SECURITY

Cisco ASA

All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance

Second Edition

Identify, mitigate, and respond to network attacks

Jazib Frahim, CCIE® No. 5459
Omar Santos

ciscopress.com

Cisco ASA

All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance, Second Edition

Jazib Frahim, CCIE No. 5459

Omar Santos

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance, Second Edition

Jazib Frahim, Omar Santos

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

Third Printing July 2011

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58705-819-6

ISBN-10: 1-58705-819-7

Warning and Disclaimer

This book is designed to provide information about Cisco ASA. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales**
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside the United States please contact:
International Sales
international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Patrick Kanouse

Project Editor: Seth Kerney

Book and Cover Designer: Louisa Adair

Composition: Mark Shirar

Proofreaders: Water Crest Publishing, Inc., Apostrophe Editing Services

Business Operation Manager, Cisco Press: Anand Sundaram

Manager Global Certification: Erik Ullanderson

Technical Editors: Randy Ivener, Jay Johnston

Development Editors: Kimberley Debus, Dayna Isley

Copy Editor: Margo Catts

Editorial Assistant: Vanessa Evans

Indexer: Ken Johnson

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

About the Authors

Jazib Frahim, CCIE No. 5459, has been with Cisco Systems for more than ten years. With a bachelor's degree in computer engineering from Illinois Institute of Technology, he started out as a TAC engineer in the LAN Switching team. He then moved to the TAC Security team, where he acted as a technical leader for the security products. He led a team of 20 engineers in resolving complicated security and VPN technologies. He is currently working as a technical leader in the Worldwide Security Services Practice of Advanced Services for Network Security. He is responsible for guiding customers in the design and implementation of their networks with a focus on network security. He holds two CCIEs, one in routing and switching and the other in security. He has written numerous Cisco online technical documents and has been an active member on the Cisco online forum NetPro. He has presented at Networkers on multiple occasions and has taught many on-site and online courses to Cisco customers, partners, and employees.

While working for Cisco, he pursued his master of business administration (MBA) degree from North Carolina State University.

He is also an author of the following Cisco Press books:

- *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*
- *Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting*
- *SSL Remote Access VPNs*

Omar Santos is an incident manager at Cisco's Product Security Incident Response Team (PSIRT). Omar has designed, implemented, and supported numerous secure networks for Fortune 500 companies and the U.S. government, including the United States Marine Corps (USMC) and the U.S. Department of Defense (DoD). He is also the author of many Cisco online technical documents and configuration guidelines. Prior to his current role, he was a technical leader within the World Wide Security Practice and Cisco's Technical Assistance Center (TAC), where he taught, led, and mentored many engineers within both organizations.

Omar has also delivered numerous technical presentations to Cisco customers and partners; as well as executive presentations to CEOs, CIOs, and CSOs of many organizations. He is also the author of the following Cisco Press books:

- *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*
- *Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting*
- *End-to-End Network Security: Defense-in-Depth*

About the Technical Reviewers

Randy Ivener, CCIE No. 10722, is a security engineer in the Cisco Security Research and Operations team. He is a CISSP and PMI PMP. He has spent many years as a network security consultant helping companies understand and secure their networks. Randy has presented security topics at industry events including Blackhat and Cisco Networkers. Before becoming immersed in information security, he spent time in software development and as a training instructor. Randy graduated from the U.S. Naval Academy and holds an MBA.

Jay Johnston, CCIE No. 17663, is a security specialist in the Cisco TAC center located in Research Triangle Park, North Carolina. His networking career began in 2002 when he joined Cisco as a co-op while attending North Carolina State University. After graduating with a bachelors of computer science in 2004, he joined Cisco full time as a TAC Engineer. He obtained his Security CCIE in 2007. He enjoys working for Cisco, especially the constant technical challenges that working with customers in the TAC provides.

Dedications

Jazib Frahim: I would like to dedicate this book to my lovely wife, Sadaf, who has patiently put up with me during the writing process.

I would also like to dedicate this book to my parents, Frahim and Perveen, who support and encourage me in all my endeavors.

Finally, I would like to thank my siblings, including my brother Shazib and sisters Erum and Sana, sister-in-law Asiya, my cute nephew Shayan, and my adorable nieces Shiza and Alisha. Thank you for your patience and understanding during the development of this book.

Omar Santos: I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.

I also dedicate this book to my parents, Jose and Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

Acknowledgments

We would like to thank the technical editors, Randy Ivener and Jay Johnston, for their time and technical expertise. They verified our work and corrected us in all the major and minor mistakes that were hard to find. Special thanks go to Aun Raza for reviewing many chapters prior to final editing.

We would like to thank the Cisco Press team, especially Brett Bartow, Dayna Isley, Kimberley Debus, and Andrew Cupp for their patience, guidance, and consideration. Their efforts are greatly appreciated.

Many thanks to our Cisco management team, including David Philips, Ken Cavanagh, and Jean Reese for their continuous support. They highly encouraged us throughout this project.

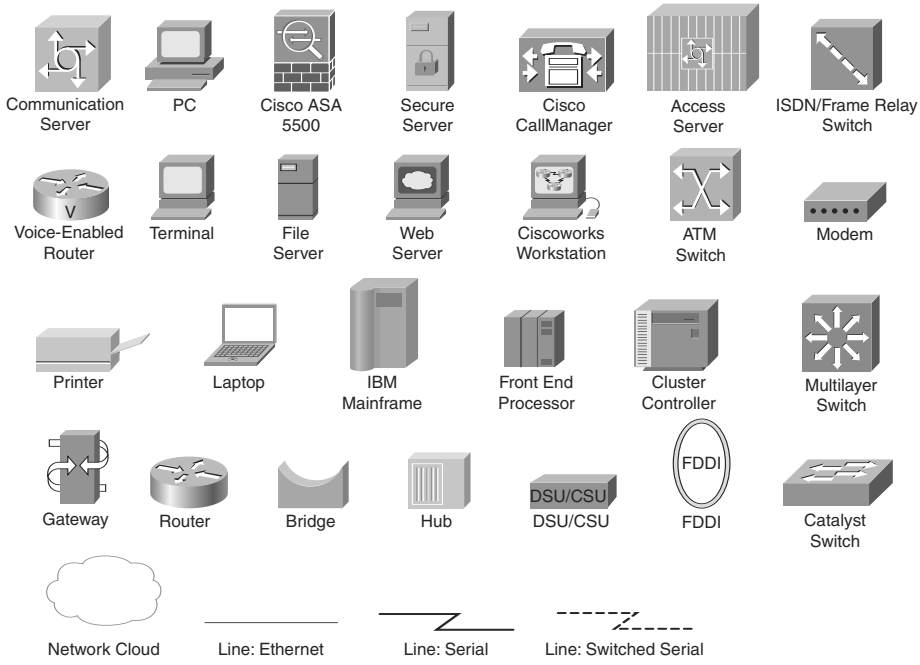
Kudos to the Cisco ASA product development team for delivering such a great product. Their support is also greatly appreciated during the development of this book.

