DATA SHEET

CISCO ADAPTIVE SECURITY DEVICE MANAGER VERSION 5.0

Cisco® Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring through an intuitive, easy-to-use Web-based management interface. Bundled with Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX® Security Appliances, Cisco ASDM accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced integrated security and networking features offered by the market-leading suite of Cisco security appliances. Its secure, Web-based design enables anytime, anywhere access to Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances.

INTEGRATED MANAGEMENT SOLUTION PROVIDES FLEXIBLE ACCESS OPTIONS

Cisco Adaptive Security Device Manager (ASDM) can be accessed directly with a Web browser from any Java plug-in enabled computer on the network, providing security administrators with rapid, secure access to their Cisco ASA 5500 Series Adaptive Security Appliances or Cisco PIX Security Appliances. It provides a unique option for administrators---a new Microsoft Windows-based launcher application can be downloaded directly from the security appliance to a management computer. This application accelerates the startup of Cisco ASDM, providing increased efficiency in managing security appliances. By running separate instances of the Cisco ASDM launcher application, administrators can connect to multiple security appliances from the convenience of a single management workstation, thus simplifying management in small business environments.

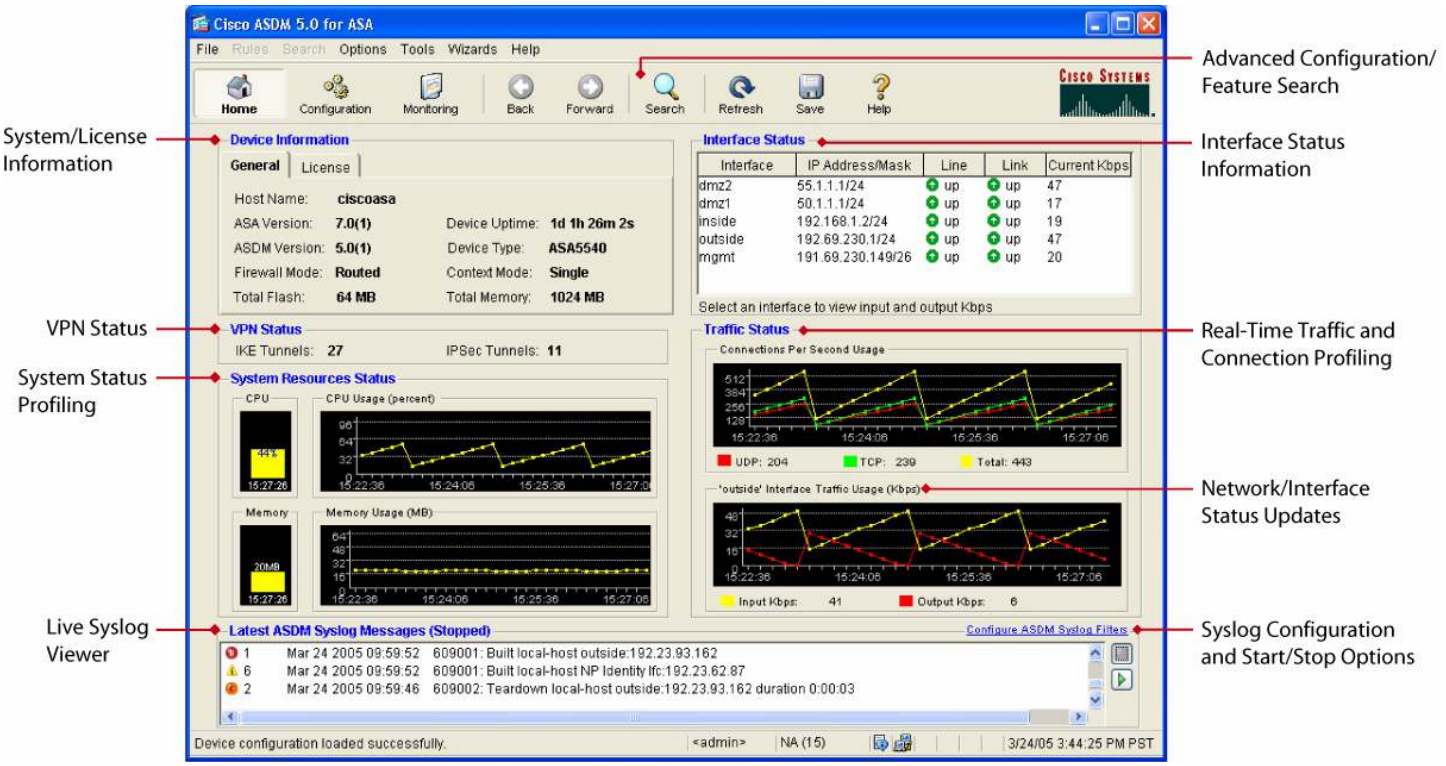
STARTUP WIZARD ACCELERATES SECURITY APPLIANCE DEPLOYMENT

Cisco ASDM features a Startup Wizard that helps accelerate the security appliance deployment process. A series of simple step-by-step configuration panels help administrators get their appliances up and running quickly and create a robust configuration that allows traffic to flow securely through their networks. The Startup Wizard provides the ability to configure optional features such as Dynamic Host Control Protocol (DHCP) server settings, Network Address Translation (NAT), administrative access, and Auto Update, a revolutionary secure remote-management capability that helps keep appliance configurations and software images up-to-date.

