Cisco Security Manager

CISCO SECURITY MANAGER IS A SCALABLE, COMPREHENSIVE SECURITY MANAGEMENT SYSTEM FOR CISCO PIX™ FIREWALLS. WITH SECURITY MANAGER, CISCO CUSTOMERS CAN DEFINE, DISTRIBUTE, ENFORCE, AND AUDIT MULTIPLE DISTRIBUTED FIREWALL SECURITY POLICIES FROM A CENTRAL LOCATION. AS THE MANAGEMENT CORNERSTONE OF THE CISCO END-TO-END SECURITY PRODUCT LINE AND A FUNDAMENTAL ELEMENT OF CISCOASSURE POLICY NETWORKING, SECURITY MANAGER CAN DRAMATICALLY SIMPLIFY FIREWALL MANAGEMENT.

Security Manager streamlines the tasks of managing complicated network security elements, such as perimeter access control and Network Address Translation (NAT). With the Security Manager intuitive graphical user interface, administrators can visually define high-level security policies for multiple Cisco PIX firewalls. Once created, these policies can be distributed from a central management system—completely eliminating the costly, time-consuming practice of implementing security commands on a device-by-device basis. In addition, Security Manager provides robust system auditing functions, including real-time alarm notification and a Web-based reporting system.

Cisco Security Manager also introduces the policy-based management foundation that will be extended in the future to support comprehensive Cisco security solutions, which include Cisco IOS® Firewall, IPSec encryption, user identity/authentication, vulnerability scanning, and intrusion detection technologies.

Solution Overview

Cisco Security Manager provides a centralized, coordinated mechanism for Cisco PIX Firewall policy management. Through its innovative product architecture, robust functionality, and easy-to-use, Windows-based interface, Cisco Security Manager provides an effective, secure system that manages the definition, enforcement, and auditing of Cisco PIX Firewall policies.

Policy Definition

Through the Cisco Security Manager graphical user interface, Policy Manager, administrators can visually create high-level security policies by specifying business objectives. This can streamline policy management for a large, distributed PIX Firewall implementation. Policy Definition capabilities include the following:

- Ability to create security policy abstracts that define resource availability through PIX Firewalls
- Policy validation mechanisms
- Grouping metaphors for services and network addressing
- Ability to determine which PIX firewalls require policy modifications
- Easy NAT management to dramatically improve integrity and confidentiality—includes unidirectional or bidirectional mapping of IP addresses, internal source address translation, and exposed services remapping

Policy Enforcement

Cisco Security Manager also provides a flexible and robust mechanism to distribute and enforce defined policies. Through the Policy Manager, an administrator can easily create a network topology and identify the devices on which policy should be enforced. Through a simple, Windows-based drag-and-drop process, the administrator can easily apply security policies to the appropriate PIX firewalls and verify correct operation. Policy Enforcement capabilities include the following:

- Automated translation of high-level business policies into the specific command-line configurations required to implement the security policies on the firewalls
- Distribution of configuration commands to the appropriate firewalls, which eliminates the need to configure firewall policy on a localized, device-by-device basis
- Easy verification of policy assignment and system operation

- Simple, graphical modification and redistribution of firewall policy when changes are required

Policy Auditing

Cisco Security Manager also provides a robust auditing system that enables administrators to log, monitor, alert, and report security policy events. All PIX Firewall events are generated via syslog and are read, logged, and acted upon as appropriate. In addition, Security Manager provides the flexibility to direct syslog messages to the appropriate targets in an administrator's environment. This enables other management systems to use event messages and syslog output for analysis and response purposes. Policy Auditing capabilities include:

- Real-time alerting to administrators about important security and integrity issues, such as policy breaches or network attacks. Automated responses include real-time e-mail, pager, visual, and script notifications
- Ability to define alerts on the basis of predefined event categories, specific events, or custom event categories defined for collections of events
- Web-based reporting system, which enables an administrator to quickly and easily analyze historic system events, summarize and consolidate this information, and generate meaningful reports on demand or on a scheduled basis
- Ability to send event messages and syslog output to third-party systems

Applications

As organizations continue to leverage the Internet for electronic commerce, corporate intranets, extranets, and other advanced applications, network security becomes increasingly critical. In the face of an escalating threat, most organizations have deployed firewalls to improve perimeter security and protect network integrity. However, to minimize costs and ensure consistent, robust security, organizations require the ability to manage these firewalls with a single, centralized management system.

