

Delivering End-to-End Security in Policy-Based Networks

The Need for Policy-Based Security

The growth of open computing has generated enormous advances in the way the world does business. The ubiquity and strength of the Internet have broadened the digital advantage, bringing main-line business operations closer to branch offices, suppliers, vendors, and customers through enhanced availability and instant communication. Digital systems enable companies to greatly reduce operations costs and time to market. In fact, companies cannot compete in today's global economy without them. In the last five years, networks have become a strategic business asset to improve operational efficiency, enhance productivity, and provide new customer services. The new "open systems" environments are inherently insecure; therefore, it is vital to protect mission-critical traffic throughout intranets, extranets, and electronic commerce applications.

Investments in enterprise security protect business productivity and ensure customer confidence. A solid security foundation helps companies build trust with their employees, suppliers, partners, and customers—trust that information is protected and transactions are reliable. An adequate security solution must pervade all users, hosts, gateways, and applications. The network is a logical place to invest in security because it touches all points. It is also more efficient and reliable to centrally manage security policy rather than rely upon users, who are prone to forgetting, misapplying, or even abusing security procedures.

Complex security technologies are necessary to protect highly available mission-critical networks from corruption and intrusion. Of particular interest in the past few years is protecting geographically dispersed enterprise networks, which use a combination of public and private WAN lines to connect remote and branch offices to major centers. Intranets, extranets, Internet connections, WANs, and LANs each have unique security requirements. Many companies wish to extend their mission-critical applications to remote offices via an intranet or communicate directly with industry partners, suppliers, and key customers via extranets. These technologies enable organizations to securely conduct business in today's open environments.

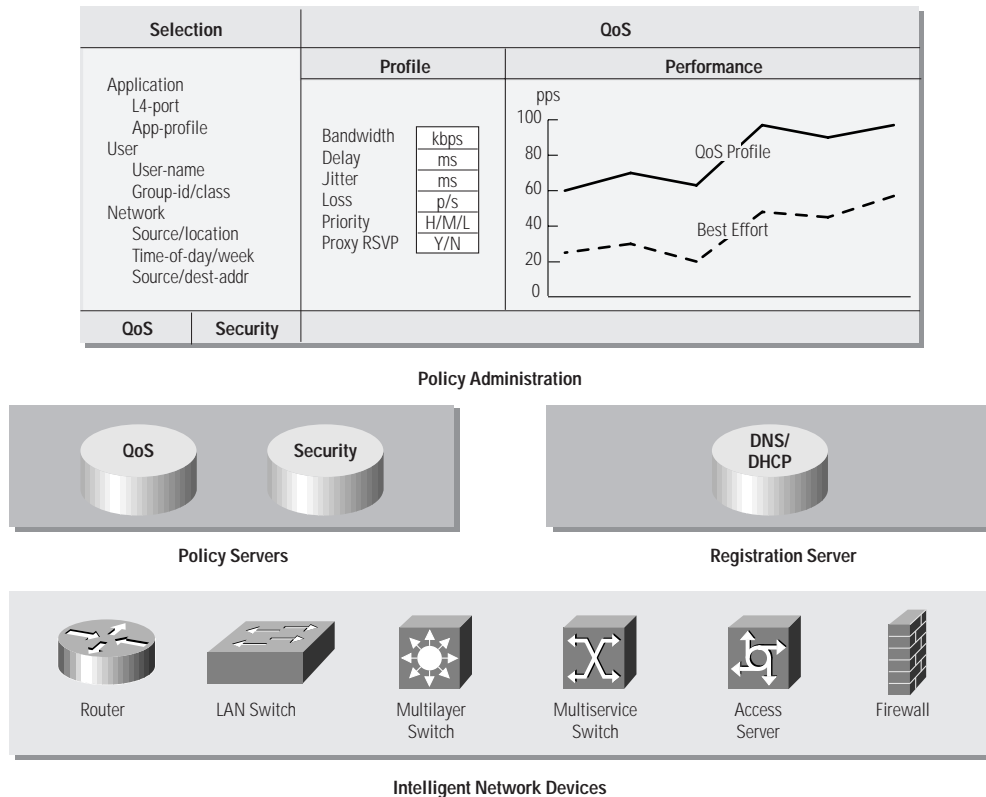
Yet with all the advanced capabilities of today's applications, it is surprising to find that the task of securing the complex networks that support them is still done by hand. Administrators often use detailed command-line interfaces (CLIs) to configure network devices one at a time across distributed enterprises. What's more, when policies change, implementation takes time. In very large networks, scalability issues can make security deployment quite expensive and can lead to misconfigured systems and inconsistent policy enforcement. No centralized, coordinated mechanism exists to implement a consistent policy throughout the network, verify that it is installed and functioning properly, change it easily as required, or detect attacks, mistakes, and misuse within the network.

