the CiscoWorks server
- Adding external connections to the CiscoWorks server
- Database administration for Firewall MC applications
- System administration
- Logging
- Diagnosing problems with the CiscoWorks server

For CiscoWorks to operate efficiently, your CiscoWorks server and client computers must meet certain hardware requirements.

Server Requirements

When installing Firewall MC, you need to understand the hardware and software requirements for the different components. To support all of the functionality provided by Firewall MC and the underlying CiscoWorks foundation, your CiscoWorks server must meet the following minimum requirements:

- IBM PC-compatible computer
- 1-gigahertz (GHz) or faster processor
- Color monitor with video card capable of viewing 256 colors
- CD-ROM drive
- 10Base-T or faster network connection
- Minimum of 1 gigabyte (GB) of random-access memory (RAM)
- 2 GB of virtual memory
- Minimum of 9 GB of free hard drive space (NTFS)
- Open Database Connectivity (ODBC) Driver Manager 3.510 or later
- Windows 2000 Professional and Windows 2000 Server (with Service Pack 3 or 4)

NOTE Requirements for the CiscoWorks server are frequently updated. For the latest server requirements, refer to the documentation on the Cisco website.

Client Requirements

Although the Firewall MC runs on a server, access to Firewall MC is by a browser running on a client system. Client systems also must meet certain minimum requirements to ensure successful system operation. Your client systems should meet the following minimum requirements:

- IBM PC-compatible
- 300-megahertz (MHz) or faster processor
- Minimum 256 MB of RAM
- 400 MB of virtual memory (free space on hard drive)

Along with these requirements, your clients must be running one of the following operating systems:

- Windows 2000 Professional or Server (with Service Pack 3 or later)
- Windows XP Professional (with Service Pack 1) with Microsoft Virtual Machine
- Windows 98

One final requirement is that your client systems must use one of the following web browsers:

- Internet Explorer 6.0 (Service Pack 1) with Microsoft Virtual Machine
- Netscape Navigator 4.78
- Java Virtual Machine (JVM) version 5.1

NOTE Requirements for the CiscoWorks clients are frequently updated. For the latest client requirements, refer to the documentation on the Cisco website.

PIX Bootstrap Commands

When you initially configure your PIX Firewall, you run the **setup** command to configure many of the basic components of the operational configuration. The **setup** command prompts you for the following items:

- Enable password
- Clock Universal Time Coordinate (UTC)
- Date
- Time
- Inside Internet Protocol (IP) address
- Inside network mask
- Host name
- Domain name
- IP address of host running PDM

Besides this information, you must also configure the firewall to allow modification from a browser connection and specify which hosts or network is allowed to initiate these Hypertext

Transfer Protocol (HTTP) connections. Complete the following steps to enable the Firewall MC server to update the configuration on your firewall:

Step 1 Enable the firewall configuration to be modified from a browser by using the following command:

```
http server enable
```

Step 2 Specify the host or network authorized to initiate HTTP connections to the firewall by using the following command:

```
http ip-address [netmask] [interface-name]
```

Step 3 Store the current configuration in Flash memory using the following command:

```
write memory
```

CiscoWorks

CiscoWorks is the heart of the Cisco family of comprehensive network management tools that allow you to access and manage the advanced capabilities of the Cisco AVVID (Architecture for Voice, Video and Integrated Data) easily. It provides the foundation upon which Firewall MC (and other management center applications such as the AUS) is built. Therefore, before you can access the Firewall MC application, you must first log in to CiscoWorks. To use Firewall MC, you need to understand the following CiscoWorks functionality:

- Login process
- User authorization roles
- Adding users

Login Process

To access the applications supported by CiscoWorks, such as Firewall MC and AUS, you must first log in to the CiscoWorks server desktop. The CiscoWorks server desktop is the interface used for CiscoWorks network management applications, such as Firewall MC.

To log in to CiscoWorks, you connect to the CiscoWorks desktop using a web browser. By default, the CiscoWorks web server listens on port 1741. So, if your CiscoWorks desktop is on a machine named *CW.cisco.com* through your Domain Name System (DNS) with an IP address of 10.10.20.10, you could connect to it by entering either of the following Universal Resource Locators (URLs):

- http://CW.cisco.com:1741/
- http://10.10.20.10:1741/

NOTE You can also enable CiscoWorks to use HTTP over SSL (HTTPS) instead of HTTP. When you install some management centers (such as the Management Center for Cisco Security Agents), they enable HTTPS on CiscoWorks automatically. When HTTPS is enabled, you need to connect to port 1742.

At the initial CiscoWorks window, log in to CiscoWorks by entering a valid username and password (see Figure 14-1).

NOTE Initially, you can log in using the administration account created during installation. The default value is *admin* for both the username and password (unless you changed these values during the installation process). For security reasons, you should change these values.

Figure 14-1 *CiscoWorks Login Window*

User Authorization Roles

CiscoWorks enables you to define different roles for different users. A role can enable a user to perform specific operations when using CiscoWorks and any of the applications that are built upon CiscoWorks (such as Firewall MC). CiscoWorks supports five different user roles that are relevant to Firewall MC operations (see Table 14-3).

Table 14-3 *CiscoWorks User Roles*

User Role	Description
Help Desk	Provides read-only access for the entire system
Approver	Can review policy changes and accept or reject changes
Network Operator	Can create and submit jobs
Network Administrator	Can perform administrative tasks on Firewall MC
System Administrator	Performs all operations

NOTE You can assign each user multiple authorization roles (depending on the user's responsibilities). CiscoWorks also supports two other roles: *Export Data* and *Developer*. These roles are not relevant to the Firewall MC operations.

Adding Users

As part of your Firewall MC configuration, you must configure accounts for the various users that need to access Firewall MC. The CiscoWorks Add User window enables you to create new accounts that have access to the CiscoWorks applications. To create a new account in CiscoWorks, perform the following steps:

Step 1 Log in to the CiscoWorks desktop.

Step 2 Choose **Server Configuration > Setup > Security > Add Users**. The Add User window appears (see Figure 14-2).

Figure 14-2 *CiscoWorks Add User Window*

Step 3 Enter values for the new user (Table 14-4 describes the various fields).

Table 14-4 *CiscoWorks Add User Fields*

Field	Description
User Name	Username of the account being added
Local Password	Password for the new user
Confirm Password	Confirmation of the user's password
E-Mail	(Optional) User's e-mail address
CCO Login	(Optional) User's Cisco Connection Online (CCO) login name
CCO Password	User's CCO password (required only if CCO login is specified)

continues

Table 14-4 *CiscoWorks Add User Fields (Continued)*

Field	Description
Confirm Password	Confirmation of user's CCO password (required only if CCO password is entered)
Proxy Login	(Optional) User's proxy login (required only if your network requires use of a proxy server)
Proxy Password	User's proxy password (required only if Proxy Login is specified)
Confirm Password	Confirmation of user's proxy login (required only if Proxy Login is specified)

Step 4 Using the **Roles** section of the **Add User** window, select the roles associated with the user's responsibilities. You can assign multiple roles to a single user, giving that user a combination of user rights.

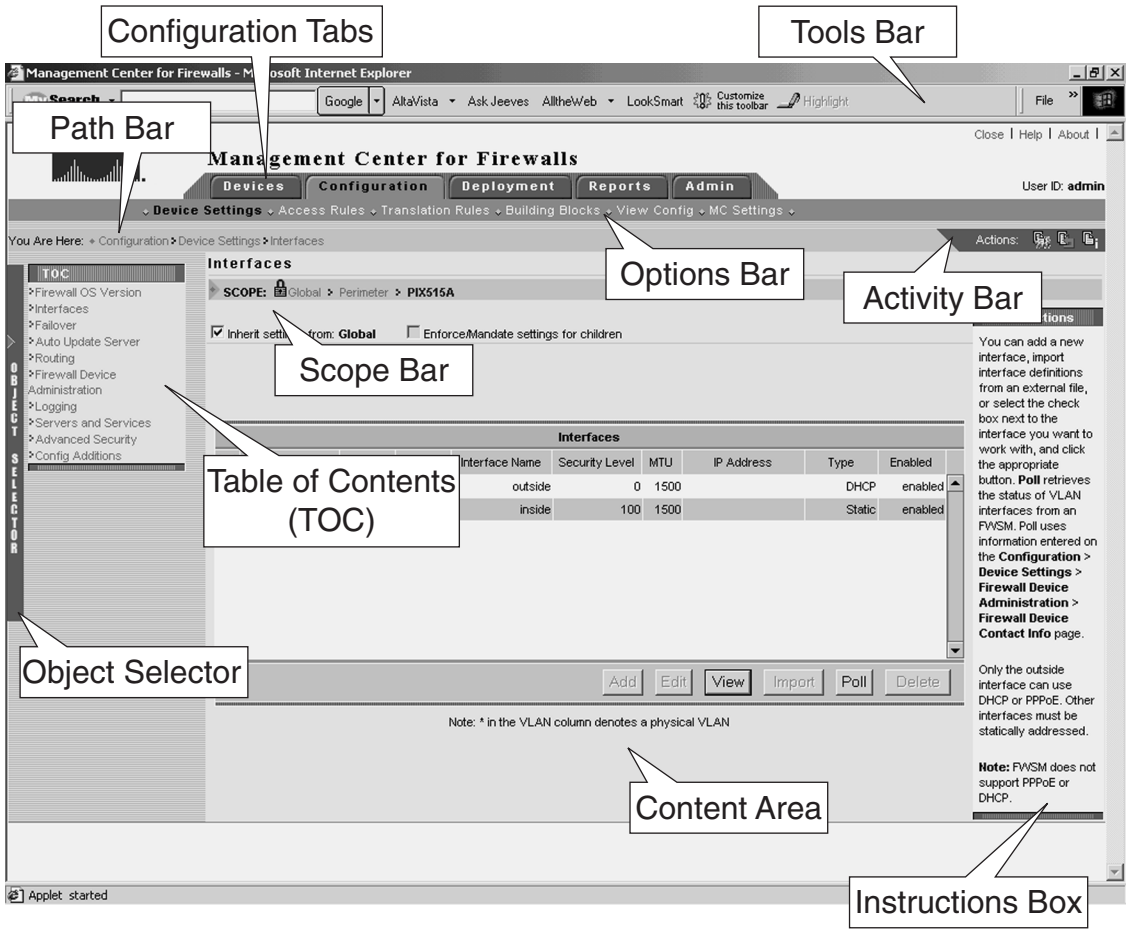
Step 5 Click **Add** to complete the addition of the user to the CiscoWorks database.

Firewall MC Interface

Although the Firewall MC user interface is graphical and easy to use, it is helpful to understand how the interface is structured. The Firewall MC user interface is composed of the following major sections (see Figure 14-3):

- Configuration tabs
- Options bar
- Table of contents (TOC)
- Path bar
- Instruction box
- Content area
- Scope bar
- Object Selector handle
- Tools bar
- Activity bar

Figure 14-3 *Firewall MC User Interface*



Configuration Tabs

The configuration tasks are broken down into the following five major categories:

- **Devices**—Enables you to import device configurations and define device groups to be managed by the system
- **Configuration**—Enables you to change the operational configuration of the devices managed by the system
- **Deployment**—Enables you to generate configuration files, manage firewall configuration files, and submit or manage new jobs

- **Reports**—Enables you to generate reports, view scheduled reports, and view reports
- **Admin**—Enables you to configure system settings

NOTE When you enable workflow, the Deployment tab changes to Workflow.

To access any of the categories, click the tab labeled with the appropriate name. The tabs are located across the top of the Firewall MC display.

Options Bar

After clicking one of the major configuration tabs, the options for that selection are displayed in a list located in the window just below the configuration tabs. Figure 14-3 shows a window in which the Configuration tab has been selected. The options associated with the Configuration tab are as follows:

- Device Settings
- Access Rules
- Translation Rules
- Building Blocks
- View Config
- MC Settings

Click an option to display the information in the content area or a menu of available choices (known as the TOC) on the left side of the Firewall MC interface.

Table of Contents

The *table of contents* (*TOC*) is a menu of choices that is displayed on the left side of the Firewall MC interface. It presents a list of suboptions you can select based on the option chosen. As shown in Figure 14-3, for instance, the Configuration > Device Settings option has the following selections:

- Firewall OS Version
- Interfaces
- Failover
- Auto Update Server
- Routing
- Firewall Device Administration
- Logging

- Servers and Services
- Advanced Security
- Config Additions

Path Bar

The *path bar* provides a visual road map indicating where you are with respect to the Firewall MC interface. It is located above the TOC and below the options bar, and it begins with the text "You Are Here."

Figure 14-3 shows a situation in which the value of the path bar is Configuration > Device Settings > Interfaces. This indicates that you performed the following steps to reach the current window:

Step 1 You clicked the **Configuration** tab.

Step 2 You clicked the **Device Settings** option.

Step 3 You clicked the **Interfaces** TOC option.

Instructions Box

Some pages provide you with an *Instructions box* on the right side of the Firewall MC display. When displayed, this box provides you with a brief overview of the page that you have selected. The Instructions box provides less information than the Help option on the tools bar.

Content Area

The *content area* displays the information associated with the option that you selected (when no TOC selections are available) or the selection in the TOC that you click.

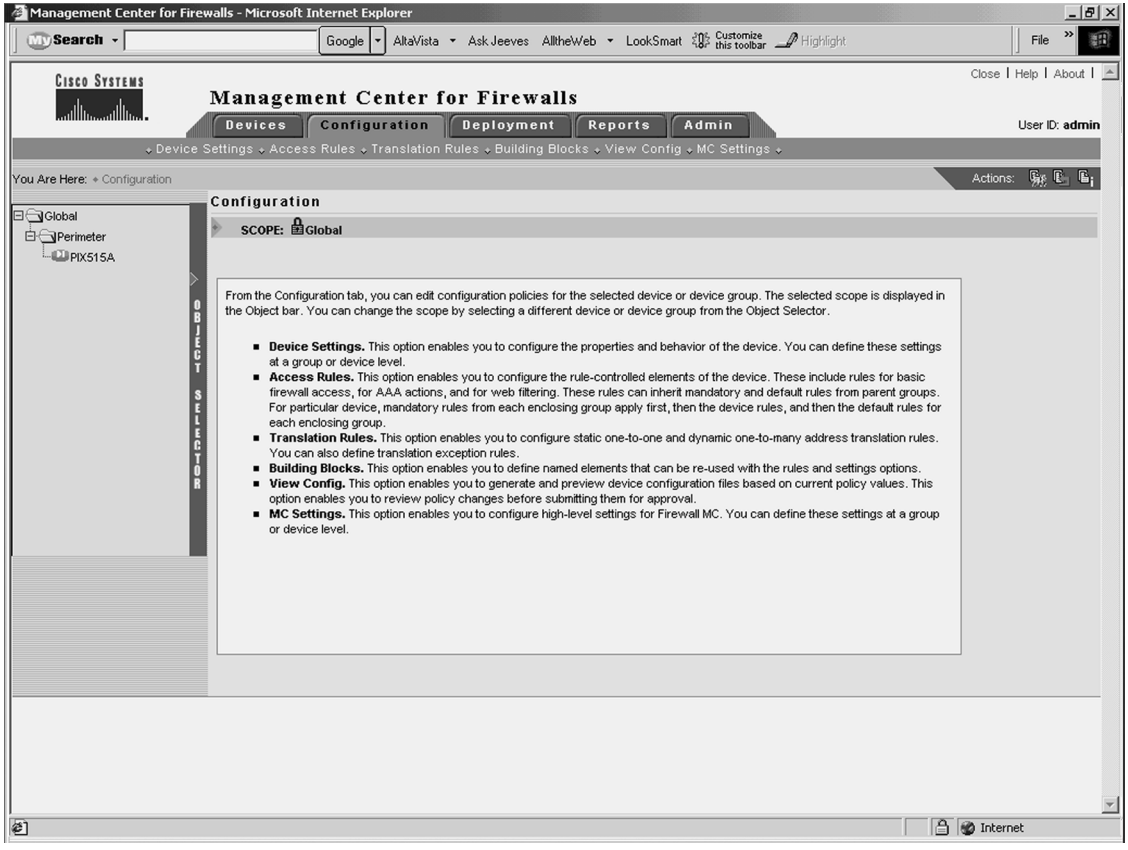
Scope Bar

The *Scope bar* displays the object or objects that you have selected using the Object Selector. Figure 14-3 shows a situation in which you have selected the firewall named PIX515A from the Perimeter firewall group, which is part of the Global group. When you perform configuration changes, the Scope bar indicates which devices will receive updated configuration information.

Object Selector

When making configuration changes using Firewall MC, you need to specify to which device or devices you want to apply changes. By clicking the *Object Selector*, you can select individual firewalls or firewall groups (see Figure 14-4). Any changes that you specify are then applied to that firewall or firewall group. The Scope bar indicates the device or group that you currently have selected.

Figure 14-4 *Object Selector*



Tools Bar

Located in the upper-right portion of the Firewall MC interface is the *Tools bar*. The Tools bar has the following options:

- Close

- Help
- About

Click **Close** to log out of the current Firewall MC user session. Select **Help** to open another browser window that displays detailed context-sensitive help information on using Firewall MC. Finally, click **About** to display information about the version of Firewall MC that you are using.

Activity Bar

The activity bar displays activities and Actions icons that vary depending on the information that you are changing. The activity bar is shown only when you are operating in either the Devices or Configuration tabs of the Firewall MC. The Actions icons that can be shown are as follows:

- **Add**—Add a new activity
- **Open**—Open a new or existing activity (selected from a popup window)
- **Close**—Close the activity shown by the activity bar
- **Save and Deploy**—Save and generate a device configuration file
- **Submit**—Submit an activity
- **Reject**—Reject an activity
- **Approve**—Approve an activity
- **Undo**—Discard the activity shown by the activity bar
- **View Details**—show the details of the current changes

NOTE Some of the activity options are not available unless you enable workflow. Workflow is explained later in the chapter.

Basic User Task Flow

Firewall MC provides you with a flexible graphical user environment in which to manage and configure the firewall devices deployed throughout the network. When you first begin to use Firewall MC, however, you might become confused as to where to start. Therefore, it is helpful to understand the basic user task flow involved in using Firewall MC. The following steps illustrate the basic task flow:

Step 1 Create device groups.

Step 2 Import/create devices.

Step 3 Configure building blocks.

Step 4 Configure device settings.

Step 5 Configure access and translation rules.

Step 6 Generate and view the configuration.

Step 7 Deploy the configuration.

NOTE The approval process for configuration changes is disabled by default. If you enable this process (see the "Workflow Setup" section later in the chapter), before you can deploy your changes you will have to follow the approval process for those changes.

Each step is explained in detail in the following sections. Each section is broken down based on the five configuration tabs available in the Firewall MC interface:

- Device management
- Configuration tasks
- Deployment tasks
- Reports
- Administration tasks

Device Management

When using the Firewall MC, all managed devices are members of a group named Global. You also can group your firewalls into subgroups that share similar properties (such as configuration settings or geographic location). Grouping similar devices facilitates management of those devices. You can also import existing configurations into Firewall MC. These activities are accessed through the Devices configuration tab. The tasks in this section include the following:

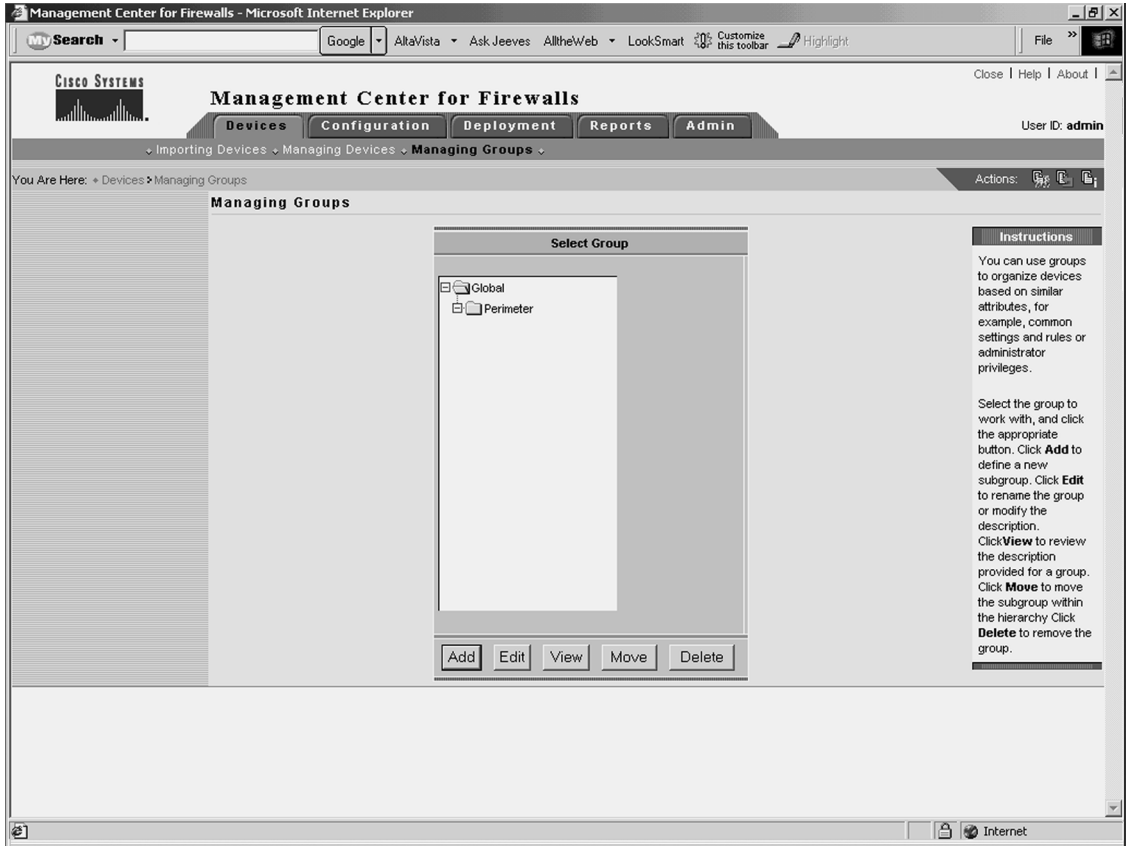
- Managing groups
- Importing devices
- Managing devices

Managing Groups

Select **Devices > Managing Groups** to add new groups to the system, modify existing groups, and delete existing groups (see Figure 14-5). When defining group names, it is helpful to use descriptive names that clearly identify the different groups. For example, you may identify your groups based on geographic region or department within the company.

NOTE Subgroup names must be unique within an enclosing group.

Figure 14-5 *Managing Groups*



When managing groups, you can perform the following operations:

- **Add**—Add new groups
- **Edit**—Rename existing groups
- **View**—View the description for a group
- **Move**—Move the group to a new location in the hierarchy
- **Delete**—Remove an existing group

Importing Devices

After defining your device groups, you can then import devices into those groups using the Devices > Import Devices option. When importing devices, you perform the following four basic steps:

Step 1 Select the target group.

Step 2 Select the import type.

Step 3 Define firewall device basic information.

Step 4 Review summary details.

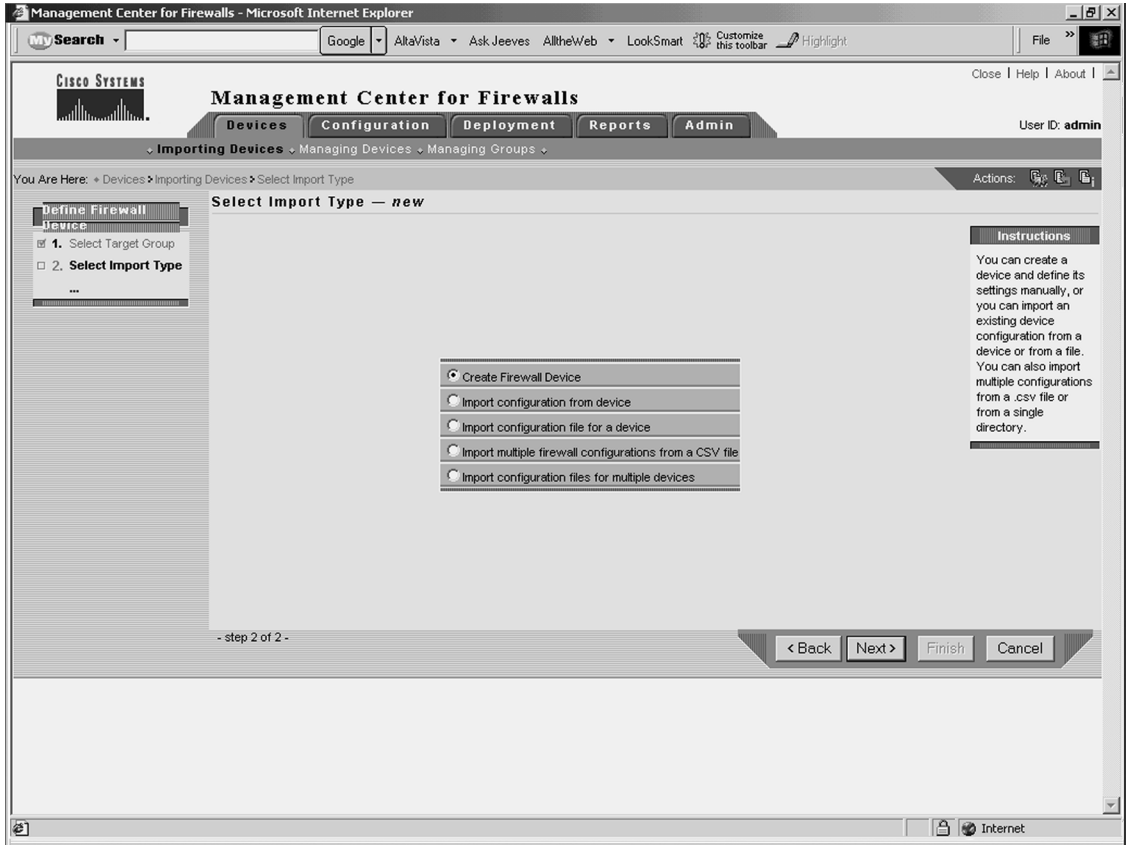
You have several options when importing devices into Firewall MC (see Figure 14-6). Table 14-5 explains the various import options that are available.

Table 14-5 *Device Import Options*

Import Option	Description
Create Firewall Device	Allows you to add a single device manually.
Import configuration from device	Allows you to provide device credentials manually that enable the Firewall MC server to communicate directly with the device to retrieve the configuration.
Import configuration file for a device	Allows you to import configuration information for a single device from a configuration file.
Import multiple firewall configurations from a CSV file	Allows the Firewall MC server to communicate directly with multiple firewalls (specified in a comma-separated value [CSV] file) to retrieve configuration information.
Import configuration files for multiple devices	Allows you to import multiple configuration files from a single directory. Each file contains configuration information for a single device.

NOTE You can import from a device only once. To reimport a device's configuration, you must first delete the device and then import it again.

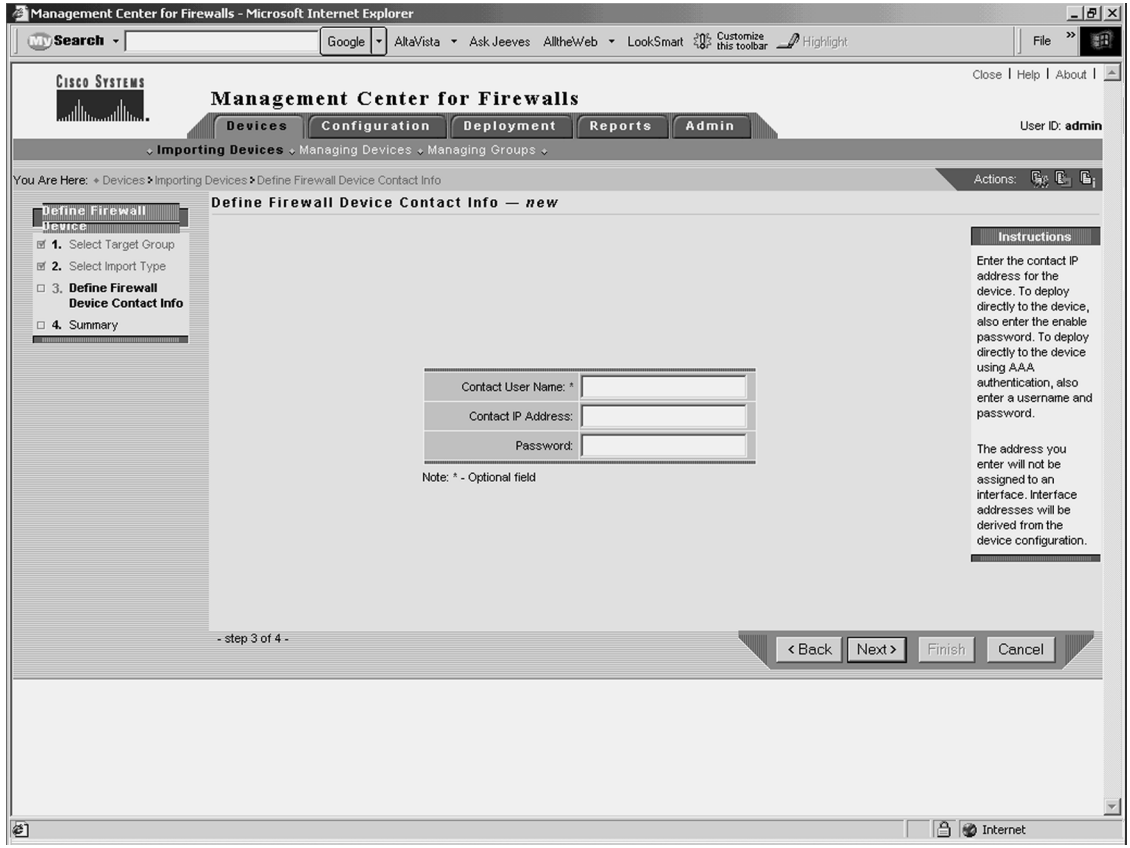
Figure 14-6 *Select Import Type*



If you select the Import configuration from device option as the import type, you must provide the following parameters that Firewall MC needs to communicate with the device being imported (see Figure 14-7):

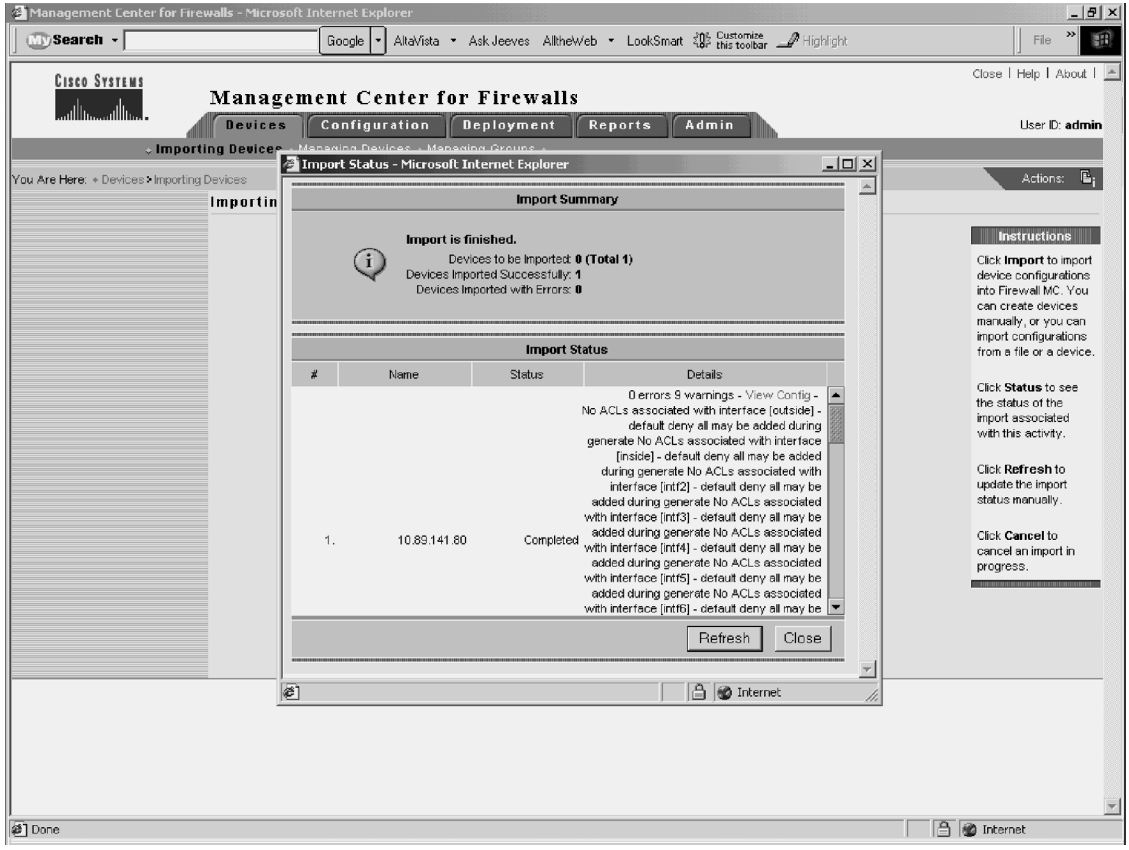
- **Contact User Name**—(Optional) The username used when connecting to the firewall
- **Contact IP Address**—The IP address used to connect to the firewall
- **Password**—The firewall enable password

Figure 14-7 *Firewall Contact Information*



After specifying all of the characteristics for the device being imported, you will see an Import Status window (see Figure 14-8). This window displays the progress of the actual import process, and it automatically updates itself every 60 seconds. You can also force the window to update by clicking the **Refresh** button.

Figure 14-8 *Import Status Window*

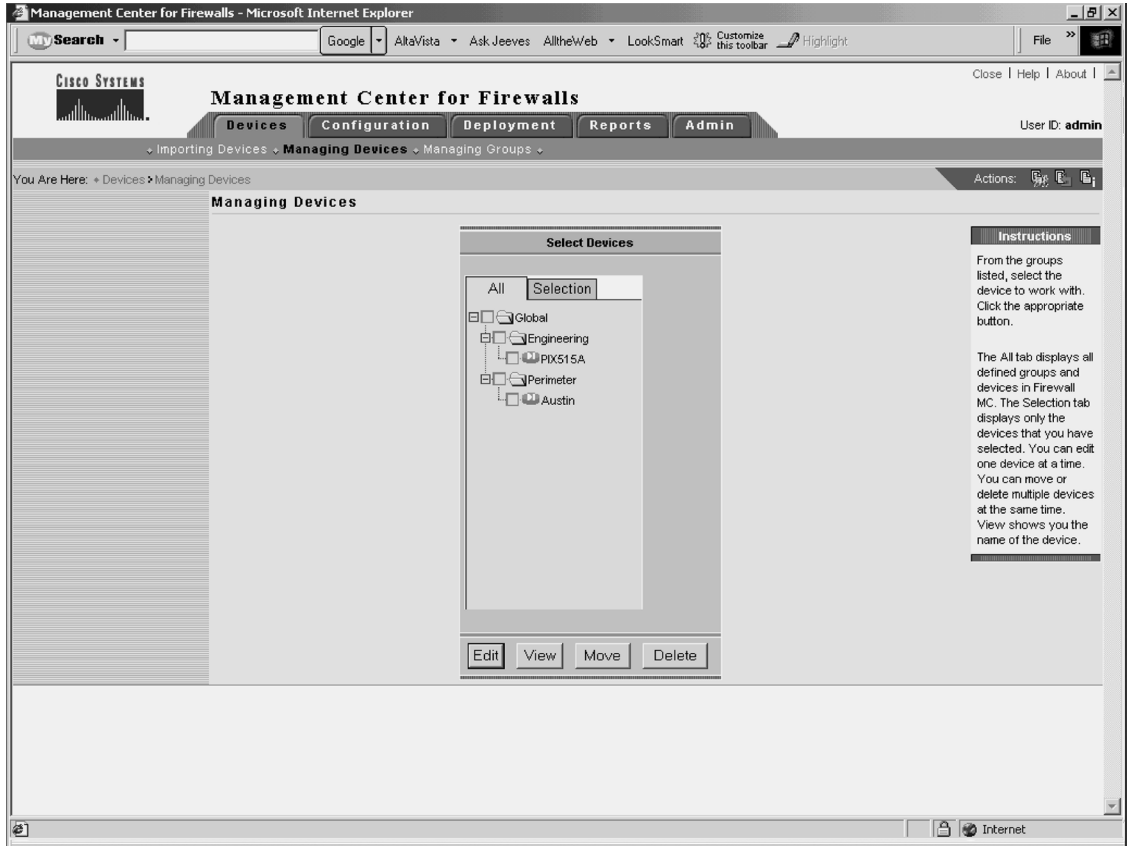


When the import is complete, you can view the configuration of the device by clicking the **View Config** link located in the Details section of the Import Status window (see Figure 14-8).

Managing Devices

Sometimes you need to remove devices or move them from one group to another. To perform these types of device operations, select **Devices > Managing Devices**. The Managing Devices window enables you to move a device from one group to another and remove existing devices (see Figure 14-9).

Figure 14-9 *Managing Devices*



Configuration Tasks

The majority of the tasks that you perform in Firewall MC involves configuration tasks. Configuration settings control individual features of a firewall device. When defining these settings, you can apply them either to a specific firewall or to all of the firewalls in a group by selecting a group instead of an individual firewall. The scope of the changes that you make depends on the object that you select using the Object Selector before making the configuration changes (see the section entitled "Object Selector" earlier in this chapter). These tasks can be broken down into the following categories, each of which is discussed in detail in this section:

- Configuring device settings

- Defining access rules
- Defining translation rules
- Creating building blocks
- Generating and viewing configuration information

Configuring Device Settings

Through the Firewall MC, you can configure many device-specific properties on your managed firewalls. Following are the majority of the device settings that you can configure through Firewall MC:

- PIX operating system version
- Interfaces
- Failover
- Routing
- PIX Firewall administration
- Logging
- Servers and services
- Advanced security
- Firewall MC controls

One common task is changing the properties of the interfaces on the firewalls managed by the Firewall MC software. If you configure a firewall using Setup, it configures only the inside interface. Before you can define the access or translation rules, you must configure the rest of the interfaces on the firewall.

Defining Access Rules

Access rules, which control the traffic that flows through your firewall, are used to define your network security policy. Each access rule is a member of an order list of rules that Firewall MC stores in a table. Rules are processed from first to last. A firewall uses the first matching rule to determine whether the traffic is permitted or denied.

You can configure the following three types of access rules (see Figure 14-10):

- Firewall rules
- Authentication, authorization, and accounting (AAA) rules
- Web filter rules

Figure 14-10 *Access Rules*

In Firewall MC, you can view a list of access rules that spans all of the different interfaces (see Figure 14-10). Each access rule shown is converted into a single entry in an access control list (ACL) on a specific interface for the managed firewall.

Defining Translation Rules

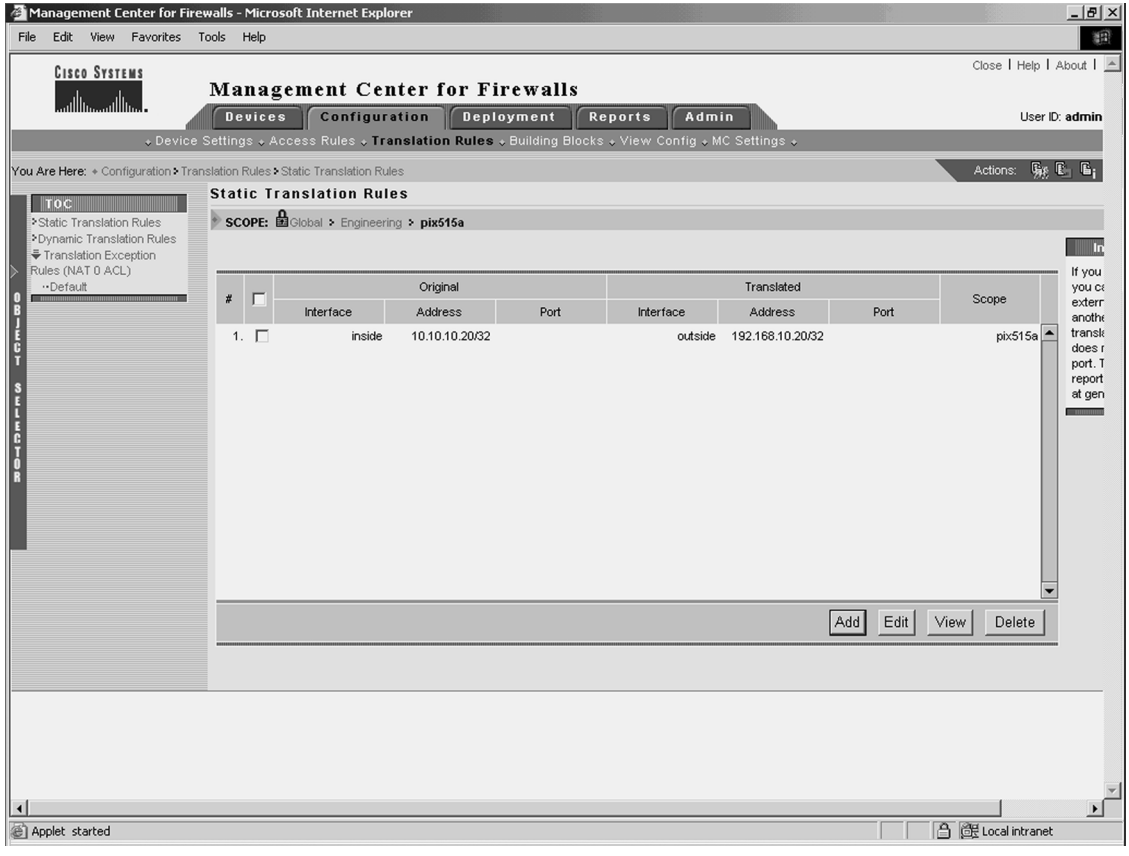
Translation rules enable you to configure and view the address translations that you are using on the network. You can configure the following types of translation rules using Firewall MC:

- Static translation rules
- Dynamic translation rules
- Translation exception rules (NAT 0 ACL)

> **NOTE** Firewall MC supports both Network Address Translation (NAT) and Port Address Translation (PAT).