DASHBOARD SUPPLIES ADMINISTRATORS WITH VITAL REAL-TIME SYSTEM STATUS INFORMATION

Cisco ASDM 5.0 includes a dynamic dashboard that provides a complete system overview and device health statistics at a glance (Figure 1). It can automatically detect the Cisco security appliances being configured; for each, it will display the software version, license information, and important statistics. In complex network environments, it presents administrators with real-time status indicators and provides a launching point to powerful analysis tools and advanced monitoring capabilities---including a real-time syslog viewer, with pattern-matching capabilities to filter syslogs based on network addresses, port numbers, host names, and more. This release introduces a powerful search engine that helps administrators locate where specific features can be configured, and provides convenient point-and-click access to the search results.

Figure 1. Cisco ASDM Homepage



ROBUST SECURITY POLICY MANAGEMENT LOWERS OPERATIONAL COSTS

Cisco ASDM Version 5.0 features powerful management services that simplify security policy definition and ongoing policy maintenance by giving security administrators the ability to create reusable network and service object groups and inspection policy maps that can be referenced by multiple security policies. It also supports the wide range of access control features offered by both Cisco ASA Software Version 7.0 and Cisco PIX Security Appliance Software Version 7.0, such as user- and group-based access lists, time-based access lists, and inbound/outbound access lists. Cisco ASDM Version 5.0 also supports the new Modular Policy Framework supported in both these software versions. This powerful, highly flexible framework allows administrators to identify a network flow or a traffic class based on different conditions, and then apply a set of customizable inspection services, Quality of Service (QoS) services, and connection services to each flow or traffic class. These advanced access control and application inspection capabilities, coupled with easy-to-use ongoing policy management services, help to ensure a robust and dynamic security profile for businesses of all sizes.

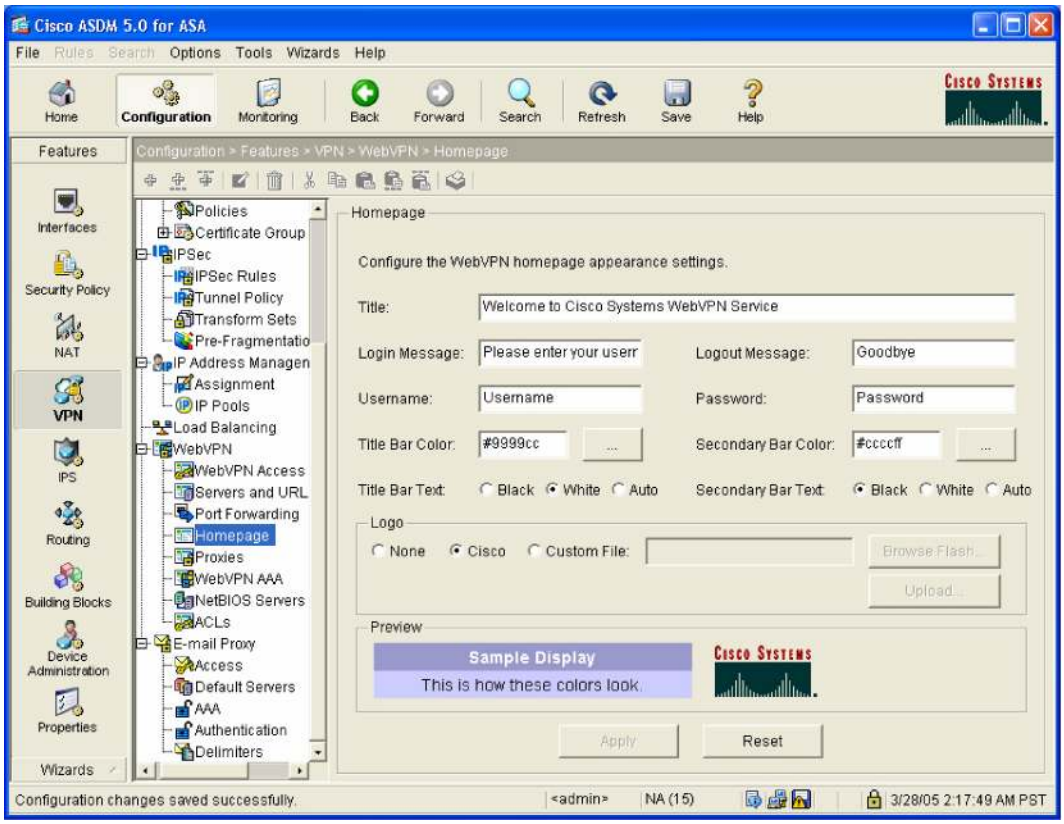
BUSINESS-CLASS SECURITY SERVICES ENFORCE SECURE, ROLE-BASED ADMINISTRATIVE ACCESS

Cisco ASDM Version 5.0 integrates an array of robust security services to prevent unauthorized administrative access to a device. It supports a wide range of methods for authenticating administrators, including a local authentication database on a Cisco ASA 5500 Series Adaptive Security Appliance or a Cisco PIX Security Appliance, or via a RADIUS/TACACS server. All communications between Cisco ASDM (running on an administrator's computer) and the security appliance are encrypted using Secure Sockets Layer (SSL) with either 56-bit Data Encryption Standard (DES) or the more secure 168-bit Triple DES (3DES) algorithm. Cisco ASDM supports up to 16 levels of customizable administrative access that grant administrators and operations personnel the appropriate level of permissions for every Cisco security appliance they manage (for example, monitoring-only, read-only access to the configuration).

RICH VPN MANAGEMENT EXTENDS SECURE CONNECTIVITY TO BUSINESS PARTNERS AND REMOTE SITES

Cisco ASDM Version 5.0 features comprehensive VPN configuration capabilities, including an intelligent VPN wizard for simplified provisioning, which allows businesses to establish Internet Key Exchange (IKE) and IP Security (IPSec) policies for site-to-site VPN deployments. Cisco ASDM also delivers full-featured management for Cisco Easy VPN remote-access VPN concentrator services, supporting features ranging from VPN client security posture enforcement, automatic software updating, VPN clustering, and more. On the Cisco ASA 5500 Series, Cisco ASDM integrates comprehensive Cisco WebVPN management features (Figure 2) to allow administrators to quickly provision and enable remote-access connectivity from any Internet-enabled Web browser and its native SSL encryption. Cisco ASDM also delivers advanced VPN monitoring capabilities, providing administrators insight with numerous statistics and graphs showing metrics such as session uptimes, data transferred per session, and more.

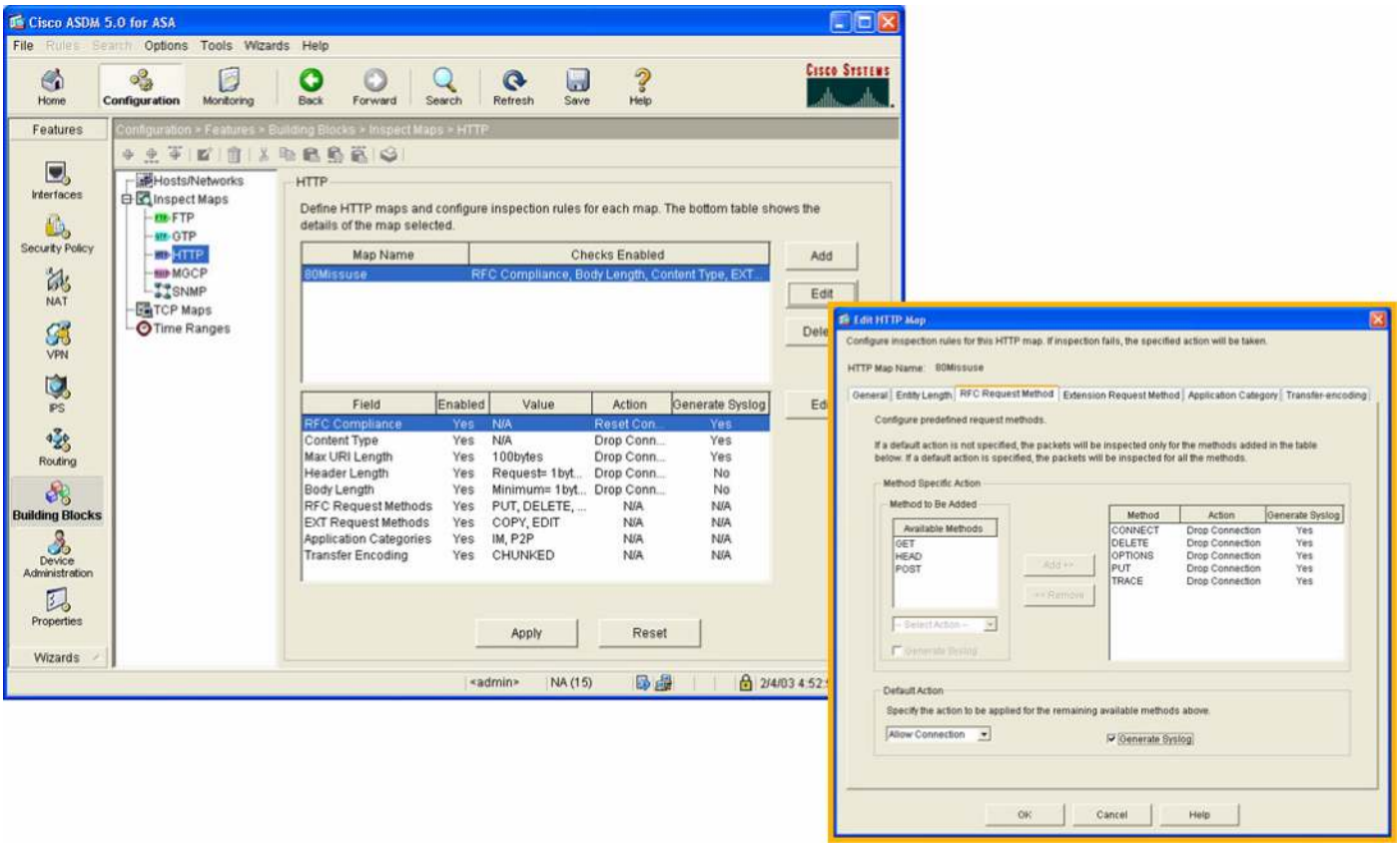
Figure 2. WebVPN Configuration



COMPREHENSIVE MANAGEMENT SERVICES COMPLEMENT ADVANCED APPLICATION INSPECTION

Cisco Adaptive Security Appliance Software Version 7.0 and Cisco PIX Security Appliance Software Version 7.0 includes more than 30 dedicated inspection engines for a range of modern applications driven by protocols such as Hyper Text Transfer Protocol (HTTP) (Figure 3), File Transfer Protocol (FTP), GPRS Tunneling Protocol (GTP), Sun Remote Procedure Call (SunRPC), H.323, and Session Initiation Protocol (SIP). Cisco ASDM Version 5.0 enables point-and-click capabilities conditioned by intelligent application defaults to quickly establish robust security profiles that protect mission-critical applications and resources from misuse and tunneling attacks. It enforces flow-based control in defining inspection services and gives administrators enterprise-class tools to exercise microscopic control over applications.

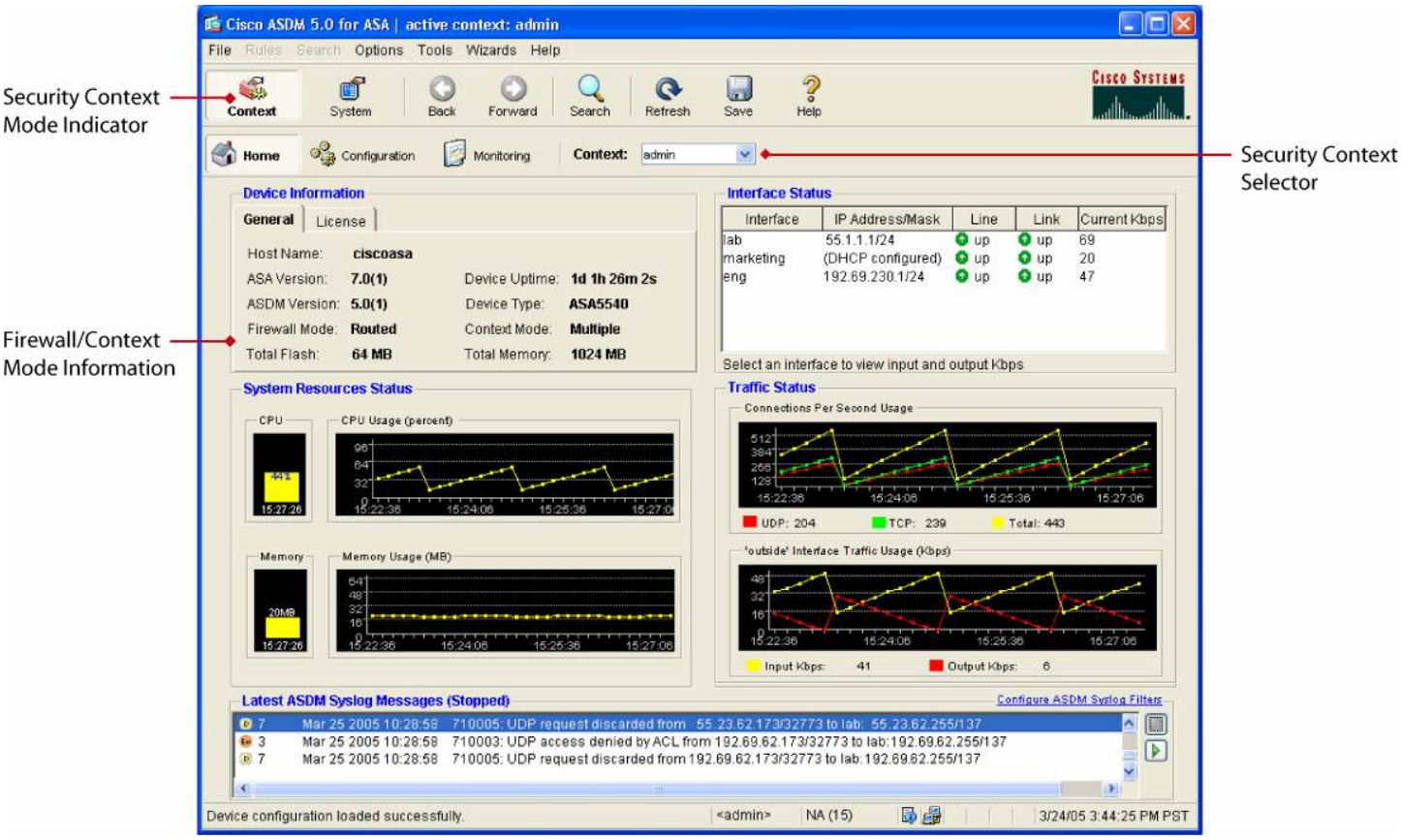
Figure 3. Advanced HTTP Inspection Services Configuration



INTELLIGENT USER INTERFACE SIMPLIFIES INTEGRATION INTO COMPLEX NETWORK ENVIRONMENTS

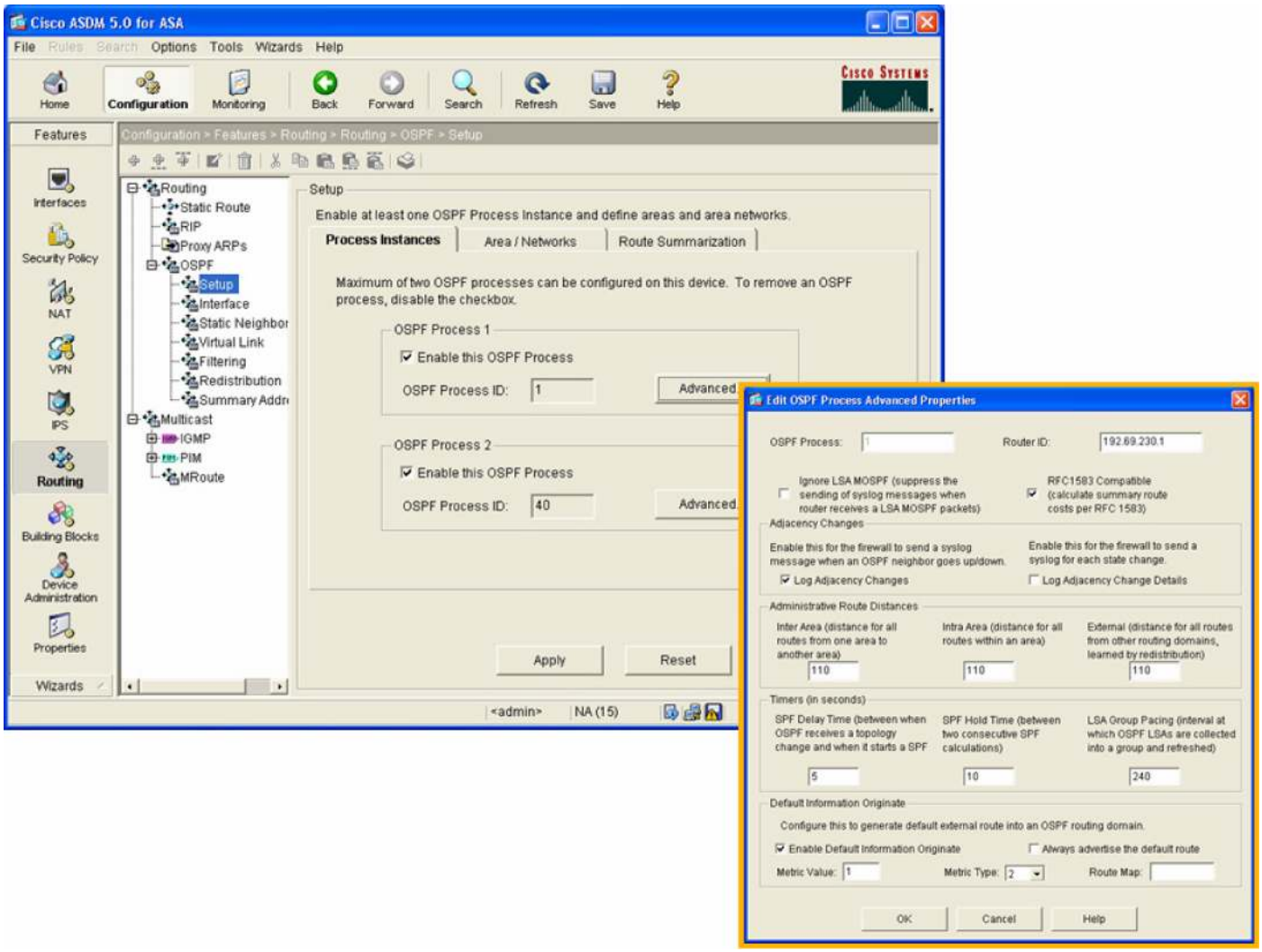
Cisco ASDM Version 5.0 provides easy and convenient access to managing the rich network integration features found in Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances. Virtualization allows the creation of multiple security contexts (virtual firewalls) within a single security appliance, with each context having its own set of security policies, logical interfaces, and administrative domain. Cisco ASDM uses an intelligent virtualization management system to provide unrestricted access for central system administrators who desire complete visibility into all virtual firewalls and features on the system (Figure 4). Individual context users get the same look and feel of Cisco ASDM, as well as the same rich management and monitoring capabilities. However, configuration and feature access are restricted only to the assigned context, and as specified by the central system administrators. Individual context users can build upon the administrator-created security policies to create a customized configuration for their virtual firewalls using Cisco ASDM.

Figure 4. System Administrator View of Security Contexts



Cisco ASDM gives administrators complete control over multicast routing protocols such as Protocol Independent Multicast (PIM), Open Shortest Path First (OSPF) dynamic routing (Figure 5), IEEE 802.1q-based VLAN interfaces, and Quality of Service (QoS) mechanisms. For novice users, it combines intelligent defaults and detailed online help to simplify configuration of these networking services. Advanced users can take full advantage of the depth of feature support to integrate Cisco security appliances into complex routing and switching environments.

Figure 5. Advanced OSPF Configuration

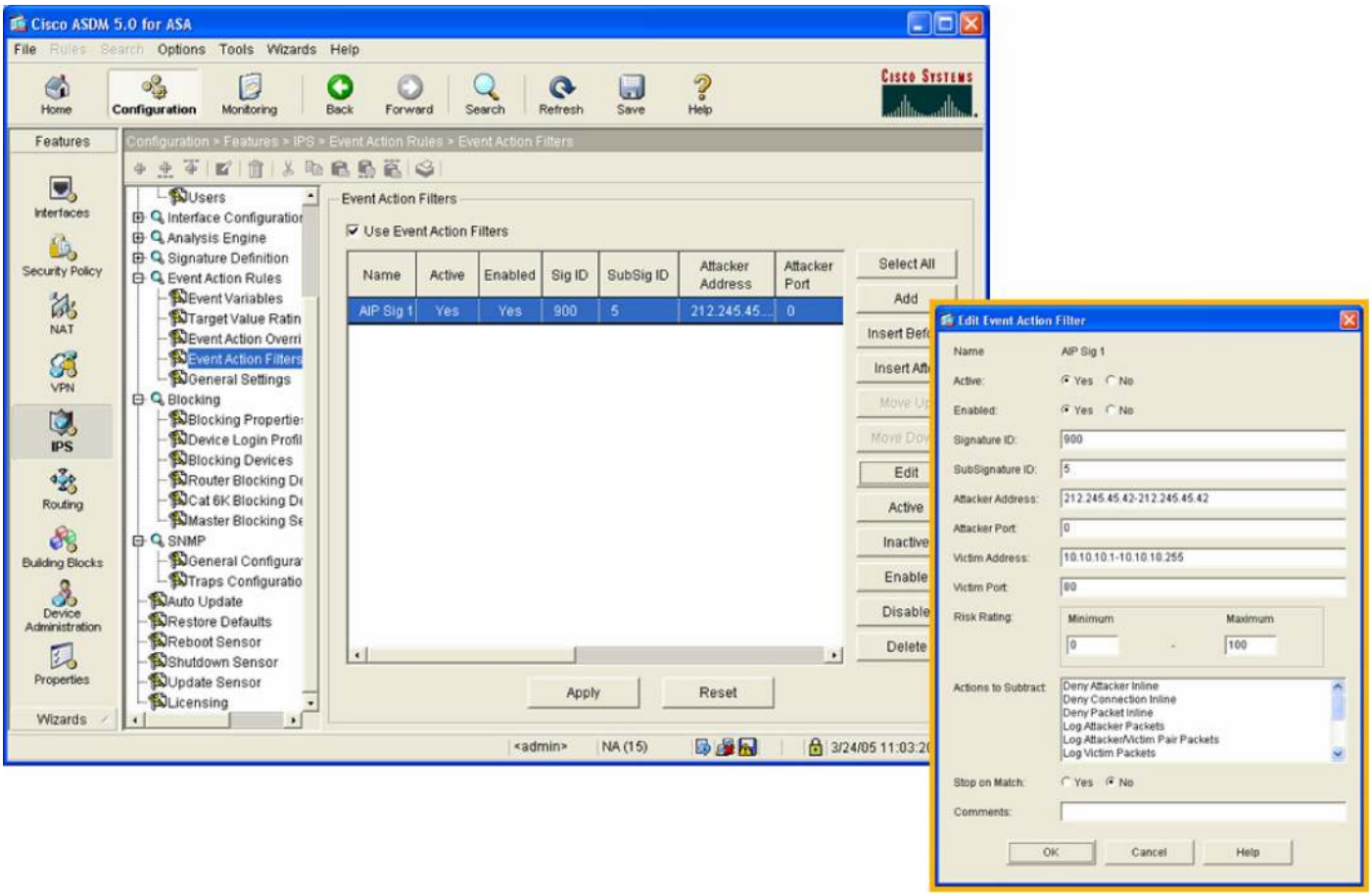


UNIQUE SECURITY MANAGEMENT INTERFACE DELIVERS CONSISTENT MANAGEMENT SERVICES

Cisco ASDM Version 5.0 delivers a single solution for all the configuration, management, and monitoring needs of the Cisco ASA 5500 Series Adaptive Security Appliances and the Cisco PIX Security Appliances. In addition to the rich configuration and management options available for best-of-breed security and VPN services, it provides a business-class solution to manage the truly adaptive security services provided by the Cisco ASA 5500 Series.

Cisco ASDM enables businesses to increase the levels of security in their network environments, while lowering operational costs by streamlining the management of the wide range of Anti-X defenses available via the Cisco Advanced Inspection and Protection Security Services Module (AIP-SSM). These services provide protection from intrusions, network attacks, Denial of Service (DoS) attacks, and malware, including worms, network viruses, Trojan horses, spyware, and adware. Cisco ASDM allows administrators to rapidly configure these services, including unique Cisco accurate prevention technologies such as Traffic Risk Rating and the Meta Event Generator (Figure 6). Cisco ASDM provides businesses with greater confidence in protecting their networks from a wide range of threats, without the risk of dropping legitimate network traffic.

Figure 6. AIP-SSM Event Action Configuration

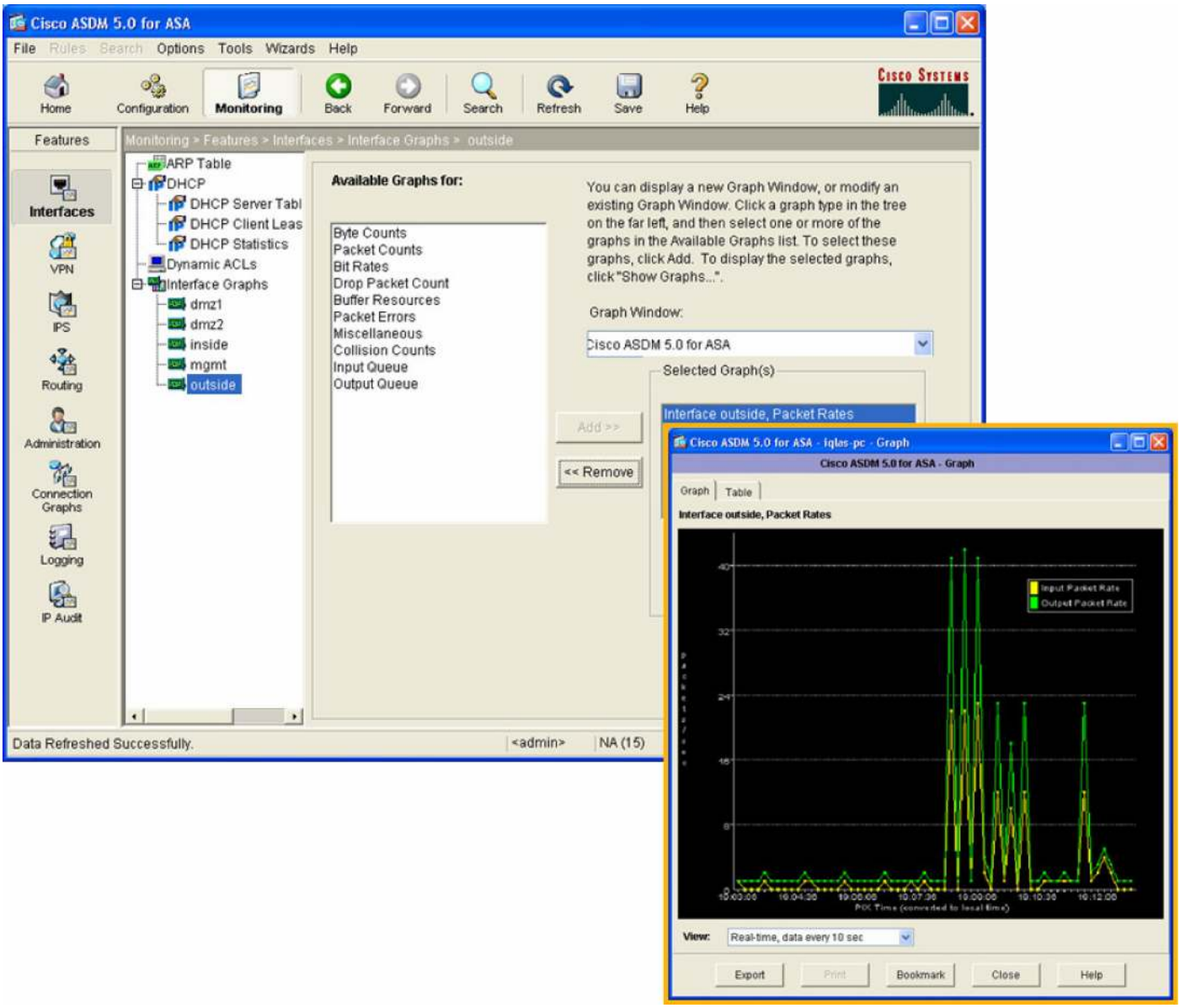


ENHANCED MONITORING AND REPORTING TOOLS ENABLE VALUABLE BUSINESS-CRITICAL ANALYSIS

Monitoring Tools

Cisco ASDM Version 5.0 offers in-depth monitoring and reporting services in addition to the at-a-glance monitoring capabilities on the new homepage (Figure 7). Versatile analysis tools create graphical summary reports showing real-time usage, security events, and network activity. Data from each graphical report can be displayed in customizable increments, where a user can choose either a 10-second snapshot or analysis over an extended timeline. The ability to view multiple graphs simultaneously allows users to perform detailed evaluations in parallel. Graphs can be conveniently bookmarked, and data can be exported for future access.

Figure 7. Monitoring



System graphs---Provide detailed status information on the Cisco ASA 5500 Series Adaptive Security Appliances and the Cisco PIX Security Appliances, including blocks used and free, current memory utilization, and CPU utilization.

Connection graphs---Track real-time session and performance monitoring data for connections; address translations; authentication, authorization, and accounting (AAA) transactions; URL filtering requests; and more, on a per-second basis. Connection graphs enable administrators to stay fully informed of their network connections and activities, without being overwhelmed.

Attack protection system graphs---Provide 16 different graphs to display potentially malicious activity. Attack signature information displays activity such as IP, Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), TCP attacks, and Portmap requests. These graphs also provide a detailed look into the list of attackers, list of events, system statistics, and diagnostics for the Cisco AIP-SSM.

Interface graphs---Provide real-time monitoring of bandwidth usage for each interface on the security appliance. Bandwidth usage is displayed for incoming and outgoing communications. Users can view packet rates, counts, and errors, as well as bit, byte, and collision counts, and more.

VPN statistics and connection graphs---Provide complete visibility into VPN connections with detailed per-tunnel statistics, including tunnel uptime and bytes/packets transferred, through support for the Cisco IPSec Flow Monitoring MIB.

Table 1 lists features and benefits of Cisco ASDM Version 5.0.

Table 1. New Features and Benefits Summary

Product Features	Benefits
Dynamic Dashboard	• Displays detailed device and licensing information for quick identification of system and available resources • Couples real-time system and traffic profiling with customizable syslog monitoring to deliver a world-class security management dashboard • Provides at-a-glance, real-time device monitoring
Web-Based Architecture	• Allows Cisco ASDM to coexist more easily with other browser-based applications • Accelerates the loading of Cisco ASDM with optimized applet caching capability • Provides anytime, anywhere access for administrators
Downloadable Cisco ASDM Launcher	• Allows users to download and run Cisco ASDM locally on Microsoft Windows-based systems • Multiple instances of Cisco ASDM Launcher provide administrative access to multiple Cisco ASA 5500 Series Adaptive Security Appliances or Cisco PIX security appliances simultaneously from the same management workstation • Automatically updates the launcher software based on the installed version on the appliance, enabling consistent security management throughout the network
Flexible Configuration and Software Image Management	• Enables effective file management on the main system via the ability to create directories and to move and delete image and configuration files • Allows users to upload both Cisco ASA 5500 Series Adaptive Security Appliance software images, Cisco PIX Security Appliance Software images, and Cisco ASDM files directly from their desktop computers to the security appliances
Complete Cisco Adaptive Security Appliance Software Version 7.0 and Cisco PIX Security Appliance Software Version 7.0 Feature Support	• Provides comprehensive support for more than 50 new features introduced in Cisco Adaptive Security Appliance Software Version 7.0 and Cisco PIX Security Appliance Software Version 7.0, such as transparent firewalling, PIM, QoS, and Active/Active failover, in addition to existing features such as OSPF and VLAN • Enhances user experience in quickly provisioning WebVPN services to enable remote-access connectivity from any Internet-enabled Web browser and its native SSL encryption. It also supports the rapid configuration and monitoring of VPN load-sharing clusters.
Advanced Application and Protocol Inspection Configuration	• Delivers robust management and monitoring capabilities for 30 specialized inspection engines that provide rich application control security services for numerous protocols, including HTTP, FTP, Extended Simple Mail Transfer Protocol (ESMTP), Domain Name System (DNS), Simple Network Management Protocol (SNMP), ICMP, SQL*Net, Network File System (NFS), H.323 Versions 1–4, SIP, Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), GTP, Internet Locator Service (ILS), and SunRPC

