Data Sheet

Cisco Adaptive Security Device Manager Version 5.1

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, increasing ASDM's 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, simplifying management in small business environments.

STARTUP WIZARD ACCELERATES SECURITY APPLIANCE DEPLOYMENT

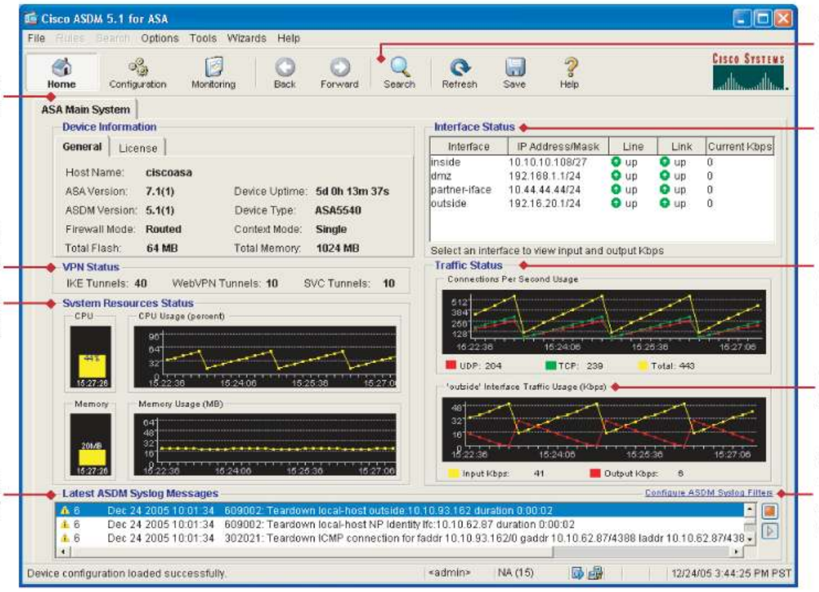
Cisco ASDM features a Startup Wizard that helps accelerate the security appliance deployment process. A series of simple step-by-step configuration panels help administrators get their appliances up and running quickly and create a robust configuration that allows traffic to flow securely through their 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 5.1 includes a dynamic dashboard that provides a complete system overview and device health statistics (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 for 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 includes a configuration search engine that helps administrators locate where specific features can be configured, and provides convenient point-and-click access to the search results.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 1. Cisco ASDM Version 5.1 Homepage



Host Name: ciscoasa
ASA Version: 7.1(1) Device Uptime: 5d 0h 13m 37s
ASDM Version: 5.1(1) Device Type: ASA5540
Firewall Mode: Routed Context Mode: Single
Total Flash: 64 MB Total Memory: 1024 MB

IKE Tunnels: 40 WebVPN Tunnels: 10 SVC Tunnels: 10

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	10.10.10.108/27	up	up	0
dmz	192.168.1.1/24	up	up	0
partner-iface	10.44.44.44/24	up	up	0
outside	192.16.20.1/24	up	up	0

Select an interface to view input and output Kbps

```
6   Dec 24 2005 10:01:34   609002: Teardown local-host outside:10.10.93.162 duration 0:00:02
6   Dec 24 2005 10:01:34   609002: Teardown local-host NP Identity Ifc:10.10.62.87 duration 0:00:02
6   Dec 24 2005 10:01:34   302021: Teardown ICMP connection for faddr 10.10.93.162/0 gaddr 10.10.62.87/4388 laddr 10.10.62.87/438
```

Device configuration loaded successfully. <admin> NA (15) 12/24/05 3:44:25 PM PST

System/License Information

IPSec/WebVPN Status

System Status Profiling

Live Syslog Viewer

Advanced Configuration/ Feature Search

Interface Status Information

Real-Time Traffic and Connection Profiling

Network/Interface Status Updates

Syslog Configuration and Start/Stop Options

ROBUST SECURITY POLICY MANAGEMENT LOWERS OPERATIONAL COSTS

Cisco ASDM Version 5.1 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 supports the wide range of access control features offered by both Cisco ASA Software Version 7.1 and Cisco PIX Security Appliance Software Version 7.1, such as user- and group-based access lists, time-based access lists, and inbound/outbound access lists. Cisco ASDM Version 5.1 also supports the new Modular Policy Framework offered in both of these software versions. This rich, 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), 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

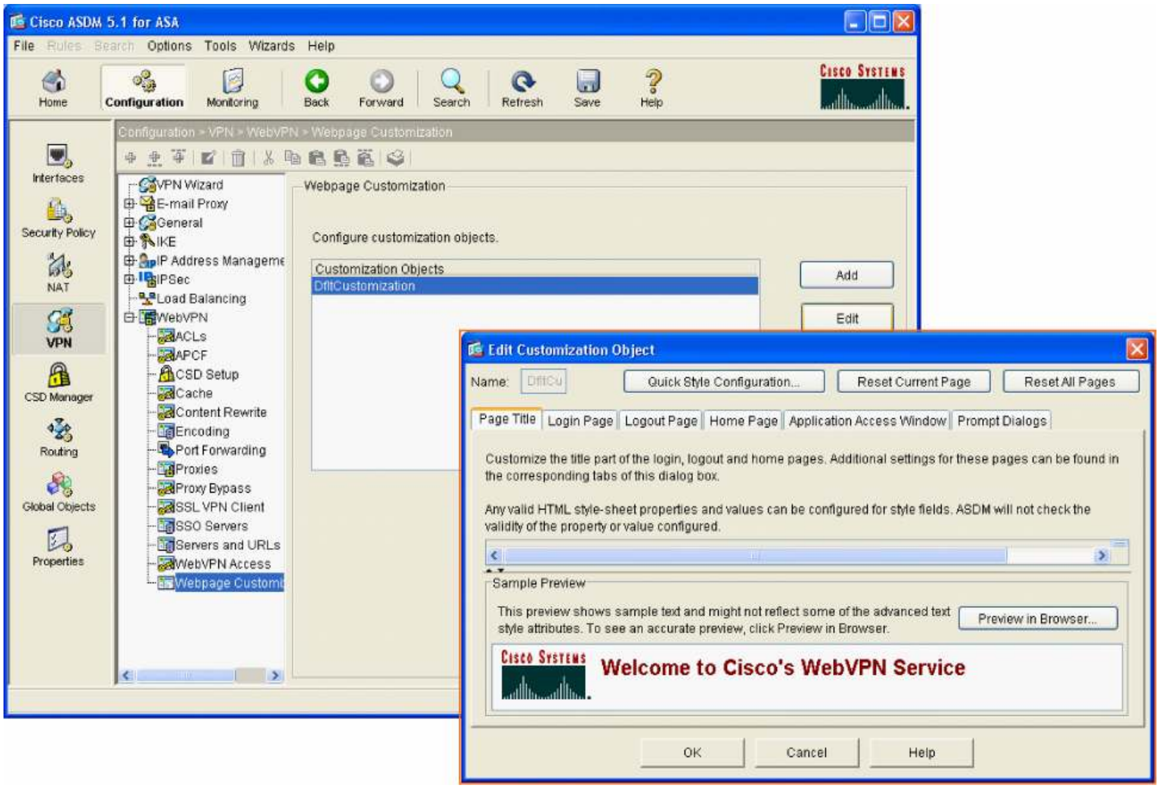
Cisco ASDM Version 5.1 integrates an array of robust security services to prevent unauthorized administrative access to a device. It supports a wide range of methods for authenticating administrators, including a local authentication database on a Cisco ASA 5500 Series Adaptive Security Appliance or 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 Version 5.1 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 5.1 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 rich Cisco SSL VPN 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.

