



WHITE PAPER

CISCO INTEGRATED SERVICES ROUTERS: THE VALUE OF INTEGRATED SECURITY FOR SMALL AND MEDIUM-SIZED BUSINESSES AND ENTERPRISE BRANCH OFFICES

In the past two decades, networks have evolved from closed infrastructures to integrated systems that enable organizations to work more closely with employees, partners, customers, and vendors worldwide by connecting and automating business processes and applications. The Web-enablement of applications has had a dramatic impact on productivity and profitability—but it also has increased the risk of malicious attacks.

Security breaches can assail a company from a wide range of sources, including the company's own networked PCs and servers. New worms and viruses also are targeting the network endpoints, a situation that is of particular concern in small or branch offices with limited IT resources to combat these challenges.

Cisco Systems® prepares organizations for attacks by helping them build self-defending networks that have dramatically improved capabilities to identify, prevent, and respond to threats. An important foundation of the evolving Cisco® Self-Defending Network is the new generation of Cisco integrated services routers. These routers are the industry's first to deliver secure, wire-speed data, voice, video, and other advanced services to small- and medium-sized businesses and enterprise branch offices.

This white paper focuses on the changing security landscape and the embedded security features of the Cisco 800, 1800, 2800, and 3800 series integrated services routers. Amid market trends that point to growing customer demand for concurrent integrated services in small businesses and branch offices, this paper outlines the value of integrating security within the router. It also illustrates how a unique systems approach from Cisco effectively addresses security challenges today and well into the future.

This paper is not intended to be a technical deployment guide. Rather, it explains how Cisco is merging best-in-class network security technology with more than 20 years of routing expertise to redefine network security and provide customers with end-to-end network protection.

UNPRECEDENTED NETWORK SECURITY CHALLENGES

In the past, threats from both internal and external sources were relatively slow-moving, and it was easier to mitigate attacks. The first generation of security challenges in the 1980s—boot viruses impacting individual computers and networks—took weeks to spread. In the 1990s, a second generation of security challenges could spread in days, including macro viruses, e-mail viruses, denial-of-service (DoS) threats, and limited hacking attempts.

In today's environment, the speed and sophistication of network security breaches and destructive attacks continues to increase at an alarming rate. Threats blending Internet worms, viruses, and Trojan horses spread across the world in minutes to multiple and regional networks, resulting in widespread intrusions and costly damage.

THE HIGH PRICE OF NETWORK SECURITY BREACHES AND ATTACKS

Average losses per security breach:

- Cost from theft of proprietary information: US \$1,136,409
- Cost from downtime and damage from viruses: US \$61,729
- Sabotage of data networks: US \$535,750
- System penetration by outsider: US \$172,448
- Denial of service: US \$108,107
- Unauthorized insider access: US \$1,008,050

Source: CSI FBI Computer Crime & Security Survey 2004

Legal Obligations Require More Due Diligence

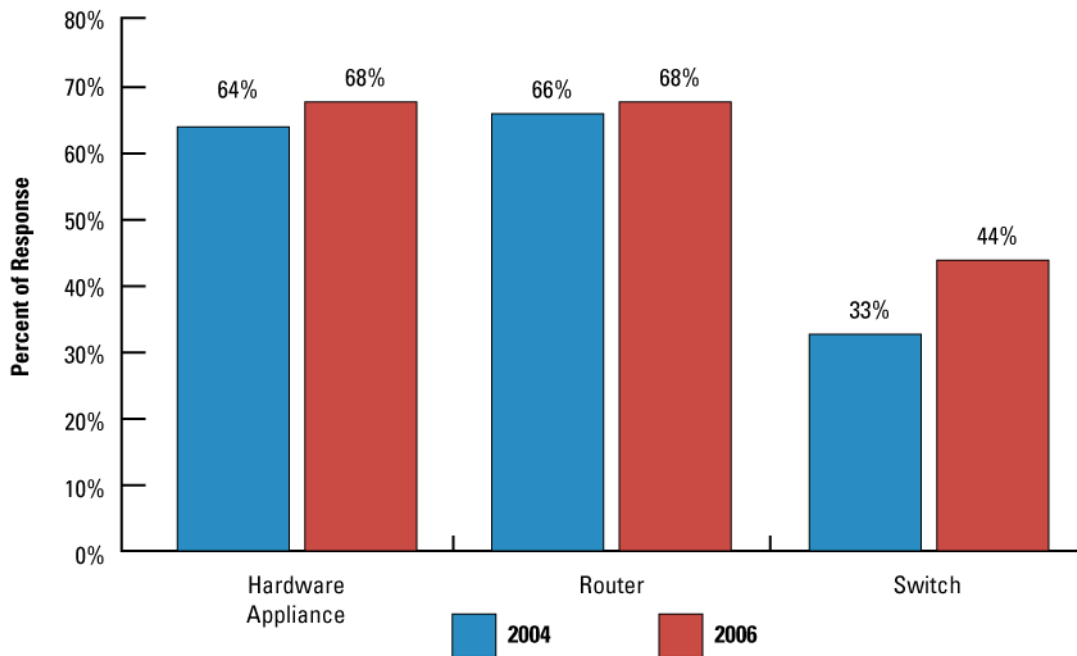
Compliance with a growing number of government regulations and standards also has prompted corporations to bolster their network security. These regulations and laws were created to enhance privacy, national security, and, in many cases, public company accountability.

Examples of these regulations include the Health Information and Patient Privacy Act (HIPPA) in the healthcare industry, the Gramm Leach Bliley Act (GLBA) in the financial services industry, and the Sarbanes-Oxley Act in the accounting field. The European Union's privacy legislation, called the Directive on Data Protection, requires that transfers of personal data take place only to non-EU countries that provide acceptable levels of privacy protection.

Growing Demand for Secure Routers

As security and privacy concerns continue to escalate, so does the desire for innovative security solutions. In the article, *Enemy at the Gates: The Evolution of Network Security* (Business Communication Review, December 2004), Jeff Wilson, principal analyst for Infonetics Research, states "While many people have been watching the security appliance market with great interest, they tend to overlook the extent to which security is actually deployed through routers and switches. Just as distributed Internet connectivity and the need for companies of all sizes to secure their networks drove the integration of multiple security technologies into single products, these same factors also drove network product manufacturers to integrate security into routers and switches." An Infonetics study referenced in the same article reports that "the percentages of respondents planning to deploy security appliances and secure routers were roughly even."

Figure 1. Planned Security Purchases



Data from Infonetics Research supports the fact that the secure router market is a fast-growing segment. In a year-end 2004 report, Matthias Machowinski, directing analyst for enterprise voice and data at Infonetics Research, states that “Twelve percent of fourth-quarter enterprise router revenue came from the sale of secure routers, up one percent from the third quarter.” The author goes on to say “We predict secure routers to continue to take up a growing slice of the router revenue pie, accounting for 29 percent of total router revenue by 2008.”

EVOLVING SECURITY SOLUTIONS FROM CISCO

Security solutions are evolving to meet changing security requirements, and Cisco continues to set the standard with best-in-class security solutions.

Synergy Research cited in a March 14, 2005, Investors.com editorial titled “Hybrid Products Lead Security’s Advance,” reports that “The market for network security products rose 28% to more than \$4 billion last year (2004).” Synergy analyst Aaron Vance states, “I would expect to see somewhat steeper growth this year and hybrid products that combine firewall, VPN and other security features will be the biggest driver. Cisco Systems, (CSCO) the No. 1 maker of network gear, leads in sales of such hybrid security products.”

Today, Cisco embeds network security into the hardware of every integrated services router shipped and offers end-to-end protection with the appropriate Cisco IOS® Software feature sets. Cisco integrated services routers have been engineered to interoperate with the Cisco 7200 Series and 7301 aggregation routers that share the same comprehensive Cisco IOS Software advanced security feature set.

VALUE OF INTEGRATED SECURITY SOLUTIONS ON THE ROUTER

Integrated security is a foundational element of the Cisco Self-Defending Network. Integrated-security solutions on the router use Cisco market-leading firewall and intrusion-prevention-system (IPS) technologies to advantage, combining robust Cisco IOS Software functions and industry-leading LAN and WAN connectivity with world-class security functions.

Integrating Cisco IOS Software security directly into the router offers many benefits. First, it takes advantage of existing network infrastructure, helping enable new security features on the router through Cisco IOS Software without deploying additional hardware. This saves time and money

because it reduces the number of devices in the network, lowering training and manageability costs for an overall lower total cost of ownership (TCO). Router network modules are also covered in existing router Cisco SMARTnet[®] maintenance contracts to further ease manageability.

Second, it provides the flexibility to apply security functions—such as firewall, inline intrusion prevention, and VPN—anywhere in the network to ensure the best defense against security threats. Cisco router-based, switch-based, and appliance-based functions combined offer the capability of end-to-end protection throughout the network.

Third, integrating Cisco IOS Software security directly into the router protects network gateways, because routers are the first points of entry into the network, and at the WAN aggregation router—the entry point into the data center. This allows deployment of best-in-class security functions at all entry points into the network, which are logical places to secure the network.

Security on the router not only protects that first point of entry into the network, it also takes advantage of the intelligence of the router as a “trusted handler” of the traffic, integrating more advanced security, quality of service (QoS), and routing features. This helps enable security capabilities to share information and coordinate a fast, accurate response to a threat to ensure high network availability. Integrated security protects the router itself, while also creating a line of defense against attacks targeted directly at the network infrastructure, such as distributed DoS (DDoS) attacks.

Many available point-product security solutions protect specific aspects of the network, but few security solutions can secure the entire infrastructure by securing all points in the network in the way that the Cisco portfolio of security solutions can.

VALUE OF USING A SYSTEMS APPROACH

Before examining some of the specific integrated security features included in the Cisco 800, 1800, 2800, and 3800 series integrated services routers, as well as the Cisco 7200 Series, consider the value of using a systems approach.

High Availability in the Branch

Cisco offers a truly formidable suite of capabilities for maintaining high availability in the branch. Designed from the ground up for always-accessible networking, Cisco’s end-to-end perspective provides IT organizations with a more easily deployed, maintainable, self-defending network architecture. The integrated services router strengthens this approach still more by providing simultaneous use of more interfaces and features while increasing performance of multiple, concurrent security, management, and integration services.

With the integrated services router, Cisco offers a comprehensive, future-proofed solution for high availability in the branch that minimizes network outages and ensures nonstop access to the most business-critical applications. Cisco’s focus on integrating new infrastructure services with performance enables companies to create networks that are more intelligent, resilient, and reliable.

For more information about the Cisco High Availability solution for branch and small offices, read the white paper, “*Maximizing Availability in the Branch with the Integrated Services Router*” at <http://www.cisco.com/go/isr>.

Performance

Using a systems approach, the Cisco integrated services routers are designed to provide appropriate WAN line-rate performance. That means if customers enable additional services such as voice or security, performance does not fall below the speed of the corresponding WAN interface. The integrated services routers are optimized to run concurrent services with the appropriate CPU power, and CPU-intensive services, such as VPN, are offloaded to dedicated accelerators.

Cisco engaged Mier Communications, Inc. to independently verify configuration, operational, and performance aspects of the new Cisco integrated services routers. Based on its thorough workout of these systems, Miercom attested to the performance of these systems during concurrent provisioning of important high-level network services to a busy branch office, including stateful Cisco IOS Firewall and Network Address Translation (NAT), IPS, voice over IP (VoIP), and analog telephony services, while under heavy data transport. The tests also verified the assurance of quality voice services under heavy transport load.

In particular, the tests confirmed the ability of the Cisco 3845 to load a T3 IP-WAN link and to employ the Advanced Encryption Standard (AES), with IP Security (IPSec) VPN, over a full T3 link of traffic. In addition to the Cisco 3845, Miercom tested the Cisco 2851, 2811, 2801, 1841, and 1812 wireless integrated services routers, as well as the Web-based Cisco Router and Security Device Manager (SDM). To access the full Miercom summary reports, visit the Web at <http://www.miercom.com>.

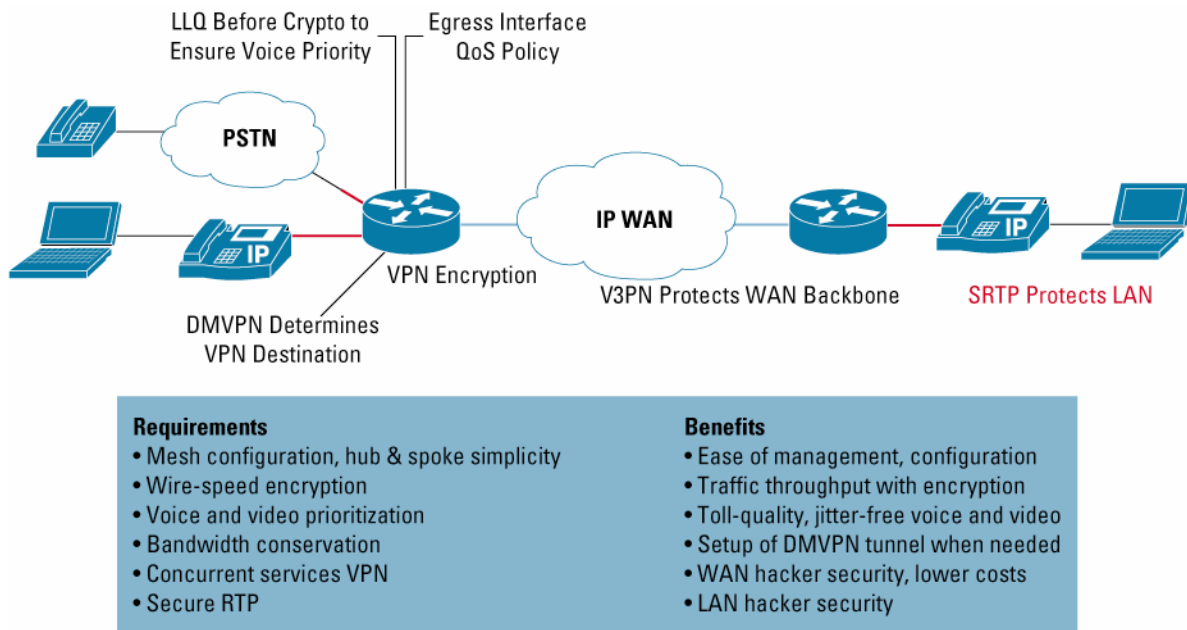
“Our tests prove the Cisco 3845 simultaneously sustains full T3 WAN rates for multiple applications. Its embedded cryptographic processor handles both 128-bit AES and IPSec VPNs with ease, concurrently delivering firewall, intrusion prevention, QoS, and data routing at maximum WAN-link speeds. Additionally, an impressive 72 streams of voice traffic, including transcoding, voice mail, AutoAttendant, fax, and Survivable Remote Site Telephony, was handled with no performance degradation in the Cisco 3845.”

*Ed Mier
President, Mier Communications, Inc.*

Intelligence

A systems approach begins with a single, resilient platform such as the Cisco integrated services routers, but it extends beyond an “all-in-one-box” approach. A systems approach combines packaging with intelligent services within and between services. The services work better together to offer tangible benefits such as Dynamic Multipoint VPN (DMVPN) to enable dynamic tunnels or Voice and Video Enabled VPN (V³PN), as shown in Figure 2.

Figure 2. Secure, Toll-Quality IP Telephony Using DMVPN, V³PN



A systems approach weaves voice, security, routing, and application services together, so that processes become more automated and more intelligent. The results are pervasive security in the network and applications; a higher QoS for data, voice, and video traffic; an increased time to productivity; and better use of network resources.

By combining best-in-class software and applications in one platform, customers can:

- More quickly deploy basic and advanced services
- Manage these services using common tools and interfaces for simplicity in operations
- Increase network security by minimizing the number of separate boxes that need to be locked down
- Take advantage of existing and future interfaces and network modules that speed data delivery and free hardware for new applications
- Troubleshoot faster, “spare” easier, and train staff more quickly—all factors in reducing operating costs
- Take advantage of bundled packaging and service agreements to reduce capital costs

DISTINGUISHING SECURITY FEATURES OF THE NEW CISCO INTEGRATED SERVICES ROUTERS

Founded on 20 years of leadership and innovation, the Cisco 800, 1800, 2800, and 3800 series integrated services routers ship with the industry’s most comprehensive security services, intelligently embedding data, security, and voice into a single, resilient system for fast, scalable delivery of mission-critical business applications.

Cisco integrated services routers were designed to incorporate security in every router by making hardware-based encryption a standard feature. This built-in, hardware-based encryption acceleration offloads the VPN processes to provide increased VPN throughput with minimal impact on the router CPU. If additional VPN throughput or scalability (for example, number of VPN tunnels) is required, optional VPN encryption advanced integration modules (AIMs) are available.

The Cisco Self-Defending Network offers four categories of protection that apply to the new routers: trust and identity, network infrastructure protection, secure connectivity, and threat defense (refer to Figure 3).

Figure 3. Integrated Services Routers and the Self-Defending Network



Trust and Identity

Trust and identity services allow the network to intelligently protect endpoints using technologies such as network admission control (NAC); identity services; and authentication, authorization, and accounting (AAA).

Network Admission Control

NAC is an industrywide collaboration effort led by Cisco to help ensure that every endpoint complies with network security policies before being granted access. NAC limits damage due to viruses and worms by interrogating devices connecting to the network to see if they comply with the latest corporate antivirus and operating system patch policies before accessing the network. Vulnerable and noncompliant hosts are isolated and given restricted network access until they are patched and secured, thus preventing them from being the source or target of worm and virus infections.

As the logical first step into a Cisco Self-Defending Network, NAC and other Cisco IOS Software integrated security services can be enabled on the Cisco 800, 1800, 2800, and 3800 series integrated services routers, and the Cisco 7200 series and 7301 aggregation routers, with the Cisco IOS Software Advanced Security, Advanced IP Services, or Advanced Enterprise Services feature sets.

Authentication, Authorization and Accounting

Cisco IOS Software AAA network security services provide the primary framework to set up access control on a router or access server. AAA is designed to allow administrators to dynamically configure the type of authentication and authorization they want on a per-line (per-user) or per-service (that is, IP, Novell Internetwork Packet Exchange [IPX], or virtual private dialup network [VPDN]) basis, using method lists that are applied to specific services or interfaces.

The 802.1x Standard

Standard 802.1x applications make unauthorized access to protected information resources more difficult by requiring valid access credentials. By deploying 802.1x applications, network administrators also can effectively eliminate the possibility of users deploying unsecured wireless access points, addressing one of the biggest concerns of easy-to-deploy wireless LAN (WLAN) equipment.

USB Port/Removable Credentials

The Cisco 800, 1800, 2800, and 3800 series integrated services routers were designed with integrated onboard USB 1.1 ports, which can be used to enable important security and storage capabilities. These capabilities enable secure user authentication, store removable credentials for establishing secure VPN connections, securely distribute configuration files, and provide bulk flash storage for files and configuration.

Network Foundation Protection

Network foundation protection (NFP) secures the network infrastructure from attacks and vulnerabilities, especially at the network level. Examples include Control Plane Policing, AutoSecure, and network-based application recognition (NBAR).

Control Plane Policing

Even the most robust software implementation and hardware architecture is vulnerable to malicious DoS attacks designed to paralyze a network infrastructure by flooding it with worthless traffic. To block these and similar threats camouflaged as specific types of control packets directed at the heart of the network, Cisco IOS Software includes programmable policing functions on routers that limit the rates of traffic destined for the control-plane processor. This feature, called Control Plane Policing (CoPP), can be configured to identify and limit certain traffic types either completely or when above a specified threshold level.

AutoSecure

A feature of Cisco IOS Software, AutoSecure simplifies router security configuration and reduces the risk of configuration errors. The interactive mode, suited for experienced users, prompts users to customize security settings and router services, providing greater control over the router security functions. The AutoSecure noninteractive mode automatically enables router security functions based on defaults set by Cisco and recommended by the International Computer Security Association (ICSA). A single command instantly configures the security posture of routers and disables nonessential system processes and services, eliminating potential network security threats.

Network Based Application Recognition

NBAR is a classification engine within Cisco IOS Software that uses deep and stateful packet inspection to recognize a wide variety of applications, including Web-based and other difficult-to-classify protocols. When used in a security context, NBAR can detect worms based on payload signatures. When NBAR recognizes and classifies an application, a network can invoke services for that specific application. Cisco SDM has an easy-to-use wizard to enable NBAR and also provides a graphical view of application traffic.

Cisco SDM

Every Cisco 800, 1800, 2800, and 3800 series router, as well as the Cisco 7200 series and 7301 aggregation routers, comes with a factory-installed Cisco SDM, an intuitive, Web-based device manager (GUI) for deployment and management of Cisco routers. Cisco SDM helps enable easy router configuration and monitoring through the use of a startup wizard for quick deployment and router lock-down, and provides smart wizards to help enable security and routing features, Cisco Technical Assistance Center (TAC)-approved router configurations, and subject-related educational content.

Secure Connectivity

Secure connectivity provides secure and scalable network connectivity, incorporating multiple types of traffic. Examples include VPN tunneling and encryption, DMVPN, Easy VPN, V³PN, Virtual Tunnel Interface (VTI), Multi-Virtual Route Forwarding (VRF), Multiprotocol Label Switching (MPLS), and secure contexts.

VPN Tunneling and Encryption

VPNs have been the fastest-growing form of network connectivity. All the Cisco 800, 1800, 2800, and 3800 series integrated services routers include built-in, hardware-based VPN encryption acceleration that offloads the IPSec encryption and VPN processes to provide increased VPN throughput with minimal impact to the router CPU. This feature supports IPSec, AES, Digital Encryption Standard (DES), and Triple DES (3DES) encryption without consuming an AIM slot.

Optional VPN encryption AIMS are available for companies that require additional VPN throughput or scalability. The result is increased VPN performance with lower overall router CPU usage. The optional AIM provides up to 10 times the encryption performance over previous models, as well as tunnel scalability.

The integrated services routers also can use an alternate tunneling technique that combines the IPSec and generic-routing-encapsulation (GRE) protocols. The IPSec-with-GRE tunneling technique is a unique Cisco solution that helps send dynamic routing protocols over the VPN, thus delivering greater network resiliency than IPSec-only solutions. In addition to providing a failover mechanism, GRE tunnels offer the ability to encrypt multicast and broadcast packets and non-IP protocols.

Dynamic Multipoint VPN

Cisco DMVPN helps enable on-demand and scalable full-mesh VPN to reduce latency, conserve bandwidth, and simplify VPN deployment. The DMVPN feature builds upon Cisco IPSec and routing expertise by helping enable dynamic configuration of GRE tunnels, IPSec encryption, Next Hop Resolution Protocol (NHRP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP).

This dynamic configuration of VPN tunnels, combined with technologies such as QoS and IP Multicast, optimizes latency-sensitive applications such as voice and video. DMVPN also eases administrative burden with no configuration at the hub when adding new spokes or when setting up spoke-to-spoke connections.

Secure Voice

Media authentication and encryption features on the Cisco portfolio of integrated services access routers ensures that voice conversations terminating on either time-division multiplexing (TDM) or analog voice gateway ports are protected from eavesdropping. These reliable, scalable features provide a secure environment for IP Communications over a LAN or WAN.

Media encryption using secure Real-Time Transport Protocol (SRTP) encrypts the voice conversation, rendering it unintelligible to internal or external hackers who have penetrated and gained access to the voice domain. As an IETF RFC 3711 standard, SRTP is designed specifically for voice packets; it supports the AES encryption algorithm. Media encryption using SRTP is more bandwidth-efficient than IPSec.

Easy VPN

Easy VPN is an IPSec solution designed to support hub-and-spoke VPN topologies with minimal effort and high scalability. Easy VPN simplifies provisioning and management of VPN solutions between Cisco PIX[®] firewalls, the Cisco VPN 3000 Client, and routers of all sizes. Proven in thousands of customer installations, Easy VPN uses “policy-push” technology to simplify configuration while retaining feature richness and policy control.

Voice and Video Enabled IPSec

The Cisco 800, 1800, 2800, and 3800 series routers and Cisco 7200 series and 7301 aggregation routers support V³PN, which provides a VPN infrastructure capable of converged data, voice, and video across a secure, QoS-enabled IPSec network and allows customers to obtain the same performance for voice and video applications over an IP transport as they would over an alternate WAN link—securely and effectively. Unlike many VPN devices on the market, Cisco integrated services routers accommodate the diverse network topology and traffic requirements that enable multiservice IPSec VPNs. The end-to-end network architecture of V³PN takes advantage of Cisco security-enabled routers with Cisco IOS Software to secure voice traffic.

Delivering toll-quality voice and video over IPSec VPNs requires more than just encrypting traffic—it requires a blend of advanced multiservice and IPSec VPN technologies. Primary Cisco IOS Software technologies that help enable Cisco V³PN include: multiservice-centric QoS, support for diverse traffic types, support for multiservice network topologies, and enhanced network failover capabilities.

Virtual Tunnel Interface

Cisco IPSec VTI is a new tool that can be used by customers to configure IPSec-based VPNs between site-to-site devices. IPSec VTI tunnels provide a designated pathway across the shared WAN and encapsulate traffic with new packet headers, helping ensure delivery to specific destinations. The network is private because traffic can enter a tunnel only at an endpoint. In addition, IPSec provides true confidentiality (as does encryption), and can carry encrypted traffic.

Multi-VRF and MPLS Secure Contexts for Service Providers

Multi-VRF is an extension of site-to-site IPSec VPN. Businesses can expect to have security and privacy as traffic travels through the provider network. However, it becomes more complex to keep the traffic segregated properly across the traditional LAN network. This is particularly key when deploying to multiple branch sites. Multi-VRF is designed to preserve privacy between segments in an elegant and affordable way.

Threat Defense

Threat-defense services prevent and respond to network attacks and threats using network services. Examples include the Cisco IOS Firewall and Cisco IOS IPS.

Cisco IOS Firewall

The Cisco IOS Firewall is a stateful inspection firewall option available for Cisco routers. Taking advantage of the same stateful firewall technologies used in the market-leading Cisco PIX Firewall, the Cisco IOS Firewall is supported on all the integrated services routers with the Cisco IOS Software Advanced Security or higher feature sets. Cisco IOS Firewall is an ideal single-box security and routing solution for protecting the WAN entry point into the network. Although the hub is a common location to locate a firewall and inspect traffic for attacks, remote offices also are important locations to consider when deploying security.

Cisco IOS Firewall has been enhanced with the introduction of Application Firewall support. Application Firewall provides Cisco IOS Firewall the intelligence to not only block non-HTTP traffic, but to ensure traffic that is assumed to be HTTP is legitimate Web-browsing and not instant messaging or similar traffic trying to gain access through the firewall. The net result is that network administrators will have more granular control of applications passing through the firewall.

The Cisco IOS Firewall not only helps enable a single point of protection at the perimeter of a network, it also makes security policy enforcement an inherent component of the network itself. The flexibility and cost-effectiveness of both dedicated and integrated policy enforcement facilitates security solutions for extranet and intranet perimeters and Internet connectivity for a branch or remote office. Integrated into the network through Cisco IOS Software, the Cisco IOS Firewall also allows customers to use advanced QoS features in the same router.

Cisco IOS Software supports IPv6 firewall and allows for IPv4 and IPv6 coexistence. Cisco IOS Firewall IPv6 offers stateful protocol inspection (anomaly detection) of IPv6 packets and IPv6 DoS attack mitigation.

Transparent Firewall

In addition to Layer 3 stateful firewalling, the Cisco 800, 1800, 2800, and 3800 series routers and Cisco 7200 series and 7301 aggregation routers can support transparent firewalling, which is the ability to provide Layer 3 firewalling for Layer 2 connectivity on the same router. Transparent firewalling provides support for subinterfaces and VLAN trunks, Spanning Tree Protocol, all standard management tools, and Dynamic Host Configuration Protocol (DHCP) pass-through to assign DHCP addresses on opposite interfaces (bidirectional). Because it does not require IP subnet renumbering or IP addresses on the interfaces, it is an easy addition to existing networks.

Inline Intrusion Prevention System

Cisco leads the industry with the first routers to offer inline IPS functions. Cisco IOS IPS is an inline, deep-packet, inspection-based solution that helps enable Cisco IOS Software to effectively mitigate network attacks. Used for intrusion prevention and event notification, the Cisco IOS IPS takes advantage of technology from the Cisco Intrusion Detection System (IDS) Sensor products, including Cisco IDS 4200 Series appliances, the Cisco Catalyst® 6500 IDS Services Module, and network module hardware IDS appliances.

Because Cisco IOS Software IPS is in line, it can drop traffic, send an alarm, or reset the connection, helping enable the router to respond immediately to security threats and protect the network. Through collaboration with IPsec VPN, GRE, and Cisco IOS Firewall, Cisco IOS IPS can allow decryption, tunnel termination, firewalling, and traffic inspection at the first point of entry into the network (branch or hub)—an industry first. Cisco IOS IPS helps stop attacking traffic as close to the source as possible.

Combined with the release of the Cisco 800, 1800, 2800, and 3800 series routers, Cisco IOS IPS now can load and help enable selected IPS signatures in the same manner as Cisco IDS Sensor appliances, allowing customers to choose from more than 1200 of the signatures supported by Cisco IDS Sensor platforms. Companies also can modify an existing signature or create a new signature to address newly discovered threats, and if

they want maximum intrusion protection, they can select an easy-to-use signature file that contains “most-likely” worm and attack signatures. Traffic matching these high confidence-rated worm and attack signatures is configured to be dropped. Cisco SDM provides an intuitive user interface to provision these signatures, including the ability to upload new signatures from Cisco.com without requiring a change in software image, and Cisco SDM configures the router appropriately for these signatures.

URL Filtering (Off-Box and On-Box Optional)

Cisco offers URL filtering to support the Cisco IOS Firewall, allowing customers to use either Websense or N2H2 URL filtering products with Cisco security routers. The Websense URL filtering feature helps enable a company’s Cisco IOS Firewall to interact with the Websense or N2H2 URL filtering software to prevent users from accessing specified Websites on the basis of their security policy. The Cisco IOS Firewall works with the Websense and N2H2 server to determine whether to allow or deny (block) a particular URL.

Advanced Security Network Modules (Cisco 2800 and 3800 Series Option)

Organizations seeking a dedicated, hardware-based solution for IDS and content security have the option of adding two security network modules to the Cisco 2800 and 3800 series routers.

The Cisco IDS Network Module helps enable a complete IDS system that works in concert with other IDS components to efficiently protect data and information infrastructure. It has a dedicated CPU for IDS and a 20-GB hard drive for logging with more than 1000 IPS signatures supported. The Cisco Content Engine Network Module offers a router-integrated content-delivery system with content security features. In addition to intelligent caching and content routing, it also can function as a URL filtering (Websense, SmartFilter) application server.

STRONG MARKET INTEREST FOR ROUTER-INTEGRATED SERVICES

Cisco is seeing a strong market interest for router-integrated services, from small businesses to large enterprises.

Ann Taylor

Ann Taylor, a billion-dollar apparel retailer with more than 600 stores in the United States and Puerto Rico, is one example. To support its expansion efforts, the retailer decided to replace its dialup network to enable Web-based sales and inventory applications, secure transactions for instant credit applications, and future in-store voice and video kiosks.

Ann Taylor rapidly deployed Cisco routers with integrated VPN in a new network providing an intranet, e-mail, online sales and fulfillment systems, a credit switch and credit card clearing system, nationwide inventory, and sales performance applications for all its locations.

The results have been impressive. A new inventory system enables sales clerks to access accurate, real-time information about merchandise and simplifies merchandise handling for sales associates. Managers can access forms and manuals, examine sales data, and update merchandise displays. Sales have spiked in all locations with the new system.

GST

GST provides transportation and logistics solutions in 34 offices employing 380 employees. The company sought to converge its data and voice networks to extend Internet access and reduce costs; simplify vendor and network management; and reduce the cost and complexity of phone moves, adds, and changes.

Using Cisco switches and routers, GST integrated data, VPN, security, and IP telephony to reduce expenses from \$52,000 per month for 19 offices to \$57,000 per month for 34 offices in fewer than three years. The company also added 15 new offices to the network, and remote employees have the same level of access to the network as employees at headquarters. Customers can now place and track orders directly through the Website.

DEDICATED SECURITY APPLIANCES OR INTEGRATED SECURITY ROUTER?

Customers deploying firewalls can choose either a Cisco best-in-class, dedicated Cisco PIX security appliance or a Cisco IOS Firewall. The router-integrated Cisco IOS Firewall takes advantage of Cisco PIX Firewall technologies combined with 20 years of routing expertise.

Cisco will continue to offer best-in-class, embedded security in its routers as well as dedicated security appliances to provide choices for customers responsible for determining how to best secure their networks. Although the line between integrated security and standalone appliances continues to blur, there are several reasons why a customer might choose one over the other or a combination of security solutions.

Integrated Security Ideal for Small Businesses or Branch Offices

One important consideration is the location of the network that needs to be secured. Many companies choose to integrate security into their edge aggregation routers. Larger enterprises, however, may opt to secure their headend with a standalone appliance and their data center with a firewall service module (FWSM) integrated into a Cisco Catalyst switch, because these areas of the network need higher throughput. Yet these same enterprises may also choose to secure all points in the network by adding routers with integrated security in their branch offices.

Small and medium-sized offices and enterprise branch offices face many of the same security issues that large headquarters do, yet typically they have little or no local IT resources to manage security solutions. With limited IT resources, deploying and managing multiple devices may not fit an enterprise's support model. For such models, integrating multiple devices onto one platform that is centrally managed can ease the troubleshooting and maintenance concerns in these smaller offices, while lowering the TCO.

The Cisco 800, 1800, 2800, and 3800 series integrated services routers are ideal for small businesses and enterprise branch offices, delivering a rich, integrated solution for connecting remote offices, mobile users, and partner extranets or service provider-managed customer premises equipment (CPE). With Cisco IOS Software-based VPN, firewall, and IPS, as well as optional enhanced VPN acceleration, IDS, and content-engine network modules (Cisco 2800 and 3800 series), Cisco offers the industry's most robust and adaptable security solution for branch-office routers.

A large grocery chain, for example, had WAN connectivity from its individual stores to the corporate headquarters with a leased line. Security of the supermarket's customer data stored at headquarters was very important, particularly because federal and state laws mandated that all customers must be notified if a breach of records occurred. To protect its corporate network from harmful attacks originating in its grocery stores, the chain decided to add a Cisco IOS Firewall in its existing routers.

Company Preferences

Choosing network integrated security or dedicated-purpose security solutions also may be influenced by customer preference, a desire to take advantage of existing infrastructure, deployment and operations architecture, or specific feature differences. Some companies simply prefer to "let routers route and switches switch." Or from a management standpoint, a company may prefer to separate its security and VPN infrastructure from its networking infrastructures because it employs a team dedicated to security and VPN management.

Future Cost Assessment

Taking advantage of existing routers or switches for security—by adding Cisco IOS Software security images and VPN modules—is a cost-effective option for extending the deployment life of an infrastructure. This maximizes the return on the initial investment and significantly reduces future costs and business interruption due to premature device replacement. The costs associated with planned and unplanned downtime can be the most significant factor in assessing future costs.

Increased integrated-services capabilities also augment overall network flexibility and availability by preparing the network for future converged multimedia deployments. These capabilities also enable organizations to react more quickly to avoid missed opportunities, reduce overall time to deploy new services, mitigate unnecessary near-term device upgrades, and lower overall TCO from increased extensibility and expandability.

Feature Differences

Because Cisco integrates technology from the Cisco PIX security appliances into the Cisco IOS Firewall, the feature sets of the two security solutions are becoming increasingly similar. That being said, Cisco continues to use security appliances to refine and validate new technologies before incorporating them into the integrated services routers. For organizations that want the most current, innovative security features, a Cisco PIX security appliance typically offers new security features before they are provided as options for the Cisco IOS Firewall.

SUMMARY

Networks remain at the core of most businesses today, and the reality of security threats keeps network security high on the list of priorities for IT managers focused on protecting their networks. As security requirements evolve to include more integrated security solutions that secure all entry points into the network, Cisco is enhancing its security portfolio to dramatically improve the ability of a network to identify, prevent, and respond to threats.

Built with embedded security hardware acceleration, the new generation of Cisco integrated services routers integrates Cisco IOS VPN, firewall, and inline IPS services across the Cisco router portfolio, delivering the industry's most comprehensive and adaptable security solutions. These routers particularly address the needs of small and remote offices that require integrated security to minimize the number of operating systems and devices to manage with limited IT resources.

By combining robust Cisco IOS Software functions and industry-leading LAN and WAN connectivity with world-class security functions, Cisco integrated security solutions help enable companies to take advantage of existing network infrastructure and deploy security where they need it most. Instead of adding hardware, Cisco IOS Software lets customers use new, integrated security features on their routers and apply those security functions anywhere in the network. The Cisco integrated services routers protect all entry points into the network, as well as defend against attacks targeted directly at the network infrastructure.

FOR MORE INFORMATION

For more information about integrated security features of the modular Cisco 1800, 2800, and 3800 series integrated services routers, refer to the following documents on the Web.

Data Sheet

Security Features on the Cisco Integrated Services Routers

http://www.cisco.com/en/US/products/ps5854/products_data_sheet0900aecd80169b0a.html

Q&A

Security Features on the Cisco Integrated Services Routers

http://www.cisco.com/en/US/products/ps5854/products_qanda_item0900aecd80169bba.shtml

White Paper

Maximizing Availability in the Branch with the Integrated Services Router

http://www.cisco.com/en/US/products/ps5854/products_white_paper0900aecd80173e40.shtml

Miercom Lab Testing Summary Reports

Cisco Integrated Services Routers

<http://www.miercom.com>

NAC

http://www.cisco.com/en/US/netso/ns466/networking_solutions_package.html

Network Infrastructure Protection

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_data_sheet09186a00801f98de.html

Cisco Router and Security Device Manager

<http://www.cisco.com/go/sdm>



Corporate 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: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website** at www.cisco.com/go/offices.

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)

205276.BO_ETMG_JR_4.05

