CHAPTER 1

Overview of the Cisco Centri Firewall Product

Introduction

This chapter introduces the various common components in the Cisco Centri Firewall product. Cisco Centri Firewall's modular architecture ensures that you can find solutions to new attack scenarios quickly and effectively. When you invest in Cisco Centri Firewall, you can rest assured that you have a simple upgrade path to more advanced security solutions. The product's design supports your growing network security needs and your investment in time spent learning and configuring the product.

In addition, your investment in Windows NT training does not go to waste. Cisco Centri Firewall allows you to administer security policies based on Windows NT Domains, Group accounts, and User accounts. You can securely administer your firewalls from any Windows NT computer on your network, and you can also administer your firewalls over a remote access services (RAS) connection hosted by a server that resides behind the firewall server on your network.

The following sections describe the primary features of the Cisco Centri Firewall product.

The Building Blocks of Cisco Centri Firewall

The Cisco Centri Firewall is based on an agent-oriented architecture that composes the five basic building blocks: the Security Subsystem, Security Knowledge Base, Reporting Subsystem, Monitoring Subsystem, and the Administrating Agent. The following sections introduce these basic building blocks.

Security Subsystem

The Security Subsystem enforces network security on the firewall server. It is responsible for capturing and monitoring all network traffic, detecting packet and data discrepancies, and enforcing security policies. The Security Subsystem thoroughly evaluates all network traffic entering or leaving the firewall server according to the active security policies. This subsystem includes the components required to authenticate end users of the security system's services. In addition, the Security Subsystem is responsible for logging all system and network traffic audit records to the Security Knowledge Base, performing system integrity checks, and authenticating the other components within the security system.

Security Knowledge Base

The Security Knowledge Base is a proprietary knowledge-based system that persistently stores configuration information, as well as audit records generated by the security system. It combines knowledge representation technology from the artificial intelligence community with object-oriented technology from the programming community to enable agents within the Cisco Centri Firewall to communicate with each other and to store data using a flexible information representation.

Reporting Subsystem

The Reporting Subsystem is responsible for generating statistical reports that provide detailed and summary information about network activity that passes across the Cisco Centri Firewall. This subsystem generates on-demand reports, which provide statistics about the running system whenever the administrator wants to view them. It also generates scheduled reports based on time periods and content choices specified by the administrator. Typical scheduled reports are daily, weekly, and monthly usage statistics, as well as network service breakdowns. Reports can be viewed with basic file editing tools or through Web browsers.

Monitoring Subsystem

The Monitoring Subsystem generates all statistical data and processes all system audit events within the Cisco Centri Firewall. It derives higher level knowledge about what is happening in the system based on what specific combinations of audit events mean from a security perspective. It also monitors all data in the Security Knowledge Base looking for audit records that indicate possible ongoing attacks and other events of interest to the security of the system. It alerts the administrator when it detects such events and can use e-mail, pager, and on-screen alerts.

Administrative Agent

The Administrative Agent is the native Windows NT graphical user interface for Cisco Centri Firewall and is responsible for translating between user input and information that other agents can understand and process. It presents system data in human-readable form and organizes it in ways that are meaningful to the end user. Its primary purpose is to simplify administration by shielding users from as much technical and system implementation detail as possible. Using the Administrative Agent, the user can develop and modify security policies, identify and organize network objects and users, define and organize network services, and apply security policies to network objects.

Feature Summary

This section summarizes the features available in Cisco Centri Firewall. These features are divided into three categories: high-level features, provided network services, and provided network applications.

High-Level Features

Table 1-1 presents the high-level features of Cisco Centri Firewall.

Table 1-1 **High-Level Features of Cisco Centri Firewall**

High-Level Feature List
Kernel Proxy Architecture
Centralized Knowledge Base
Basic Network Address Translation
Authenticate Administrators
System Integrity Checks
Java Applet, ActiveX Control, and VBScript\JavaScript Blocking

Table 1-1 High-Level Features of Cisco Centri Firewall (Continued)

High-Level Feature List
HTTP Object Filtering
Wizard-based Installation
Decision Tree-based Security Policies
Policy Checks based on Time of Day, Day of Week, Destination, and Network Service
Apply Policies to Windows NT Domains, Group, and User Accounts
Apply Policies to Logical and Physical Network Objects
HTML-based Report Formats
Real-Time Visual and E-mail-based Notifications
Audit Event Filtering
Expose Internal Network Servers to External Networks
Customizable Network Services and Applications
Remote User Authentication
Secure Remote Administration
Configurable Notification Methods and Thresholds
Pager-based Notifications
Archival to OBDC-compliant Databases

Network Service Support

Table 1-2 lists the network service supported by Cisco Centri Firewall. Because you can define new network services, this list is not finite.

Table 1-2 Network Services Supported by Cisco Centri Firewall

Network Service List
ICMP
Telnet
Gopher
FTP
NNTP
SMTP
POP-2
POP-3
LDAP
DNS
IMAP
HTTP
Secure Sockets Layer-based HTTP (SLL)
Custom Network Services based on IP, ICMP, TCP, and UDP

Network Application Support

Table 1-3 lists the network applications supported by Cisco Centri Firewall. Because you can define new network applications, this list is not finite.

Table 1-3 Network Applications Supported by Cisco Centri Firewall

Network Application List
America Online Service (AOL)
CompuServe Information Service (CIS)
The Microsoft Network (MSN)
VDOLive
RealPlayer (RealAudio and RealVideo)
Lotus Notes
Netscape CoolTalk
Netscape Mail Server
Netscape Navigator
Netscape News Server
Microsoft Exchange
Microsoft Internet Explorer
Microsoft NetMeeting
Additional Network Applications and Bundled Applications

The next chapter explains the security threats that exist for organizations wanting to connect to the Internet. In essence, it provides a basis for understanding what the Cisco Centri Firewall protects against.