
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 its 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.

DASHBOARD SUPPLIES ADMINISTRATORS WITH VITAL REAL-TIME SYSTEM STATUS INFORMATION

Cisco ASDM Version 5.2 includes a dynamic dashboard that provides 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 and severity-based coloring 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.
QUICK INSTALL WIZARDS ACCELERATE SECURITY APPLIANCE DEPLOYMENT

Cisco ASDM features a host of intelligent wizards that accelerate the deployment of Cisco ASA and Cisco PIX security appliances in diverse firewall and VPN environments. Using a series of simple step-by-step configuration panels, the Startup Wizard helps 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. The VPN Wizard uses a similar set of intelligent panels to help users quickly set up site-to-site VPN tunnels for extending secure business connectivity, or remote-access VPN tunnels to allow secure employee access to corporate resources.

Cisco ASDM Version 5.2 introduces a High-Availability and Scalability Wizard that enables rapid security deployment in networks that require resiliency in the form of failover or VPN clustering. This new wizard allows users to quickly set up their Cisco ASA or Cisco PIX security appliances in Active/Active or Active/Standby high-availability modes using a single management interface. This intuitive wizard simplifies the entire deployment process and eliminates configuration errors by first checking both participating appliances for connectivity and compatibility, and then proceeding to install the necessary parameters on the respective units. It also supports the VPN clustering and load-balancing feature of Cisco ASA security appliances, which allows users to gracefully scale their VPN user capacity. It allows both the integration of a Cisco ASA appliance into an existing cluster or the initialization of a new cluster, in a matter of minutes. A Cisco ASA Adaptive Security Appliance VPN Cluster can support up to a maximum of 10 units. Figure 2 shows the High-Availability and Scalability Wizard as it configures Active/Active high availability.
 PACKET TRACER UTILITY FOR RELIABLE SECURITY POLICY VALIDATION AND ENFORCEMENT

As modern network environments adapt to support advanced converged security services, and as businesses continue to expand to new boundaries and scale to higher user densities, network security policies become increasingly complex. Policies rely on multiple network elements, and enforcing them and managing changes becomes an arduous day-to-day task. At the same time, troubleshooting and monitoring updates requires expertise that comes with a higher cost of maintenance.

Cisco ASDM Version 5.2 introduces a revolutionary patent-pending Packet Tracer utility that enables rapid troubleshooting for security appliance deployments of any nature, including those with complex security policies, numerous access rules, or layered security services. By employing an animated packet flow model, the Packet Tracer utility allows the security administrator to emulate a TCP/UDP/IP flow sequence that can be targeted toward any specific application or protocol. Upon starting the Packet Tracer, this emulated packet is virtually passed through the entire device configuration. As it flows through the configured parameters, Cisco ASDM provides visual aids to indicate the status of each transaction, and the action performed at that stage of that packet’s lifetime. Visual indicators at each stage notify administrators of incorrect policy definition, which can be in the form of erroneous network translation policies, or access-rules, inspection engines, and Cisco Security Service Modules (Figure 3). Administrators can simply click on the highlighted policy in error, which opens an editing panel for exploration-free quick troubleshooting. A successful pass-through indicates that security policies are accurately deployed and can handle live traffic predictably.
ROBUST SECURITY POLICY MANAGEMENT LOWERS OPERATIONAL COSTS

Cisco ASDM Version 5.2 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. This release adds complete management support network, service, protocol, and Internet Control Message Protocol (ICMP)-type object groups. It supports the powerful access control features offered by both Cisco ASA Software Version 7.0 and Cisco PIX Security Appliance Software Version 7.2, such as user- and group-based access lists, time-based access lists, and inbound/outbound access lists.

Cisco ASDM Version 5.2 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 4). It also provides a new Rule Query option to allow administrators to quickly filter the various network elements and object groups of interest for focused monitoring and troubleshooting security policies that employ them.
BUSINESS-CLASS SECURITY SERVICES ENFORCE SECURE, ROLE-BASED ADMINISTRATIVE ACCESS

Cisco ASDM Version 5.2 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 5.2 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 5.2 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 such as VPN client security posture enforcement, automatic software updating, VPN clustering, and more.