Cisco Security Manager supports the diverse requirements of Cisco customers, including small to medium-sized businesses looking to establish an Internet connection; large enterprises with multiple, distributed PIX firewalls; and service providers looking to provide managed firewall services. The Security Manager distributed architecture and remote management capability enable deployment in a multitude of environments and provide significant flexibility to customers.

Features and Benefits Summary

Features	Benefits
Centralized Management for Cisco PIX Firewalls	• Provides centralized, coordinated management system for a large, distributed implementation of Cisco PIX firewalls • Dramatically simplifies management requirements and costs
Scalability	• Provides management support for up to 100 Cisco PIX firewalls • Enables an organization to meet large-scale security requirements and support network growth
Distributed Architecture for Internet, Intranet, and Extranet Support	• Supports PIX Firewall implementations in multiple topologies—Internet, intranet, or extranet—to meet the diverse requirements of Cisco customers • Provides flexible deployment of major system components to serve an array of implementation scenarios
Remote Firewall Configuration Capability	• Enables enterprise-wide modifications without the support of local or field network administrators • Promotes centralization of key security personnel resources and consistent policy implementation throughout the network
High-Level Policy Management	• Allows the administrator to define security policies by specifying business objectives; enables an organization to accurately define its security policies and easily map requirements to the network • Removes the administrator from having to implement security configuration information via CLI on a device-by-device basis; dramatically reduces security administration and cost of ownership
Centralized Visual Security Policy Development	• Allows an administrator to define policy quickly and easily using a simple graphical user interface • Provides the ability to define abstract security policies and distribute them to specific PIX firewalls via a drag-and-drop approach
Network Address Translation (NAT) Management	• Provides an easy mechanism to define and manage NAT policies for Cisco firewalls • Enables an administrator to hide internal addresses from external view, specify how network services should be exposed, and create one-to-one address mapping
Consistency Checking Mechanism	• Validates policy consistency prior to distribution
Configuration Roll-Back Mechanism	• Enables automated configuration roll-back to previous policy
Built-in Auditing and Reporting System	• Provides real-time alarms via e-mail, pager, visual, and script notifications • Provides a Web-based reporting system for on-demand and scheduled report generation; reports present critical warning and usage information • Supports interoperability with third-party reporting systems

Features	Benefits
Windows-Based System Managed from Windows 95/98/NT	• Simplifies installation and reduces costs • Leverages familiar, easy-to-use environment • Employs standard industry platforms

Specifications

Hardware Recommendations

- Intel-based Pentium II processor, 400 MHz
- 128 MB RAM
- 4 GB free hard drive space available
- Video display, 800 x 640, with 256 colors minimum

Software Requirements

- Microsoft Windows NT Server Version 4.0 with Service Pack 4
- Microsoft Internet Explorer Version 4.0 or later

Devices Supported

- PIX Firewall with software v4.2.2

Cisco Service and Support Options

Cisco Security Manager is supported under the Cisco Software Application Service program. Customers can purchase Cisco Security Manager with a support contract.

Service and support for Cisco Security Manager is available on a one-time or annual contract basis. Support ranges from help desk assistance to proactive, onsite consultation. Software subscription service is also available for Cisco Security Manager. Software Application Service provides 24 x 7 technical support (online or by telephone) and access to Cisco Connection Online (CCO). Contact a local Cisco sales office for further information.

Ordering Information

Cisco Security Manager is scheduled to be orderable in Q2CY'99. To order Cisco Security Manager, contact a local Cisco sales representative.

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

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

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

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Connection Online Web site at http://www.cisco.com/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • 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 • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela