14

Advance Management

Terms you’ll need to understand:

✓ CiscoWorks VPN/Security Management Solution (VMS)
✓ CiscoWorks Management Center for Firewall (PIX MC)
✓ Cisco Firewall Services Module (FWSM)
✓ CiscoWorks Auto Update Server (AUS)
✓ Mandatory access rules
✓ Default access rules
✓ Device access rules
✓ PIX MC default groups
✓ PIX MC access rules

Techniques you’ll need to master:

✓ Remembering CiscoWorks port numbers
✓ Knowing PIX MC management tabs
✓ Knowing the Auto Update Server process

Advanced Management

Cisco offers several advanced management tools that can help manage the PIX firewall from small- to large enterprise-sized companies. This chapter covers some of the possible modules, such as PIX Management Center (MC) and the Auto Update Server, which can be added to CiscoWorks products.

CiscoWorks

CiscoWorks is Cisco's flagship enterprise suite of integrated network management tools designed to simplify the administration and maintenance of small- to medium-sized business networks. The product line is quite extensive and could be a book in itself. However, a few modules are important to the PIX firewall, which we discuss here.

CiscoWorks VPN/Security Management Solution

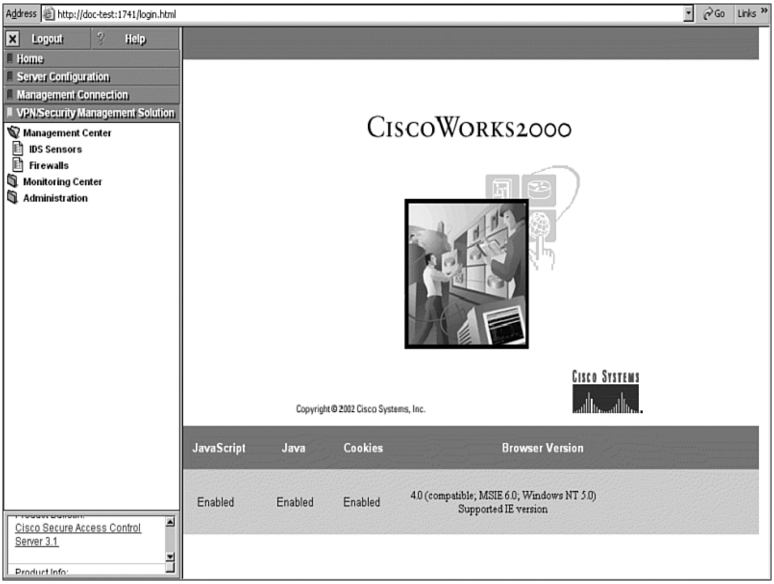
The VPN/Security Management Solution (VMS) is a Web-based tool used for configuring, monitoring, and troubleshooting firewalls, VPNs, and intrusion detection systems (IDSs). The following is a list of the functions this product provides:

- Firewall management
- VPN monitoring
- Security monitoring
- Operation management
- VPN router management
- IDS management

This chapter focuses only on the firewall management section and not on VPNs or the IDS capabilities of CiscoWorks. Figure 14.1 displays the CiscoWorks screen that allows access to the PIX Management Center.

EXAM ALERT

By default, CiscoWorks uses port 1741 on the Web server.



Address: http://doc-test:1741/login.html

JavaScript	Java	Cookies	Browser Version
Enabled	Enabled	Enabled	4.0 (compatible; MSIE 6.0; Windows NT 5.0) Supported IE version

Figure 14.1 CiscoWorks VPN/Security screen.

CiscoWorks Management Center for Firewall

The PIX MC is a Web-based interface tool used inside Cisco VPN/Security Management Solution within CiscoWorks. The tool is similar to the PIX Device Manager (PDM) that is used to manage a single PIX firewall. However, PIX MC offers centralized management of up to 1,000 firewalls at the same time.

The PIX MC enables you to configure new firewalls and import current firewall configurations. When paired with the PIX Auto Update Server, it can additionally download configurations, software upgrades, and PDM software to your PIX firewalls.

PIX MC works not only with the PIX firewalls, but also with the Firewall Service Modules (FWSM) that are used inside a 6500 Catalyst switch.

NOTE The Cisco Firewall Services Module is an integrated firewall module for Cisco Catalyst 6500 switches and Cisco 7600 Series routers. The FWSM provides fast firewall data throughput, based on the Cisco PIX firewall.

