Cisco Adaptive Security Device Manager Version 5.2F for Cisco Firewall Services Module Software Version 3.2

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 the Cisco Firewall Services Module (FWSM), Cisco ASDM accelerates security deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced integrated security and networking features offered by the Cisco FWSM. The secure, Web-based design of Cisco ASDM enables anytime, anywhere access to Cisco FWSMs located in any part of the network. Based on Cisco ASDM Version 5.2 for Cisco ASA 5500 Series and Cisco PIX security appliances running Cisco PIX® Software Version 7.2, Cisco ASDM Version 5.2F enables administrators to use their knowledge to deploy the market-leading suite of Cisco security appliances and services modules.

Integrated Management Solution Provides Flexible Access Options

Cisco Adaptive Security Device Manager (ASDM) can be accessed directly with an Internet browser from any Java plug-in enabled computer or from a Microsoft Windows PC with Cisco ASDM Launcher installed, providing security administrators with rapid and secure access to their Cisco Firewall Services Module (FWSM). The Cisco ASDM Launcher can be downloaded directly from the FWSM and installed on 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 FWSMs from the convenience of a single management workstation business.

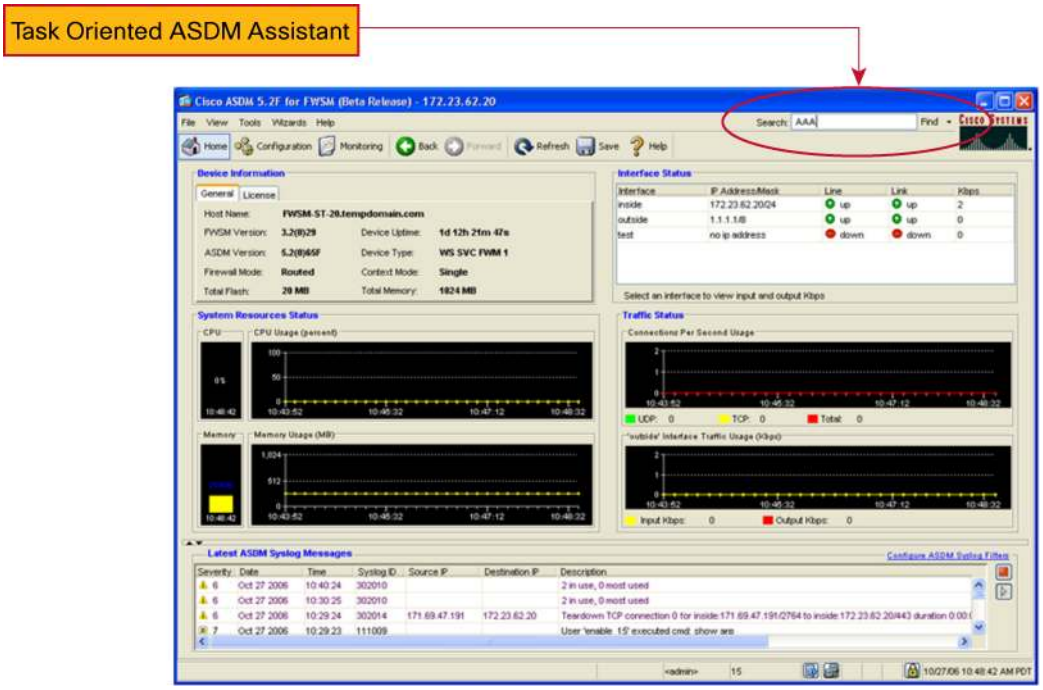
Startup Wizard Accelerates Security Deployment

Cisco ASDM features a startup wizard that helps accelerate the FWSM deployment process. A series of simple step-by-step configuration panels help administrators get their appliances operating 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), and administrative access. In Multiple Contexts Mode, the startup wizard can also be used for initial setup of newly created contexts.

Dashboard Supplies Administrators with Vital Real-Time System Status Information

Cisco ASDM 5.0F 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 FWSM 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 Version 5.2F Homepage

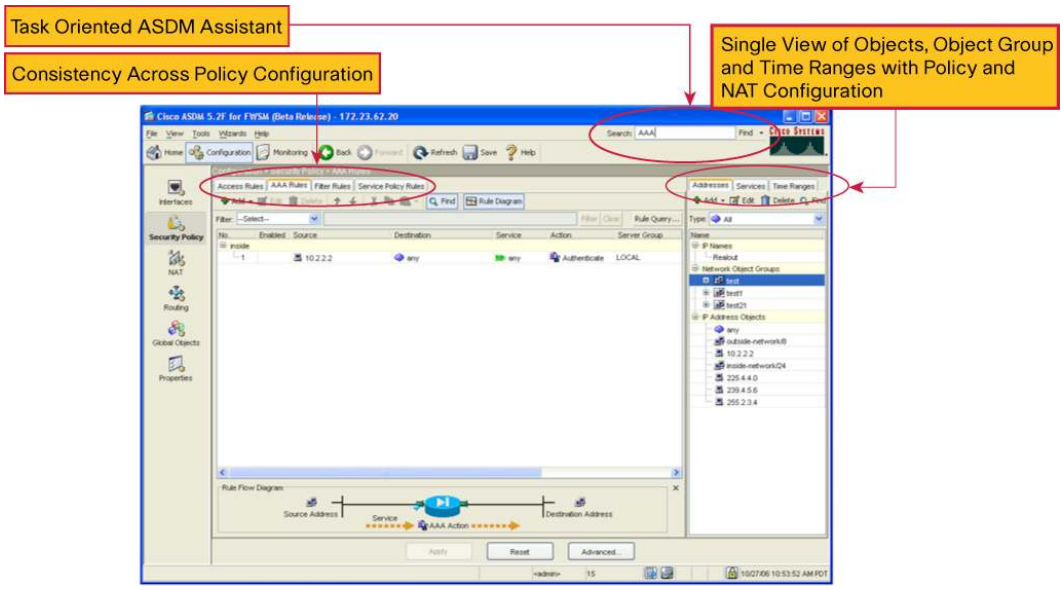


Robust Security Policy Management Lowers Operational Costs

Cisco ASDM 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. ASDM v5.2F adds complete management support for network, service, protocol, and Internet Control Message Protocol (ICMP)-type object groups to ease configuration. It also supports the wide range of access control features offered by Cisco FWSM Software Version 3.1 and 3.2, such as user-, group-, and time-based access control lists (ACLs), and inbound/outbound ACLs. Cisco ASDM also supports the new powerful and highly flexible Modular Policy Framework, which allows administrators to identify a network flow or a traffic class based on different conditions, and then apply a set of customizable inspection 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.

Cisco ASDM v5.2F features an all-new integrated policy table that allows administrators to view their complete security policy from the convenience of a single animated panel. Simply clicking on a listed policy allows the editing of all parameters associated with it, thereby simplifying configuration changes and updates. A new object group selector sidebar enables the inline editing of all network and service object groups so they can be rapidly referenced and modified in real time (Figure 2). It also provides a new Rule Query option to allow administrators to quickly filter the various network elements nad object groups of interest for focused monitoring and troubleshooting security policies that employ them.

Figure 2. Integrated Policy Rule Table



Business-Class Security Services Enforce Secure, Role-Based Administrative Access

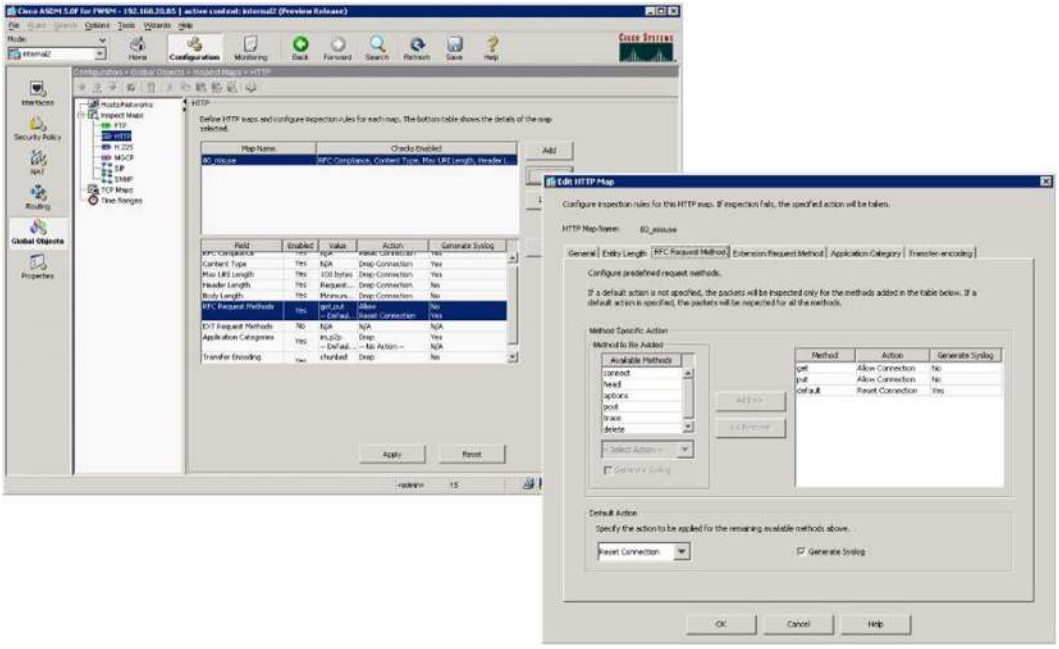
Cisco ASDM Version 5.0F integrates an array of robust security services to prevent unauthorized administrative access to a device. It supports a wide range of methods for authenticating administrators, including a local authentication database on a Cisco FWSM, or via a RADIUS/TACACS server. All communications 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, granting administrators and operations personnel the appropriate level of permissions for every Cisco security appliance they manage (for example, monitor-only, read-only access to the configuration).

Comprehensive Management Services Complement Advanced Application Inspection

Cisco FWSM Software Version 3.1and Version 3.2 includes more than 30 dedicated inspection engines for a range of modern applications driven by protocols such as HTTP (Figure 3), FTP, General Packet Radio Service (GPRS) Tunneling Protocol (GTP), Sun Remote Procedure Call (SunRPC), H.323, and Session Initiation Protocol (SIP). Cisco ASDM 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 provides easy and convenient access to managing the rich network integration features found in the Cisco FWSM. 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. Individual context users get the same interface as 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.

Cisco ASDM gives administrators complete control over multicast routing protocols such as Protocol Independent Multicast (PIM) (Figure 4), Open Shortest Path First (OSPF) dynamic routing (Figure 5), and IEEE 802.1q-based VLAN interface 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 FWSM into complex routing and switching environments.