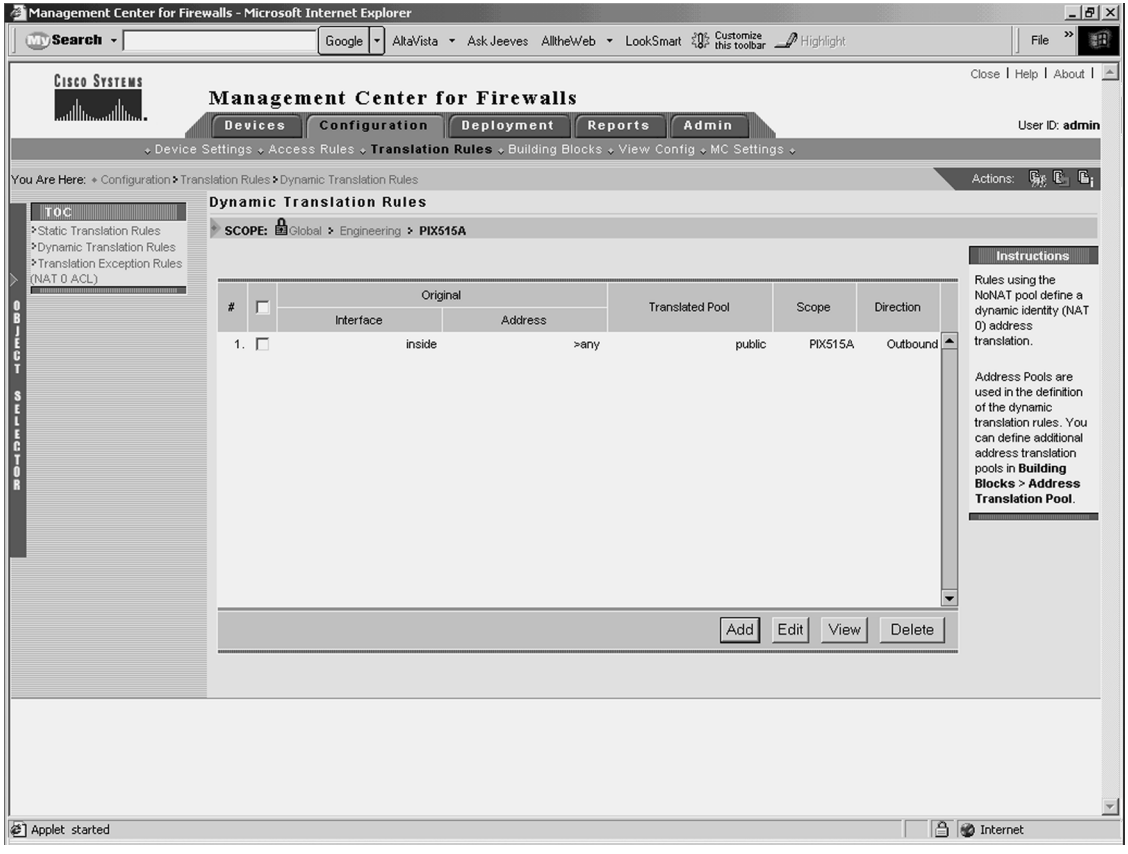
Static translation rules permanently map an internal IP address to a publicly accessible global IP address. These rules assign a host on a higher-security-level interface to a global IP address on a lower-security interface. This enables the hosts from the lower-security zone to communicate with the host from the higher-security zone. Figure 14-11 shows a static translation rule that assigns the local address of a protected host (10.10.10.20/32 on the inside interface) to a global address (192.168.10.20/32 on the outside) that is accessible by external systems.

Figure 14-11 *Static Translation Rules*



Unlike static translation rules, dynamic translation rules do not permanently map an internal IP address to a global IP address. These rules dynamically map an internal IP address to a global IP address from a pool of IP addresses when using NAT or to a single IP address when using PAT. Figure 14-12 shows a dynamic translation rule that translates traffic from any address on the inside interface to a global address using the address translation pool named *public* for outbound traffic.

Figure 14-12 *Dynamic Translation Rules*



Before you can configure a dynamic translation rule, however, you need to define the appropriate address translation pool. This pool identifies which addresses can be temporarily associated with outbound traffic from a specific internal host. For more information on address translation pools, refer to the following section, "Creating Building Blocks."

Creating Building Blocks

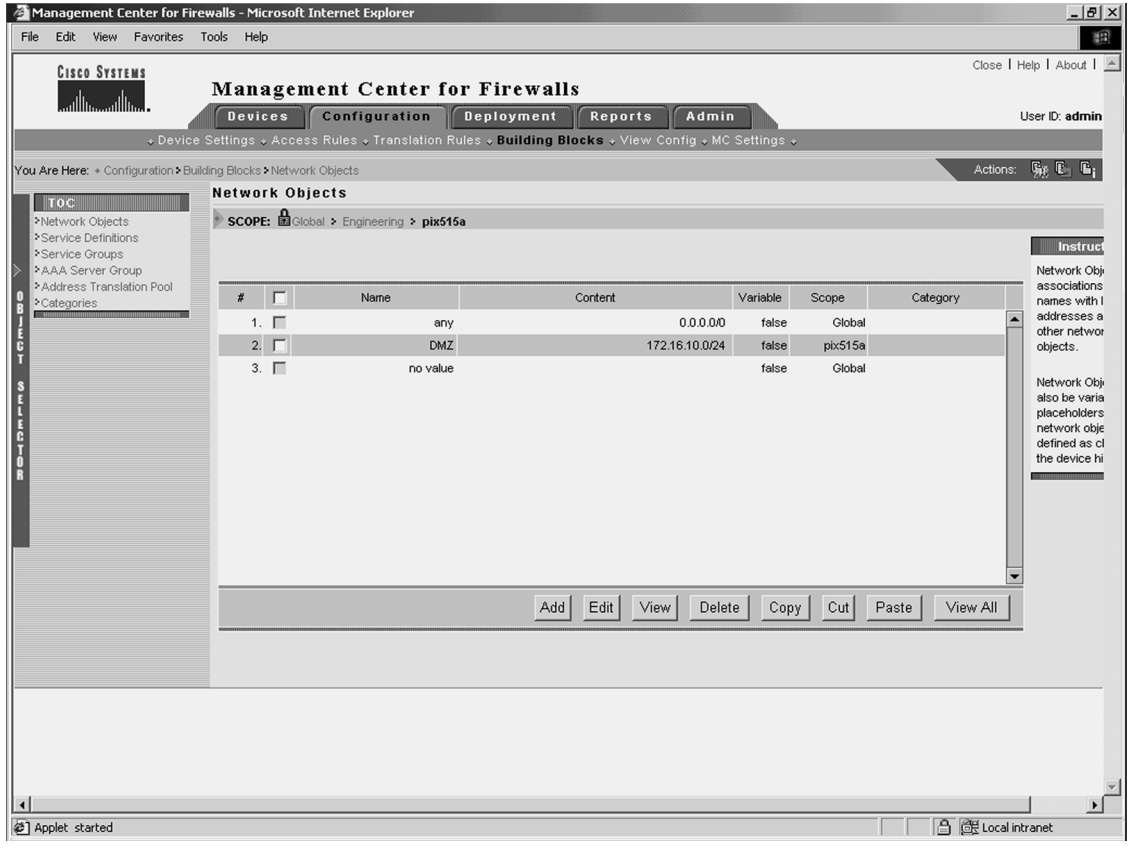
Building blocks enable you to optimize your configuration. Building blocks define groups of objects such as hosts, protocols, or services. You can then issue a command that affects every item in the group by specifying the name of the group. Basically, you can use the names of the building blocks in place of corresponding data values when configuring device settings or defining rules. You can configure the following types of building blocks, each of which is described within this section:

- Network objects
- Service definitions
- Service groups
- AAA server groups
- Address translation pools

Network Objects

Network objects enable you to group a range of network addresses specified by an IP address and a network mask. These network objects can then be used in access rules and translation rules. In Figure 14-13, the network object named DMZ is associated with the Class C network 172.16.10.0/24.

Figure 14-13 *Network Objects*



You can use DMZ in access and translation rules by clicking the **Select** button whenever you normally specify an IP address (see Figure 14-14). The Selecting Network Objects window is displayed (see Figure 14-15). To use one of the list objects, click the object name, and then click **Select=>** to move the name to the Selected Objects column.

Figure 14-14 *Creating a Static Translation Rule*

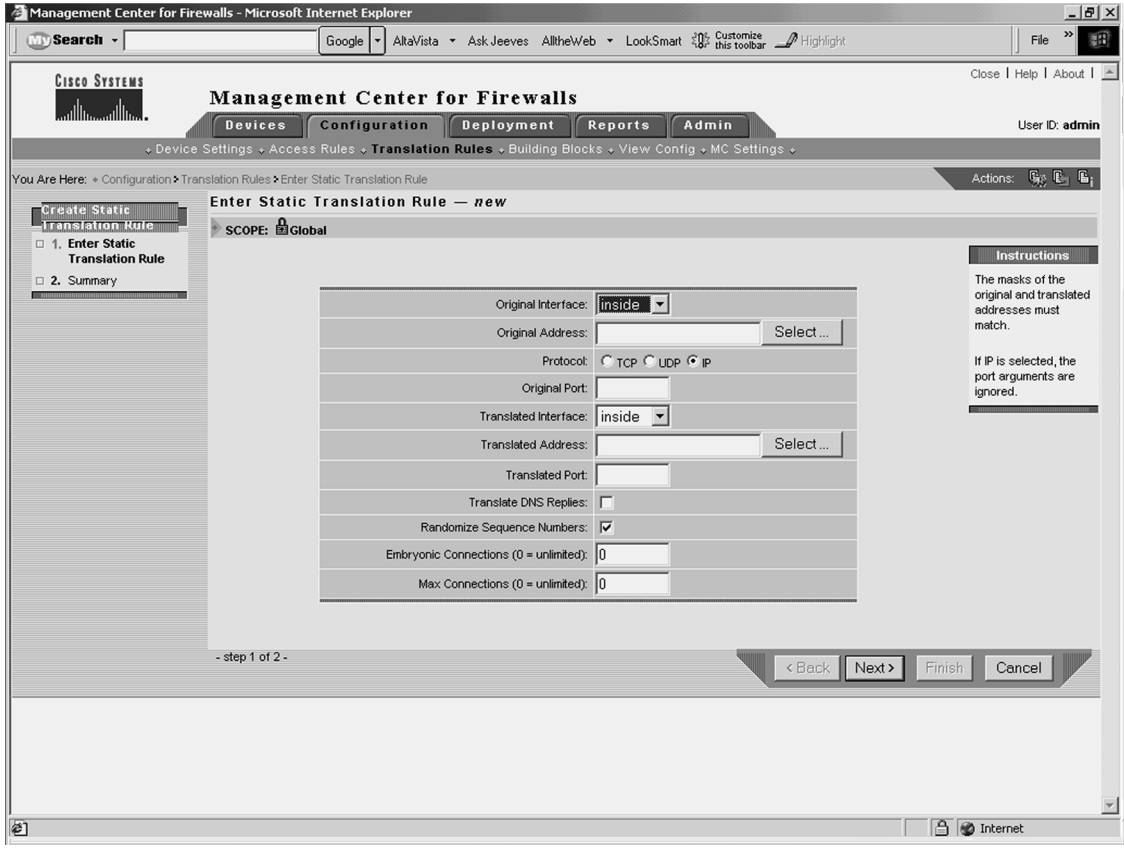
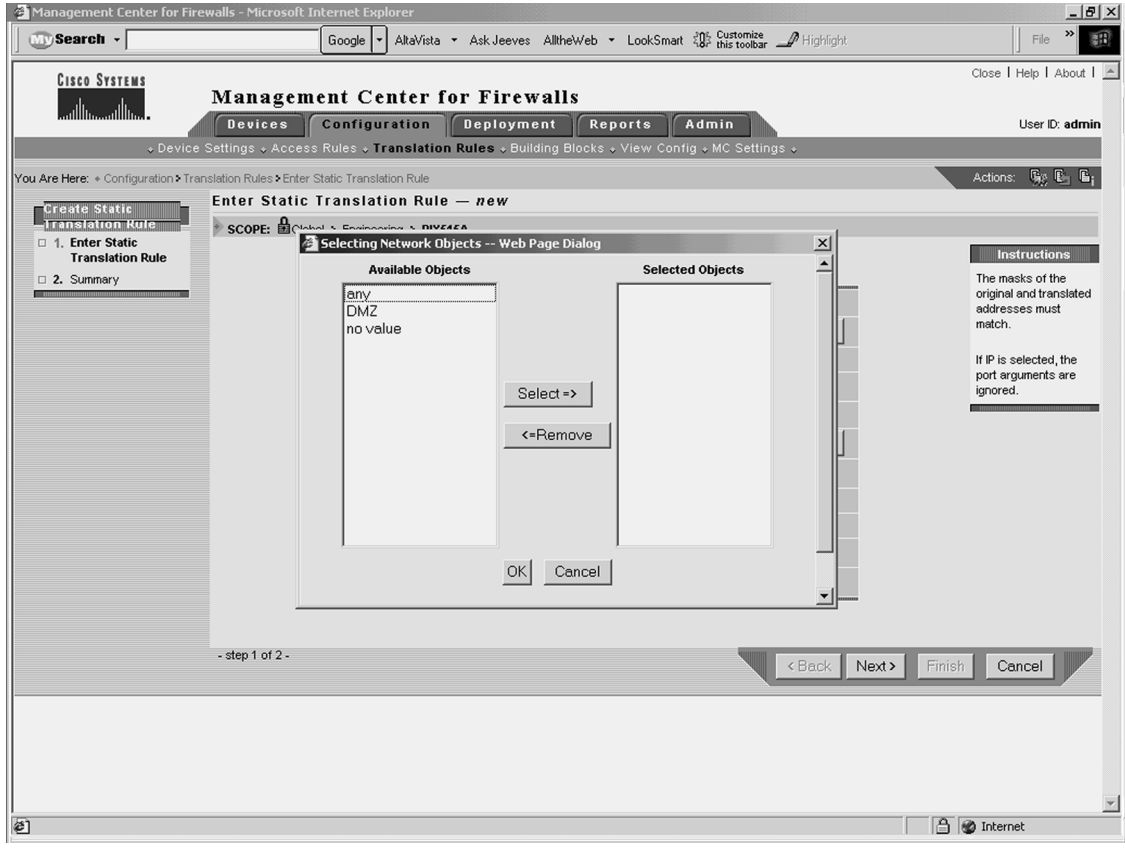


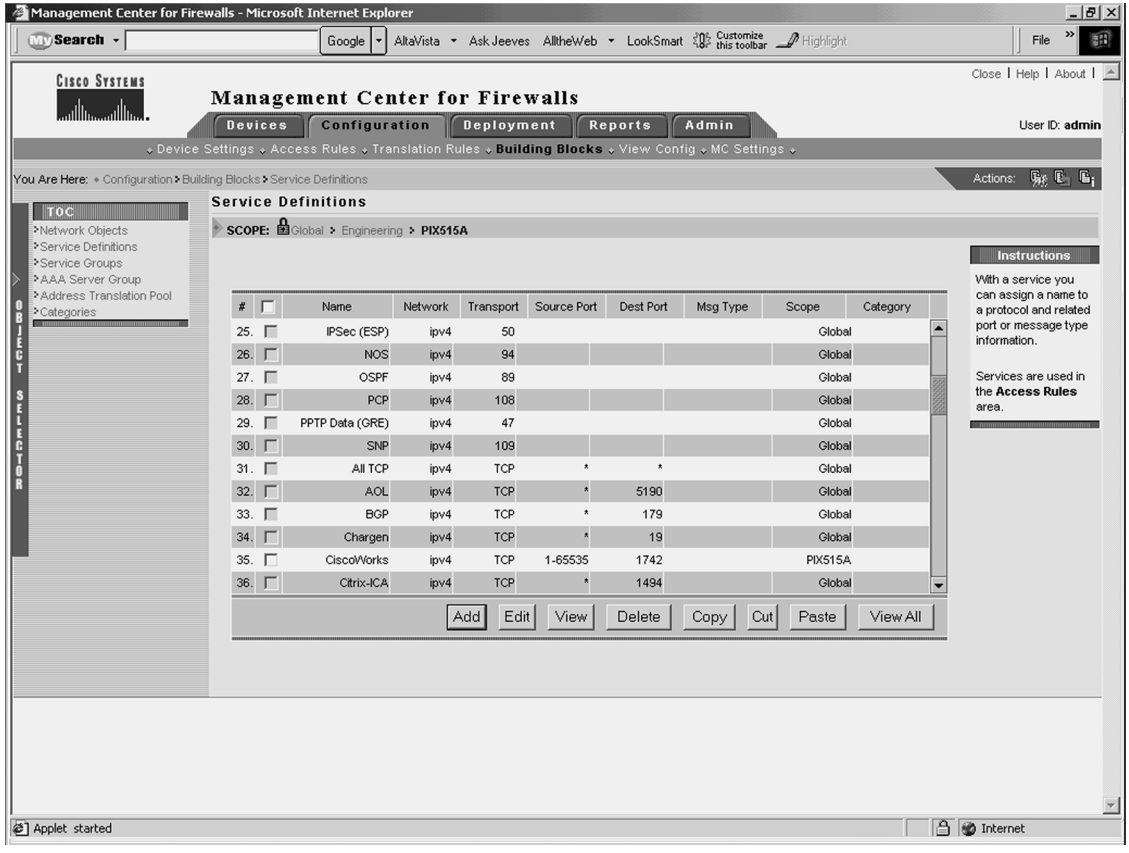
Figure 14-15 *Selecting Network Objects*



Service Definitions

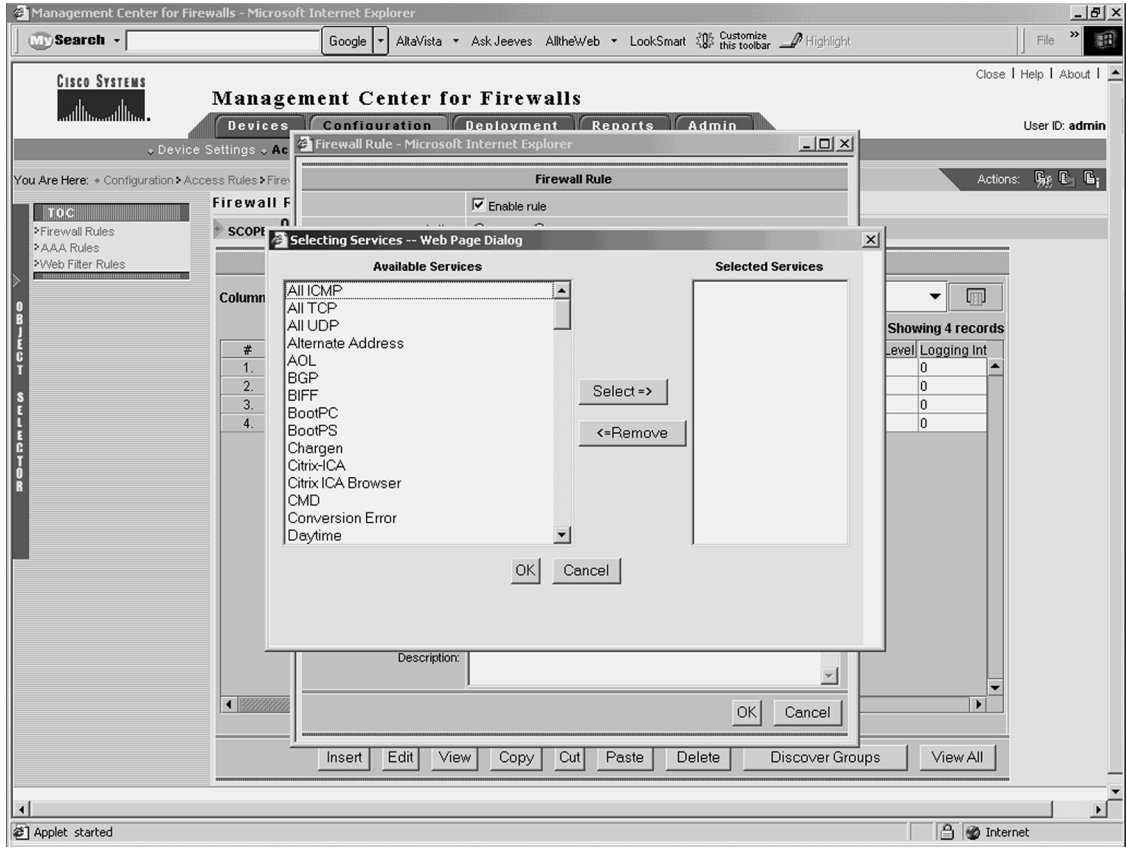
Service definitions enable you to define objects that associate IP protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) source and destination ports, and Internet Control Message Protocol (ICMP) message types with a specific name (see Figure 14-16). These service definitions are then used in firewall device protocol groups, service groups, and ICMP-type groups, respectively.