Figure 2. SSL VPN Configuration



Configure customization objects.

Name: DfltCu

Customize the title part of the login, logout and home pages. Additional settings for these pages can be found in the corresponding tabs of this dialog box.

Any valid HTML style-sheet properties and values can be configured for style fields. ASDM will not check the validity of the property or value configured.

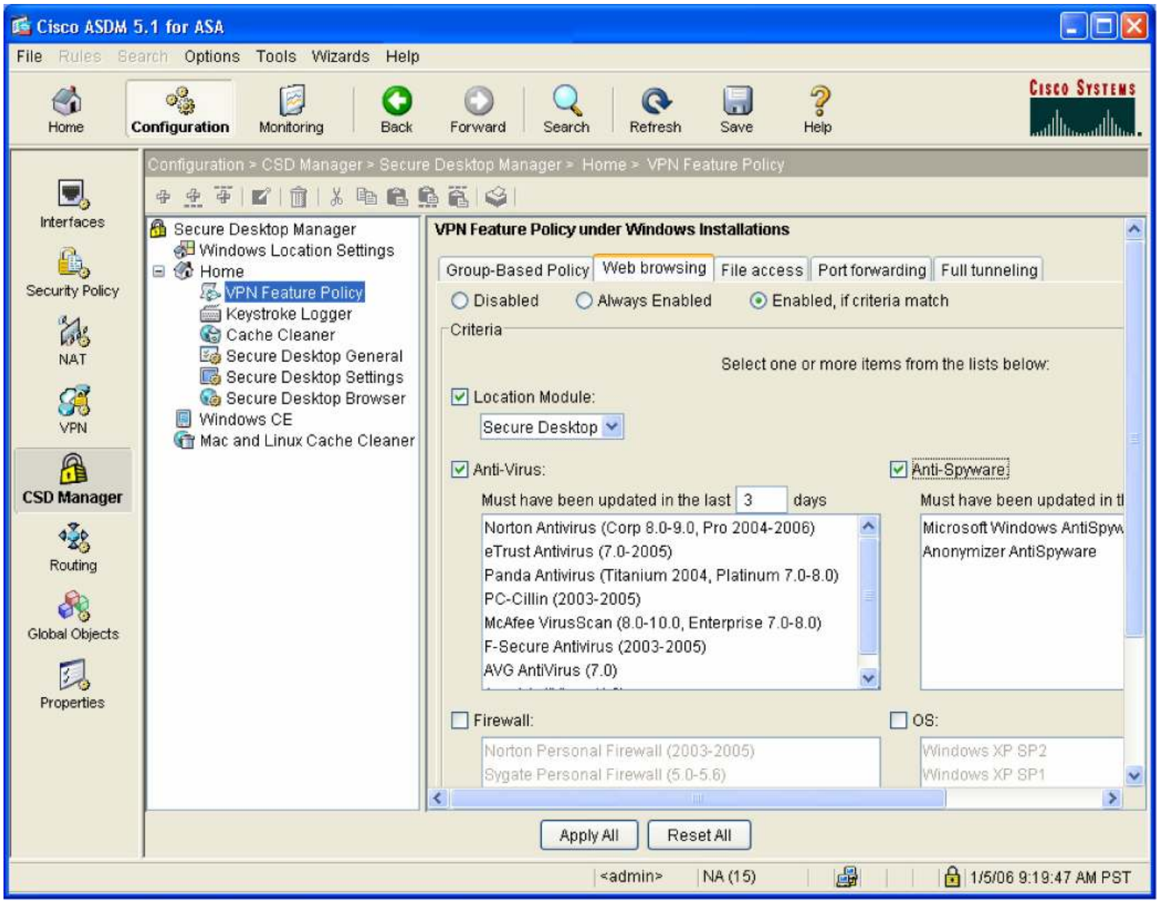
This preview shows sample text and might not reflect some of the advanced text style attributes. To see an accurate preview, click Preview in Browser.

Welcome to Cisco's WebVPN Service

A core component of Cisco SSL VPN is the Cisco Secure Desktop, delivered as part of Cisco ASA 5500 Series Software Version 7.1. The Cisco Secure Desktop seeks to minimize data such as cookies, browser history, temporary files, and downloaded content from being left behind after an SSL VPN session terminates. Protection is increased against data theft and client system malware by encrypting data and files associated with or downloaded during the SSL VPN session. Cisco ASDM enables rapid deployment and control of Cisco Secure Desktop functions through a dedicated Cisco Secure Desktop Manager (Figure 3). Cisco ASDM also delivers advanced VPN monitoring capabilities, providing administrators with numerous statistics and graphs showing metrics such as session uptimes, data transferred per session, and more.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 3. Cisco Secure Desktop Configuration



Configuration > CSD Manager > Secure Desktop Manager > Home > VPN Feature Policy

VPN Feature Policy under Windows Installations

Group-Based Policy | Web browsing | File access | Port forwarding | Full tunneling

○ Disabled ○ Always Enabled ● Enabled, if criteria match

Criteria

Select one or more items from the lists below:

☑ Location Module: Secure Desktop

☑ Anti-Virus:

Must have been updated in the last 3 days

- Norton Antivirus (Corp 8.0-9.0, Pro 2004-2006)
- eTrust Antivirus (7.0-2005)
- Panda Antivirus (Titanium 2004, Platinum 7.0-8.0)
- PC-Cillin (2003-2005)
- McAfee VirusScan (8.0-10.0, Enterprise 7.0-8.0)
- F-Secure Antivirus (2003-2005)
- AVG AntiVirus (7.0)

☑ Anti-Spyware:

Must have been updated in tl

- Microsoft Windows AntiSpyw
- Anonymizer AntiSpyware

□ Firewall:

- Norton Personal Firewall (2003-2005)
- Sygate Personal Firewall (5.0-5.6)

□ OS:

- Windows XP SP2
- Windows XP SP1

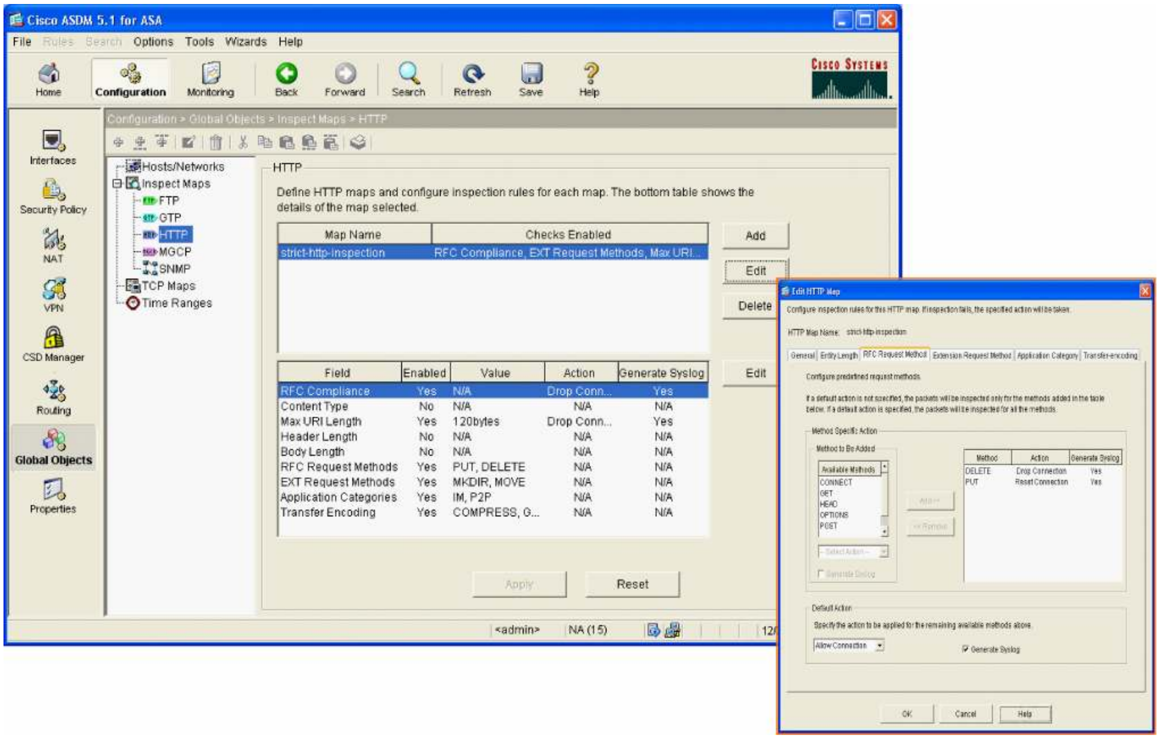
<admin> NA (15) 1/5/06 9:19:47 AM PST

COMPREHENSIVE MANAGEMENT SERVICES COMPLEMENT ADVANCED APPLICATION INSPECTION

Cisco Adaptive Security Appliance Software Version 7.1 and Cisco PIX Security Appliance Software Version 7.1 include more than 30 dedicated inspection engines for a range of modern applications driven by protocols such as HTTP (Figure 4), FTP, GPRS Tunneling Protocol (GTP), Sun Remote Procedure Call (SunRPC), H.323, and Session Initiation Protocol (SIP). Cisco ASDM Version 5.1 point-and-click capabilities, which have been conditioned by intelligent application defaults, enable the quick creation of security profiles that protect mission-critical applications and resources from misuse and tunneling attacks. Cisco ASDM Version 5.1 enforces flow-based control in defining inspection services and gives administrators enterprise-class tools to exercise microscopic control over applications.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 4. Advanced HTTP Inspection Services Configuration



Define HTTP maps and configure inspection rules for each map. The bottom table shows the details of the map selected.

Map Name	Checks Enabled
strict-http-inspection	RFC Compliance, EXT Request Methods, Max URI...

Field	Enabled	Value	Action	Generate Syslog
RFC Compliance	Yes	N/A	Drop Conn...	Yes
Content Type	No	N/A	N/A	N/A
Max URI Length	Yes	120bytes	Drop Conn...	Yes
Header Length	No	N/A	N/A	N/A
Body Length	No	N/A	N/A	N/A
RFC Request Methods	Yes	PUT, DELETE	N/A	N/A
EXT Request Methods	Yes	MKDIR, MOVE	N/A	N/A
Application Categories	Yes	IM, P2P	N/A	N/A
Transfer Encoding	Yes	COMPRESS, G...	N/A	N/A

Configure inspection rules for this HTTP map. If inspection fails, the specified action will be taken.

HTTP Map Name: strict-http-inspection

Configure predefined request methods.

If a default action is not specified, the packets will be inspected only for the methods added in the table below. If a default action is specified, the packets will be inspected for all the methods.

Available Methods: CONNECT, GET, HEAD, OPTIONS, POST

Method	Action	Generate Syslog
DELETE	Drop Connection	Yes
PUT	Reset Connection	Yes

Specify the action to be applied for the remaining available methods above.

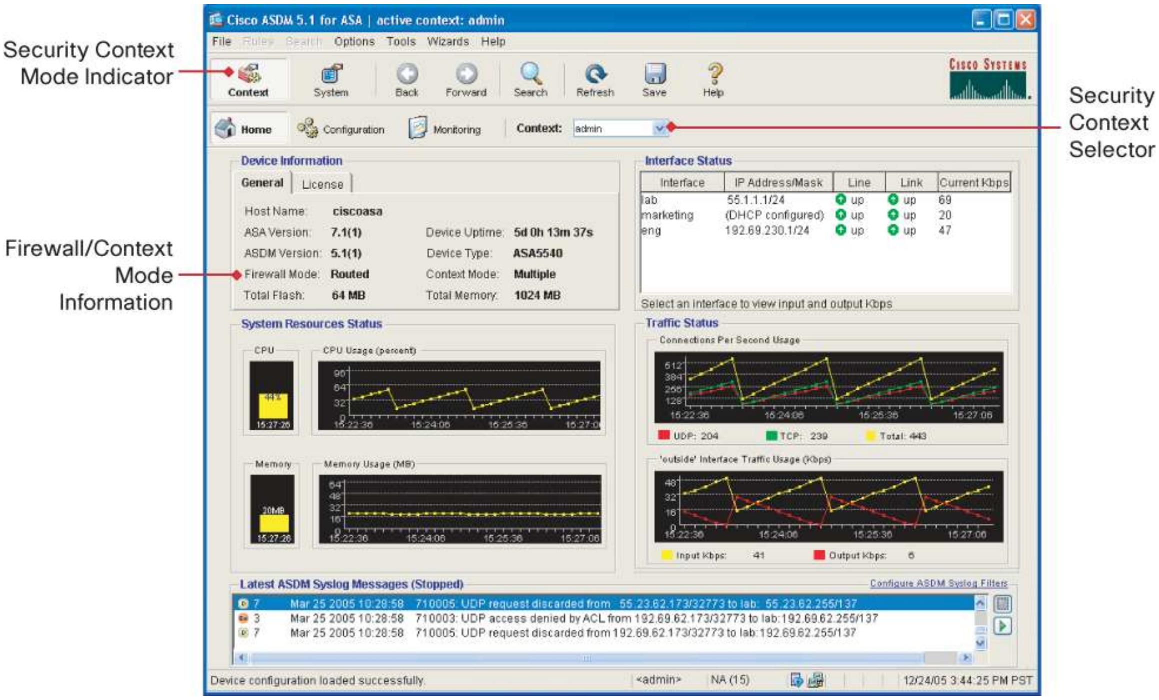
Allow Connection ☑ Generate Syslog

INTELLIGENT USER INTERFACE SIMPLIFIES INTEGRATION INTO COMPLEX NETWORK ENVIRONMENTS

Cisco ASDM Version 5.1 provides easy and convenient access to managing the rich network integration features found in Cisco ASA 5500 Series 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 5). 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.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 5. System Administrator View of Security Contexts



Context: admin

Device Information

Host Name: ciscoasa
ASA Version: 7.1(1) Device Uptime: 5d 0h 13m 37s
ASDM Version: 5.1(1) Device Type: ASA5540
Firewall Mode: Routed Context Mode: Multiple
Total Flash: 64 MB Total Memory: 1024 MB

Interface Status

Interface	IP Address/Mask	Line	Link	Current Kbps
lab	55.1.1.1/24	up	up	69
marketing	(DHCP configured)	up	up	20
eng	192.69.230.1/24	up	up	47

Select an interface to view input and output Kbps

🟥 UDP: 204 🟩 TCP: 239 🟨 Total: 443

🟨 Input Kbps: 41 🟥 Output Kbps: 6

Latest ASDM Syslog Messages (Stopped)

```
7    Mar 25 2005 10:28:58   710005: UDP request discarded from  55.23.62.173/32773 to lab:  55.23.62.255/137
3    Mar 25 2005 10:28:58   710003: UDP access denied by ACL from 192.69.62.173/32773 to lab:192.69.62.255/137
7    Mar 25 2005 10:28:58   710005: UDP request discarded from 192.69.62.173/32773 to lab:192.69.62.255/137
```

Device configuration loaded successfully. <admin> NA (15) 12/24/05 3:44:25 PM PST

Cisco ASDM Version 5.1 gives administrators complete control over multicast routing protocols such as Protocol Independent Multicast (PIM), Open Shortest Path First (OSPF) dynamic routing, IEEE 802.1q-based VLAN interfaces, and 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.

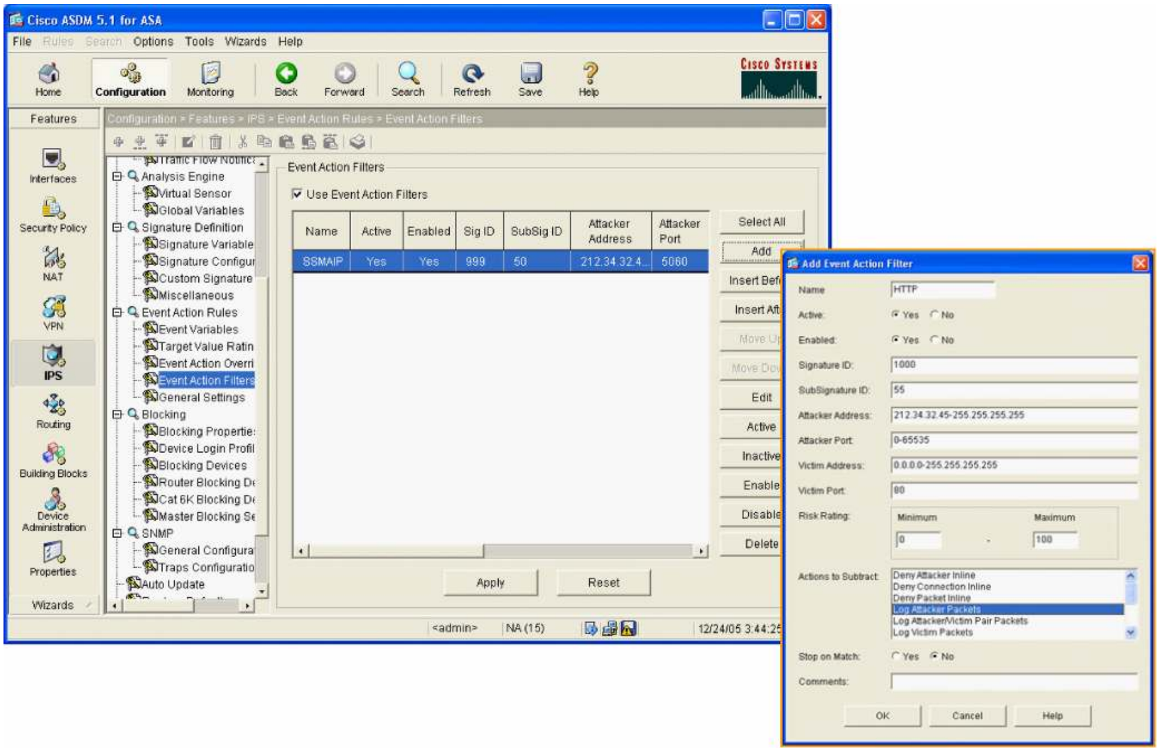
ADAPTABLE SECURITY MANAGEMENT INTERFACE ENHANCES THE UNIFIED THREAT MANAGEMENT EXPERIENCE

Cisco ASDM Version 5.1 delivers a single solution for all the configuration, management, and monitoring needs of Cisco ASA 5500 Series and Cisco PIX security appliances. It provides a business-class solution to manage the truly adaptive security services provided by the Cisco ASA 5500 Series.

Managing Inline Intrusion Prevention Services and Network-Based Worm Mitigation

Cisco ASDM Version 5.1 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 through 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 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. Cisco AIP SSM Event Action Configuration



Event Action Filters

☑ Use Event Action Filters

Name	Active	Enabled	Sig ID	SubSig ID	Attacker Address	Attacker Port
SSMAIP	Yes	Yes	999	50	212.34.32.4...	5060

Add Event Action Filter

Name: HTTP

Active: ● Yes ○ No

Enabled: ● Yes ○ No

Signature ID: 1000

SubSignature ID: 55

Attacker Address: 212.34.32.45-255.255.255.255

Attacker Port: 0-65535

Victim Address: 0.0.0.0-255.255.255.255

Victim Port: 80

Risk Rating: Minimum 0 - Maximum 100

Actions to Subtract: Deny Attacker Inline, Deny Connection Inline, Deny Packet Inline, Log Attacker Packets (selected), Log Attacker/Victim Pair Packets, Log Victim Packets

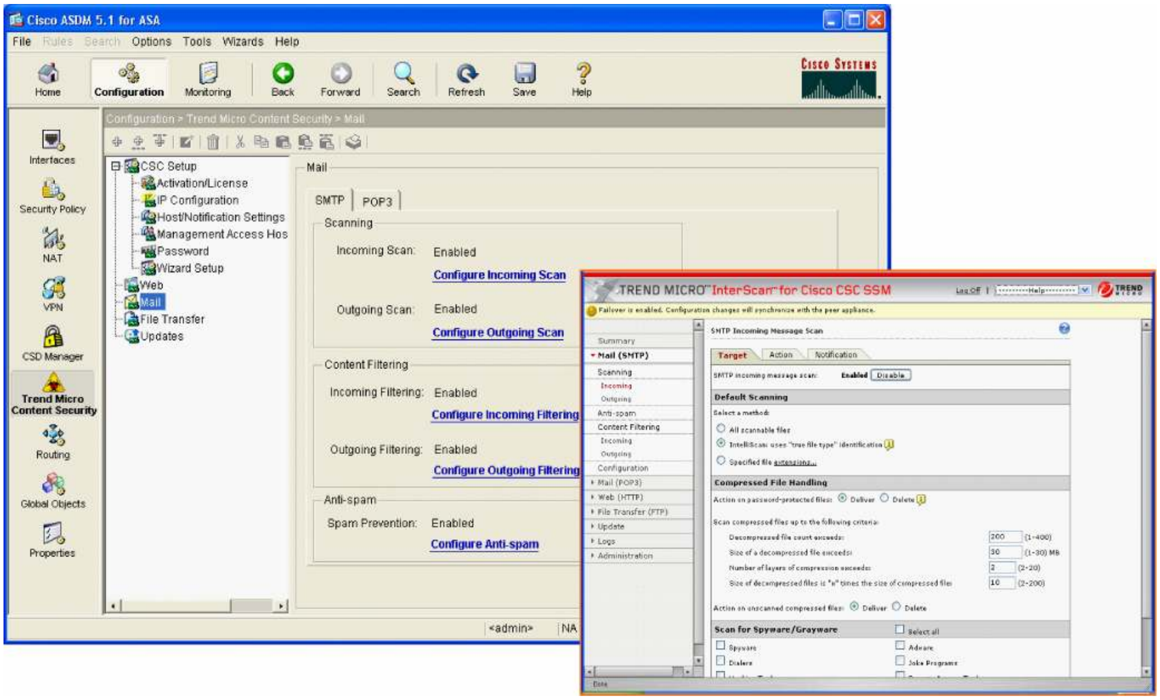
Stop on Match: ○ Yes ● No

Comments:

Managing Content Security and Anti-X Services

The Cisco ASA 5500 Series Content Security and Control Security Services Module (CSC SSM) delivers high-performance anti-X services on a single services card. The Cisco CSC SSM incorporates security technology from Trend Micro’s industry-leading and award-winning InterScan suite of secure content management products. The Cisco CSC SSM delivers comprehensive protection and control for the Internet gateway, including antivirus, antispam, and antiphishing, as well as URL blocking and filtering services. In conjunction with the CSC SSM, Cisco ASDM Version 5.1 delivers an industry-first solution that blends the simplicity of Trend Micro’s HTML-based configuration panels with the ingenuity of Cisco ASDM (Figure 8). This helps ensure consistent policy enforcement, and simplifies the complete provisioning, configuration, and monitoring processes for these rich unified threat management functions.

Figure 7. Cisco CSC SSM SMTP Incoming Mail Scanning Configuration



Mail

SMTP | POP3

Scanning

Incoming Scan: Enabled
Configure Incoming Scan

Outgoing Scan: Enabled
Configure Outgoing Scan

Content Filtering

Incoming Filtering: Enabled
Configure Incoming Filtering

Outgoing Filtering: Enabled
Configure Outgoing Filtering

Anti-spam

Spam Prevention: Enabled
Configure Anti-spam

Failover is enabled. Configuration changes will synchronize with the peer appliance.

SMTP Incoming Message Scan

Target | Action | Notification

SMTP incoming message scan: **Enabled** Disable

Default Scanning

Select a method:

○ All scannable files
● IntelliScan: uses "true file type" identification
○ Specified file extensions...

Compressed File Handling

Action on password-protected files: ● Deliver ○ Delete

Scan compressed files up to the following criteria:

Decompressed file count exceeds:	200	(1-400)
Size of a decompressed file exceeds:	30	(1-30) MB
Number of layers of compression exceeds:	2	(2-20)
Size of decompressed files is "x" times the size of compressed file:	10	(2-200)

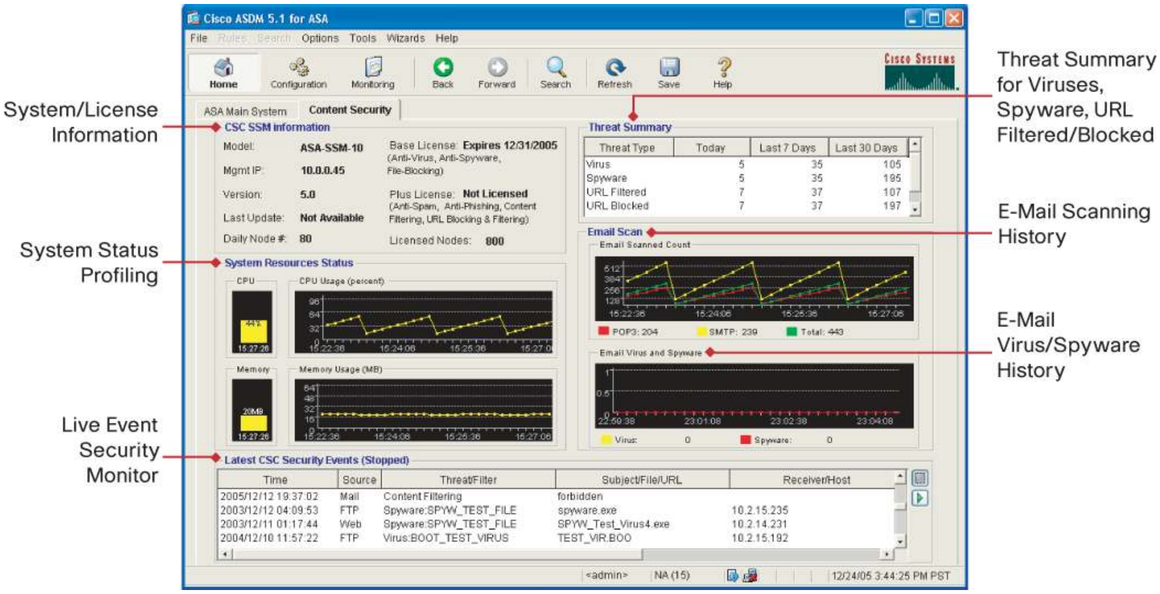
Action on unscanned compressed files: ● Deliver ○ Delete

Scan for Spyware/Grayware □ Select all

□ Spyware □ Adware
□ Dialers □ Joke Programs

Cisco ASDM Version 5.1 provides a complementary monitoring solution with a new CSC SSM homepage and new monitoring panels. Once a CSC SSM is installed, the main ASDM homepage is automatically updated to display a new CSC SSM panel (Figure 8), which provides a historic view into threats, e-mail viruses, live events, vital module statistics such as last installed software/signature updates, system resources, and more.

Figure 8. Cisco CSC SSM Homepage



CSC SSM information

Model:	ASA-SSM-10	Base License:	Expires 12/31/2005 (Anti-Virus, Anti-Spyware, File-Blocking)
Mgmt IP:	10.0.0.45		
Version:	5.0	Plus License:	Not Licensed (Anti-Spam, Anti-Phishing, Content Filtering, URL Blocking & Filtering)
Last Update:	Not Available		
Daily Node #:	80	Licensed Nodes:	800

Threat Summary

Threat Type	Today	Last 7 Days	Last 30 Days
Virus	5	35	105
Spyware	5	35	195
URL Filtered	7	37	107
URL Blocked	7	37	197

🟥 POP3: 204 🟨 SMTP: 239 🟩 Total: 443

🟨 Virus: 0 🟥 Spyware: 0

Latest CSC Security Events (Stopped)

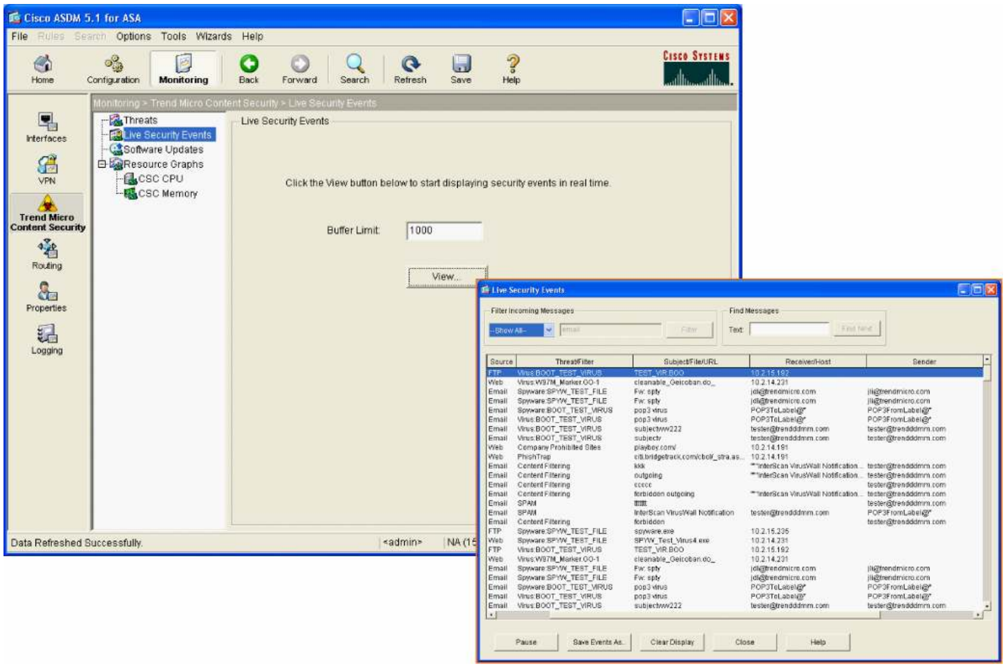
Time	Source	Threat/Filter	Subject/File/URL	Receiver/Host
2005/12/12 19:37:02	Mail	Content Filtering	forbidden	
2003/12/12 04:09:53	FTP	Spyware:SPYW_TEST_FILE	spyware.exe	10.2.15.235
2003/12/11 01:17:44	Web	Spyware:SPYW_TEST_FILE	SPYW_Test_Virus4.exe	10.2.14.231
2004/12/10 11:57:22	FTP	Virus:BOOT_TEST_VIRUS	TEST_VIR.BOO	10.2.15.192

<admin> NA (15) 12/24/05 3:44:25 PM PST

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Within the monitoring section of Cisco ASDM Version 5.1, a rich set of analysis tools provide detailed visibility into threats, software updates, resource graphs, and more. The Live Security Event Monitor (Figure 9) is a new troubleshooting and monitoring tool that provides real-time updates regarding scanned or blocked e-mail messages, identified viruses/worms, and detected attacks. It gives administrators the option to filter messages using regular-expression string matching, so specific attack types and messages can be focused on and analyzed in detail.

Figure 9. Cisco CSC SSM Monitoring Panel and Live Security Event Monitor



Monitoring > Trend Micro Content Security > Live Security Events

Live Security Events

Click the View button below to start displaying security events in real time.

Buffer Limit: 1000

Data Refreshed Successfully.

Text:

Source	Threat/Filter	Subject/File/URL	Receiver/Host	Sender
FTP	Virus:BOOT_TEST_VIRUS	TEST_VIR.BOO	10.2.15.192	
Web	Virus:W97M_Marker.GO-1	cleanable_Geicoban.do_	10.2.14.231	
Email	Spyware:SPYW_TEST_FILE	Fw: spfy	jdl@trendmicro.com	jli@trendmicro.com
Email	Spyware:SPYW_TEST_FILE	Fw: spfy	jdl@trendmicro.com	jli@trendmicro.com
Email	Spyware:BOOT_TEST_VIRUS	pop3 virus	POP3ToLabel@*	POP3FromLabel@*
Email	Virus:BOOT_TEST_VIRUS	pop3 virus	POP3ToLabel@*	POP3FromLabel@*
Email	Virus:BOOT_TEST_VIRUS	subjectww222	tester@trendddmm.com	tester@trendddmm.com
Email	Virus:BOOT_TEST_VIRUS	subjectv	tester@trendddmm.com	tester@trendddmm.com
Web	Company Prohibited Sites	playboy.com/	10.2.14.191	
Web	PhishTrap	citi.bridgetrack.com/cbol/_stra.as...	10.2.14.191	
Email	Content Filtering	kkk	**InterScan VirusWall Notification...	tester@trendddmm.com
Email	Content Filtering	outgoing	**InterScan VirusWall Notification...	tester@trendddmm.com
Email	Content Filtering	ccccc		tester@trendddmm.com
Email	Content Filtering	forbidden outgoing	**InterScan VirusWall Notification...	tester@trendddmm.com
Email	SPAM	ttttt		tester@trendddmm.com
Email	SPAM	InterScan VirusWall Notification	tester@trendddmm.com	POP3FromLabel@*
Email	Content Filtering	forbidden		tester@trendddmm.com
FTP	Spyware:SPYW_TEST_FILE	spyware.exe	10.2.15.235	
Web	Spyware:SPYW_TEST_FILE	SPYW_Test_Virus4.exe	10.2.14.231	
FTP	Virus:BOOT_TEST_VIRUS	TEST_VIR.BOO	10.2.15.192	
Web	Virus:W97M_Marker.GO-1	cleanable_Geicoban.do_	10.2.14.231	
Email	Spyware:SPYW_TEST_FILE	Fw: spfy	jdl@trendmicro.com	jli@trendmicro.com
Email	Spyware:SPYW_TEST_FILE	Fw: spfy	jdl@trendmicro.com	jli@trendmicro.com
Email	Spyware:BOOT_TEST_VIRUS	pop3 virus	POP3ToLabel@*	POP3FromLabel@*
Email	Virus:BOOT_TEST_VIRUS	pop3 virus	POP3ToLabel@*	POP3FromLabel@*
Email	Virus:BOOT_TEST_VIRUS	subjectww222	tester@trendddmm.com	tester@trendddmm.com

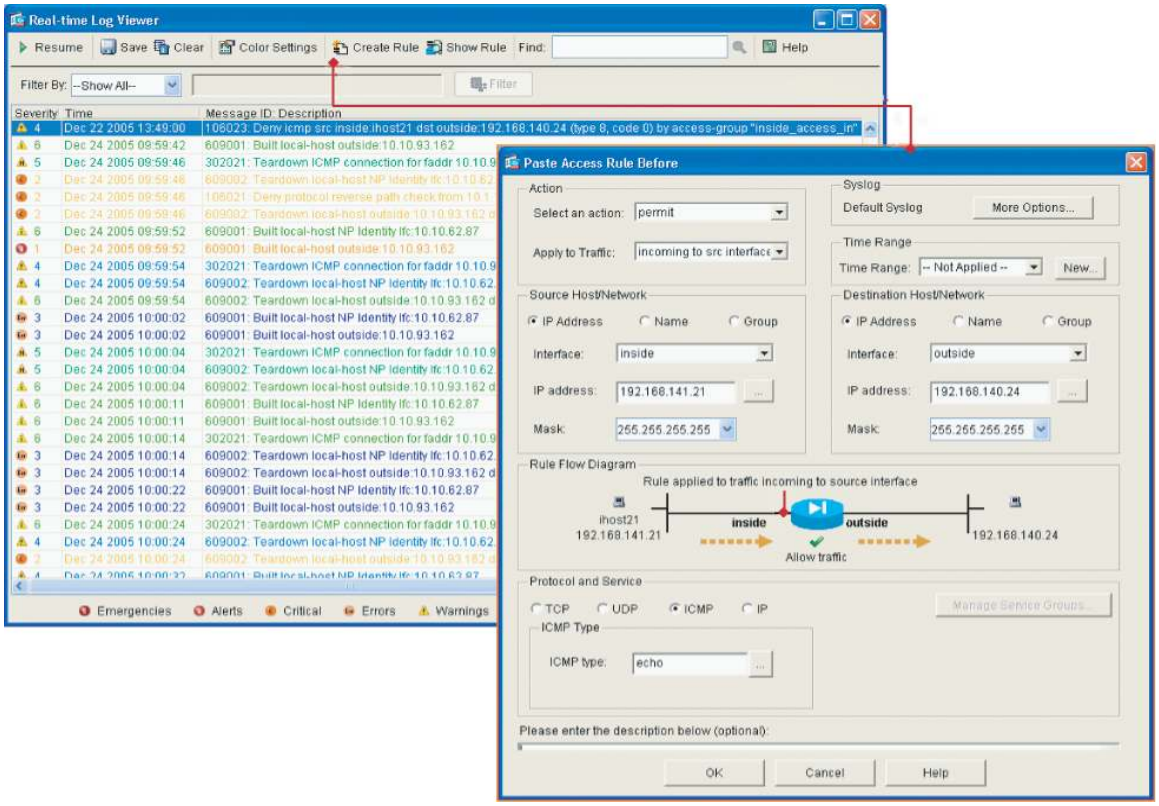
ENHANCED MONITORING AND REPORTING TOOLS ENABLE VALUABLE BUSINESS-CRITICAL ANALYSIS

Syslog to Access Rule Correlation

Cisco ASDM Version 5.1 introduces a new 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. 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 10), 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 10 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.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 10. Syslog to Access Rule Correlation Tool



Filter By: --Show All--

```
Severity Time                  Message ID: Description
4        Dec 22 2005 13:49:00  106023: Deny icmp src inside:ihost21 dst outside:192.168.140.24 (type 8, code 0) by access-group "inside_access_in"
6        Dec 24 2005 09:59:42  609001: Built local-host outside:10.10.93.162
5        Dec 24 2005 09:59:46  302021: Teardown ICMP connection for faddr 10.10.9
2        Dec 24 2005 09:59:46  609002: Teardown local-host NP Identity Ifc:10.10.62
2        Dec 24 2005 09:59:46  106021: Deny protocol reverse path check from 10.1.
2        Dec 24 2005 09:59:46  609002: Teardown local-host outside:10.10.93.162 d
6        Dec 24 2005 09:59:52  609001: Built local-host NP Identity Ifc:10.10.62.87
1        Dec 24 2005 09:59:52  609001: Built local-host outside:10.10.93.162
4        Dec 24 2005 09:59:54  302021: Teardown ICMP connection for faddr 10.10.9
4        Dec 24 2005 09:59:54  609002: Teardown local-host NP Identity Ifc:10.10.62.
6        Dec 24 2005 09:59:54  609002: Teardown local-host outside:10.10.93.162 d
3        Dec 24 2005 10:00:02  609001: Built local-host NP Identity Ifc:10.10.62.87
3        Dec 24 2005 10:00:02  609001: Built local-host outside:10.10.93.162
5        Dec 24 2005 10:00:04  302021: Teardown ICMP connection for faddr 10.10.9
5        Dec 24 2005 10:00:04  609002: Teardown local-host NP Identity Ifc:10.10.62.
6        Dec 24 2005 10:00:04  609002: Teardown local-host outside:10.10.93.162 d
6        Dec 24 2005 10:00:11  609001: Built local-host NP Identity Ifc:10.10.62.87
6        Dec 24 2005 10:00:11  609001: Built local-host outside:10.10.93.162
6        Dec 24 2005 10:00:14  302021: Teardown ICMP connection for faddr 10.10.9
3        Dec 24 2005 10:00:14  609002: Teardown local-host NP Identity Ifc:10.10.62.
3        Dec 24 2005 10:00:14  609002: Teardown local-host outside:10.10.93.162 d
3        Dec 24 2005 10:00:22  609001: Built local-host NP Identity Ifc:10.10.62.87
3        Dec 24 2005 10:00:22  609001: Built local-host outside:10.10.93.162
6        Dec 24 2005 10:00:24  302021: Teardown ICMP connection for faddr 10.10.9
4        Dec 24 2005 10:00:24  609002: Teardown local-host NP Identity Ifc:10.10.62.
2        Dec 24 2005 10:00:24  609002: Teardown local-host outside:10.10.93.162 d
4        Dec 24 2005 10:00:32  609001: Built local-host NP Identity Ifc:10.10.62.87
```

Action
Select an action: permit
Apply to Traffic: incoming to src interface

Syslog
Default Syslog

Time Range
Time Range: -- Not Applied --

Source Host/Network
● IP Address ○ Name ○ Group
Interface: inside
IP address: 192.168.141.21
Mask: 255.255.255.255

Destination Host/Network
● IP Address ○ Name ○ Group
Interface: outside
IP address: 192.168.140.24
Mask: 255.255.255.255

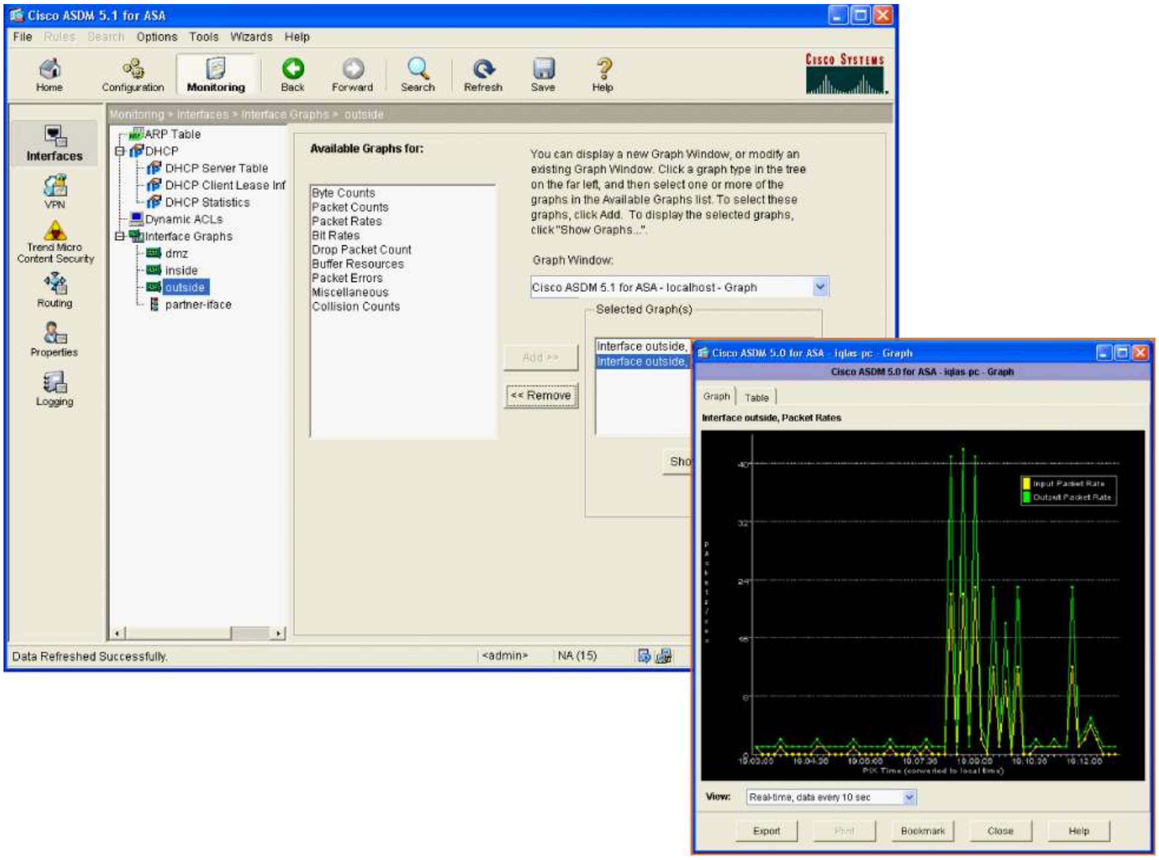
Protocol and Service
○ TCP ○ UDP ● ICMP ○ IP
ICMP Type
ICMP type: echo

Please enter the description below (optional):

Monitoring Tools

Cisco ASDM Version 5.1 offers in-depth monitoring and reporting services in addition to the at-a-glance monitoring capabilities on the new homepage (Figure 11). 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—for example, 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 11. Monitoring on the Cisco ASDM Homepage



You can display a new Graph Window, or modify an existing Graph Window. Click a graph type in the tree on the far left, and then select one or more of the graphs in the Available Graphs list. To select these graphs, click Add. To display the selected graphs, click "Show Graphs...".

Graph Window: Cisco ASDM 5.1 for ASA - localhost - Graph

View: Real-time, data every 10 sec

Data Refreshed Successfully.

- **System graphs**—Provide detailed status information on Cisco ASA 5500 Series and 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 5.1.

Table 1. Table 1. Cisco ASDM Version 5.1 Features and Benefits Summary

Product Features	Benefits
Complete Cisco ASA Software Version 7.1 and Cisco PIX Security Appliance Software Version 7.1 Feature Support	• Provides rich configuration and monitoring support for the new features introduced in Cisco ASA Software Version 7.1 and Cisco PIX Security Appliance Software Version 7.1.
New SSL VPN Features with Cisco Secure Desktop Support	• Makes it easier for users to quickly provision SSL VPN 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. • Enables intuitive management support for all Cisco SSL VPN enhancements delivered by Cisco ASA Software Version 7.1 (complete SSL VPN feature parity with Cisco VPN 3000 Software Version 4.7). • Accelerates the configuration and monitoring of Cisco Secure Desktop parameters, including software updates. • Delivers enhanced at-a-glance, real-time VPN monitoring.
Comprehensive Management and Monitoring Capabilities for the CSC SSM	• Introduces a new CSC SSM homepage to provide at-a-glance information on system licensing, anti X parameters, and system health information. • Blends the Trend Micro and Cisco management interfaces to facilitate easy configuration and monitoring. • Provides a Live Security Event Monitor to provide real-time statistics on the latest viruses, worms, and attacks through the network.
Syslog to Access Rule Correlation, and Customizable Syslog Coloring	• Enables rapid troubleshooting by allowing users to create and modify access rules in real time, by simply clicking on syslog messages in the syslog viewer. • Allows for rapid critical system message identification and convenient syslog monitoring by allowing the colored grouping of syslog messages according to syslog level. Users can select the default coloring options, or create their own unique colored syslog profiles for ease of identification.

LICENSING

Cisco ASDM Version 5.1 is included with Cisco ASA Software Version 7.1 (1) or Cisco PIX Security Appliance Software Version 7.1 and higher. Cisco ASDM Version 5.0 is included with Cisco ASA Software Version 7.0 or Cisco PIX Security Appliance Software Version 7.0 and higher.

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

A separate license for Cisco ASDM is not required, but a DES or 3DES license is required on the host Cisco ASA 5500 Series or Cisco PIX security appliance. Users who currently do not have encryption enabled on their base Cisco ASA 5500 Series 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 Appliance
- **RAM**: 256 MB
- **Flash memory**: 64 MB

Software

- **Cisco ASA Software**: Version 7.1
- **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
- **Flash memory**: 16 MB

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

Software

- **Cisco PIX Security Appliance Software**: Version 7.1
- **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 5.1.

Table 2. Supported Operating Systems and Web Browsers

Operating Systems	Browsers (JavaScript- and Java-Enabled)
• Windows 2000 with Service Pack 4 (English/Japanese) • Windows XP (English/Japanese)	• Microsoft Internet Explorer 6.0 with Java Plug-In v1.4.2 or 1.5.0 • 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 or 1.5.0

Note: Cisco ASDM Version 5.1 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 is 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

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- **Cisco PIX Security Appliances**: http://www.cisco.com/go/pix
- **Safe Blueprint from Cisco**: http://www.cisco.com/go/safe

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.**

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Printed in USA C78-60047-02 08/07