The following list displays some of the features PIX MC can provide:

- A Web-based interface for configuring and managing multiple firewall devices without requiring Command Line Interface (CLI) knowledge
- The importation of configurations from existing firewall devices
- A configuration hierarchy is used to configure rules and building blocks that are applied to groups, subgroups, and devices
- The configuration settings can be written to a file, directly to a firewall device, or to an AUS
- Support for firewall device operating systems 6.0, 6.1, and 6.2
- Multiple PIX MC user support
- Support for up to 1,000 devices
- A workflow and audit trail

Using the PIX MC

The PIX MC enables you to configure your PIX firewalls without the use of the command-line interface (CLI). The CiscoWorks Web interface requires you to log in to the system before you can access the PIX MC graphical user interface (GUI). Figure 14.2 displays the splash screen you will see when entering the PIX MC.

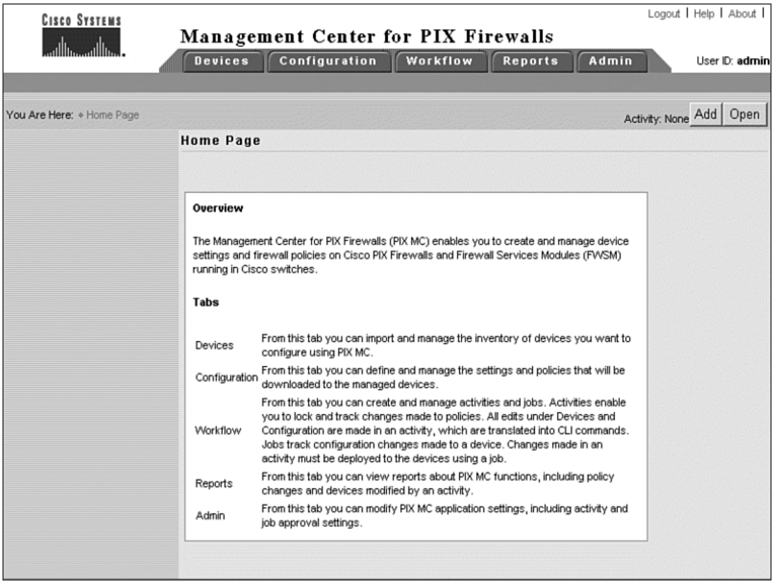
Table 14.1 lists the five main upper tabs—Devices, Configuration, Workflow, Reports, and Admin—and their submenu items.

Table 14.1 PIX MC Configuration Tabs

Tab	Submenu Items
Devices	Importing Devices Managing Devices Managing Groups
Configuration	Settings Access Rules Translation Rules Building Blocks View Config

Table 14.1 PIX MC Configuration Tabs *(continued)*

Tab	Submenu Items
Workflow	Activity Management Job Management
Reports	Activity
Admin	Workflow Maintenance Support



Home Page

Overview

The Management Center for PIX Firewalls (PIX MC) enables you to create and manage device settings and firewall policies on Cisco PIX Firewalls and Firewall Services Modules (FWSM) running in Cisco switches.

Tabs

Devices	From this tab you can import and manage the inventory of devices you want to configure using PIX MC.
Configuration	From this tab you can define and manage the settings and policies that will be downloaded to the managed devices.
Workflow	From this tab you can create and manage activities and jobs. Activities enable you to lock and track changes made to policies. All edits under Devices and Configuration are made in an activity, which are translated into CLI commands. Jobs track configuration changes made to a device. Changes made in an activity must be deployed to the devices using a job.
Reports	From this tab you can view reports about PIX MC functions, including policy changes and devices modified by an activity.
Admin	From this tab you can modify PIX MC application settings, including activity and job approval settings.

Figure 14.2 The PIX MC splash screen.

The Devices Tab

This tab is used to import and manage the PIX firewall device configuration settings. Table 14.2 contains this tab's three main submenu items with basic descriptions of what they do.

Table 14.2 PIX MC Devices Tab

Subitem	Description
Importing Devices	This enables you to import firewall configurations from a firewall or file.
Managing Devices	This enables you to move and place firewalls within groups created using the Managing Groups subitem.

Table 14.2 PIX MC Devices Tab *(continued)*

Subitem	Description
Managing Groups	This enables you to create groups of devices that contain similar attributes.