Figure 14-16 *Service Definitions*



Similar to other building blocks, you can use service definitions whenever you would normally specify a service (such as defining firewall rules) by clicking the **Add** button. This opens the Selecting Services window (see Figure 14-17), enabling you to select the appropriate service definition.

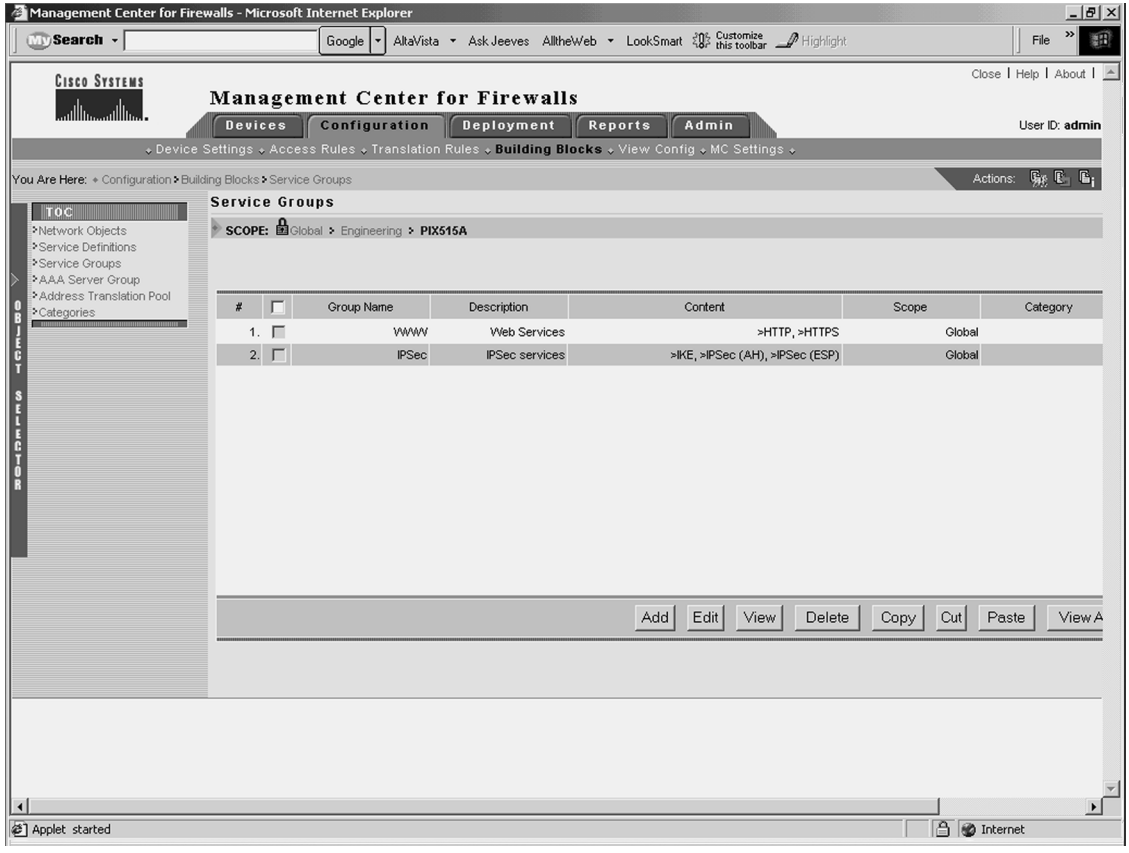
Figure 14-17 *Selecting Services*



Service Groups

Service groups enable you to define objects that associate a name with a group of service definitions (see Figure 14-18). For instance, you can create a service group that permits both HTTPS and Secure Shell (SSH) traffic.

Figure 14-18 *Service Groups*



AAA Server Groups

AAA server groups enable you to define separate groups of Terminal Access Controller Access Control System Plus (TACACS+) and Remote Authentication Dial-In User Service (RADIUS) servers that are used for different types of traffic. Traffic will attempt to authenticate with the fist server in the AAA server group. If this server is inaccessible, the next server in the group is tried.

> **NOTE** You can define 14 AAA server groups, each containing 14 distinct AAA servers, supporting a total of 196 AAA servers.

Address Translation Pools

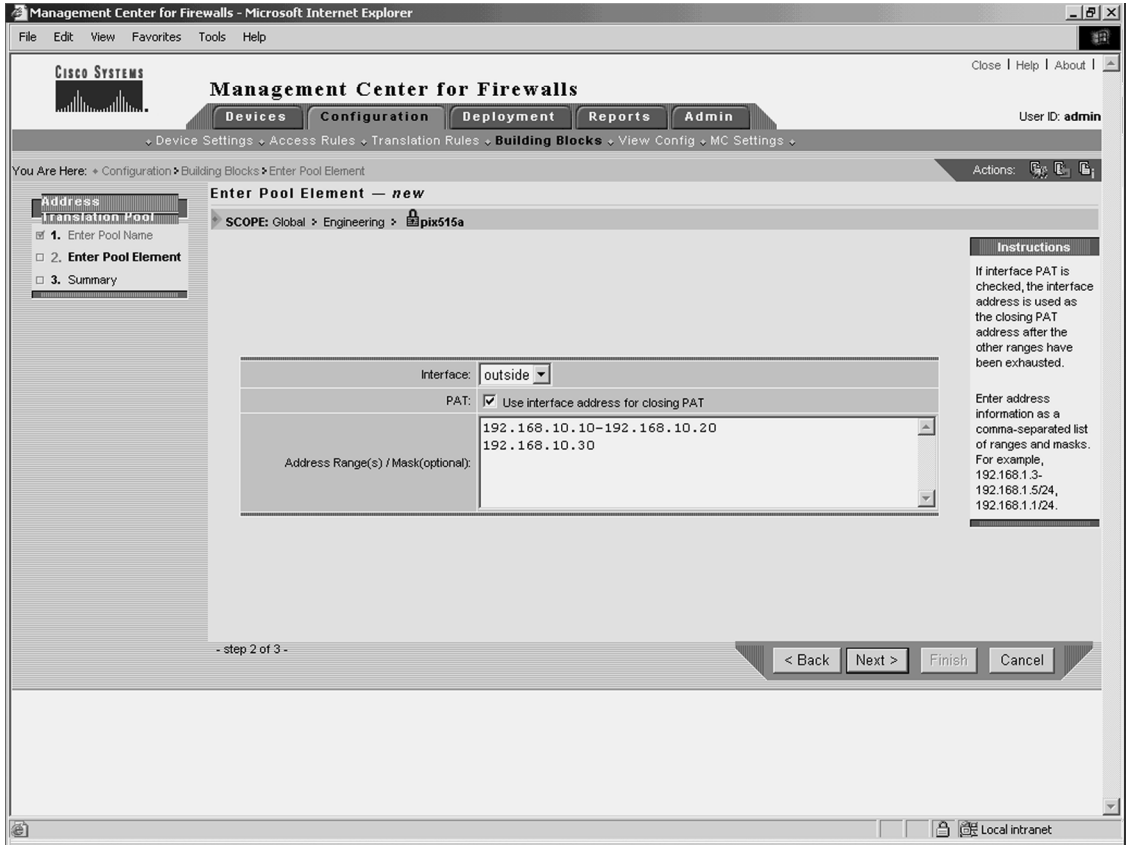
Address translation pools enable you to associate a name with a group of addresses that will be used to create dynamic address translations for outbound traffic. When defining an address translation pool, you need to specify the parameters shown in Table 14-6.

Table 14-6 *Address Translation Pool Parameters*

Parameter	Description
Pool Name	Name used when applying the pool to a dynamic translation rule.
Interface	Logical name of the interface where the pool will be used.
PAT: Use interface address for closing PAT Check Box	Select this check box to indicate that the IP address of the interface will be used as the PAT address when all of the other addresses in the pool have been used.
Address Range(s)/Mask (optional)	Set of addresses (in addition to the interface address) that will be used for dynamic translations.

For address translation pools, PAT is used when you have more internal addresses than external addresses. The firewall automatically uses the last available address to perform PAT. If you select the **PAT** check box (see Figure 14-19) when defining the address translation pool, after all of the addresses in the pool are used, the interface address is used for PAT.

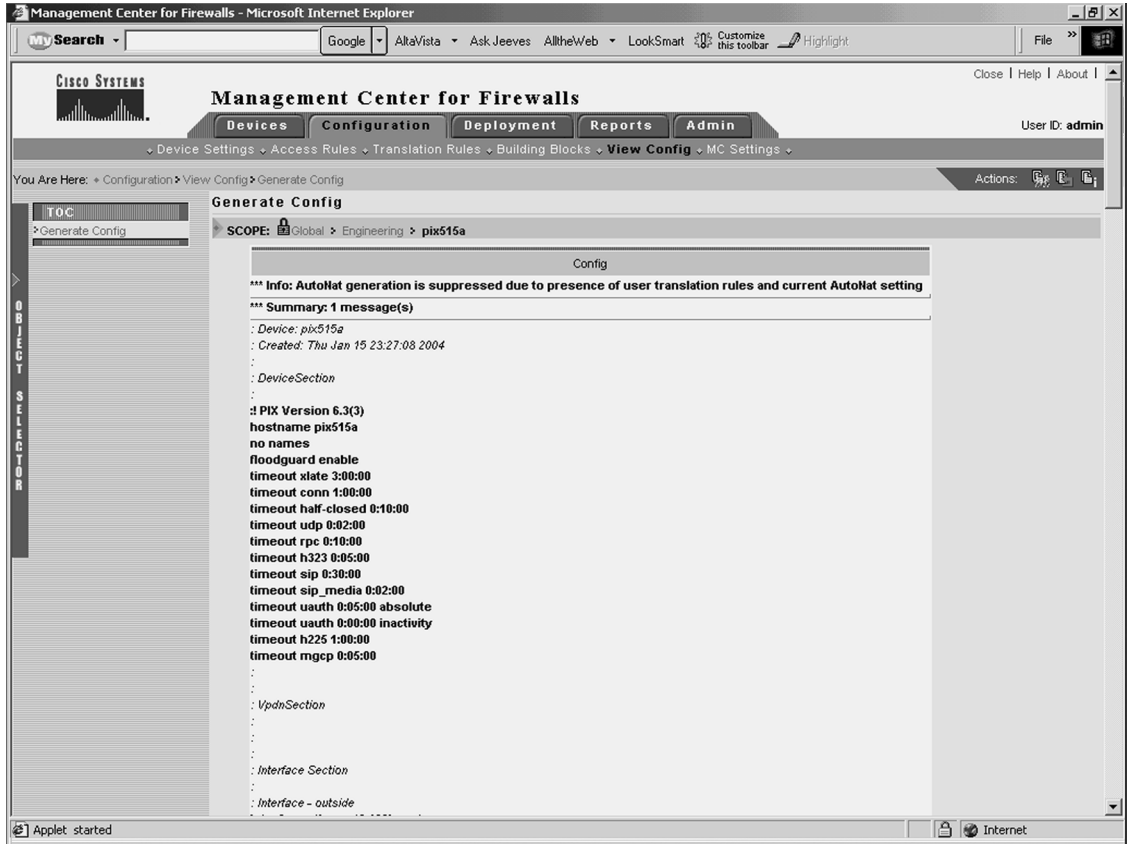
Figure 14-19 *Defining an Address Translation Pool*



Generating and Viewing Configuration Information

Selecting **Configuration > View Config > Generate Config** allows you to generate the configuration for a specific device. The Scope bar indicates for which device the configuration will be generated. Once the configuration is generated, you can then view the information in the content area (see Figure 14-20).

Figure 14-20 *Viewing Generated Configuration*



MC Settings

Selecting **Configuration > MC Settings** allows you to control how Firewall MC operates when it discovers commands configured outside of Firewall MC or unsupported and error commands imported into Firewall MC. It also identifies the directories in which imported and deployed configurations will be placed.

When configuring the MC settings, you have the following options:

- Management
- Deployment
- Import

- Feature Tracking
- Object Grouping

NOTE When configuring the AUS, you use the Deployment option to redirect configuration updates to the AUS instead of sending them directly to the managed device.

Deployment Tasks

After you make changes to the configuration for a managed device, you must deploy those changes on the actual firewalls on your network. You have the following two options when you select the Deployment configuration tab:

- Deploy Saved Changes
- Summary Report

NOTE These are the options available when workflow is not enabled. If workflow is enabled, refer to the "Workflow Setup" section later in the chapter for the options that are available.

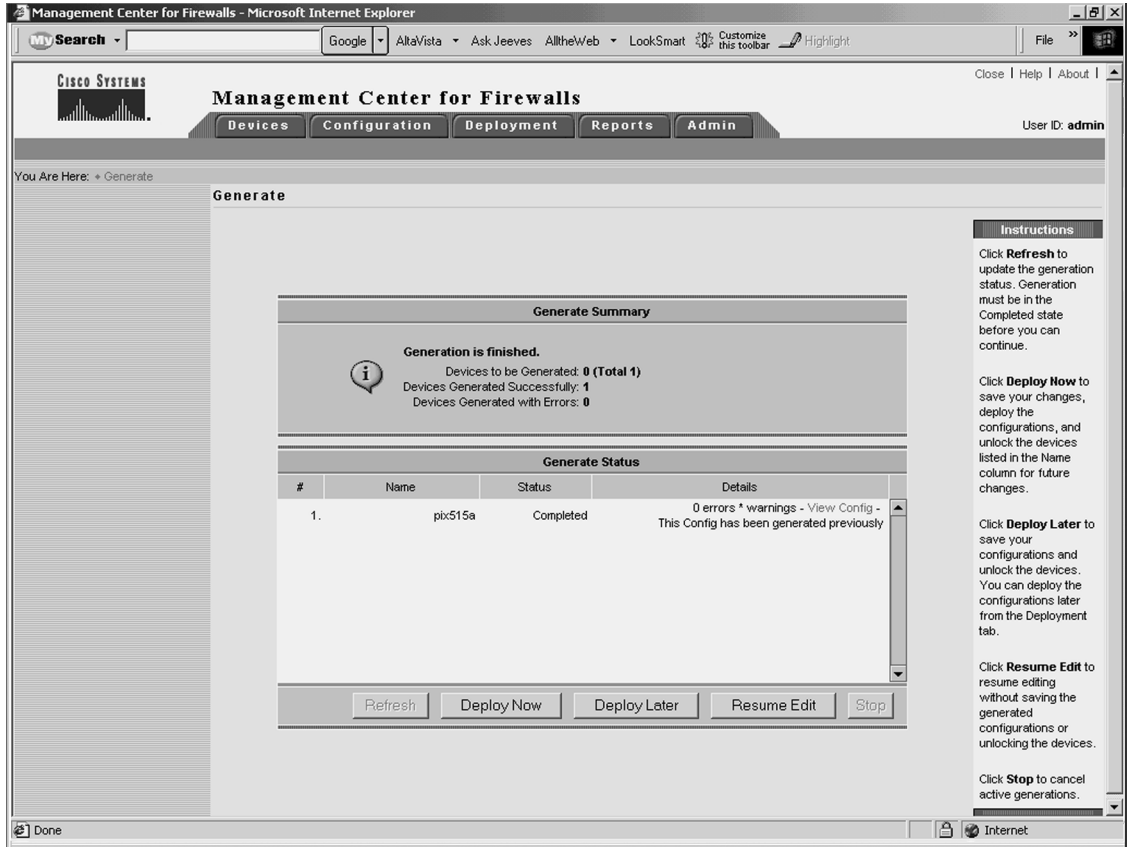
Deploy Saved Changes

Select **Deployment > Deploy Saved Changes** to cause the Firewall MC to generate the updated configuration files for the device or devices specified by the Scope bar. The Generate Summary window initially shows the deployment options as unavailable until the generation process is complete. Once the generation process is finished, you can deploy the changes to your managed firewalls (see Figure 14-21) using the following options:

- Deploy Now
- Deploy Later

NOTE Click the **Save & Deploy** icon on the activity bar to select the **Deploy Saved Changes** functionality without accessing it through the Deployment configuration tab.

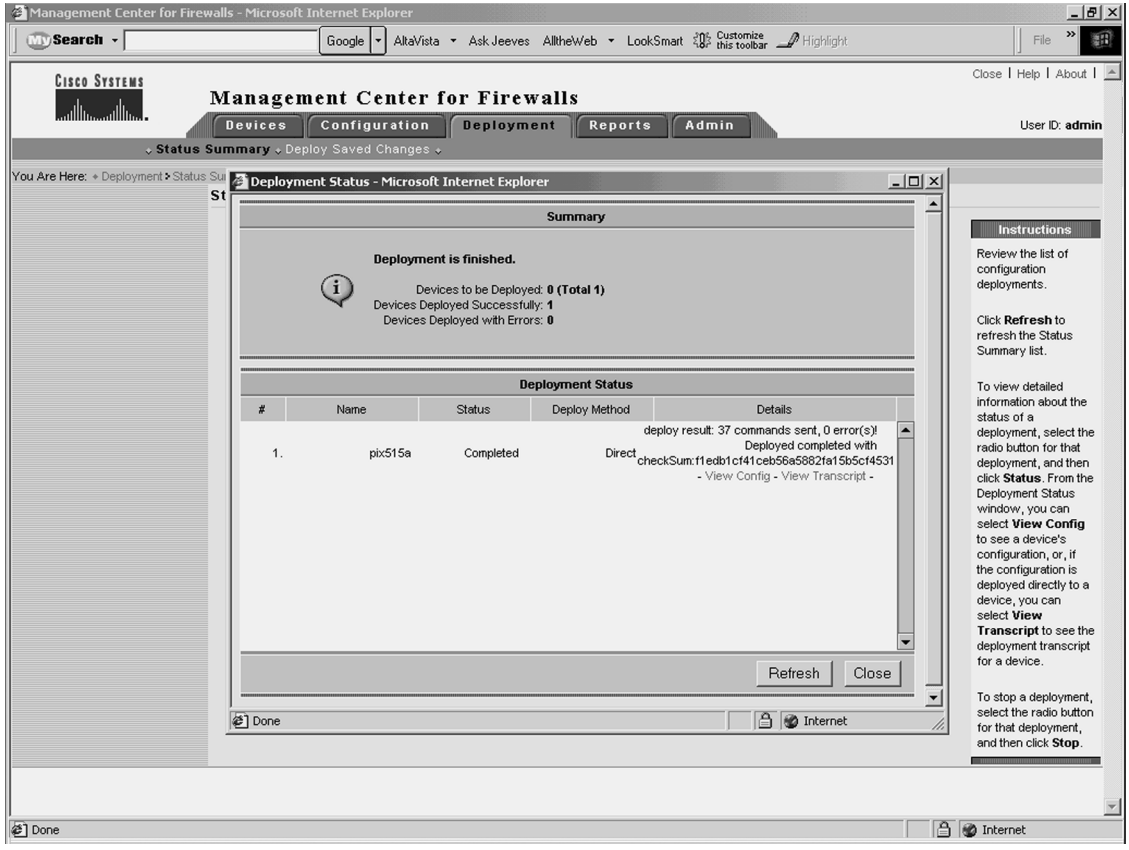
Figure 14-21 *Generate Summary Window*



Click the **Deploy Now** button to deploy the new configurations to your managed devices immediately, or click the **Deploy Later** button to delay deploying the new configurations.