Cisco Systems believes that administrators should be able to define, deploy, and enforce a security policy without requiring network administrators to work one-by-one across dozens, perhaps hundreds or thousands, of devices. This paper focuses on describing end-to-end security policy management through the CiscoAssure policy networking initiative. CiscoAssure policy networking places a layer of intelligence between the administrator and the network itself. This layer provides translation between the intuitive policies developed to support business processes and the implementation of it in network devices. This feature simplifies and organizes the task of consistently enforcing security policy throughout large, distributed networks. By automating the implementation and centralized administration of a robust, end-to-end security solution, CiscoAssure lets organizations securely leverage the power of networks to improve productivity and lower costs.

CiscoAssure: End-to-End Security Policy Management

Planning, deploying, and enforcing security policies historically have been very time-intensive—and thus expensive. It is also true that effectively implementing an end-to-end security policy in enterprise networks requires staff expertise that is in short supply worldwide. Cisco Systems answers the business and technical needs for simplified, automated network control with CiscoAssure, its new policy-based networking initiative. CiscoAssure is a family of policy elements based upon four major building blocks (Figure 1).

Figure 1 CiscoAssure Architecture



The building blocks are:

- **Intelligent network devices**—Network devices must be “application-aware,” that is, capable of interpreting policy instructions and applying security controls for each user or application.
- **Quality of service (QoS) and security policy services**—Server-based control systems that provide the interface between the administrator and network. Translation capabilities make it possible to automate actual device configuration throughout the network from a central console and optimize that network according to policy. Security is communicated to network elements using Common Open Policy Service (COPS) protocol.
- **Registration and directory services**—Provide dynamic binding between policy services and network addresses, user profiles, application profiles, and other information vital to proper policy implementation and enforcement. These services are based upon a Domain Name Server/Dynamic Host Configuration Protocol (DNS/DHCP) server system and Lightweight Directory Access Protocol (LDAP)v3-based directories.
- **Centralized policy administration**—The administrator interacts with the CiscoAssure policy server system via a graphical user interface (GUI) that simplifies policy definition and provides the capability to centrally configure business rules and map these rules onto the intelligent network. The GUI gives administrators multiple levels of control to accept/deny traffic and impose policy based on IP address, application, user, time of day, or location. This GUI lets administrators create and enforce consistent policies across multiple Cisco security elements such as routers, firewalls, and intrusion-detection devices.

The focus of this paper is on security policy management as part of the CiscoAssure initiative, which provides an end-to-end security management system and architecture encompassing all Cisco security solution components. Security solution offerings can be grouped into the following technology “families:”

- **Identity**—Who is allowed to do what from where? Cisco currently offers the CiscoSecure authentication, authorization, and accounting (AAA) server, and digital certificate solutions with partners Verisign, Entrust, Microsoft Corporation, and Netscape Communications.

- **Integrity**—Protects information and resources from unauthorized access. The Cisco firewall offerings include the PIX™ Firewall and the Cisco IOS® Firewall feature set. Other Cisco IOS integrity features include access control lists (ACLs), and IPSec-based encryption.
- **Active audit**—Monitors network traffic, identifies security risks, enforces security policy, and eliminates unauthorized activity. Cisco products in this area include the NetRanger™ system, a real-time intrusion-detection system, and the NetSonar™ scanner, a proactive vulnerability scanner.

A robust security solution includes components from all of these technology families to create an intelligent, self-defending network environment. Yet the most critical component is the ability to manage the entire system. CiscoAssure provides this vital piece of the security puzzle, with a centrally manageable, comprehensive system and architecture.

Why Cisco?

For a policy networking solution to be truly effective, it must meet three criteria. Cisco Systems is the only networking vendor that meets all three.