The Configuration Tab

This tab is used to define and manage settings that can be downloaded to the firewalls. Table 14.3 displays the Configuration tab's items and their descriptions.

Table 14.3 PIX MC Configuration Tab

Subitem	Description
Settings	This enables the use of wizards to configure firewalls based on group memberships.
Access Rules	This enables you to control traffic through the device. Access rules use ACLs to provide traffic control.
Translation Rules	This enables you to view and configure translation settings for NAT or PAT across your firewall.
Building Blocks	This enables you to create ACL **object-group** commands without using the CLI.
View Config	This enables you to view configuration files.

The Workflow Tab

The Workflow tab enables you to control and manage activity workflow and to create new activities that are used to control policy changes against a device (firewall). Table 14.4 displays the Workflow tab's subitems.

Table 14.4 PIX MC Workflow Tab

Subitem	Description
Activity Management	This tab is used to view, edit, and create activity tasks for your PIX firewalls. For example, if a firewall needs configuration, this tab is used to create an activity requesting some change that needs to take effect.
Job Management	This tab is used to manage jobs. A *job* represents a set of configurations that need to be deployed to a device, a configuration file, or an AUS.

The Reports Tab

This tab enables you to view reports about actions administrators have performed within an activity. Only one selection is available on this tab; it's called Activity. Table 14.5 displays the details of the activity report.

Table 14.5 PIX MC Reports Tab's Activity Report

Report View	Description
Basic Information	Displays the activity name and any comments from the administrator
State Changes	Displays a history of the date and time the action occurred and who performed the action
Policy Changes	Displays which devices and groups were acted upon and identifies the policy changes made as part of that activity

The Admin Tab

The Admin tab configures the global settings for the PIX MC, such as enabling workflow and audit record retention. Table 14.6 describes the three submenu items available.

Table 14.6 PIX MC Admin Tab

Report View	Description
Workflow	This option enables you to set whether workflow activities should require approval.
Maintenance	This option enables you to delete records and specify how long records should be retained.
Support	This option collects configuration and system information into a **.zip** file called **MDCSupportInformation.zip**. This file can be sent to tech support for assistance.

PIX MC Groups

The PIX MC provides the ability to place PIX firewall devices with similar attributes into groups. These groups enable you to configure these devices with similar settings. The default group, called Global, is the highest-level group; from here you can create subgroups. Devices are placed within these subgroups. Figure 14.3 displays three firewalls placed into the group called Corvallis Firewalls.

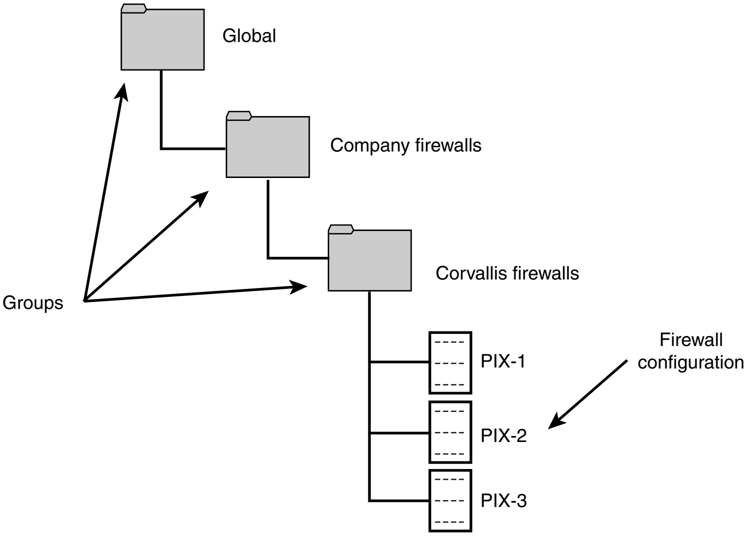


Figure 14.3 PIX MC Groups for attributes.

The PIX MC provides the ability to group devices with similar attributes. By using the Devices tab, you can create more groups. However, the default group is called Global.

After groups are created, device (firewall) configurations can be imported into the group. Figure 14.3 shows three configurations currently imported: PIX-1, PIX-2, and PIX-3.

PIX MC Access Rules

The PIX MC enables you to define access rules, which are used to configure network security policies on your firewall. Access rules are grouped by interfaces that eventually are translated into access list (ACL) entries assigned to that interface. These rules are assigned to a group or subgroup and are merged to provide access control on the firewall.

The following shows the three types of access rules that can be created in the order of precedence:

1. Mandatory access rules
2. Device access rules
3. Default access rules

Mandatory access rules are the most important rules and take precedence over any other rules. This places them first in the ACL that is created. Device access rules are next. If no mandatory access rule opposes a device rule, the rule affects the PIX. Lastly are the default rules, which take effect only if no other rule overrides them.

Figure 14.4 displays access rules coming from each group and the device. The access rules from groups can be either mandatory or default. Access rules from a device are device rules applied only to that specific device. All these rules are combined and converted into the ACL for the device.

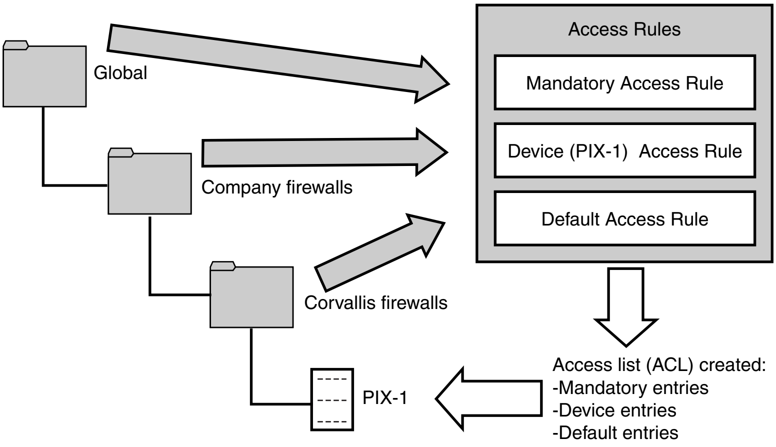


Figure 14.4 Access rules.

Mandatory rules cannot be overridden, are applied at the group, and are ordered down to a device.

Default rules can be overridden and are ordered from the device up to the enclosing groups.

CiscoWorks Auto Update Server

The Auto Update Server provides a Web-based interface module inside CiscoWorks for upgrading device configuration files, software images, and PDM images. It is designed to interoperate with PIX MC to deploy the configuration files and to operate alone for updating PDM images.

AUS works off the principal of the devices (firewalls) periodically polling it for updates. If an update exists, the device requests to download the newer image or configuration file. Figure 14.5 displays the step-by-step flow of the PIX interacting with an AUS server.

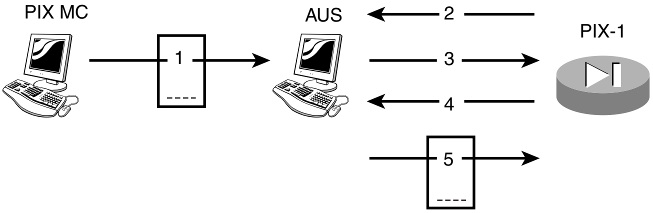


Figure 14.5 Auto Update Server updated process.

The following step numbers correspond to the numbers found on Figure 14.5:

1. The MC deploys the configuration file to the Auto Update Server.
2. The PIX periodically polls the AUS server for a list of updates.
3. The AUS sends the list of files to the PIX.
4. The PIX verifies it has the latest files; if it doesn't, it requests the latest version.
5. The newer configuration files are downloaded.

EXAM ALERT

The Auto Update Server operates on port 443 (HTTPS).

Auto Update Server Configuration Tabs

The Web interface for the AUS is similar to PIX MC. It contains; Devices, Files (Images), Assignments, Reports, and Admin tabs are used to set up and configure the AUS system. Table 14.7 contains a brief description of each tab.

Table 14.7 CiscoWorks Auto Update Server Configuration Tab

Tab	Description
Devices	Provides summary information about devices.
Files (Images)	Provides details about configuration files, PIX firewall software images, and PDM images. It also enables you to add and delete images.
Assignments	Enables you to assign images to devices.
Reports	Displays reports.
Admin	Enables you to configure the AUS and change the database password.

In this chapter, we talked about CiscoWorks as the main enterprise software management product that can incorporate several modules to configure firewalls. The Cisco PIX MC is used to create groups of devices with similar attributes and provide configuration files. These configuration files can then be downloaded to the devices using the AUS feature of CiscoWorks.