After you deploy new configurations, a deployment summary window appears (see Figure 14-22). This window summarizes the results of the deployment process and lets you know the status of the deployment process. It also indicates whether the deployment generated any errors or warnings on the managed firewalls when the configuration commands were executed.

Figure 14-22 *Deployment Status Summary Window*



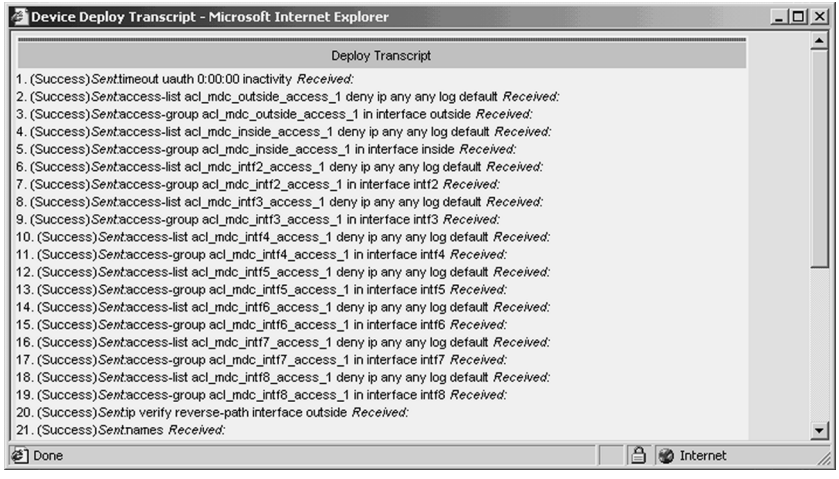
The Deployment Status Summary window (in Figure 14-22) contains the following two links that you can use to view information about your deployed changes:

- View Config
- View Transcript

Click the **View Config** link to display the deployed configuration for the managed firewall (see Figure 14-23), or click the **View Transcript** link to display a window that shows a transcript of all configuration commands that were executed and their success status (see Figure 14-24).

Figure 14-23 *Viewing the Config Window*

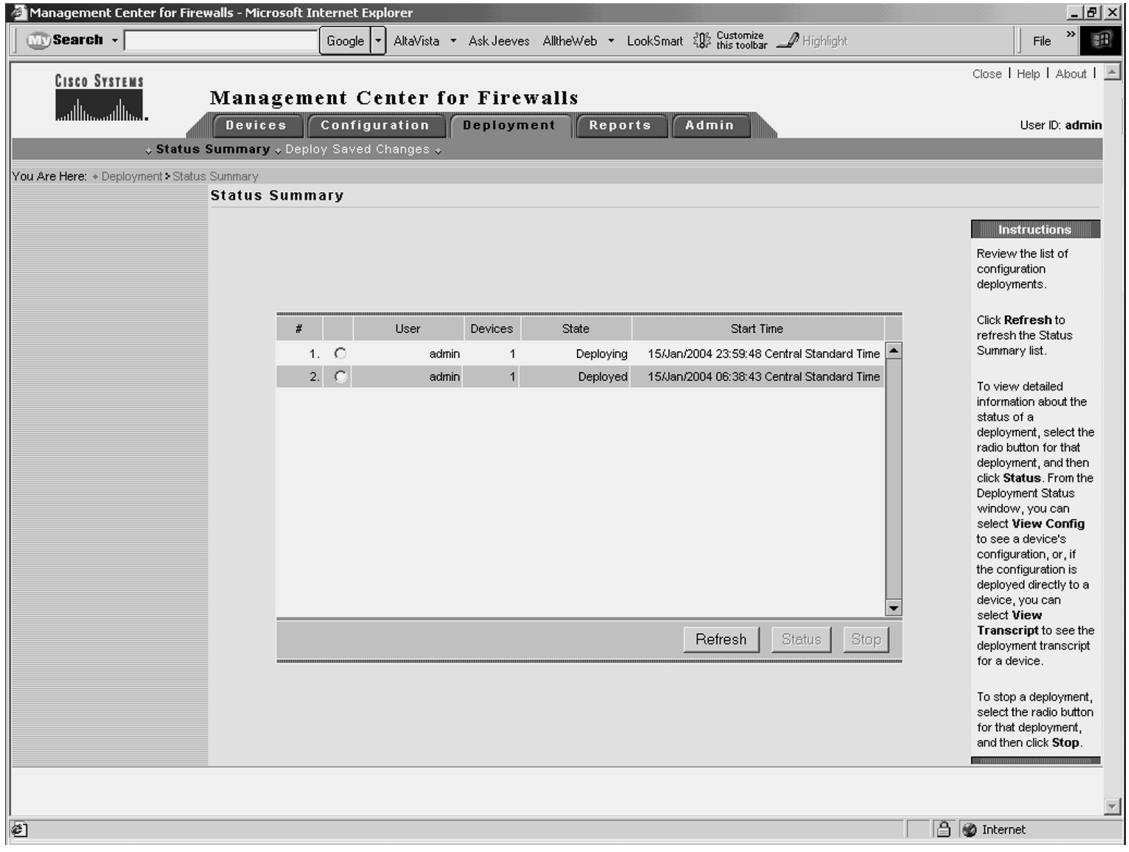
Figure 14-24 *Viewing the Deploy Transcript Window*



Summary Report

Select **Deployment > Status Summary** to display the history of the deployment changes that you have made to your managed firewalls (see Figure 14-25).

Figure 14-25 *Status Summary Window*



Reports

In the Reports tab, you can view the following three reports:

- Activity Report
- Configuration Differences report
- Device Setting Report

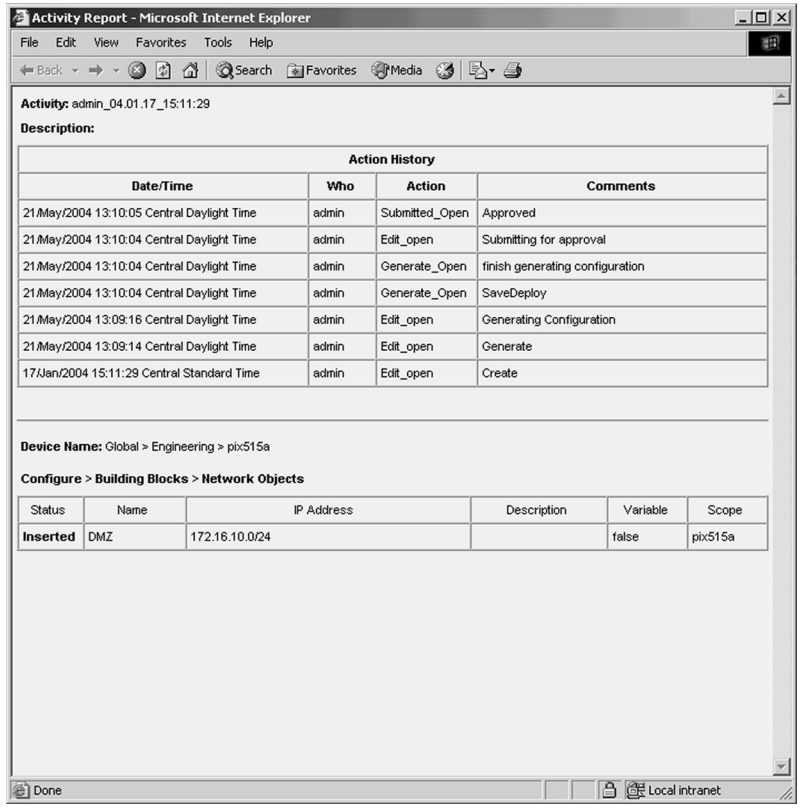
Activity Report

The Activity Report, as the name implies, displays information about the activities or configuration changes that have occurred on the Firewall MC (see Figure 14-26). For each activity, the report provides the following two pieces of information:

- User that performed the activity and when the change happened
- The actual configuration changes that were made

NOTE If you do not have workflow enabled, the Activity Report shows only the changes that were made. It does not identify the user that performed the changes.

Figure 14-26 *Activity Report*



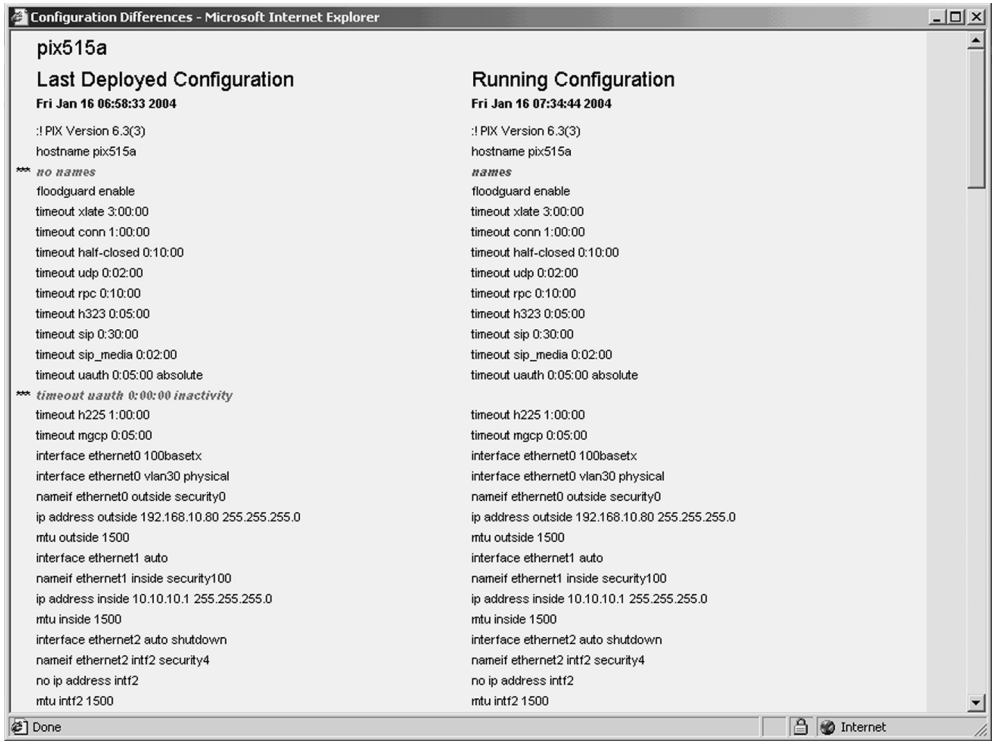
Configuration Differences Report

The Configuration Differences report enables you to determine if the running configuration on a managed firewall matches the latest configuration that you deployed to it. You can also use this report to determine which managed firewalls have an updated configuration waiting to be deployed. You can generate reports based on the following two options:

- The approved configuration does not match the deployed configuration.
- The deployed configuration does not match the running configuration.

Initially, you select the device or group on which you want to check for configuration differences. This displays a window indicating the firewalls that have configuration differences. To view the actual differences, click the **View Configuration Differences** link next to a specific device. This displays a window outlining the actual configuration differences (see Figure 14-27).

Figure 14-27 *Configuration Differences Report*



Device Setting Report

The Device Setting Report enables you to view the device settings for a device or device group. Each setting also indicates how the setting was derived. Each setting is determined based on one of the following categories:

- Inherited
- Mandatory
- Overridden

You have the following two options when generating this report:

- Show inheritance only
- Show inheritance and values

The Show inheritance only option displays a list of all of the device settings, indicating how the setting was derived (see Figure 14-28). The Show inheritance and values option includes the actual values for the settings in addition to how the settings were derived (see Figure 14-29).

Figure 14-28 *Show Inheritance Only Device Setting Report*

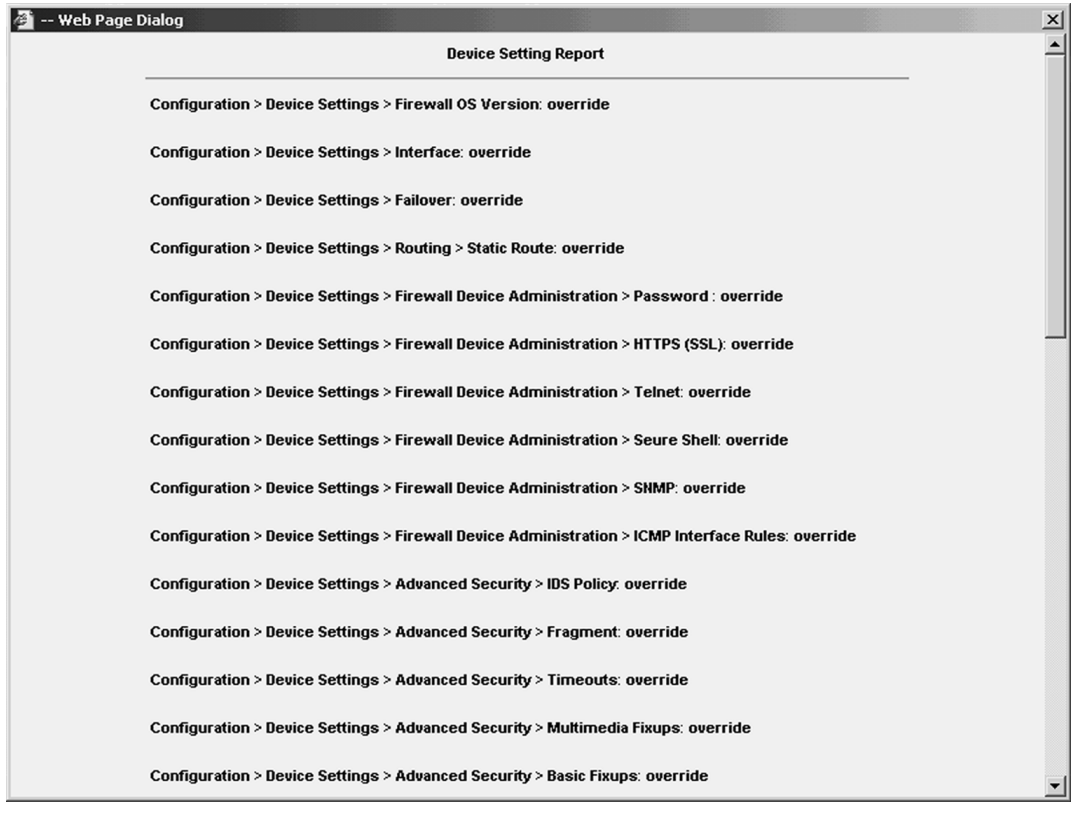
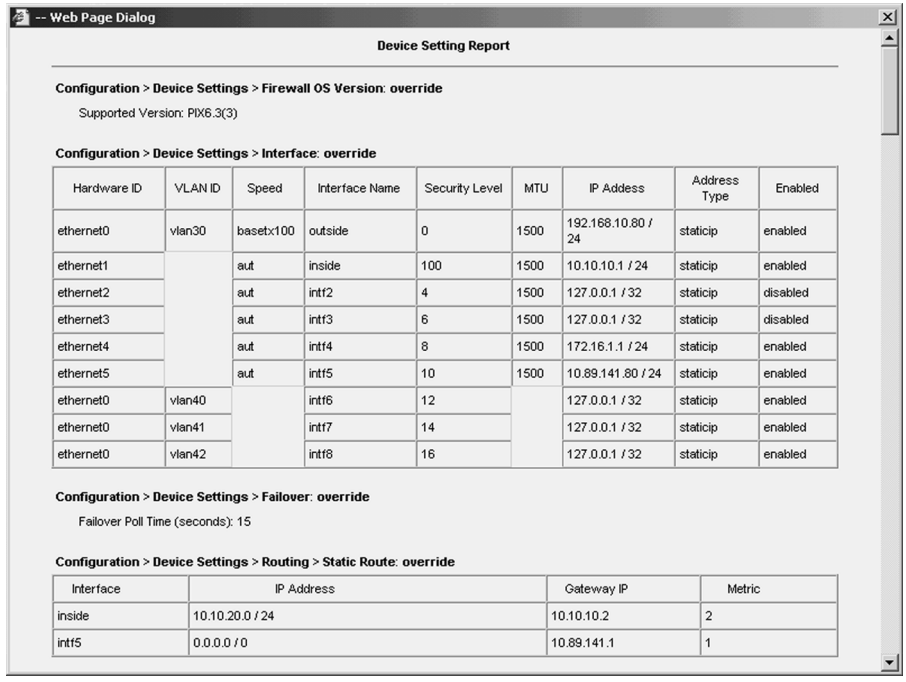


Figure 14-29 *Show Inheritance and Values Device Setting Report*


-- Web Page Dialog

Device Setting Report

Configuration > Device Settings > Firewall OS Version: override

Supported Version: PIX6.3(3)

Configuration > Device Settings > Interface: override

Hardware ID	VLAN ID	Speed	Interface Name	Security Level	MTU	IP Address	Address Type	Enabled
ethernet0	vlan30	basetx100	outside	0	1500	192.168.10.80 / 24	staticip	enabled
ethernet1		aut	inside	100	1500	10.10.10.1 / 24	staticip	enabled
ethernet2		aut	intf2	4	1500	127.0.0.1 / 32	staticip	disabled
ethernet3		aut	intf3	6	1500	127.0.0.1 / 32	staticip	disabled
ethernet4		aut	intf4	8	1500	172.16.1.1 / 24	staticip	enabled
ethernet5		aut	intf5	10	1500	10.89.141.80 / 24	staticip	enabled
ethernet0	vlan40		intf6	12		127.0.0.1 / 32	staticip	enabled
ethernet0	vlan41		intf7	14		127.0.0.1 / 32	staticip	enabled
ethernet0	vlan42		intf8	16		127.0.0.1 / 32	staticip	enabled

Configuration > Device Settings > Failover: override

Failover Poll Time (seconds): 15

Configuration > Device Settings > Routing > Static Route: override

Interface	IP Address	Gateway IP	Metric
inside	10.10.20.0 / 24	10.10.10.2	2
intf5	0.0.0.0 / 0	10.89.141.1	1

Administration Tasks

The administration tasks fall into the following categories:

- Workflow Setup
- Maintenance
- Support

Workflow Setup

The Firewall MC software enables you to configure firewalls as well as groups of firewalls. By default, when you make changes, they are propagated to your firewalls as soon as you save and deploy the changes. If you enable workflow (by selecting **Admin > Workflow Setup**), however, there is a distinct process that you must follow to deploy your changes to the appropriate firewalls. This process allows you to track changes down to the individual user

that performed the changes. The workflow process establishes the following three distinct steps in the configuration process:

Step 1 Define configuration changes.

Step 2 Approve configuration changes.

Step 3 Deploy configuration changes.

A separate person can be in charge of each step, thus dividing the responsibility for updating the configuration on the managed firewalls.

When using workflow, policy changes (known as *activities* and *jobs*) regulate the deployment of configuration files. You can require formal approval for activities, jobs, or both. The Firewall MC interface also changes. The Deployment configuration tab is replaced with a Workflow configuration tab (see Figure 14-30).

Figure 14-30 *Firewall MC Interface with Workflow Enabled*

Through workflow, you regulate activities (configuration changes) by using the following options:

- **Add**—Creates a new activity
- **Open**—Opens an existing activity to add more configuration changes
- **Close**—Changes the state of the activity so that it can be submitted
- **Status**—Displays the status of an activity
- **Info**—Displays the changes that make up the activity
- **Submit**—Submits an activity for approval
- **Undo**—Rolls back activity changes
- **Approve**—Approves the changes in an activity
- **Reject**—Rejects the changes in an activity
- **Cancel**—Cancels an active import or any generate actions currently in operation for the activity

NOTE The various activity options are unavailable unless they are valid for the activity selected. For instance, you cannot approve an activity that has not been submitted.

Creating a job to deploy configuration changes (from specified activities) involves the following steps:

Step 1 Specify a job name.

Step 2 Select the activities to be deployed.

Step 3 Select the devices to receive the changes.

Step 4 Review the devices selected.