Product Features	Benefits
Comprehensive Management Services for the Cisco AIP-SSM	• Provides smooth integration and support for managing the Cisco AIP-SSM, which delivers a wide range of Anti-X services • Enables rapid configuration, accurate attack monitoring, and network threat mitigation capabilities through the use of multivector threat identification and accurate prevention technologies, providing greater confidence in protecting modern networks from worms, spyware, and other forms of malware, without the risk of dropping legitimate traffic
World-Class Management of Virtualized Security Services	• Enables the quick creation of multiple security contexts (virtual firewalls) within a single Cisco ASA 5500 Series Adaptive Security Appliance or a Cisco PIX Security Appliance, with each context having its own set of security policies, logical interfaces, and administrative domain • Gives businesses a convenient way of consolidating multiple firewalls into a single physical appliance or failover pair while retaining the ability to manage each of these virtual instances separately • Allows service providers to deliver resilient multitenant firewall services with a pair of redundant appliances
Robust Security Features	• Protects against unauthorized access • SSL protocol support provides high-grade encryption in addition to support for DES and 3DES • Provides 16 levels of user authorization • Includes an integrated local authentication database with optional authentication support via a RADIUS or TACACS server
Multiple Language Operating System Support	• Cisco ASDM Version 5.0 supports both the English and Japanese versions of the Microsoft Windows operating system

LICENSING

Cisco ASDM Version 5.0 is included with Cisco Adaptive Security Appliance Software Version 7.0 (1) or Cisco PIX Security Appliance Software Version 7.0(1) and higher.

Cisco PIX Device Manager Version 2.x is included with Cisco PIX Security Appliance Software Version 6.2. Cisco PIX Device Manager Version 3.x is included with Cisco PIX Security Appliance Software Version 6.3.

A separate license for Cisco ASDM is not required, but either a DES or 3DES license is required on the host Cisco ASA 5500 Series Adaptive Security Appliance or Cisco PIX Security Appliance. Users who currently do not have encryption-enabled on their base Cisco ASA 5500 Series Adaptive Security Appliances or Cisco PIX Security Appliances can request free DES/3DES activation keys; alternately, users can upgrade from their current DES licenses to 3DES licenses free of cost, by completing the online forms at: http://www.cisco.com/go/license

TECHNICAL SPECIFICATIONS

Cisco ASA 5500 Series System Requirements

Hardware

Platform: Cisco ASA 5510, 5520, or 5540 Adaptive Security Appliances

RAM: 256 MB

Flash memory: 64 MB

Software

Cisco Adaptive Security Appliance Software: Version 7.0

Encryption: DES- or 3DES-enabled

Cisco PIX Security Appliance System Requirements

Hardware

Platform: Cisco PIX 515/515E, 525, or 535 Security Appliances (Cisco PIX 501 and 506/506E Security Appliances are not currently supported)

RAM: 64 MB

Note: This release requires more memory for Cisco PIX 515/515E Security Appliances than previous software releases---a memory upgrade may be required.

Flash memory: 16 MB

Software

Cisco PIX Security Appliance Software: Version 7.0

Encryption: DES- or 3DES-enabled

User System Requirements

Hardware

Processor: Intel Pentium III 450 MHz; Pentium 4 or equivalent 500 MHz (recommended)

RAM: 256 MB (minimum)

Display resolution: 1024 x 768 pixels (minimum)

Display colors: 256 (16-bit high color recommended)

Software

Table 2 lists the operating systems and Web browsers supported by Cisco ASDM Version 5.0.

Table 2. Supported Operating Systems and Web Browsers

Operating Systems	Browsers (JavaScript- and Java-Enabled)
Windows 2000 with Service Pack 4 (English/Japanese)	Microsoft Internet Explorer 6.0 with Java Plug-In v1.4.2 or 1.5.0
Windows XP (English/Japanese)	Netscape Communicator 7.2 with Java Plug-In v1.4.2 or 1.5.0
Sun Solaris 2.8 or Higher Running CDE	Mozilla 1.7.3 with Java Plug-In v1.4.2 or 1.5.0
Red Hat Linux 9.0 Running GNOME or KDE **Red Hat Enterprise Linux WS Version 3**	Mozilla 1.7.3 with Java Plug-In v1.4.2

Note: Cisco ASDM Version 5.0 does not support Windows 95, Windows 98, Windows ME, Windows NT, or Sun Solaris OpenWindows.

Network Connection

Connection speed: 56 Kbps (384 Kbps or higher strongly recommended)

ADDITIONAL INFORMATION

For more information, please visit the following links.

Cisco ASDM: http://www.cisco.com/go/asdm

Cisco ASA 5500 Series Adaptive Security Appliances: http://www.cisco.com/go/asa

Cisco PIX Security Appliance Series: http://www.cisco.com/go/pix

SAFE Blueprint from Cisco: http://www.cisco.com/go/safe

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

205226.q_ETMG_KM_4.05

Printed in the USA