Finally, we would like to acknowledge the Cisco TAC. Some of the best and brightest minds in the networking industry work there, supporting our Cisco customers often under very stressful conditions and working miracles daily. They are truly unsung heroes, and we are all honored to have had the privilege of working side by side with them in the trenches of the TAC.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Network security has always been a challenge for many organizations that cannot deploy separate devices to provide firewall, intrusion prevention, and virtual private network (VPN) services. The Cisco ASA is a high-performance, multifunction security appliance that offers firewall, IPS, network antivirus, and VPN services. The Cisco ASA delivers these features through improved network integration, resiliency, and scalability.

This book is an insider's guide to planning, implementing, configuring, and troubleshooting the Cisco Adaptive Security Appliances. It delivers expert guidance from senior Cisco network security consulting engineers. It demonstrates how adaptive identification and mitigation services on the Cisco ASA provide a sophisticated network security solution to small, medium, and large organizations. This book brings together expert guidance for virtually every challenge you will face—from building basic network security policies to advanced VPN and IPS implementations.

Who Should Read This Book?

This book serves as a guide for any network professional who manages network security or installs and configures firewalls, VPN devices, or intrusion detection/prevention systems. It encompasses topics from an introductory level to advanced topics on security and VPNs. The requirements of the reader include a basic knowledge of TCP/IP and networking.

How This Book Is Organized

This book has five parts, which provide a Cisco ASA product introduction and then focus on firewall features, intrusion prevention, content security, and VPNs. Each part includes many sample configurations, accompanied by in-depth analyses of design scenarios. Your learning is further enhanced by a discussion of a set of debugs included in each technology. Groundbreaking features, such as SSL VPN and virtual and Layer 2 firewalls, are discussed extensively.

The core chapters, Chapters 2 through 12, cover the following topics:

- Part I, "Product Overview," includes the following chapters:
  - Chapter 1, "Introduction to Security Technologies"—This chapter provides an overview of different technologies that are supported by the Cisco ASA and widely used by today's network security professionals.
  - Chapter 2, "Cisco ASA Product and Solution Overview"—This chapter describes how the Cisco ASA incorporates features from each of these products, integrating comprehensive firewall, intrusion detection and prevention, and VPN technologies in a cost-effective, single-box format. Additionally, it provides a hardware overview of the Cisco ASA, including detailed technical specifications and installation guidelines. It also covers an overview of the Adaptive Inspection and Prevention Security Services Module (AIP-SSM) and Content Security and Control Security Services Module (CSC-SSM).

- Chapter 3, "Initial Setup and System Maintenance"—A comprehensive list of initial setup tasks and system maintenance procedures is included in this chapter. These tasks and procedures are intended to be used by network professionals who will be installing, configuring, and managing the Cisco ASA.

- Part II, "Firewall Technology," includes the following chapters:
  - Chapter 4, "Controlling Network Access"—The Cisco ASA can protect one or more networks from intruders. Connections between these networks can be carefully controlled by advanced firewall capabilities, enabling you to ensure that all traffic from and to the protected networks passes only through the firewall based on the organization's security policy. This chapter shows you how to implement your organization's security policy, using the features the Cisco ASA provides.
  - Chapter 5, "IP Routing"—This chapter covers the different routing capabilities of the Cisco ASA.
  - Chapter 6, "Authentication, Authorization, and Accounting (AAA)"—The Cisco ASA supports a wide range of AAA features. This chapter provides guidelines on how to configure AAA services by defining a list of authentication methods applied to various implementations.
  - Chapter 7, "Application Inspection"—The Cisco ASA stateful application inspection helps to secure the use of applications and services in your network. This chapter describes how to use and configure application inspection.
  - Chapter 8, "Virtualization"—The Cisco ASA virtual firewall feature introduces the concept of operating multiple instances of firewalls (contexts) within the same hardware platform. This chapter shows how to configure and troubleshoot each of these security contexts.
  - Chapter 9, "Transparent Firewalls"—This chapter introduces the transparent (Layer 2) firewall model within the Cisco ASA. It explains how users can configure the Cisco ASA in transparent single mode and multiple mode while accommodating their security needs.
  - Chapter 10, "Failover and Redundancy"—This chapter discusses the different redundancy and failover mechanisms that the Cisco ASA provides. It includes not only the overview and configuration, but also detailed troubleshooting procedures.
  - Chapter 11, "Quality of Service"—QoS is a network feature that lets you give priority to certain types of traffic. This chapter covers how to configure and troubleshoot QoS in the Cisco ASA.

- Part III, "Intrusion Prevention System (IPS) Solutions," includes the following chapters:
  - Chapter 12, "Configuring and Troubleshooting Intrusion Prevention System (IPS)"—Intrusion detection and prevention systems provide a level of protection beyond the firewall by securing the network against internal and external

attacks and threats. This chapter describes the integration of Intrusion Prevention System (IPS) features within the Cisco ASA and expert guidance on how to configure the AIP-SSM IPS software. Troubleshooting scenarios are also included to enhance learning.

- Chapter 13, "Tuning and Monitoring IPS"—This chapter covers the IPS tuning process, as well as best practices on how to monitor IPS events.

- Part IV, "Content Security," includes the following chapters:
  - Chapter 14, "Configuring Cisco Content Security and Control Security Services Module"—The Content Security and Control Security Services Module (CSC-SSM) is used to detect and take action on viruses, worms, Trojans, and other security threats. It supports the inspection of SMTP, POP3, HTTP, and FTP network traffic. This chapter provides configuration and troubleshooting guidelines to successfully deploy the CSC-SSM within your organization.
  - Chapter 15, "Monitoring and Troubleshooting the Cisco Content Security and Control Security Services Module"—This chapter provides best practices and methodologies used while monitoring the CSC-SSM and troubleshooting any problems you may encounter.
- Part V, "Virtual Private Network (VPN) Solutions," includes the following chapters:
  - Chapter 16, "Site-to-Site IPSec VPNs"—The Cisco ASA supports IPSec VPN features that enable you to connect networks in different geographic locations. This chapter provides configuration and troubleshooting guidelines to successfully deploy site-to-site IPSec VPNs.
  - Chapter 17, "IPSec Remote-Access VPNs"—This chapter discusses two IPSec remote-access VPN solutions (Cisco IPSec and L2TP over IPSec) that are supported on the Cisco ASA. A large number of sample configurations and troubleshooting scenarios are provided.
  - Chapter 18, "Public Key Infrastructure (PKI)"—This chapter starts by introducing PKI concepts. It then covers the configuration and troubleshooting of PKI in the Cisco ASA.
  - Chapter 19, "Clientless Remote-Access SSL VPNs"—This chapter provides details about the Clientless SSL VPN functionality in Cisco ASA. This chapter covers the Cisco Secure Desktop (CSD) solution in detail and also discusses the Host Scan feature that is used to collect posture information about end-workstations. The dynamic access policy (DAP) feature, its usage, and detailed configuration examples are also provided. To reinforce learning, many different deployment scenarios are presented along with their configurations.
  - Chapter 20, "Client-Based Remote-Access SSL VPNs"— This chapter provides details about the AnyConnect SSL VPN functionality in Cisco ASA.

This page intentionally left blank

Chapter 3

Initial Setup and System Maintenance

This chapter covers the following topics:

- Accessing the Cisco ASA appliances
- Managing licenses
- Initial setup
- IP version 6
- Setting up the system clock
- Configuration management
- Remote system management
- System maintenance
- System monitoring

Cisco Adaptive Security Appliance (ASA) can be set up in a number of ways to adapt to any network topology. However, proper planning is essential for successful implementations of the security features that Cisco ASA offers. This chapter guides you through the initial configuration of the security appliance and shows ways to monitor the system's health and status.

Accessing the Cisco ASA Appliances

Cisco ASA provides two types of user interfaces:

- **Command-line interface (CLI)—**The CLI provides non-graphical access to the Cisco ASA. The CLI can be accessed from a console, Telnet, or Secure Shell (SSH) session. Telnet and SSH are discussed later in the chapter, under "Remote System Management."

- **Graphical user interface (GUI) via ASDM—**Cisco Adaptive Security Device Manager (ASDM) provides an easy-to-navigate and simple graphical interface to set up and manage the different features that Cisco Adaptive Security Appliance (ASA) provides. It is bundled with a variety of administration and monitoring tools to check the health of the appliance and the traffic traversing through it. ASDM access requires IP connectivity between the ASDM client and the security appliance. If you have a new security appliance, you can assign the initial IP address via the CLI and then establish a GUI ASDM connection.

Establishing a Console Connection

A new security appliance, by default, has no configuration and thus it does not have IP addresses assigned to any of its interfaces. To access the CLI, you need a successful connection to the console port of the security appliance. The console port is a serial asynchronous port with the settings listed in Table 3-1.

You can connect the console port on the security appliance to a serial port on a PC by using a flat rolled console cable, with a DB9 serial adapter on one end and a RJ-45 port on the other. The DB9 side of the cable goes to the serial port of a PC, and the RJ-45 end of the cable goes to the console port of the security appliance, as illustrated in Figure 3-1.

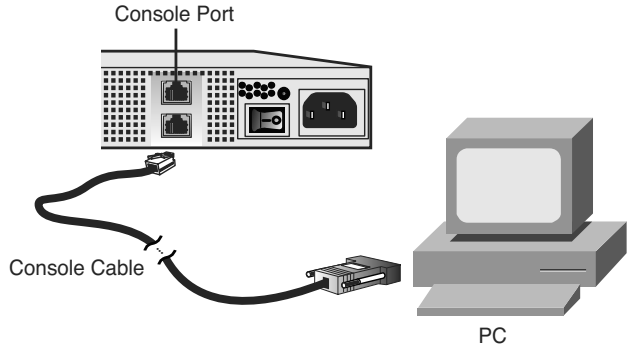


Figure 3-1 *Console Port Connectivity from a Computer*

After connecting the console cable to the security appliance and the computer, launch terminal-emulation software, such as HyperTerminal or TeraTerm, to send and receive output. You can launch HyperTerminal by navigating to **Start > Programs > Accessories > Communications > HyperTerminal** on a Windows-based PC. The initial configuration window of HyperTerminal is shown in Figure 3-2. In the Connection Description dialog box, enter a connection name to identify this session as a unique connection. A connection name of **Console Connection to the Cisco ASA** is specified in Figure 3-2. You can choose an icon to associate with the connection entry. After filling out the connection name and selecting an icon, click **OK** to proceed.

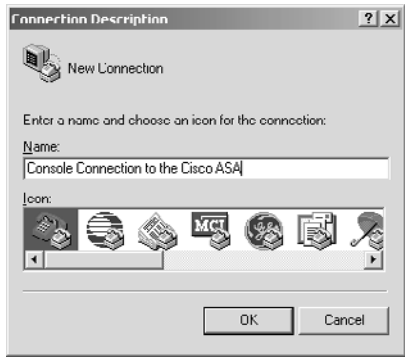


Figure 3-2 *Initial Configuration of HyperTerminal*

Specify the connection type in the Connect To window. Because the console port uses an asynchronous serial connection, the HyperTerminal setting must use a COM port. As illustrated in Figure 3-3, COM3 is being set up for the serial connection to the security appliance. After you are finished, click **OK** to proceed to the next configuration window.

Figure 3-3 *Setting HyperTerminal Connection Type*

Table 3-1 *Console Port Settings*

Parameters	Value
Baud rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware

The last window is used to configure port properties, such as the baud rate and flow control. Figure 3-4 shows HyperTerminal set up with the values listed in Table 3-1. After configuring the port settings, click **OK** to complete the configuration setup.

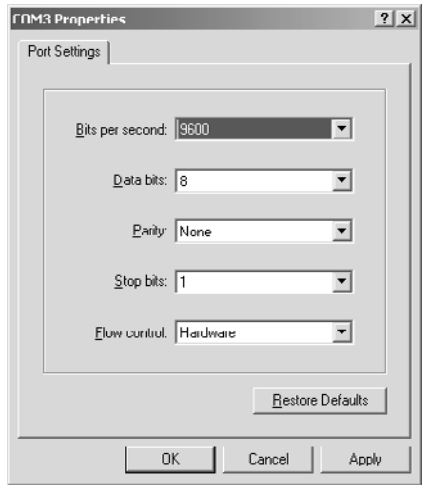


Figure 3-4 *Setting HyperTerminal Port Specification*

The HyperTerminal application is ready to transmit and receive data from the security appliance. If you press **Enter** a couple of times, you should see a **ciscoasa>** prompt in the HyperTerminal window.

The next section describes how to use the CLI after establishing a successful console connection.

Command-Line Interface

After a successful console connection, the security appliance is ready to accept your commands. The Cisco ASA contains a command set structure similar to that of a Cisco IOS router and offers the following access modes:

- User mode, also known as user access mode
- Privileged mode
- Configuration mode
- Sub-configuration mode
- ROMMON mode

User mode, shown as the hostname with a **>** sign, is the first mode of access available when you log in to the security appliance. This mode offers a limited set of commands that

are useful in obtaining basic information about the security appliance. One of the important commands in this mode is **enable**, which prompts a user to specify a password to log in to privileged mode.

Privileged mode, shown as the hostname with a **#** sign, gives full access to a user after a successful logon. This mode also allows execution of all the commands that are available in user mode. The security appliance offers a rich set of monitoring and troubleshooting commands to check the health of different processes and features in the security appliance. One of the important commands in this mode is **configure terminal**, which places a user in configuration mode.

Note The security appliance enables you to restrict the commands a user can run by implementing command authorization. This is covered in Chapter 6, "Authentication, Authorization, and Accounting (AAA) Services."

Configuration mode, displayed as the host name with a **(config)#** prompt, allows a user to enable or disable a feature, set up security and networking components, and tweak the default parameters. This mode not only enables the user to configure the security appliance, but also allows the use of all the commands that are available in the user and privileged modes. A user may enter into the sub-configuration mode of different features from this mode.

Sub-configuration mode, displayed as the hostname with a **(config-*xx*)#** prompt, lets a user configure specific networking or security features on the security appliance. The *xx* is replaced by the process/feature keyword that is being configured on the security appliance. For example, if a user is setting up specific parameters on an interface, the prompt changes to **(config-if)#**. Sub-configuration mode enables the user to execute all the configuration mode commands as well as the user and privileged mode commands.

In Example 3-1, a user logs in to privileged mode from user access mode by typing the **enable** command. The security appliance prompts a user to specify a password to gain privileged mode access. If the security appliance has the default configuration, it uses a null (no) password to grant access. After logging in to privileged mode, the user types **configure terminal** to access configuration mode. The user enters into interface sub-configuration mode by typing the **interface GigabitEthernet0/0** command. To go back to the previous mode, the user can enter **exit** or **quit**, as shown in Example 3-1.

Example 3-1 *Accessing the Privileged and Configuration Modes*

```
ciscoasa> enable
Password: <cr>
ciscoasa# configure terminal
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# exit
ciscoasa(config)# exit
ciscoasa#
```

Tip In the preceding example, the administrator of the security appliance typed **exit** twice to return to the privileged mode prompt. Optionally, you can type **end** to return to privileged mode from any configuration mode.

Like a Cisco IOS router, the security appliance also allows you to press the Tab key to complete a partial command. For example, to enter a **show** command, type **sho** and press the Tab key. The security appliance displays the complete **show** command on the screen.

The security appliance allows you to abbreviate commands and keywords to the number of characters that identify a distinct abbreviation. For example, you can abbreviate the **enable** command as **en**.

All the supported options and arguments of a command are displayed when you type **?** after the command. For example, you can type **show ?** to see all the options that are supported under the **show** command.

The security appliance also provides a brief description and command syntax when you type **help** followed by the command. For example, when you type **help reload**, the security appliance shows the command syntax for **reload**, a description, and the supported arguments.

The security appliance uses *ROMMON mode* (*Read-Only-Memory Monitor mode*) when it does not find a bootable image or when an administrator forces it to enter into that mode. In ROMMON mode, you can use a TFTP server to load a system image into the security appliance. ROMMON mode is also used to recover the system password, discussed later in this chapter under "Image Recovery Using ROMMON."

Managing Licenses

As mentioned in Chapter 2, "Cisco ASA Product and Solution Overview," the security appliance controls the security and networking features through the use of a license key. You can obtain the information of the currently installed license key by issuing the **show version** command. This command also displays other system information, such as:

- The current version and the location of the system image
- The ASDM version, if installed
- The security appliance uptime
- The security appliance hardware model number, including the memory and flash information
- The physical interface and the associated IRQs (Interrupt Requests)
- The current features that are active on the security appliance
- The license information

- The security appliance's serial number
- Configuration register setting
- Information about last configuration modification

Example 3-2 shows the output of **show version**, which has a VPN Plus–based license key installed.

Example 3-2 *Output of show version*

```
Chicago> show version
Cisco Adaptive Security Appliance Software Version 8.2(1)
Device Manager Version 6.2(1)

Compiled on Tue 05-May-09 22:45 by builders
System image file is "disk0:/asa821-k8.bin"
Config file at boot was "startup-config"

Chicago up 31 days 4 hours

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 64MB
BIOS Flash M50FW016 @ 0xffe00000, 2048KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                              Boot microcode    : &#x263B;CN1000-MC-BOOT-2.00
                              SSL/IKE microcode: ♥CNLite-MC-SSLm-PLUS-2.03
                             IPSec microcode   : &#x263A;CNlite-MC-IPSECm-MAIN-2.04
 0: Ext: GigabitEthernet0/0  : address is 000f.f775.4b54, irq 9
 1: Ext: GigabitEthernet0/1  : address is 000f.f775.4b55, irq 9
 2: Ext: GigabitEthernet0/2  : address is 000f.f775.4b56, irq 9
 3: Ext: GigabitEthernet0/3  : address is 000f.f775.4b57, irq 9
 4: Ext: Management0/0       : address is 000f.f775.4b53, irq 11
 5: Int: Internal-Data0/0    : address is 0000.0001.0002, irq 11
 6: Int: Internal-Control0/0 : address is 0000.0001.0001, irq 5

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 150
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 10
GTP/GPRS                     : Enabled
```

```
SSL VPN Peers                  : 2
Total VPN Peers                : 750
Shared License                 : Disabled
AnyConnect for Mobile          : Disabled
AnyConnect for Linksys phone : Disabled
AnyConnect Essentials          : Disabled
Advanced Endpoint Assessment : Disabled
UC Phone Proxy Sessions        : 2
Total UC Proxy Sessions        : 2
Botnet Traffic Filter          : Disabled

This platform has an ASA 5520 VPN Plus license.

Serial Number: JAB00000001
Running Activation Key: 0x00000001 0x00000001 0x00000001 0x00000001 0x00000001
Configuration register is 0x1
Configuration last modified by cisco at 20:45:09.870 UTC Mon Jul 20 2009
```

In Example 3-2, the security appliance is running a system image of 8.2(1) with the ASDM image of 6.2(1). The hardware model is ASA5520, running the Plus license. The serial number and the license activation key are masked to protect this system's identity. The configuration register is set to 0x1, which instructs the security appliance to load the image from flash. The configuration register is discussed later in the "Password Recovery Process" section.

You can change the installed license key by using the **activation-key** command followed by the five-tuple key, as shown in Example 3-3. After the new activation key is entered, the security appliance shows the features set activated by the new license key. In this example, a VPN premium license key is installed.

Example 3-3 *Changing the Activation Key*

```
Chicago# activation-key 0x11223344 0x55667788 0x9900aabb 0xccddeeff 0x01234567

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs                : 100
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 50
GTP/GPRS                     : Disabled
VPN Peers                    : 5000
This machine has a VPN Premium license.
```

```
Both running and flash activation keys were updated with the requested key.
```

Note Feature-specific activation keys are discussed in their respective chapters. For example, Chapter 19 discusses the license model for SSL VPN tunnels.

Initial Setup

If you are setting up a new security appliance, it must be configured from the CLI first. You cannot use ASDM until the security appliance is configured with the appropriate IP addresses and it has IP connectivity to ASDM client machine.

Initial Setup via CLI

When the security appliance is booted with no configuration, it offers a setup menu that enables you to configure the initial parameters such as the device name and the IP address. You can choose to go through the initial setup menu for quick configuration.

In Example 3-4, a security appliance prompts users to specify whether they wish to go through the interactive menu to preconfigure the device. If a user types **no**, the interactive menu is not shown and the security appliance shows the **ciscoasa>** prompt. If a user types **yes**, the default option, the security appliance walks the user through the configuration of ten parameters. The security appliance shows the default values in brackets ([]) before prompting the user to accept or change them. To accept the default input, press Enter. After going through the initial setup menu, the security appliance displays the summary of the new configuration before prompting the user to accept or reject it.

Example 3-4 *Initial Setup Menu*

```
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]:
Enable password [<use current password>]: C1$c0123
Allow password recovery [yes]?
Clock (UTC):
  Year [2009]:
  Month [Jul]: Nov
  Day [21]:
  Time [01:08:57]: 21:27:00
Inside IP address: 192.168.10.1
Inside network mask: 255.255.255.0
Host name: Chicago
Domain name: securemeinc.com
IP address of host running Device Manager: 192.168.10.77
```

```
The following configuration will be used:
Enable password: cisco123
Allow password recovery: yes
Clock (UTC): 21:27:00 Nov 21 2009
Firewall Mode: Routed
Inside IP address: 192.168.10.1
Inside network mask: 255.255.255.0
Host name: Chicago
Domain name: securemeinc.com
IP address of host running Device Manager: 192.168.10.77

Use this configuration and write to flash? yes
INFO: Security level for "inside" set to 100 by default.
WARNING: http server is not yet enabled to allow ASDM access.
Cryptochecksum: e15ea3e4 a499e6cf e84f5b82 1994bde0

1809 bytes copied in 3.490 secs (621 bytes/sec)
Type help or '?' for a list of available commands.
Chicago>
```

Table 3-2 lists all the parameters that can be configured in the initial setup menu. It also provides a brief description of each parameter, along with the default and configured values.

You can define the initial parameters and features by using either the CLI commands or the ASDM. They are discussed throughout this chapter. The next section discusses how to configure a device name from the ASDM.

Tip You can rerun the interactive setup process by using the **setup** command in configuration mode.

Initial Setup of ASDM

Before you can access the ASDM graphical console, you must install the ASDM software image on the local flash of the security appliance. The ASDM console can manage a local security appliance only. Therefore, if you need to manage multiple security appliances, the ASDM software must be installed on all the Cisco ASAs. However, a single workstation can launch multiple instances of ASDM clients to manage the different appliances. Optionally, you can leverage Cisco Security Manager (CSM) to configure multiple appliances simultaneously.

Table 3-2 *Initial Setup Parameters and Their Values*

Parameter	Description	Default Value	Configured Value
Enable password	Specifies the enable password	None	**C1$c0123**
Firewall mode	Sets up the security appliance as a Layer 2 (Transparent) or Layer 3 (Routed) firewall	Routed	**Routed**
Inside IP address	Specifies the IP address on the inside interface	None	**192.168.10.1**
Inside subnet mask	Specifies the subnet mask on the inside interface	None	**255.255.255.0**
Host name	Sets the hostname on the device	ciscoasa	**Chicago**
Domain name	Sets the domain name on the device	None	**securemeinc.com**
IP address of host running Device Manager	Specifies the IP address of the host machine responsible for managing the Cisco ASA	None	**192.168.10.77**
Clock	Sets up the current time on the Cisco ASA	varies	**9:27 PM November 21st 2009**
Save configuration	Prompts the user if configuration needs to be saved	Yes	**Yes**
Allow password recovery	Prompts the user if password recovery is allowed	Yes	**Yes**

Note This book focuses on setting up Cisco ASA through ASDM and the CLI. Configuring ASA through CSM is beyond the scope of this book.

Uploading ASDM

You can use the **dir** command to determine whether the ASDM software is installed. If the security appliance does not have the ASDM software, your first step is to upload the image from an external file server, using the one of the supported protocols. The appliance needs to be set up for basic configuration, such as the interface names, security levels, IP addresses, and proper routes, discussed later in this chapter. After setting up basic information, use the **copy** command to transfer the image file, as shown in Example 3-5, where an ASDM file, named **asdm-621.bin**, is being copied from a TFTP server located at

192.168.10.10. Verify the content of the local flash after the file is successfully uploaded. Copying images is discussed later in this chapter.

Example 3-5 *Uploading the ASDM Image to the Local Flash*

```
Chicago# copy tftp flash
Address or name of remote host []? 192.168.10.10
Source filename []? asdm-621.bin
Destination filename [asdm-621.bin]? asdm-621.bin

Accessing tftp://192.168.10.10/asdm-621.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Output omitted for brevity.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/asdm-621.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Output omitted for brevity.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
6889764 bytes copied in 161.420 secs (36500 bytes/sec)
Chicago# dir
Directory of disk0:/
1260    -rw-  14524416     16:47:34 May 13 2009  asa821-k8.bin
2511    -rw-  6889764      17:38:14 May 13 2009  asdm-621.bin

62881792 bytes total (46723072 bytes free)
```

Setting Up the Appliance

When the ASDM file is accessed, the Cisco ASA loads the first ASDM image that it finds from the local flash. If multiple ASDM images exist in the flash, use the **asdm image** command and specify the location of the ASDM image you want to load. This ensures that the appliance always loads the specified image when ASDM is launched. In Example 3-6, the appliance is set up to use **asdm-621.bin** as the ASDM image file.

Example 3-6 *Specifying the ASDM Location*

```
Chicago(config)# asdm image disk0:/asdm-621.bin
```

The security appliance uses the Secure Socket Layer (SSL) protocol to communicate with the client. Consequently, the security appliance acts as a web server to process the requests from the clients. You must enable the web server on the appliance by using the **http server enable** command.

The security appliance discards the incoming requests until the ASDM client's IP address is in the trusted network to access the HTTP engine. In Example 3-7, the administrator enables the HTTP engine and sets up the appliance to trust the **192.168.10.0/24** network connected toward the **inside** interface.

Example 3-7 *Enabling the HTTP Server*

```
Chicago(config)# http server enable
Chicago(config)# http 192.168.10.0 255.255.255.0 inside
```

Note The SSL VPN implementation on the appliance also requires you to run the HTTP server on the appliance. Starting from version 8.0, you can set up the security appliance to terminate both the SSL VPN as well as the ASDM sessions on the same interface, using the default port of 443. Use https://<ASAipaddress>/admin to access the GUI for admin and management purposes. This is discussed in Chapter 19.

Accessing ASDM

ASDM's interface can be accessed from any workstation whose IP address is in the trusted network list. Before you establish the secure connection to the appliance, verify that IP connectivity exists between the workstation and the Cisco ASA.

To establish an SSL connection, launch a browser and point the URL to the appliance's IP address. In Figure 3-5, the administrator accesses ASDM by entering **https://192.168.10.1/admin** as the URL. The URL is redirected to https://192.168.10.1/admin/public/index.html.

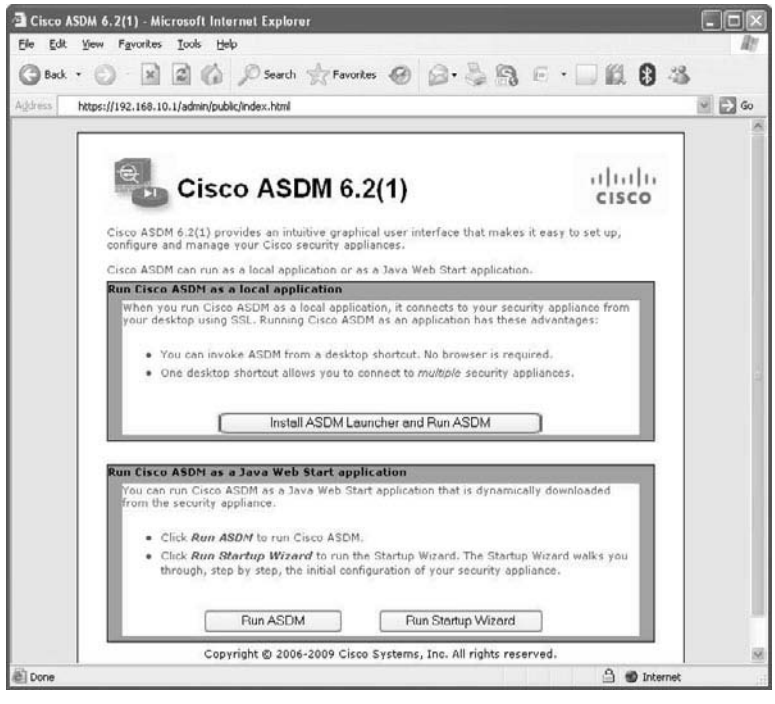


Figure 3-5 *Accessing the ASDM URL*

Note ASDM requires Sun Java plug-in 1.4(2), 1.5.0, or 6.0 installed on the web browser. The supported operating systems include Microsoft Windows Vista, 2003 Server, XP, 2000 Service Pack 4, Macintosh OS X, Red Hat Desktop, and Enterprise version 4.

The new security appliance presents its self-signed certificate to the workstation so that a secure connection can be established. If the certificate is accepted, the security appliance prompts the user to present authentication credentials. If the ASDM authentication or enable password is not set up, there is no default username or password. If enable password is defined, there is no default username and you must use enable password as the login password. If user authentication is enabled on the security appliance through use of the **aaa authentication http console** command, then those login credentials must be provided. After a successful user authentication, the appliance presents two ways to launch ASDM:

- **Run ASDM as Java web start application—**The security appliance launches ASDM in the client's browser as a Java applet. This option is not feasible if a firewall that filters out Java applets exists between the client and the security appliance.
- **Run ASDM as a local application—**The security appliance offers a setup utility called asdm-launcher.msi, which can be saved to the workstation's local hard drive.

Note ASDM as a local application feature is currently supported on Windows-based operating systems.

When the ASDM application is launched, it prompts for the IP address of the security appliance to which you are trying to connect, as well as the user authentication credentials. Figure 3-6 illustrates this, where an SSL connection is being made to an appliance located at 192.168.10.1. If you have an enable password configured, specify it under Password and leave the Username blank to log in to ASDM.

Figure 3-6 *Launching ASDM*

Note If you are running version 8.2(1) on the security appliance, make sure that you use version 6.2(1) of ASDM. For more information about ASDM, consult http://www.cisco.com/go/asdm.

If the user authentication is successful, ASDM checks the current version of the installer application and downloads a new copy if necessary. It loads the current configuration from the security appliance and displays it in the GUI, as shown in Figure 3-7.

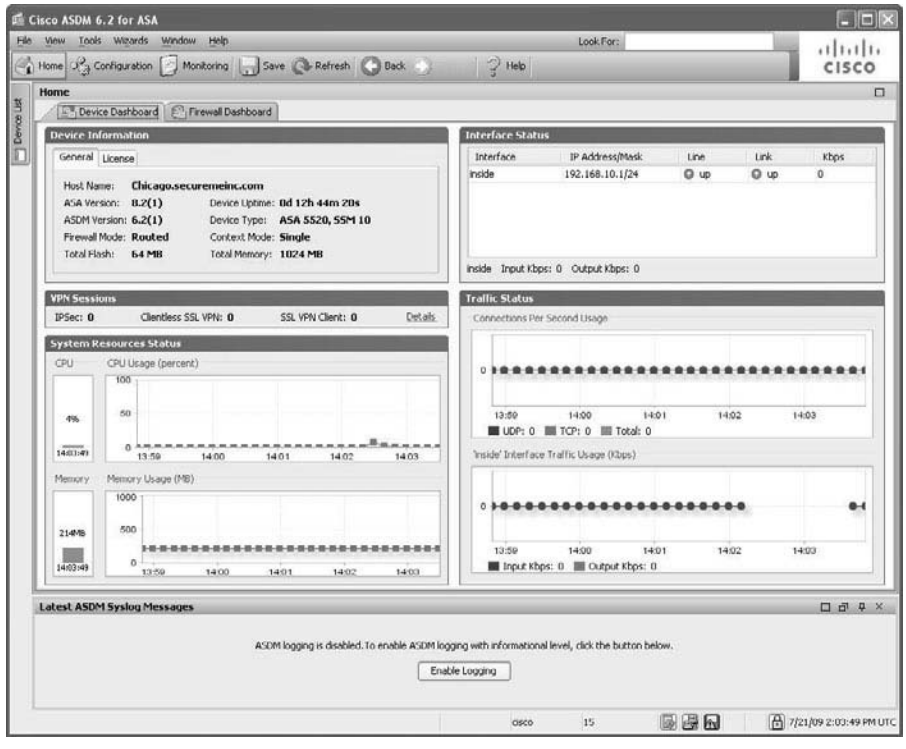


Figure 3-7 *Initial ASDM Screen*

Tip ASDM logs debug and error messages into a file to troubleshoot any application-related issues. The name of the file is asdm-log-[timestamp].txt, and it is located at *user_home_directory*\.asdm\log. For example, C:\Documents and Settings\user\.asdm\log.

ASDM divides the initial screen, also known as the Home screen, into the following six sections:

- **Device Information—**Displays the hardware and software information of the security appliance, such as the current version of operating system and the device type. If

the License tab is selected, ASDM shows the features that are enabled on the security appliance.

- **VPN Sessions—**Displays the number of active IPSec, clientless, and AnyConnect SSL VPN tunnels
- **System Resources Status—** Provides the current status of CPU and memory usage on the appliance.
- **Interface Status—**Displays the interface name and the assigned IP address. It also shows the link information of the currently configured interfaces and the rate of traffic passing through them.
- **Traffic Status—**Provides information about the number of active TCP and UDP connections and the traffic rate passing through the outside interface.
- **Latest ASDM Syslog Messages—**Shows the latest ASDM syslog messages that are generated by the security appliance. Syslogging is disabled by default and needs to be enabled for log monitoring. When enabled, the security appliance sends the messages to the ASDM client. This is discussed later in the chapter, in the "System Logging" section.

The statistics on the Home screen are refreshed every 10 seconds and show the information for the last 5 minutes.

ASDM shows three additional tabs on the home screen. They include

- **Firewall Dashboard Tab—**The Firewall Dashboard tab presents statistical information about the traffic passing through your security appliance. This includes the number of connections, NAT translations, dropped packets, attacks, and top usage statistics.
- **Content Security Tab—**The Content Security tab displays information about the Content Security and Control (CSC) SSM. This pane appears only if a CSC SSM is installed in the adaptive security appliance.
- **IPS Tab—**The Intrusion Prevention System tab displays information about the IPS module, if present.

Functional Screens of ASDM

In addition to the Home screen, the ASDM interface comes with the following two functional screens:

- Configuration screen
- Monitoring screen

Configuration Screen

The Configuration screen is useful when the new or existing configuration needs to be modified. On the left side, it contains five to six features icons, depending on the hardware setup of the appliance, as shown in Figure 3-8.

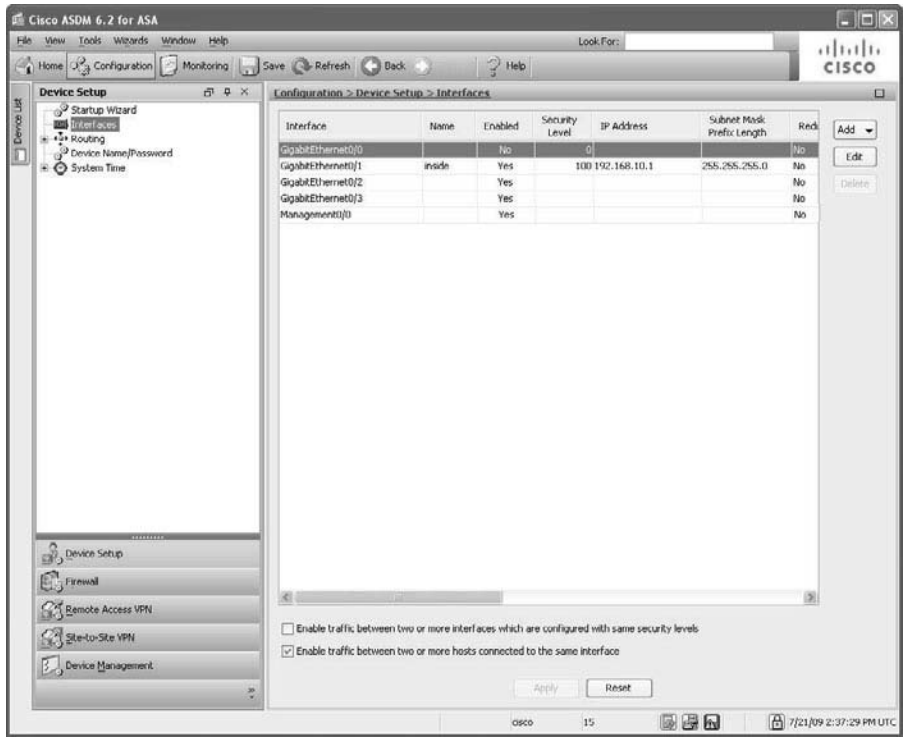


Figure 3-8 *Configuration Screen*

The Feature icons of the Configuration screen are as follows:

- **Device Setup—**Configures interfaces and sub-interfaces on the security appliance. This panel is discussed in the section "Configuring an Interface," later in the chapter.
- **Firewall—**Helpful in creating security policies to filter and to translate packets traversing through the appliance. Also enables you to define Failover, QoS, AAA, certificates, and many other firewall-related features.
- **Remote Access VPN—**Sets up the remote access VPN connections such as IPSec, L2TP over IPSec, Clientless SSL VPN, and AnyConnect tunnels.
- **Site-to-site VPN—**Sets up the site-to-site VPN tunnels.
- **IPS—**Sets up policies for the SSM card to monitor and drop unauthorized packets. This icon is not visible if an SSM card is not present.
- **Device Management—**Here, the basic device features can be set up. Most of these features are discussed later in this chapter. Helpful in setting up the basic software features, such as system logging and failover.

Monitoring Screen

The Monitoring screen displays statistics about the hardware and software features of the security appliance. ASDM provides real-time graphs to monitor the appliance's health and status. Figure 3-9 shows the initial Monitoring screen.

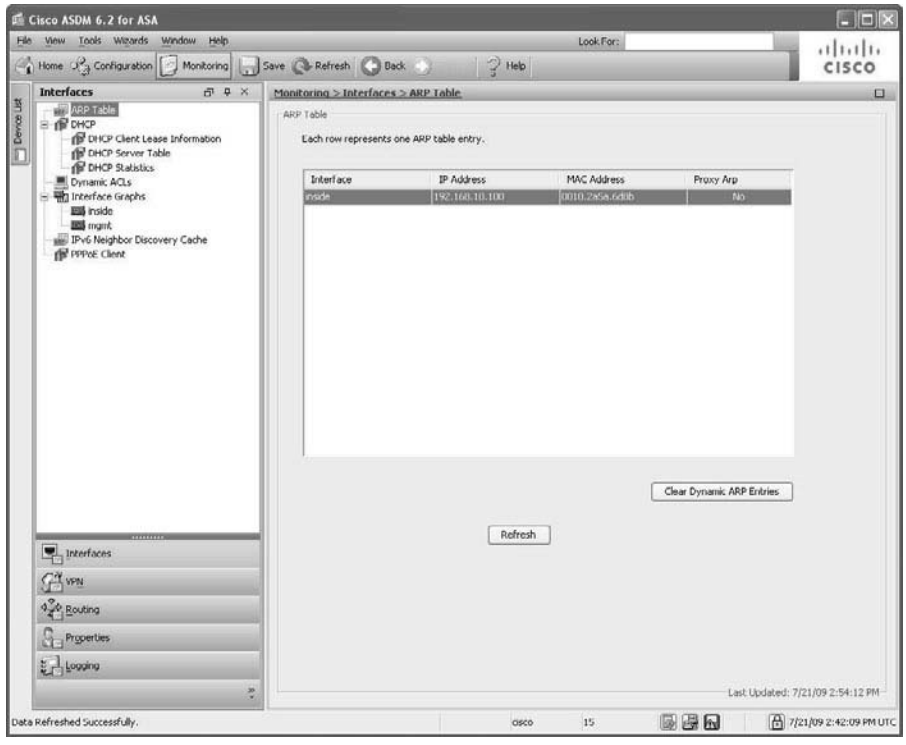


Figure 3-9 *Monitoring Screen*

Similar to the Configuration screen, the Monitoring screen also displays five or six icons, depending on whether or not you have the SSM module installed.

The Features icons of the Monitoring screen are described below:

- **Interfaces—**Monitors interfaces and sub-interfaces by maintaining ARP, DHCP, and dynamic ACLs tables. It also provides a graphical representation of interface utilization and packet throughput.
- **VPN—**Monitors the active VPN connections on the security appliance. It provides graphs and statistical analysis of the site-to-site, IPSec, and SSL VPN–based remote-access tunnels.
- **IPS—**Provides statistical information for the packets going through the IPS engine. This icon is not present if the IPS module is not installed.

- **Routing—**Displays the current routing table and provides information on EIGRP and OSPF neighbors.
- **Properties—**Monitors active administrative sessions such as Telnet, SSH, and ASDM. It also provides graphical information about CPU, memory, and blocks utilization. Provides graphical information about the active translations and UDP/TCP connections. It provides graphical information of the IP audit, WCCP, CRL, and DNS Cache features
- **Logging—**Displays log messages as live events. It also shows log messages from the buffer space.
- **Trend Micro Content Security—**ASDM enables you to monitor the CSC SSM statistics, as well as CSC SSM-related features such as types of threats detected by the module, live event logs for real-time monitoring, and resource utilization graphs.

Note If you use ASDM as the primary mode of configuring a security appliance, it is highly recommended that you enable the Preview Command Before Sending Them to the Device option in ASDM. This way, before the commands are pushed to the ASA, ASDM shows them to you for verification. You can enable this feature on ASDM under **Tools > Preferences** and selecting **Preview commands before sending them to the device.**

Device Setup

After you have connectivity to the security appliance, either via CLI or ASDM, you are ready to start configuring the device. This section guides you to configure the security appliance for basic setup.

Setting Up Device Name and Passwords

The default device name—also known as the hostname—of a security appliance is **ciscoasa**. It is highly recommended that you set a unique device name to identify the security appliance on the network. Additionally, networking devices usually belong to a network domain. A domain name appends the unqualified hostnames with the configured domain name. For example, if the security appliance tries to reach a host, **secweb**, by its hostname and the configured domain name on the security appliance is **securemeinc.com**, then the fully qualified domain name (FQDN) will be **secweb.securemeinc.com**.

In a new security appliance, you can configure the Telnet and enable password. The Telnet password is used to authenticate remote sessions either via the Telnet or SSH protocol, discussed later in this chapter. By default, the Telnet password is **cisco**. For the SSH sessions, the default username is **pix**. The enable password, on the other hand, gives you access to the privileged exec mode if you are on the user mode. The enable password is also used for ASDM user authentication. There is no enable password by default.

Note If you have user authentication configured for Telnet and/or SSH access, the security appliance does not use the Telnet/enable passwords for those sessions.

To configure the hostname, domain name, and the Telnet/enable passwords via ASDM, navigate to **Configuration > Device Setup > Device Name/Password** and specify the new settings. As shown in Figure 3-10, the hostname is **Chicago** and the domain name is **securemeinc.com**. If you want to configure a new Telnet and/or enable password, select the appropriate change the Telnet and/or enable password option and specify the current and the new passwords. In Figure 3-10, both passwords are set to **C1$c0123** (masked).

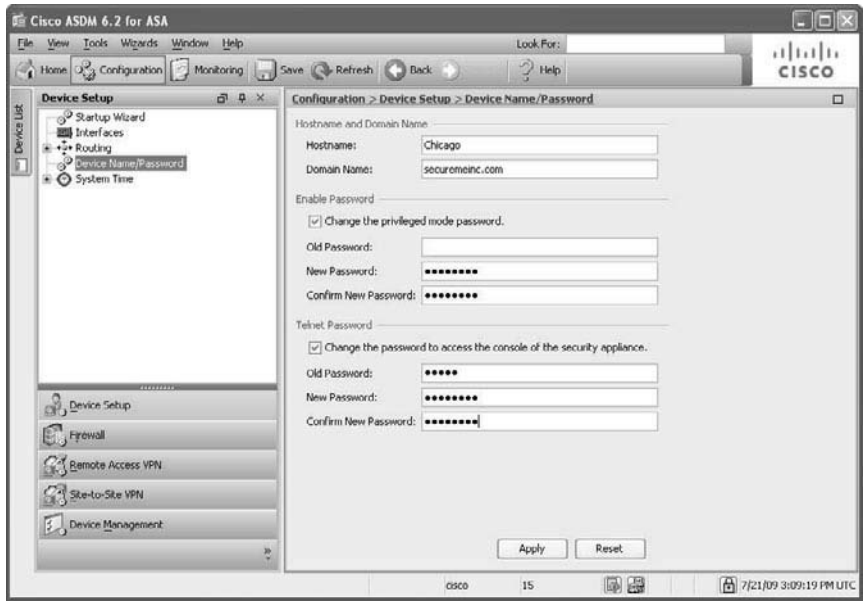


Figure 3-10 *Configuring Hostname, Domain Name, and Local Passwords*

If you prefer to use the CLI, Example 3-8 shows the identical configuration of Figure 3-10. The hostname is changed using the **hostname** command, the domain name is changed using the **domain-name** command, and the Telnet and enable passwords are changed using the **passwd** and **enable password** commands, respectively.

Example 3-8 *Setting Up the Hostname, Domain Name, and Passwords*

```
ciscoasa# configure terminal
ciscoasa(config)# hostname Chicago
Chicago(config)# domain-name securemeinc.com
Chicago(config)# passwd C1$c0123
Chicago(config)# enable password C1$c0123
```

Index

SYMBOLS

A

B

C

D

E

F

G

H

I

J - K

L

M

N

O

P

Q

R

S

T

U

V

W

X - Y - Z