Step 5 Change the job state.

Step 6 Examine summary information.

You regulate and manage jobs using the following options:

- **Add**—Creates a new job
- **Status**—Displays detailed status of a job
- **Submit**—Submits a job for approval
- **Rollback**—Enables you to roll back the configuration on a firewall to a previous version
- **Approve**—Approves the job for deployment

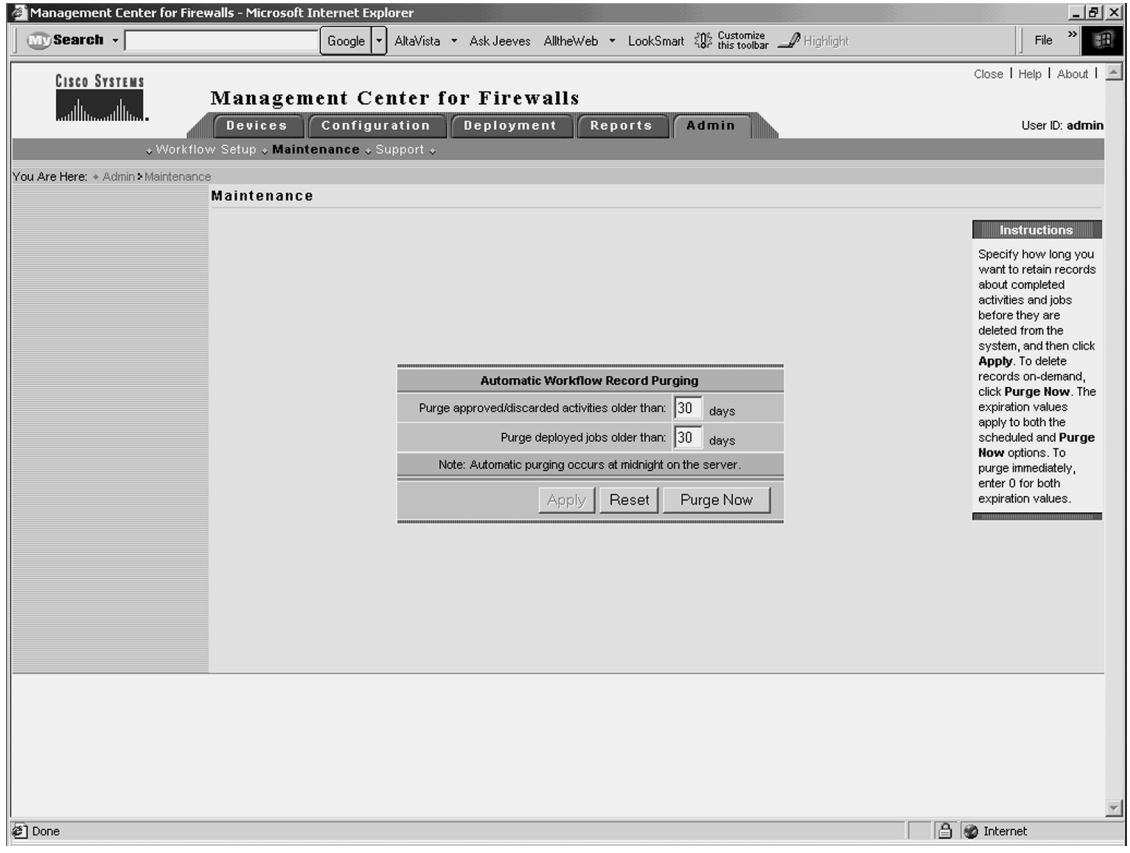
- **Reject**—Rejects the job
- **Deploy**—Deploys the changes in an approved job
- **Cancel**—Cancels the deployment or rollback operation that is currently in process

NOTE The various job options are unavailable unless they are valid for the activity selected. For instance, you cannot approve a job that has not been submitted.

Maintenance

Depending on how frequently you perform configuration updates, you may want to remove old activity and job records periodically. Select **Admin > Maintenance** to configure how often activity and job records are automatically purged from the database (see Figure 14-31). For both activities and jobs, you can specify how old an entry must be before it is automatically removed from the database (the default is 30 days).

Figure 14-31 *Maintenance Window*



Support

When debugging your system, you may need to obtain some important operational information about your system. Select **Admin > Support** to run a program specifically designed to collect information to assist in troubleshooting the operation of your Firewall MC system.

CiscoWorks Auto Update Server

Maintaining current images on your managed devices can be a time-consuming task. The AUS is a tool that you can use to upgrade device configuration files and maintain current software images on your managed firewalls. The main advantage of AUS is that it can manage devices that obtain their addresses through Dynamic Host Configuration Protocol (DHCP). Remotely managed PIX Firewalls are often dynamically addressed, which means they cannot be managed by traditional network management servers.

The managed devices use an auto update feature to initiate a management connection periodically to the AUS. The device provides AUS with its current state and device information. The AUS then responds to the device by providing a list of versions of the software images and configuration files that the device should be running. The device compares the file versions with the versions it is running. If there are differences, the device downloads the new versions from the URLs provided by the AUS. Once the device is up-to-date with the new file versions, it sends AUS its state and device information again.

Some of the major features provided by AUS (Version 1.0) include the following:

- Web-based interface for maintaining multiple PIX Firewalls
- Support for PIX Firewall Version 6.0 and later (Version 6.2 and later for AUS Version 1.1)
- Support for dynamically addressed PIX Firewalls
- Support for up to 1000 PIX Firewalls

AUS Version 1.1 adds new functionality, including the following major features:

- Installation on Solaris
- Additional report formats
- Support for configuration files

Supported Devices

AUS supports PIX Firewalls running Versions 6.0 and later. In addition, AUS supports the following PIX hardware platforms:

- PIX 501
- PIX 506/506E
- PIX 515/515E
- PIX 525
- PIX 535

Installation

CiscoWorks Common Services (Version 2.2) is required for AUS. The requirements for the CiscoWorks server are described in the "CiscoWorks Management Center for Firewalls Overview" section earlier in this chapter. Once you have the CiscoWorks server built, the installation of AUS is easy and involves the following steps:

Step 1 Insert the AUS CD into the CD drive on the CiscoWorks server. If autorun is enabled, the installation process starts automatically. If not, you must locate the setup.exe file and run it. Once the installation process starts, the Welcome window is displayed.

Step 2 Click **Next.** The software license window is displayed.

Step 3 If you agree to the software license agreement, click **Yes**. (If you click **No**, the installation process will stop.) The system requirements window is displayed.

Step 4 Click **Next.** The Verification window is displayed.

Step 5 Click **Next**. A popup window is displayed that asks if you want to change the AUS database password. Click **Yes** to change the password.

Step 6 Click **Finish**. The AUS installation is now complete.

NOTE AUS operates in unison with the Firewall MC to update the configuration files on firewalls running in auto update mode. AUS and the Firewall MC, however, do not have to be collocated on the same machine. Because of their different roles and responsibilities, these systems are typically installed on separate machines with Firewall MC located in your network operations center (NOC) and the AUS deployed on a demilitarized zone (DMZ) network.

Communication Settings

To configure and use AUS effectively, you need to understand the AUS communication architecture. The following steps describe the interaction between the PIX Firewall, Firewall MC, and AUS (see Figure 14-32).

Step 1 The Firewall MC deploys a configuration file to the AUS.

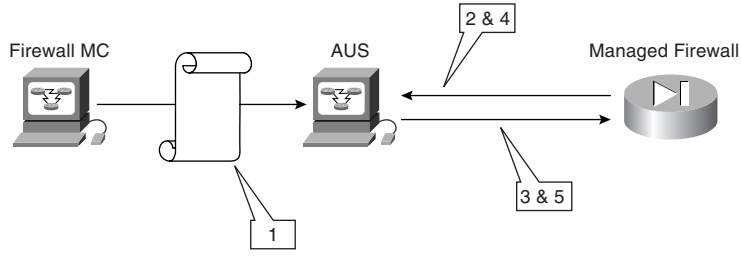
Step 2 At a configured polling interval, the managed PIX Firewall contacts the AUS to determine if there are any pending updates.

Step 3 The AUS sends a list of image files and/or configuration files that the PIX Firewall should be running.

Step 4 The PIX Firewall checks its configuration and image against the information provided by the AUS. If the PIX Firewall is not using the most current files, it requests the updated files from the AUS.

Step 5 The needed files are downloaded to the PIX Firewall.

Figure 14-32 *AUS Communication Flow*



AUS Activation

To enable your managed firewalls to communicate with the AUS, you need to perform certain configuration changes using Firewall MC. The sequence of the changes is as follows:

Step 1 From the PIX console, enable the firewall to accept HTTP connections from the AUS.

Step 2 From Firewall MC, configure the following items:

- AUS and PIX Firewall communications
- PIX Firewall unique identification parameters
- AUS contact information

Step 3 Deploy the updated configuration to the managed firewall.

Step 4 From Firewall MC, modify the PIX Firewall Configuration Deployment options so that configuration updates are sent to the AUS server instead of the device.

Auto Update Server and PIX Firewall Communications

After you configure the PIX Firewall to accept HTTP connections from the AUS, you need to configure the AUS communications parameters on the PIX Firewall by completing the following steps:

Step 1 Log in to CiscoWorks, and launch Firewall MC.

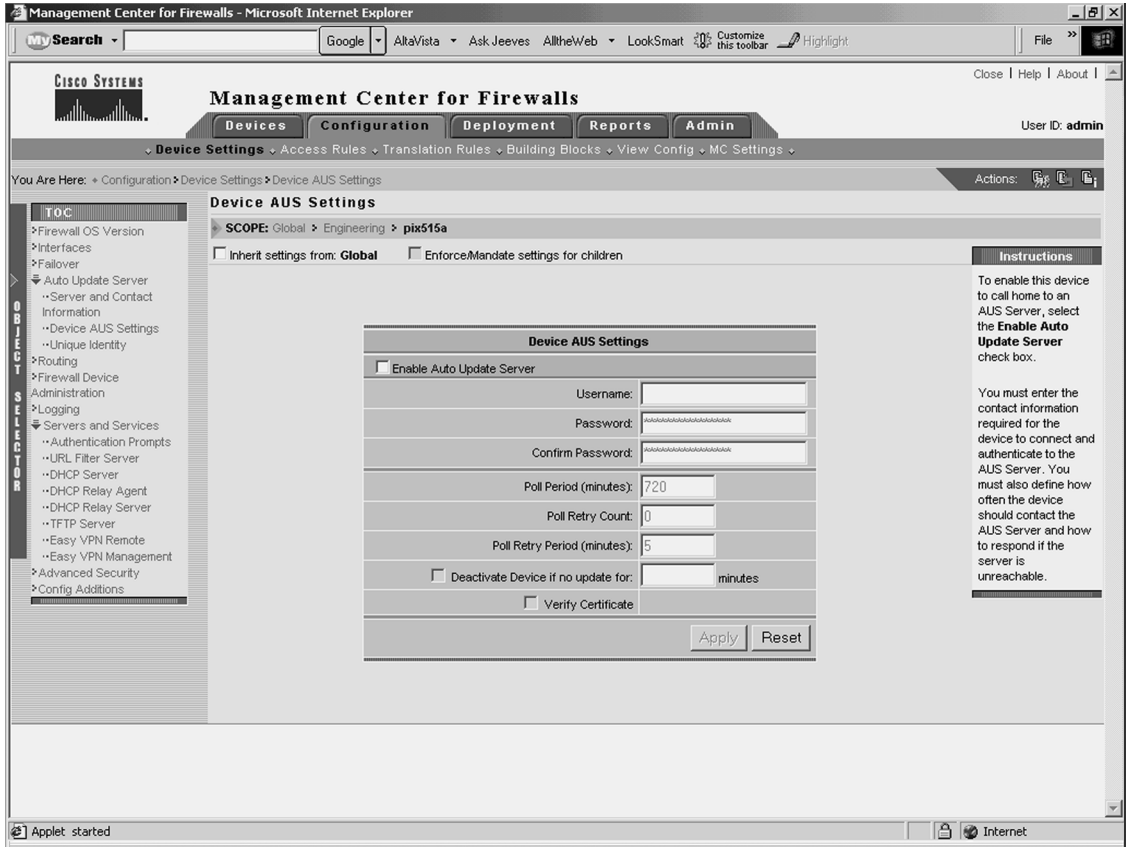
Step 2 Choose **Configuration > Device Settings** to access the device configuration settings.

Step 3 If workflow is enabled, you need to select an existing activity or create a new activity from the activity bar.

Step 4 Use the Object Selector to select a specific group or device.

Step 5 Select **Auto Update Server > Device AUS Settings** from the TOC. The Device AUS Settings window is displayed (see Figure 14-33).

Figure 14-33 *Device AUS Settings Window*



Step 6 Check the **Enable Auto Update Server** check box.

Step 7 Enter the unique ID (username) the PIX Firewall will use to contact the AUS in the **Username** field.

Step 8 Enter the password for the username specified.

Step 9 Confirm the password by entering it in the **Confirm Password** field.

Step 10 Enter the number of minutes in the **Poll Period** field (the default is 720 minutes). This parameter specifies the time that the PIX Firewall will wait between connections to the AUS to check for updates.

Step 11 Enter the number of times that the PIX Firewall will try to contact the AUS (if the initial attempt fails) in the **Poll Retry Count** field (the default is 0).

Step 12 Enter the number of minutes between poll retries in the **Poll Retry Period** field (the default is 5 minutes).

Step 13 If you want the PIX Firewall to deactivate itself if an update is not received in a specified number of minutes, check the **Deactivate Device if no update for** check box and specify the number of minutes.

Step 14 Click **Apply**.

PIX Firewall Unique Identification Parameters

When the PIX Firewall communicates with the AUS, the PIX Firewall must uniquely identify itself to the AUS. This unique identification enables the AUS to search its database of current assignments to locate entries that pertain to the specific PIX Firewall that is communicating with it. To configure the PIX Firewall unique identity parameters, complete the following steps:

Step 1 Log in to CiscoWorks, and launch Firewall MC.

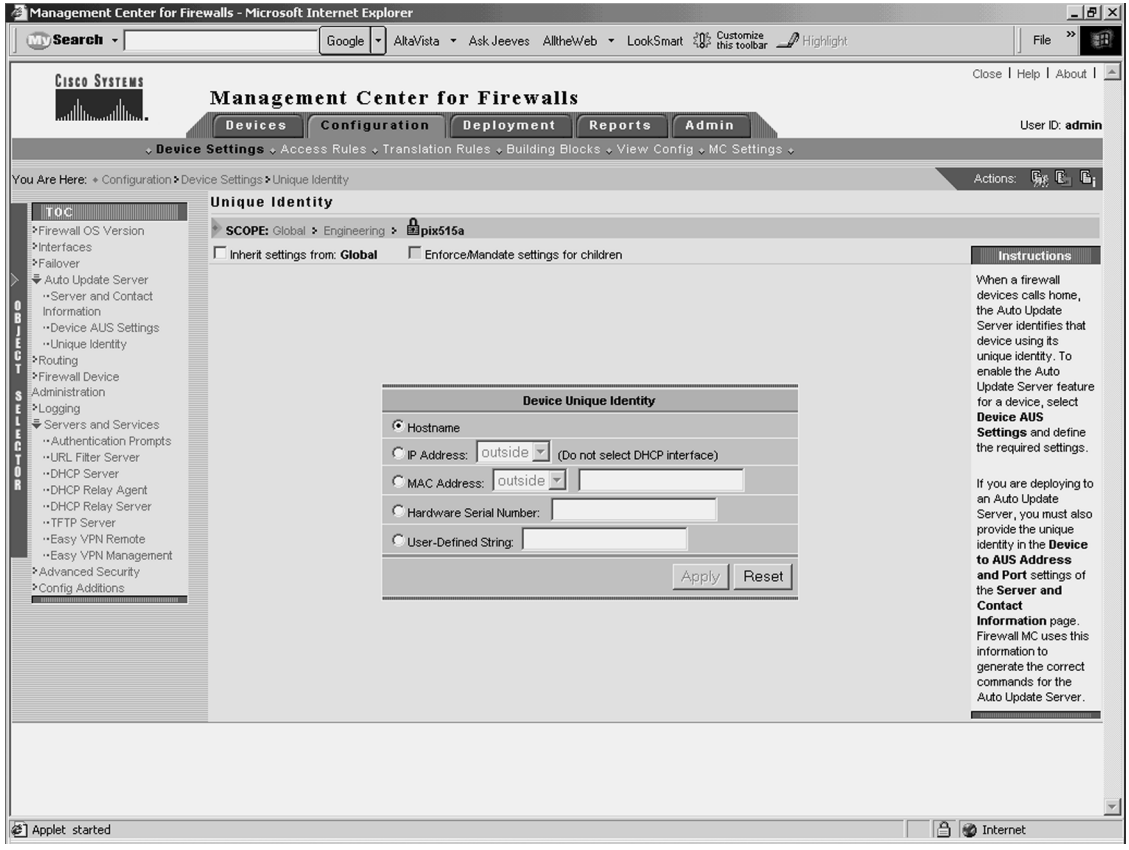
Step 2 Choose **Configuration > Device Settings** to access the device configuration settings.

Step 3 If workflow is enabled, you need to select an existing activity or create a new activity from the activity bar.

Step 4 Use the Object Selector to select a specific group or device.

Step 5 Select **Auto Update Server > Unique Identity** from the TOC. The Device Unique Identity window is displayed (see Figure 14-34).

Figure 14-34 *Device Unique Identity Window*



Step 6 Choose the unique identifier by selecting the radio button next to one of the following items:

- Hostname
- IP Address
- MAC Address
- Hardware Serial Number
- User-Defined String

Step 7 Click **Apply.**

Auto Update Server Contact information

Next you need to specify the contact information for the AUS. The Firewall MC will use this information to communicate with the AUS. To configure the AUS contact information, complete the following steps:

Step 1 Log in to CiscoWorks, and launch Firewall MC.

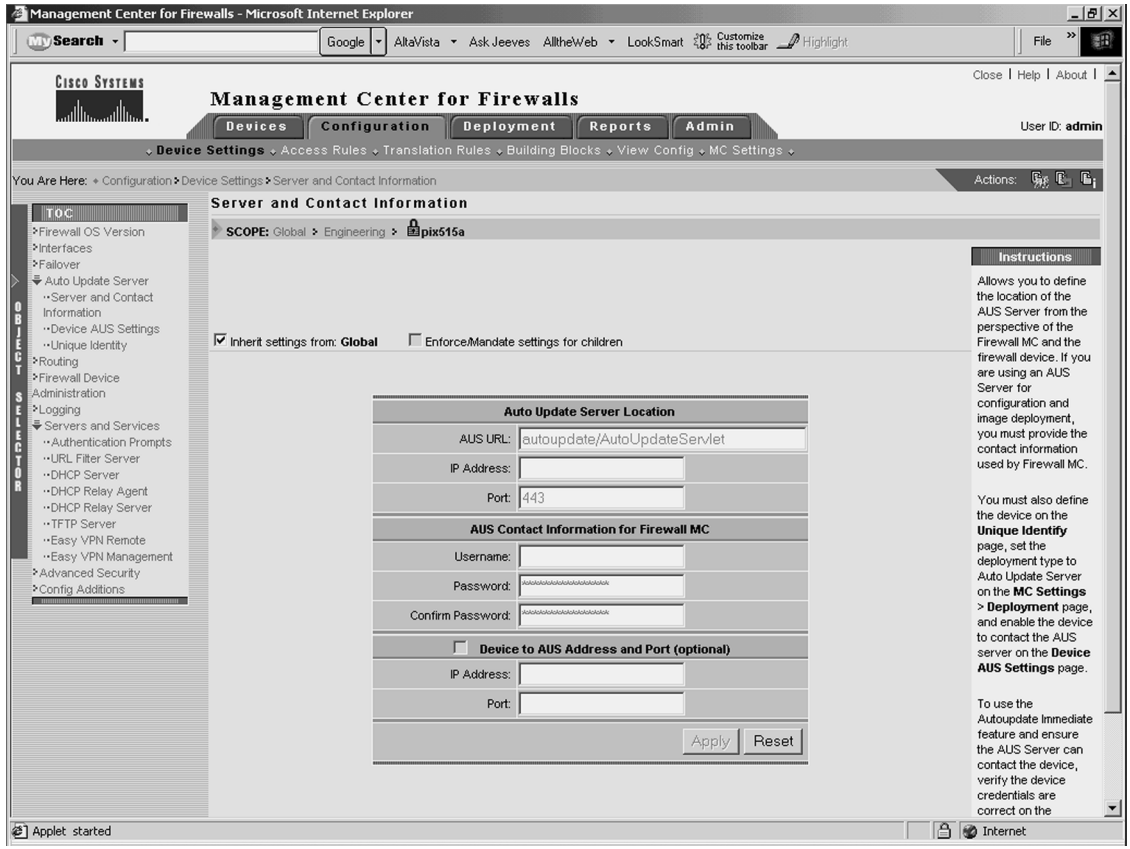
Step 2 Choose **Configuration > Device Settings** to access the device configuration settings.

Step 3 If workflow is enabled, you need to select an existing activity or create a new activity from the activity bar.

Step 4 Use the Object Selector to select a specific group or device.

Step 5 Select **Auto Update Server > Server and Contact Information** from the TOC. The Server and Contact Information window is displayed (see Figure 14-35).

Figure 14-35 *AUS Server and Contact Information Window*



Step 6 Enter the directory path where the updates are stored on the AUS (the default path is Autoupdate/AutoUpdateServlet).

Step 7 Enter the IP address of the AUS server.

Step 8 Enter the port (default 443).

Step 9 In the **Username** field, enter the CiscoWorks username that Firewall MC will use to communicate with the AUS.

Step 10 In the **Password** field, enter the password for the username specified.

Step 11 In the **Confirm Password** field, confirm the password by entering it again.

Step 12 Click **Apply.**

PIX Firewall Configuration Deployment

Finally, you need to configure the Firewall MC to send configuration updates to the AUS instead of the actual device. To specify this configuration change, complete the following steps:

Step 1 Log in to CiscoWorks, and launch Firewall MC.

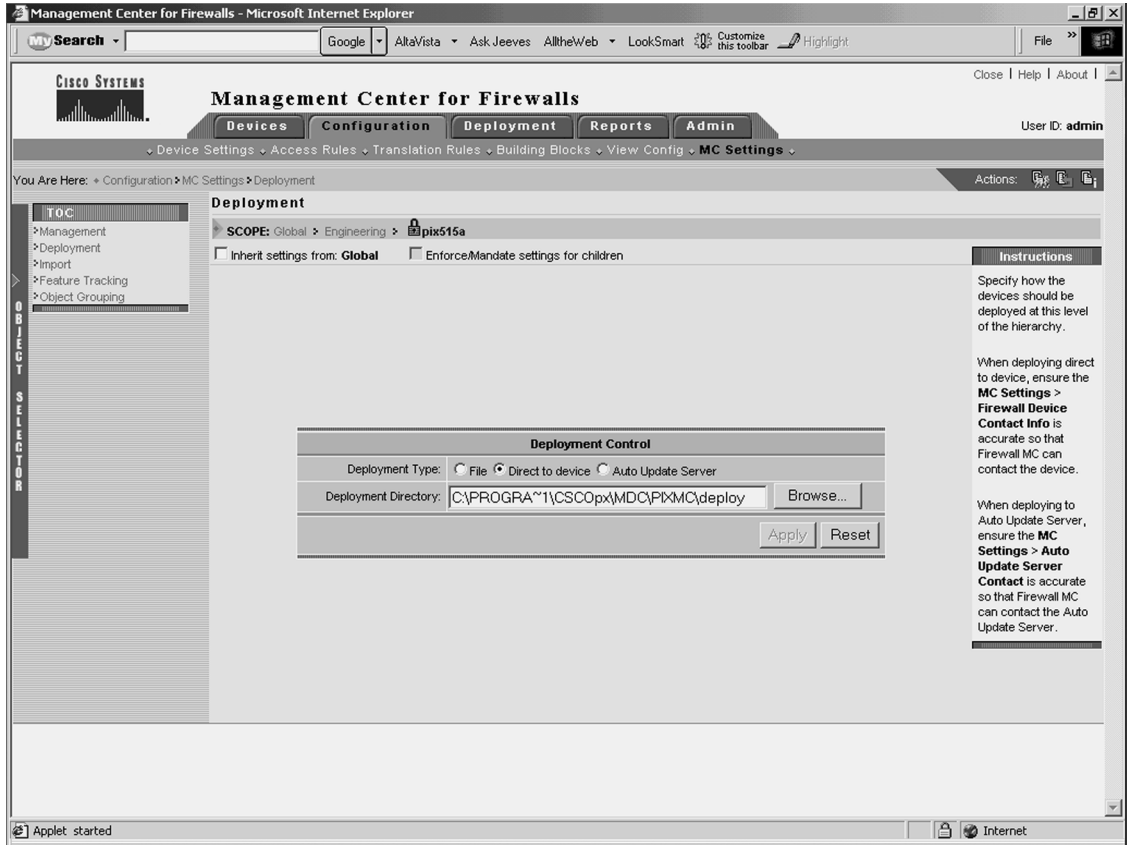
Step 2 Choose **Configuration > MC Settings** to access the Firewall MC configuration settings.

Step 3 If workflow is enabled, you need to select an existing activity or create a new activity from the activity bar.

Step 4 Use the Object Selector to select a specific group or device.

Step 5 Select **Deployment** from the TOC. The Deployment window is displayed (see Figure 14-36).

Figure 14-36 *Deployment Window*



Step 6 Select the **Auto Update Server** radio button.

Step 7 Click **Apply.**

NOTE Before changing the deployment parameters, you need to verify that you have deployed the initial AUS configuration information to the managed firewall. Once you change the deployment options, the device will not receive any more updates from the Firewall MC (because the updates are then sent to the AUS). If the managed firewall does not have the AUS settings, it will be unable to obtain any configuration updates.

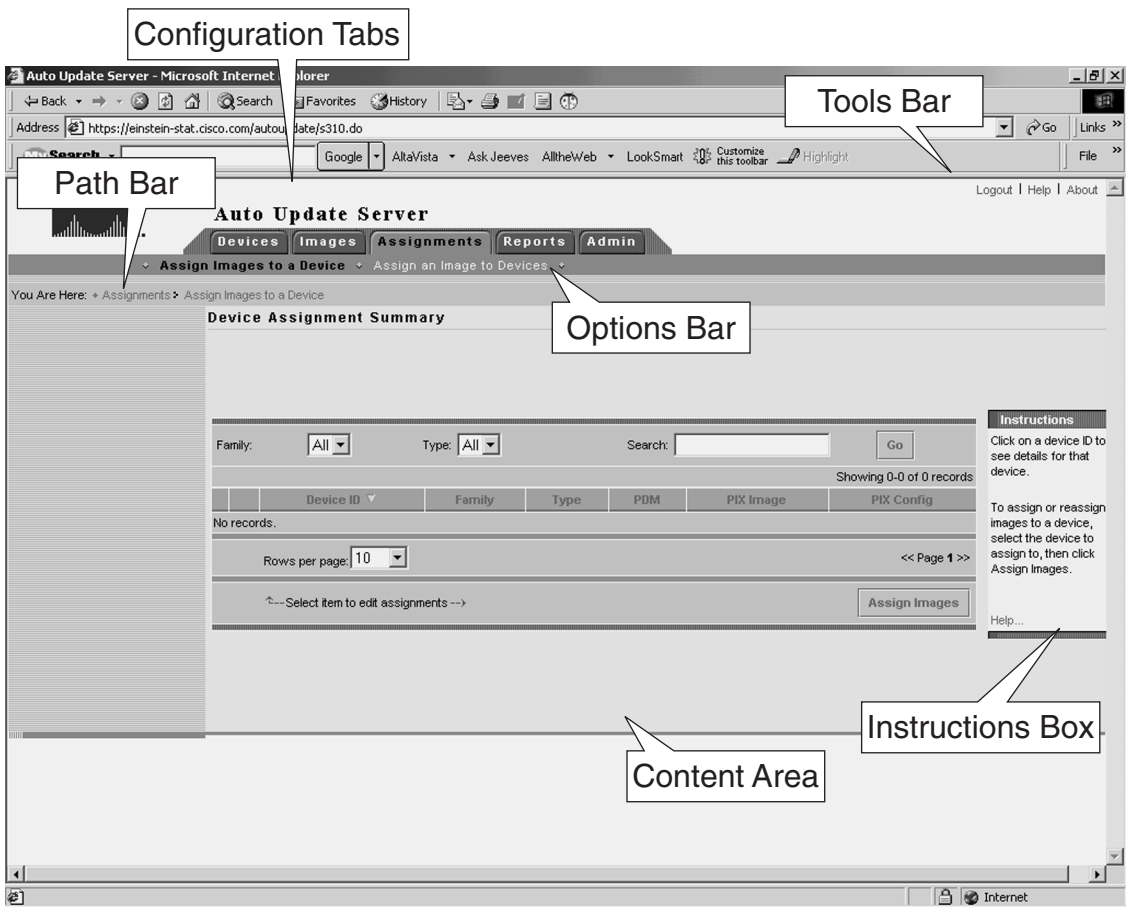
Auto Update Server Interface

Besides configuring the communication between the AUS, Firewall MC, and your managed firewalls, you also need to understand the AUS interface to use it efficiently. The interface is divided into the following sections (see Figure 14-37):

- Path bar
- Options bar
- Configuration tabs
- Tools bar
- Instructions box
- Content area

NOTE You access the AUS by first logging in to CiscoWorks (refer to the "CiscoWorks" section earlier in the chapter). After logging in to CiscoWorks, you launch the AUS by clicking the AUS option VPN/Security Management Solution drawer.

Figure 14-37 *AUS User Interface*



Path Bar

The path bar provides a visual road map indicating where you are with respect to the AUS interface. It is located below the options bar and begins with the text "You Are Here."

Figure 14-37 shows a situation in which the value of the path bar is Assignments > Assign Images to a Device. This indicates that you performed the following steps to reach the current window:

Step 1 You clicked the **Assignments** tab.

Step 2 You clicked the **Assign Images to a Device** option.

Options Bar

After clicking one of the major configuration tabs, the options for that selection are displayed in a list that is located on the screen just below the configuration tabs. Figure 14-37 shows a window in which the user clicked the Assignments tab. The options associated with the Assignments tab are as follows:

- Assign Images to a Device
- Assign an Image to Devices

Configuration Tabs

The configuration tasks are broken down into the following five major categories:

- **Devices**—Displays summary information about devices
- **Images**—Provides information about PIX Firewall software images, PDM images, and configuration files and allows you to add and delete PIX Firewall software images and PDM images
- **Assignments**—Allows you to view and change device-to-image assignments and image-to-device assignments
- **Reports**—Displays reports
- **Admin**—Enables you to perform administrative tasks, such as configuring NAT settings and changing your database password

To access one of the categories, click the tab labeled with the appropriate name. The tabs are located across the top of the AUS display.

Tools Bar

Located at the upper-right portion of the AUS interface is the tools bar. From the tools bar, you can access the following items:

- Logout
- Help
- About

Click **Logout** to log out of the current AUS user session. Click **Help** to open another browser window that displays detailed context-sensitive help information for using AUS. Finally, click the **About** option to display information about the version of AUS that you are using.

Instructions Box

Some pages provide you with an Instructions box on the right side of the AUS display. When displayed, this box provides you with a brief overview of the page that you have selected. The Instructions box provides less information than that provided through the **Help** option on the tools bar.

Content Area

The content area is the portion of the window in which you perform application tasks.

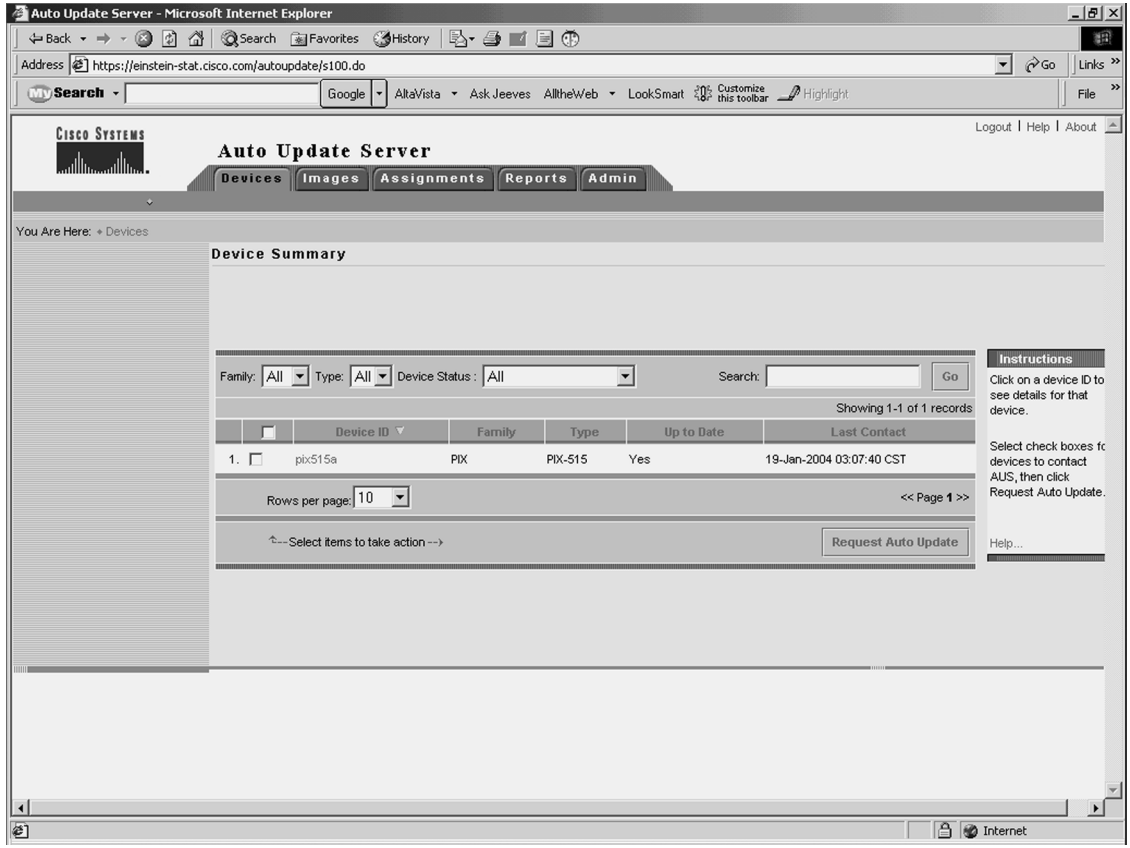
Configuring Devices

Click the **Devices** tab to display the Device Summary table (see Figure 14-38). The table shows all of PIX Firewalls being managed by the AUS. The table provides information such as the device ID, platform family, and the last time that the PIX Firewall contacted the AUS (see Table 14-7). To sort the table by a specific column, click the name of a column. You can also filter the information displayed by using the drop-down menus for Family, Type, or Device Status. Another option for limiting the number of entries displayed is to search for specific devices by entering a textual search string.

Table 14-7 *Device Summary Table Parameters*

Parameter	Description
Device ID	Displays the name the firewall uses to identify itself to the AUS.
Family	Series to which the firewall belongs (such as PIX)
Type	The type of device within the device family (such as PIX 515)
Up to Date	Indicates whether the devices is running the latest files
Last Contact	Indicates the last time that the firewall contacted the AUS

Figure 14-38 *Device Summary Table*



Configuring Images

The AUS enables you to manage the following items for your managed firewalls:

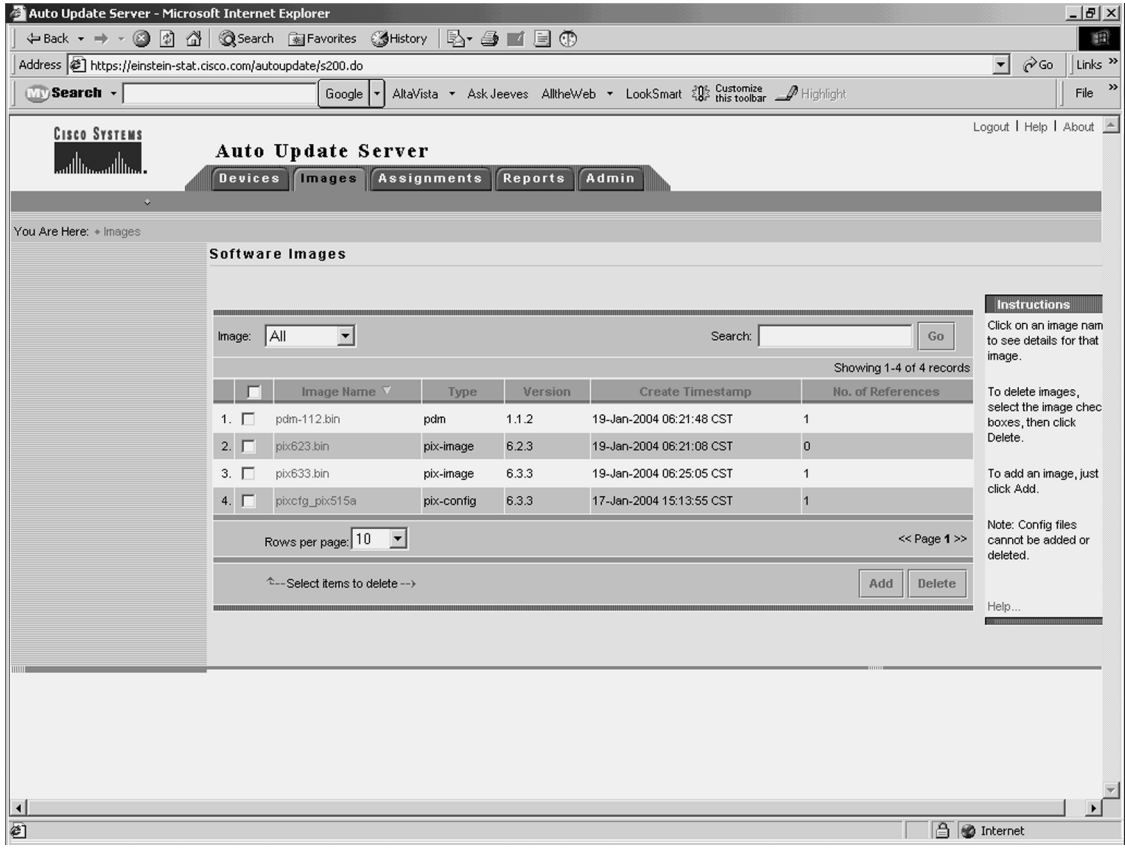
- PIX Firewall images
- PDM images
- PIX Firewall configuration files

In the Images configuration tab, you can add or delete both PIX Firewall software images and PDM images (see Figure 14-39). PIX Firewall configuration files can be added to AUS only by deploying them from Firewall MC. Table 14-8 describes the fields in the Software Images table.

Table 14-8 *Software Images Table Parameters*

Parameter	Description
Image Name	Name of the image that is stored in AUS
Type	Type of image (either PIX image, PDM image, or configuration file)
Version	Version of the image
Create Timestamp	Time the image was added to AUS
No. of References	Number of devices that have been assigned to the image

Figure 14-39 *Software Images Table*



Configuring Assignments

When a new image becomes available, you can perform the following steps:

Step 1 Download the image file.

Step 2 Add the image to AUS.

Step 3 Assign the image to one or more devices.

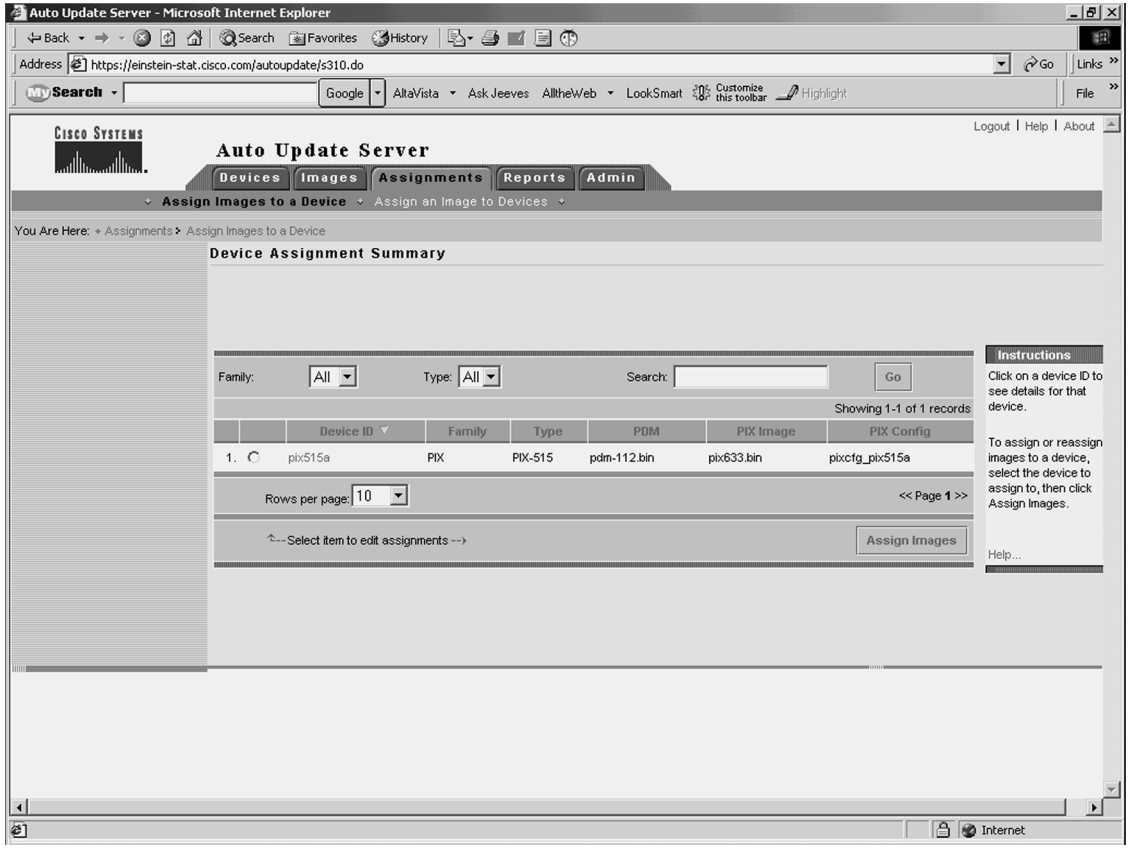
Click the **Assignments** tab to assign image files to specific managed firewalls. You have the following two options when assigning images to your managed firewalls:

- Assign Images to a Device
- Assign an Image to Devices

Assign Images to a Device

The Assign Images to a Device option enables you to view the images assigned to your managed devices based on a table that is sorted by the device ID (see Figure 14-40). Besides viewing the currently assigned images, you can also assign a different image for a specific device based on its device ID.

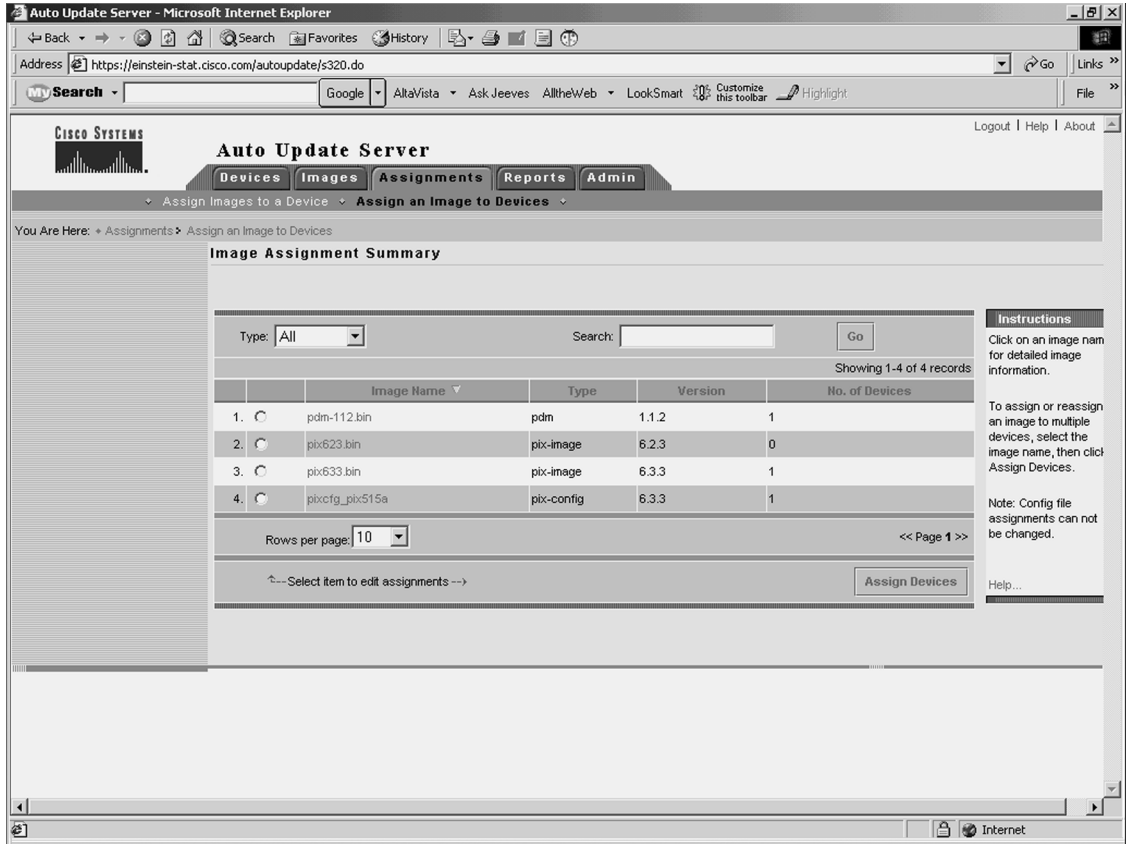
Figure 14-40 *Device Assignment Summary Table*



Assign an Image to Devices

The Assign an Image to Devices option enables you to view the images assigned to your managed devices based on a table that is sorted by the image name (see Figure 14-41). You also can assign a specific image listed in the table to one or more managed devices.

Figure 14-41 *Image Assignment Summary Table*



Reports

The Reports tab enables you to view the different reports supported by AUS. The AUS supports the following two types of reports:

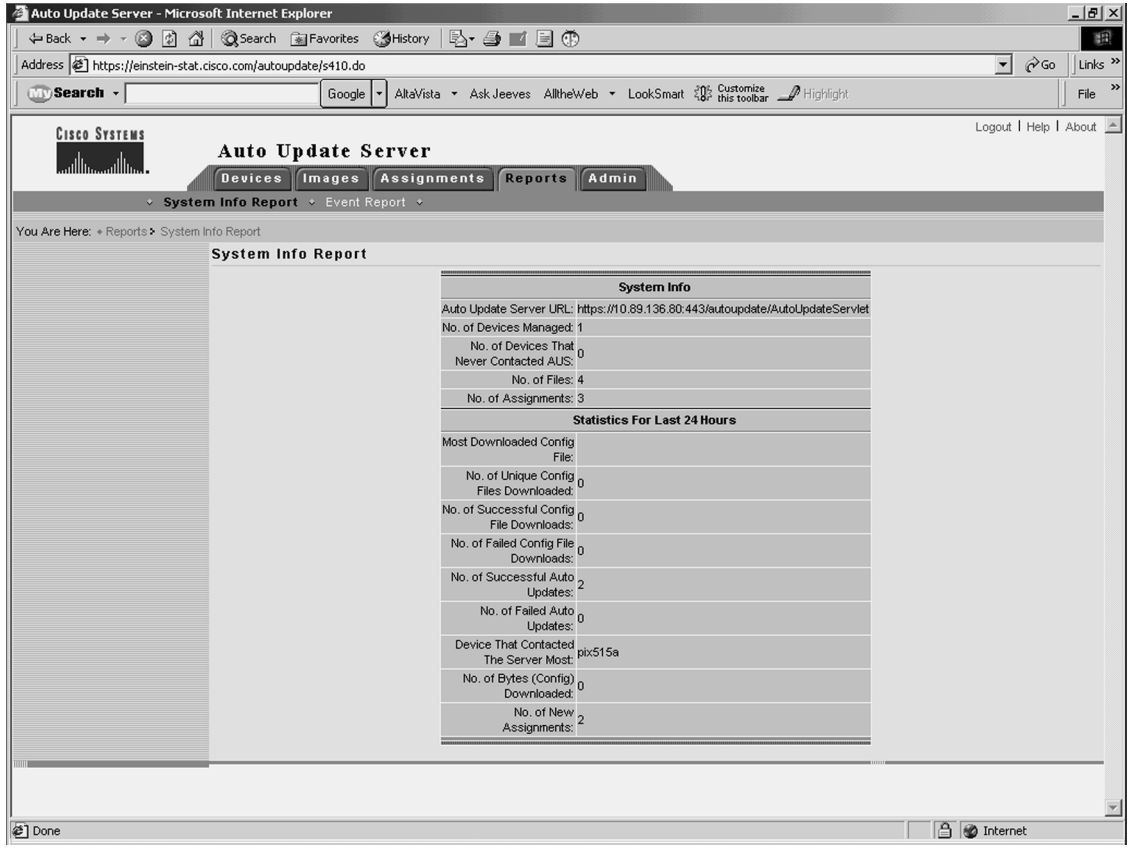
- System Info Report
- Event Report

System Info Report

The System Info Report displays general system information about the AUS along with the statistics for the last 24 hours (see Figure 14-42). The information provided by the System Info Report includes the following:

- AUS URL
- Number of devices managed
- Number of files that the AUS contains
- Number of assignments
- Most downloaded configuration file (in the last 24 hours)
- Number of unique configuration files downloaded (in the last 24 hours)
- Number of successful configuration file downloads (in the last 24 hours)
- Number of failed configuration file downloads (in the last 24 hours)
- Number of successful auto updates (in the last 24 hours)
- Number of failed auto updates (in the last 24 hours)
- Device that contacted the server most (in the last 24 hours)
- Number of bytes downloaded (in the last 24 hours)
- Number of new assignments (in the last 24 hours)

Figure 14-42 *System Info Report*



Event Report

The Event Report displays information about the devices that have contacted the AUS (see Figure 14-43). Each entry in the report represents an event and the result of the event. These events can also be notifications from the managed firewalls indicating errors (such as problems with a downloaded configuration file). Some of the events that you may observe are shown in Table 14-9.

Figure 14-43 *Event Report*

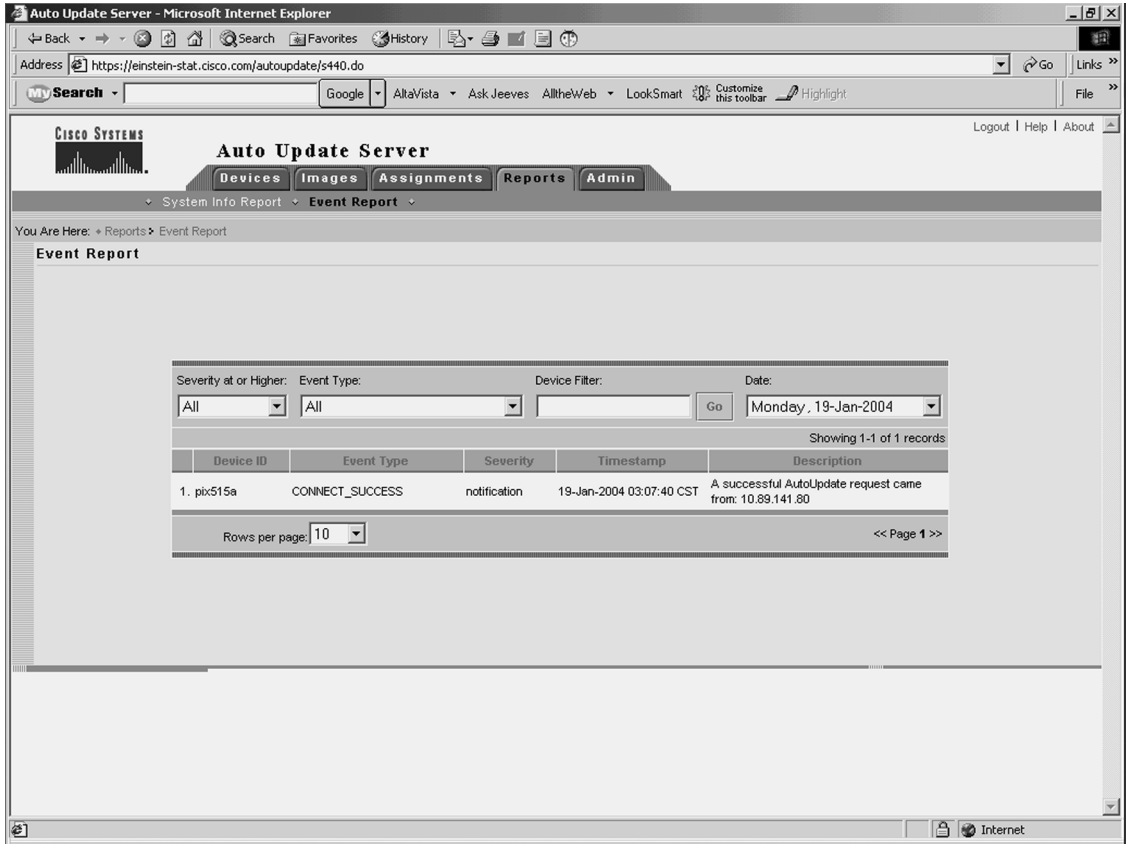


Table 14-9 *Event Types*

Event	Description
CONNECT-SUCCESS	A managed firewall contacted the AUS successfully.
CONNECT-FAILURE	A problem occurred during an auto update attempt. Some possible causes include the following: • Error while parsing XML information • Invalid login credentials • Connectivity problems
DEVICE-CONFIG-ERROR	The managed firewall reported to the AUS that errors occurred while loading the downloaded configuration file.

Table 14-9 *Event Types (Continued)*

Event	Description
GENERAL-DEVICE-ERROR	The managed firewall reported a nonconfiguration file error to AUS. Some possible causes include the following: • Problems connecting to AUS servlet • Invalid checksum for downloaded image
DOWNLAOD-SUCCESS	The file was successfully sent to the managed firewall (does not necessarily indicate that image file is successfully installed).
DOWNLOAD-FAILURE	An error occurred while the image or configuration was being downloaded. Possible causes included the following: • Connectivity problems • Invalid credentials
AUS-IMMEDIATE-SUCCESS	The AUS successfully contacted and updated the managed device.
AUS-IMMEDIATE-FAILURE	An error occurred while updating a managed device. Possible causes include the following: • The server does not have connectivity to device (NAT problems) • The login credentials are incorrect
SYSTEM-ERROR	An internal error occurred.

Administrative Tasks

The Administrative tab enables you to change the following characteristics of the AUS:

- NAT settings
- Database password change

The NAT Settings option enables you to configure the actual address of the AUS server along with a NAT address. This option is used when the AUS server is separated from the managed devices by a NAT device.

The Database Password Change option lets you change the password that is used to authenticate access to the AUS database.

Foundation Summary

The "Foundation Summary" provides a convenient review of many key concepts in this chapter. If you are already comfortable with the topics in this chapter, this summary can help you recall a few details. If you just read this chapter, this review should help solidify some key facts. If you are doing your final preparation before the exam, this summary provides a convenient way to review the day before the exam.

CiscoWorks Management Center for Firewalls (Firewall MC) enables you to manage multiple firewalls across your network. The Firewall MC software operates on top of CiscoWorks Common Services (Version 2.2) that provide basic functionality such as user authentication. Some of the features of Firewall MC include the following:

- Web-based interface for configuring and managing multiple firewalls
- Configuration hierarchy and user interface to facilitate configuration of firewall settings
- Support for PIX Firewall Version 6.0 and later
- Ability to import configurations from existing firewalls
- Ability to support dynamically addressed PIX Firewalls
- Support for up to 1000 PIX Firewalls
- SSL protocol support for client communications to CiscoWorks
- Support for workflow and audit trails

Firewall MC supports the following firewall platforms:

- PIX 501
- PIX 506/506E
- PIX 515/515E
- PIX 525
- PIX 535
- FWSM

To manage firewalls using Firewall MC, you must configure the firewall to allow HTTP access from the Firewall MC. The Firewall MC interface is divided into the following major configuration tabs:

- **Devices**—Enables you to import device configurations and define device groups to be managed by the system

- **Configuration**—Enables you to change the operational configuration of the devices managed by the system
- **Deployment**—Enables you to generate configuration files, manage firewall configuration files, and submit or manage new jobs
- **Reports**—Enables you to generate reports, view scheduled reports, and view reports
- **Admin**—Enables you to configure system settings

The basic user task flow for using Firewall MC involves the following steps:

Step 1 Create device groups.

Step 2 Import/create devices.

Step 3 Configure building blocks.

Step 4 Configure device settings.

Step 5 Configure access and translation rules.

Step 6 Generate and view the configuration.

Step 7 Deploy the configuration.

You must define the firewalls that Firewall MC will manage. Device management falls into the following categories:

- Managing groups
- Importing devices
- Managing devices

After importing the device to be managed, you must perform various configuration tasks. Configuration tasks using the Firewall MC fall into the following topics:

- Configuring device settings
- Defining access rules
- Defining translation rules
- Creating building blocks
- Generating and viewing configuration information

Some of the device settings that you can configure through Firewall MC include the following:

- PIX operating system version
- Interfaces

- Fail over
- Routing
- PIX Firewall administration
- Logging
- Servers and services
- Advanced security
- Firewall MC controls
- Configuring access and translation rules

Access rules define your network security policy by controlling the flow of network traffic through your firewalls. The three types of access rules are as follows:

- Firewall rules
- AAA rules
- Web filter rules

Translation rules define the translation of private IP addresses to public IP address and fall into the following three categories:

- Static translation rules
- Dynamic translation rules
- Translation exception rules (NAT 0 ACL)

To optimize your configuration, you can define building blocks that can then be used when defining other items (such as access and translation rules). You can configure the following types of building blocks:

- Network objects
- Service definitions
- Service groups
- AAA server groups
- Address translation pools

Firewall MC supports the following types of reports:

- Activity Report
- Configuration Differences report
- Device Setting Report

After making configuration changes, you need to deploy those changes to your managed firewalls. By default these changes are deployed to your managed firewalls as soon as you save your configuration changes. If you enable workflow, however, then updating configurations involves the following three steps:

Step 1 Define configuration changes.

Step 2 Approve configuration changes.

Step 3 Deploy configuration changes.

Using workflow, configuration changes become activities, and deploying those activities become jobs. You can require approval for activities, jobs, or both.

The AUS enables you to maintain current images efficiently on your managed firewalls. Like Firewall MC, the AUS runs on top of CiscoWorks Common Services. AUS supports the following types of images:

- PIX Firewall software images
- PDM software images
- PIX configuration files

Some of the major features provided by AUS (Version 1.0) include the following:

- Web-based interface for maintaining multiple PIX Firewalls
- Support for PIX Firewall operating system 6.0 and later
- Support for dynamically addressed PIX Firewalls
- Support for up to 1000 PIX Firewalls

AUS Version 1.1 added new functionality including the following major features:

- Installation on Solaris
- Additional report formats
- Support for configuration files

PIX Firewall software images and PDM software images can be directly added to the AUS. PIX configuration files must be deployed from Firewall MC to be added to the AUS.

The configuration tasks in the AUS (Version 1.0) are broken down into the following five major categories:

- **Devices**—Displays summary information about devices
- **Images**—Provides information about PIX Firewall software images, PDM images, and configuration files and allows you to add and delete PIX Firewall software images and PDM images
- **Assignments**—Allows you to view and change device-to-image assignments and image-to-device assignments
- **Reports**—Displays reports
- **Admin**—Enables you to perform administrative tasks, such as configuring NAT settings and changing your database password

Q&A

As mentioned in the Introduction, the questions in this book are more difficult than what you should experience on the exam. The questions are designed to ensure your understanding of the concepts discussed in this chapter and adequately prepare you to complete the exam. You should use the simulated exams on the CD to practice for the exam.

The answers to these questions can be found in Appendix A.

1. Which software performs user authentication for Firewall MC and AUS?
2. Which type of building block enables you to associate multiple protocols with a single name?
3. What types of translation rules can you configure in Firewall MC?
4. What types of access rules does Firewall MC enable you to configure?
5. What types of images does AUS support?
6. Which images can you not add directly through the AUS interface?
7. Which type of translation rule defines a permanent mapping between private IP addresses and public IP addresses?
8. What is an address translation pool?
9. What is a network object?
10. What are three of the device settings that you can configure through Firewall MC?
11. What type of building block do you need to define to create a dynamic translation rule?
12. What is workflow?
13. Can AUS be used to manage firewalls that use dynamic addresses assigned by DHCP?
14. What building blocks can you configure with Firewall MC, and how are they used?
15. What three reports does Firewall MC support?
16. Name the three possible methods from which each device setting in a managed configuration can be derived.
17. What are the four steps used to import a device into Firewall MC?
18. What are the steps required to add images to AUS?