Figure 4. Advanced PIM-SPARSE Multicast Configuration

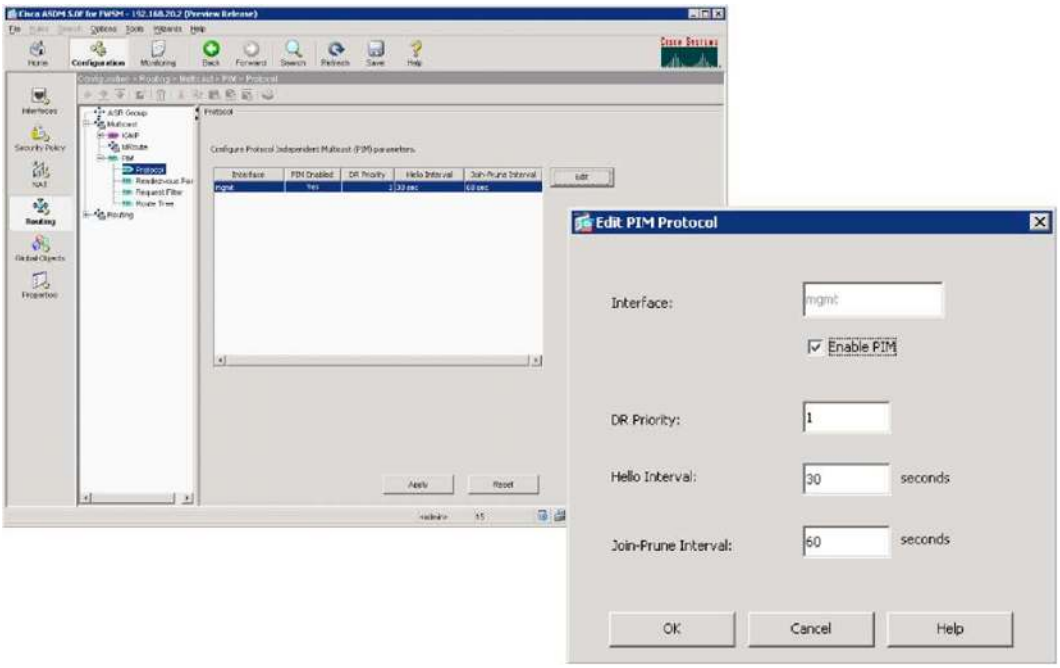
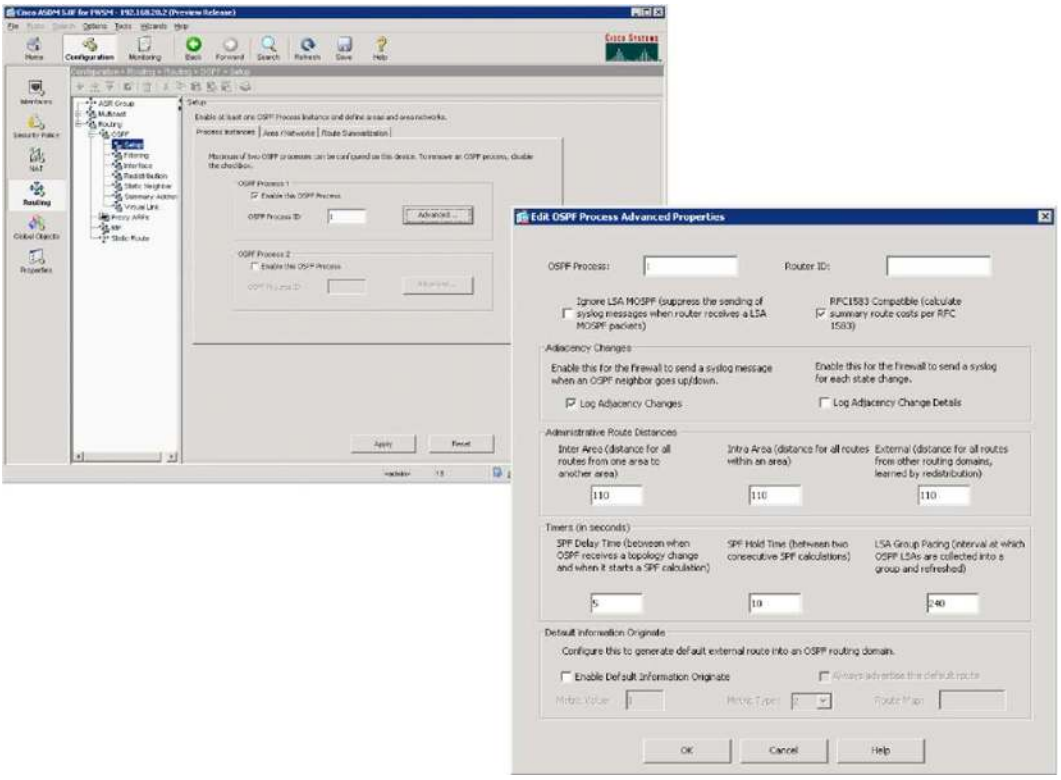


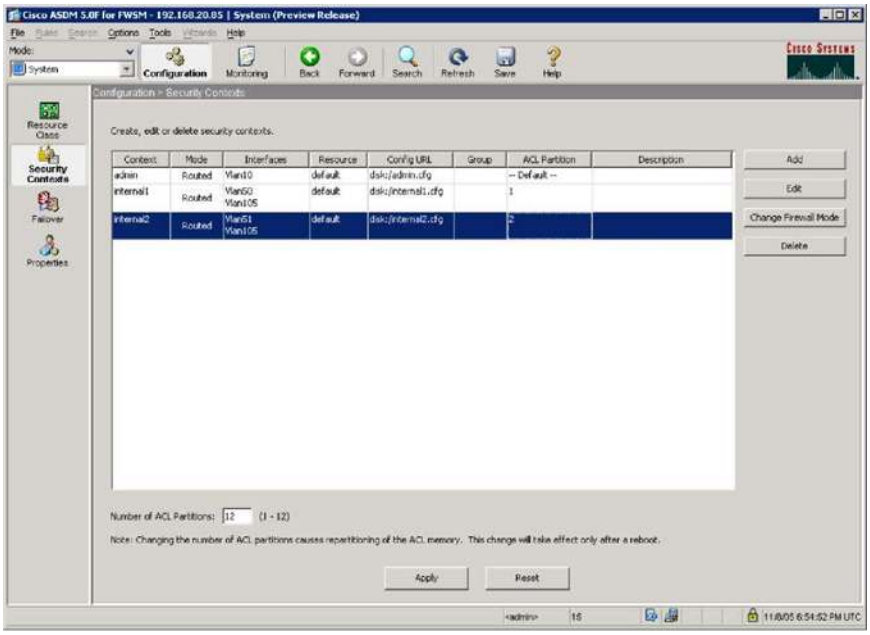
Figure 5. Advanced OSPF Configuration



Resource Management

Cisco ASDM allows administrators to manage the resources for ACLs in Multiple Security Contexts Mode. Resources, such as ACL memory pool or ACL tree instances, which are used when compiling ACLs, can be assigned to security contexts by the administrator to optimize resource usage.