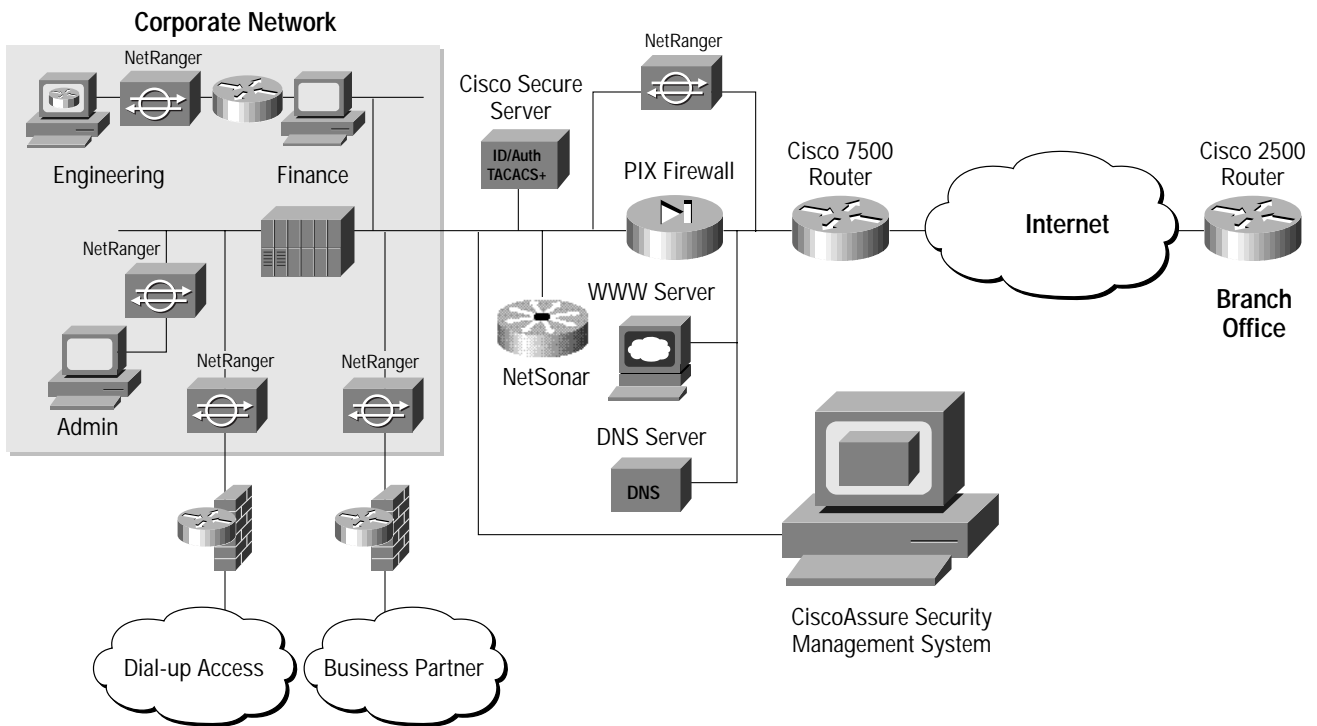
- First, the solution must be deployable end to end across very large networks, spanning multiple media and protocol environments. It must implement policy seamlessly across intranets, extranets, and virtual private networks, no matter the underlying infrastructure. Cisco has a proven track record of interoperability in heterogeneous networks with its embedded Cisco IOS software and compatible appliances.
- Second, a solid policy networking solution requires an intelligent network infrastructure for robust policy implementation and enforcement. Cisco networks contain embedded technologies that provide this intelligence—through Cisco IOS software and technologies in switches and routers—and optimized features in Internet appliances such as the Cisco PIX Firewall
- Third, the solution must be centrally manageable, with capacity for high scalability. The CiscoAssure initiative is designed to deliver policy networking from a centralized location for entire enterprise networks. Its very design concept provides for scalability by automating work now done manually, one device at a time.

How CiscoAssure Works

Let's say that an organization sets a simple security policy such as, "no Telnet access permitted into the router protecting the Engineering R & D server at any time." How would network managers use CiscoAssure policy networking to implement and enforce this policy? First, the policy is entered at the central administration GUI, with encrypted commands communicated to the network devices via COPS as policy binding information. Cisco security devices translate policy binding information and modify local security enforcement mechanisms (router ACLs, firewall policy filters, NetRanger alarm settings, and so on) as required.

How does CiscoAssure intelligently enforce and modify this policy? Imagine that a rogue engineer enters the enterprise network from a remote location. Let's assume that the engineer's communication is encrypted at the remote office branch Cisco 2500 router, using IPSec, and decrypted at the corporate PIX Firewall located behind a Cisco 7500 router (Figure 2). The intruder is authenticated via the CiscoSecure access control server using the TACACS+ protocol. Then the PIX Firewall grants access to the network.

Figure 2 Enforcing a Security Policy



Suppose this engineer then attempts to telnet into the Engineering R & D router previously mentioned in the policy. The Cisco NetRanger system detects this unauthorized activity in real time and sends an alarm to the central administration console. At this point, the CiscoAssure policy management system would dynamically modify either the Cisco 7500 router ACLs or PIX Firewall policy filters to automatically eliminate the unauthorized activity and "shun" the intruder from the network. Detailed alarms, logs, and reports provided by the CiscoAssure policy management system allow administrators to examine the incident in more detail and understand the organization's security posture. The result is an intelligent, self-defending network that is managed by CiscoAssure and driven by the security policy.

The Cisco Advantage for End-to-End Security

Security continues to be a significant concern in organizations that leverage networking technology to compete in today's global economy. Currently, security management is a daunting task, lacking a centralized mechanism for consistent policy implementation, verification, and enforcement in distributed enterprise networks.

Cisco is committed to providing enterprise network managers with a comprehensive security management solution that gives them the ability to minimize and manage risk. The CiscoAssure policy networking initiative provides a single, comprehensive system and architecture so that Cisco security solutions conform to an organization's policies. CiscoAssure enables efficient administration of an intelligent network infrastructure that addresses most of the major security concerns, freeing administrators to focus valuable time and resources on other issues.



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 6918 61 00
Fax: 33 1 6928 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>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China (PRC) • Colombia • Costa Rica • Czech Republic • Denmark
England • France • Germany • Greece • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Russia • Saudi Arabia • Scotland • Singapore