On the Cisco ASA 5500 Series, Cisco ASDM integrates rich Cisco WebVPN management features (Figure 5) to allow administrators to quickly provision and enable remote-access connectivity from any Internet-enabled Web browser and its native SSL encryption.
Cisco ASA Software Version 7.0 and Cisco PIX Security Appliance Software Version 7.2 offer a wide range of application inspection and control services for a suite of protocols such as HTTP, FTP, instant messaging protocols, Session Initiation Protocol (SIP), Skinny Call Control Protocol (SCCP), H.323, GPRS Tunneling Protocol (GTP), DNS, Microsoft and Sun Remote Procedure Call (DCE-RPC and SunRPC), and more. Cisco ASDM Version 5.2 enables the accelerated deployment of these rich application security services by enabling preconfigured Low, Medium, and High security profiles (Figure 6 shows the Medium security profile for SIP). Basic application security deployments can use these preconfigured profiles to allow the quick pass-through of supported applications and protocols across the security appliances with the required level of security. This version also allows the customization of any of these preconfigured profiles to allow microscopic control over traffic flows and provide advanced applications with a stronger protection profile. Users can also create their own regular-expression-based signatures for dynamic threat protection against new application vulnerabilities and attacks. Using this unique blend of preconfigured profiles and customizable point-and-click options that have been conditioned by intelligent application defaults, Cisco ASDM Version 5.2 enables the rapid deployment of Cisco ASA and Cisco PIX security appliances to protect mission-critical applications and sensitive resources from application misuse and tunneling attacks.
INTELLIGENT USER INTERFACE SIMPLIFIES INTEGRATION INTO COMPLEX NETWORK ENVIRONMENTS

Cisco ASDM Version 5.2 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 need complete visibility into all virtual firewalls and features on the system (Figure 7). Individual context users get the same Cisco ASDM interface, 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 Version 5.2 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 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.

**ADAPTABLE SECURITY MANAGEMENT INTERFACE ENHANCES THE UNIFIED THREAT MANAGEMENT EXPERIENCE**

Cisco ASDM Version 5.2 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 5.2 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 accurate prevention technologies such as Cisco Traffic Risk Rating and the Cisco Meta Event Generator (Figure 8). 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.
Cisco ASDM Version 5.2 also provides a new Intrusion Prevention homepage for the AIP-SSM, along with real-time monitoring panels. Once an AIP-SSM is installed, the main ASDM homepage is automatically updated to display a new Intrusion Prevention panel (Figure 9), which provides a historic view into IPS statistics, system resources, threat alerts, and more.
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, delivering 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 5.2 delivers an industry-first solution that blends the simplicity of Trend Micro’s HTML-based configuration panels with the ingenuity of Cisco ASDM (Figure 10). This helps ensure consistent policy enforcement, and simplifies the complete provisioning, configuration, and monitoring processes for these rich unified threat management functions.
Cisco ASDM Version 5.2 provides a complementing 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 11), which provides a historic view into threats, e-mail viruses, live events, and vital module statistics such as last installed software/signature updates, system resources, and more.
Within the monitoring section of Cisco ASDM Version 5.2, a rich set of analysis tools provide detailed visibility into threats, software updates, resource graphs, and more. The Live Security Event Monitor (Figure 12) 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.
ENHANCED MONITORING AND REPORTING TOOLS ENABLE VALUABLE BUSINESS-CRITICAL ANALYSIS

**Syslog to Access Rule Correlation**

Cisco ASDM Version 5.2 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 13), 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 13 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.
Monitoring Tools
Cisco ASDM Version 5.2 offers in-depth monitoring and reporting services in addition to the at-a-glance monitoring capabilities on the new homepage (Figure 14). 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 14. Monitoring on the Cisco ASDM Homepage

System graphs—Provide detailed status information on Cisco ASA 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, 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; 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 5.2.
Table 1. Cisco ASDM Version 5.2 Features and Benefits Summary

<table>
<thead>
<tr>
<th>Product Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete Cisco ASA Software Version 7.2 and Cisco PIX Security Appliance Software Version 7.2 feature support</td>
<td>• Provides rich configuration and monitoring support for new features introduced in Cisco ASA Software Version 7.2 and Cisco PIX Security Appliance Software Version 7.2</td>
</tr>
</tbody>
</table>
| Patent-pending Packet Tracer utility | • Accelerates the troubleshooting process that verifies the impact of real traffic flows on entire system configuration  
• Sketches animated results as each policy is rigorously tested and provides direct links to correct failed tests for exploration free policy tuning |
| Profile based management for all application inspection and control capabilities | • Uses preconfigured Low, Medium, and High security profiles for each of the application inspection engines for rapid deployment in any security environment  
• Enables the granular customization of any of the security profiles to cater to the needs of advanced applications  
• Provides easy integration of user-defined regular expressions into existing security policies to allow rapid threat mitigation against new and upcoming application attacks |
| New High-Availability and Scalability wizard | • Simplifies the deployment of Active/Active and Active/Standby high availability or VPN clustering and load balancing features through the convenience of a single management connection  
• Helps ensure comprehensive connectivity testing and error verification for smooth and accurate deployment |
| Integrated security policy and access control table | • Enhances the policy configuration and management experience by providing a streamlined, in-depth perspective into all the access rules, AAA, and security policies of the system  
• Facilitates rapid troubleshooting through a new rule query option that enables administrators to quickly search for network elements and the policies employing them  
• Enables the rapid editing of all network and service object groups via a new object group selector panel |
| Troubleshooting enhancements | • Integrates syslog references to provide brief explanations and recommended actions for each message for isolating and resolving security issues quickly  
• Enables the parsing of syslog messages for customizable views based on time, date, syslog IDs, and IP addresses  
• Provides Traceroute support for network connectivity testing and verification  
• Delivers an ASDM Assistance Guide that provides task-oriented methods to configure features such as AAA, logging filters, SSL VPN client, and more |

LICENSING
Cisco ASDM Version 5.2 is included with Cisco ASA Software Version 7.2 (1) or Cisco PIX Security Appliance Software Version 7.2(1), and higher.

A separate license for Cisco ASDM is not required, but 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 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 5505, 5510, 5520, 5540, or 5550 Adaptive Security Appliance
- RAM: 256 MB
- Flash memory: 64 MB
Software
- Cisco ASA Software: Version 7.2
- 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 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 7.2
- 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 5.2.

Table 2. Supported Operating Systems and Web Browsers

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Browsers (JavaScript- and Java-Enabled)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 with Service Pack 4</td>
<td>Microsoft Internet Explorer 6.0 with Java Plug-In v1.4.2 or 1.5.0</td>
</tr>
<tr>
<td>(English/Japanese)</td>
<td>Firefox 1.5 with Java Plug-in v1.4.2 or 1.5.0</td>
</tr>
<tr>
<td>Windows XP (English/Japanese)</td>
<td>Netscape Communicator 7.2 with Java Plug-In v1.4.2 or 1.5.0</td>
</tr>
<tr>
<td>Sun Solaris 2.8 or higher running CDE</td>
<td>Mozilla 1.7.3 with Java Plug-In v1.4.2 or 1.5.0</td>
</tr>
<tr>
<td>Red Hat Linux 9.0 running GNOME or KDE</td>
<td>Firefox 1.5 with Java Plug-In v1.4.2 or 1.5.0</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux WS Version 3</td>
<td></td>
</tr>
</tbody>
</table>

Note: Cisco ASDM Version 5.2 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)
SERVICE AND SUPPORT

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, see Cisco Technical Support Services or Cisco Advanced Services.

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 Appliances:
http://www.cisco.com/go/pix

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

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 Appliances:
http://www.cisco.com/go/pix

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