Figure 6. Resource Manager for ACL Memory Pool in Cisco ASDM

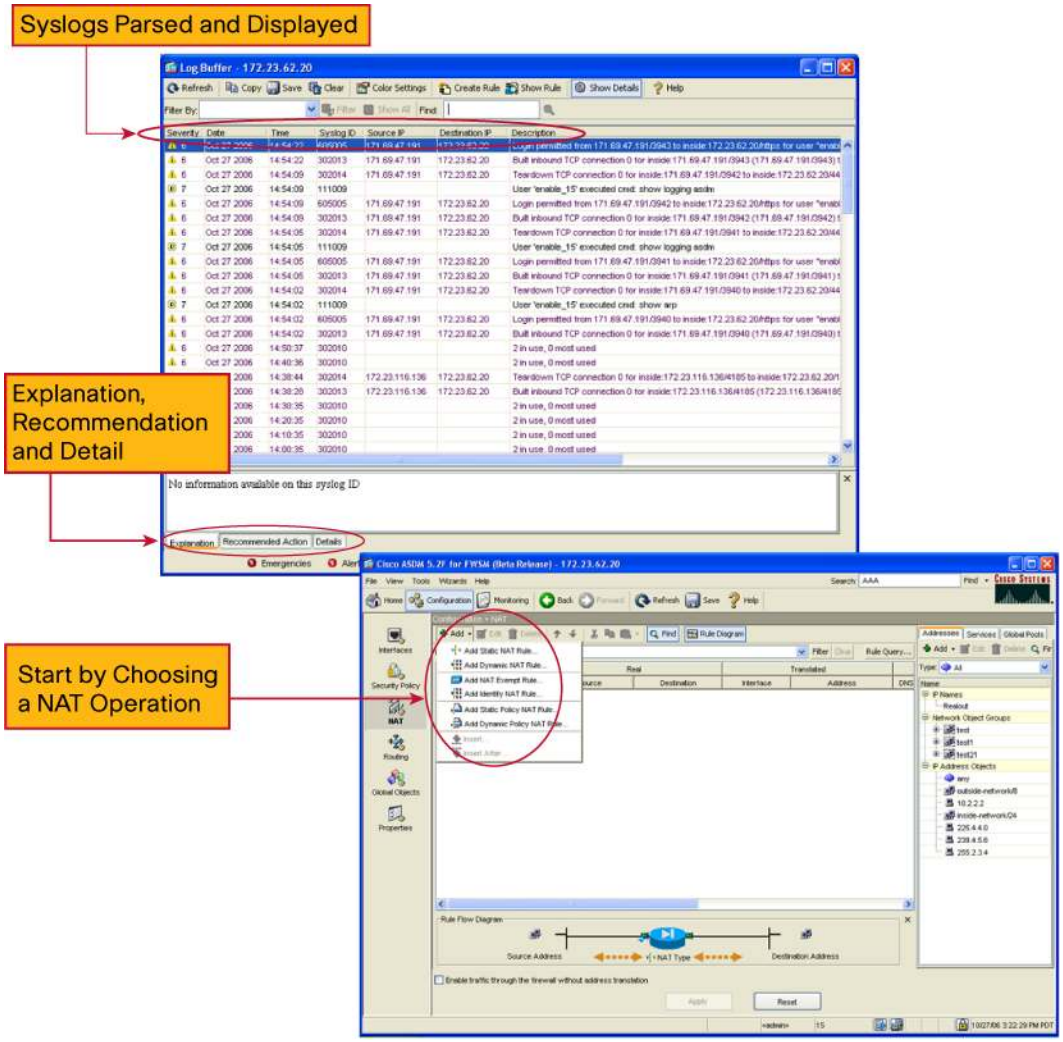


Enhanced Monitoring and Reporting Tools Enable Valuable Business-Critical Analysis

Syslog to Access Rule Correlation

Cisco ASDM includes a Syslog to Access Rule Correlation tool that greatly enhances day-to-day security management and troubleshooting activities. With this dynamic tool, security administrators can quickly resolve common configuration issues, along with most user and network connectivity problems. With ASDM 5.2F, users can select a syslog message within the Real-Time Syslog Viewer panel, and by simply clicking the “Create” button at the top of the panel (Figure 7), can invoke the access-control options for that specific syslog. Intelligent defaults help ensure that the configuration process is simple, which helps improve operational efficiency and response times for business-critical functions. The Syslog to Access Rule Correlation tool also offers an intuitive view into syslog messages invoked by user-configured access rules. Administrators can closely observe enterprise traffic patterns and monitor resource access behavior. Figure 7 indicates the Syslog to Access Rule Correlation capability where a user has selected a syslog message, and has clicked on the Create button to define policies for that flow.

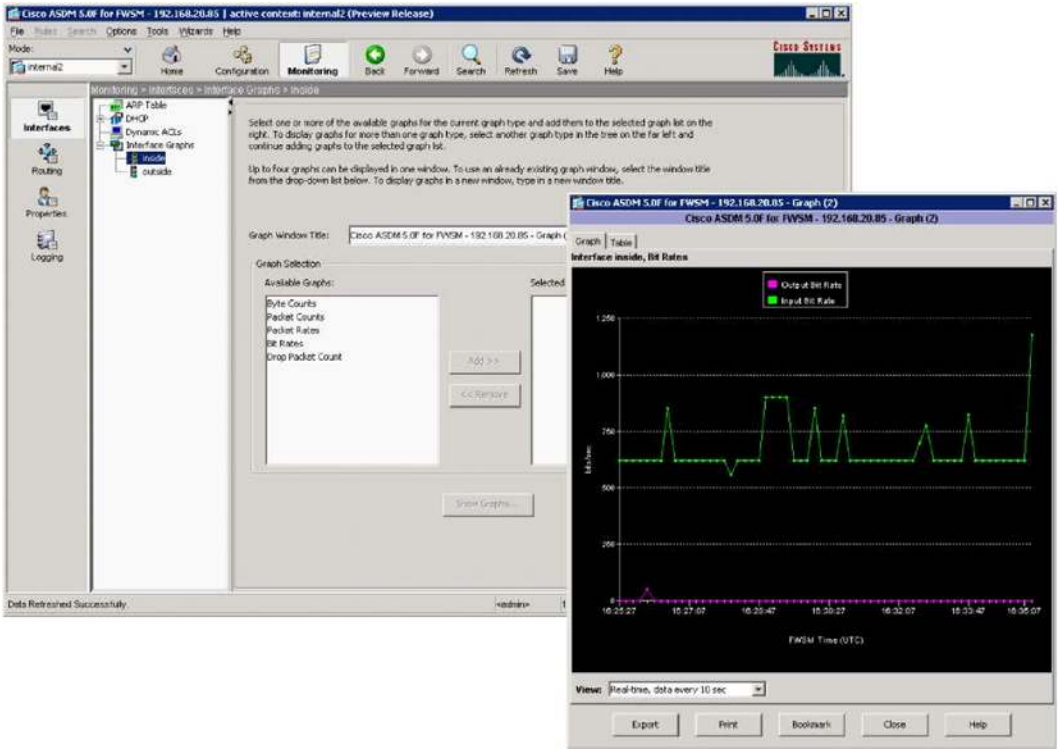
Figure 7. Syslog to Access Rule Correlation Tool



Monitoring Tools

Cisco ASDM offers in-depth monitoring and reporting services in addition to the at-a-glance monitoring capabilities on the new homepage (Figure 8). 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 8. Advanced Monitoring Options with Customizable Graphs



- **System Graphs**—Provide detailed status information on the Cisco FWSM, including used and free blocks, 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.
- **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.

Table 1 provides an overall feature summary of Cisco ASDM Version 5.0F.

Table 1. Cisco ASDM Version 5.2F Overall Feature Summary

Complete Cisco FWSM Version 3.2 Feature Support	
Dynamic Dashboard	Detailed device and licensing information Real-time system and traffic profiling Customizable syslog monitoring Real-time device monitoring
Web-Based Architecture	Advanced Application and Protocol Inspection Configuration
Up to 80 simultaneous ASDM HTTPS connections	Web GUI for Modular Policy Framework
Downloadable Cisco ASDM Launcher	Streamlined policy creation provides easy access to all items needed for ACL management, including easy object group creation/modification/viewing, and a policy visualizer.

Demo Mode supported	• Policy query capability gives administrators advanced search capabilities for their ACLs • New object group selector panel enables rapid editing of all network and service object groups
Rich Syslog Support	Robust Security Features
Syslog to ACE (Access Control Element) correlation and instant viewing of syslogs being generated based on a selected ACL	HTTPS authentication proxy for administrative access
Create opposite ACE based on syslog entry	16 levels of user authorization
Search on any text in syslog table	Local authentication database
Many customizations	RADIUS or TACACS authentication support
Rule table and syslog integration enables single-click rule creation from syslog and provides explanation of syslog messages and recommended actions.	
New syslog viewer provides syslog parsing for customizable views based on time, date, syslog IDs, IP addresses, and coloring of logs based on severity.	
World-Class Management of Virtualized Security Services	Flexible Configuration and Software Image Management
Create security policies, logical interfaces, and administrative domains for	Effective file management with directories
multiple virtual firewalls (security contexts)	Direct upload from desktop to FWSM
Resource Manager	Scheduled or immediate reload of FWSM image
Context caching	

Note: Cisco ASDM Version 5.2F is used to configure and manage the new features in FWSM Software Version 3.2.
Cisco ASDM Version 5.0F incorporates all of the features from Cisco ASDM Version 5.0 that are applicable to the Cisco FWSM. All Cisco FWSM Software Version 3.1 features are configurable with Cisco ASDM Version 5.0F except IPv6, which requires CLI configuration.

Licensing

Cisco ASDM Version 5.2F is included with Cisco FWSM Software Version 3.2.

Cisco ASDM Version 5.0F is included with Cisco FWSM Software Version 3.1.

Cisco PIX Device Manager Version 4.1 is included with Cisco FWSM Software Version 2.2 and 2.3.

Cisco PIX Device Manager Version 2.1 is included with Cisco FWSM Software Version 1.1.

User System Requirements

Hardware

- **Processor:** Pentium 4, AMD Athlon or equivalent
- **RAM:** 512 MB (minimum) for Microsoft Windows and Sun SPARC, 256MB (minimum) for Red Hat Linux
- **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
Windows 2000 with Service Pack 4, Windows XP (English/Japanese version)	Microsoft Internet Explorer 6.0 with Java 1.4.2 or 1.5 Firefox 1.5 with Java 1.4.2 or 1.5
Sun SPARC Solaris 2.8 or 2.9	Firefox 1.5 with Java 1.4.2 or 1.5
RedHat Desktop, RedHat Enterprise Linux WS 3.0	Firefox 1.5 with Java 1.4.2 or 1.5 GNOME or KDE desktop environment

Note: Cisco ASDM Version 5.0F does not support Windows 95, Windows 98, Windows ME, Windows NT, or the Macintosh operating system.

Additional Information

For more information, please visit the following links.

- **Cisco ASDM:** http://www.cisco.com/go/asdm
- **Cisco FWSM:** http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html
- **Cisco ASA 5500 Series Adaptive Security Appliances:** http://www.cisco.com/go/asa

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**

Printed in USA C78-340998-01 12/06

