



Cisco Integrated Services Routers: The Value of Integrated Security For Small and Medium-Sized Businesses

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. Bringing applications to the Internet has had a dramatic impact on productivity and profitability – but it has also increased the risk of attacks.

Security breaches can occur from a wide range of sources, including a company's own networked PCs and servers. New worms and viruses are targeting network endpoints. This is of particular concern to small and medium-sized offices, which often have limited IT resources to combat these challenges. Cisco Systems® prepares organizations for attacks by helping them build self-defending networks with dramatically improved capabilities to identify, prevent, and respond to threats. An important component of the Cisco® Secure Network Foundation and the Cisco Self-Defending Network is the new generation of Cisco integrated services routers. These routers are the 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 Cisco 800, 1800, 2800, and 3800 Series Integrated Services Routers. Market trends point to growing customer demand for concurrent integrated services in small businesses; this paper outlines the value of integrating security within the router. It also illustrates how the Cisco Smart Business Roadmap and a unique systems approach from Cisco effectively address security challenges today and well into the future.

This paper is not 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

Whether from internal or external sources, early network security threats were slow-moving and easier to mitigate. The first generation of security challenges in the 1980s – boot viruses affecting individual computers and networks – took weeks to spread. In the 1990s, the second generation of security challenges, including macro viruses, e-mail viruses, denial-of-service (DoS) threats, and limited hacking attempts, could spread in days.

Today, the speed and sophistication of network security breaches and destructive attacks continues to increase. Threats blending Internet worms, viruses, and Trojan horses spread across the world to multiple and regional networks in minutes, resulting in widespread intrusions and costly damage.

The High Price of Network Security Breaches and Attacks

Average losses per security breach:

- Theft of proprietary information: US\$30,933,000
- Downtime and damage from viruses: US\$42,787,767
- Insider abuse: US\$6,856,450
- System penetration by outsider: US\$841,400
- Denial of service: US\$7,310,725
- Unauthorized access: US\$31,233,100

Source: CSI FBI Computer Crime and Security Survey 2005

Legal Obligations Require More Due Diligence

Compliance with a growing number of government regulations and standards has also prompted companies to bolster their network security. These regulations and laws were created to enhance customer privacy, national security, and public company accountability. Examples of these regulations in the United States include the Health Insurance Portability and Accountability Act (HIPAA) in the healthcare industry, the Gramm Leach Bliley Act (GLBA) in the financial services industry, and the Sarbanes-Oxley Act in the accounting industry. The European Union's privacy legislation, 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.

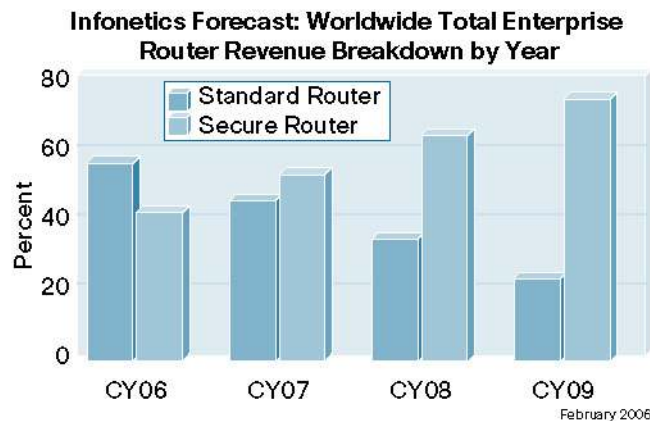
Growing Demand for Secure Routers

As security and privacy concerns continue to escalate, so does the need for innovative security solutions. An article in *Business Communication Review* states that 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 switches¹. It also notes that 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 reported that the percentages of respondents planning to deploy security appliances and secure routers were roughly even.

As seen in Figure 1, data from Infonetics Research supports the fact that the secure router market segment is fast-growing. A recent article stated that growth in the secure router segment, both in terms of units and revenues, was positive. Secure router revenues on a year-over-year basis grew by 121 percent to US\$803 million in 2005; and shipments nearly tripled².

Figure 1.

Trend Toward Purchases of Secure Routers



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. Today, Cisco embeds network security into the hardware of every integrated services router and offers end-to-end protection with Cisco IOS® Software feature sets. Cisco integrated services routers interoperate with Cisco 7200 Series and Cisco 7301 aggregation routers, which share the same comprehensive Cisco IOS Software Advanced Security feature set.

¹ "Enemy at the Gates: The Evolution of Network Security," *Business Communication Review*, December 2004, Jeff Wilson

² "Secure Router Market More Than Doubled in 2005" (internetnews.com, February 2006), Matthias Machowinski

Value of Integrated Security Solutions on the Router

Integrated security is a foundational element of the Cisco Self-Defending Network. Cisco router-based integrated security solutions use market-leading Cisco firewall and intrusion prevention technologies, combining Cisco IOS Software functions and LAN and WAN connectivity with world-class security.

Integrating Cisco IOS Software security directly into the router offers many benefits. It uses the existing network infrastructure, helping enable new security features on the router without deploying additional hardware. This 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.

Integration provides the flexibility to apply security functions, such as firewall, inline intrusion prevention, and VPNs, anywhere in the network to ensure the best defense against security threats. Router-based, switch-based, and appliance-based functions combine to offer end-to-end protection throughout the network. Integrating security directly into the router also protects network gateways, because routers are the first points of entry into the network. 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 the first point of entry into the network, but 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. At the router, security information can be shared and a fast, accurate response to a threat coordinated, helping to ensure high network availability. And integrated security protects the router itself, while creating a line of defense against attacks targeted directly at the network infrastructure, such as distributed DoS (DDoS) attacks.

Many third-party point product security solutions protect specific aspects of the network, but few 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

Small Office High Availability

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

Cisco integrated services routers offer offices a comprehensive solution for high availability that minimizes network outages and helps ensure nonstop access to the most business-critical applications. Cisco focus on integrating new infrastructure services with performance enables companies to create networks that are more intelligent, resilient, and reliable – today and in the future.

For more information about Cisco high-availability solutions for 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, Cisco integrated services routers provide appropriate WAN line-rate performance. This means that if customers enable additional services such as voice or security, performance does not fall below the speed of the corresponding WAN interface. 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.

Mier Communications, Inc. (Miercom) independently verified configuration, operational, and performance aspects of the new Cisco integrated services routers. 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), intrusion prevention, 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 Integrated Services Router 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. Miercom also 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) application.

To access the full Miercom summary reports, visit <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, voicemail, Auto Attendant, fax, and Survivable Remote Site Telephony, were handled with no performance degradation in the Cisco 3845.”

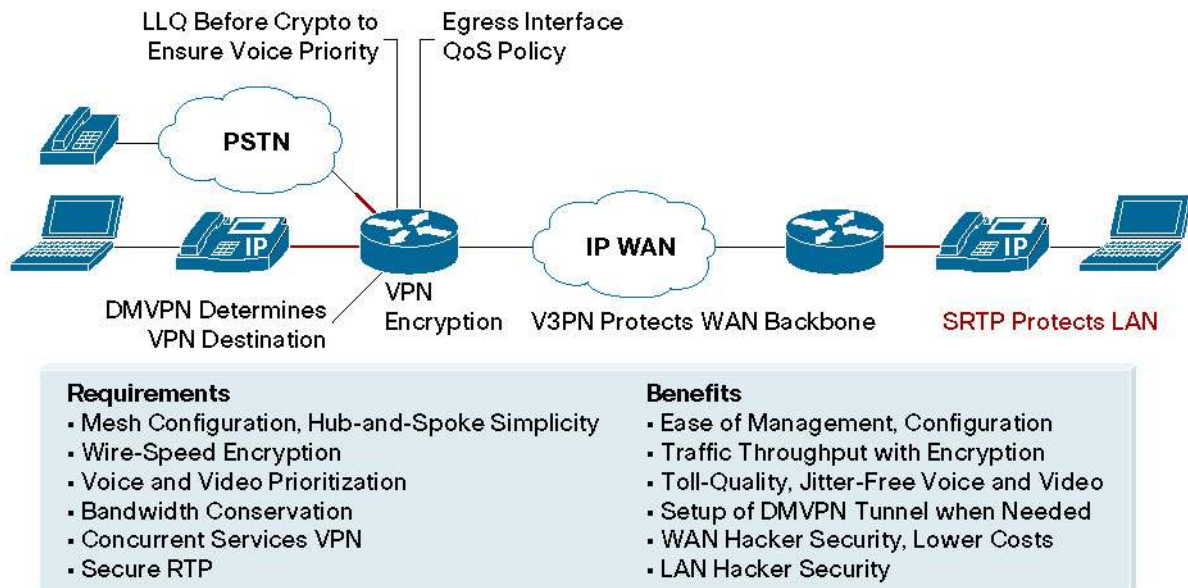
—Ed Mier, President, Mier Communications, Inc.

Intelligence

A systems approach begins with a single, resilient platform such as the Cisco integrated services router, but it must extend beyond a “one-box” approach and combine packaging with intelligent services. When working together, intelligent services 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; higher QoS for data, voice, and video traffic; increased time to productivity; and better use of network resources.

A Strategic Approach to Growth

Small and medium-sized businesses need to protect and fully utilize their network investments and make the most of limited support resources, at a pace that's right for them. The Cisco Secure Network Foundation is a flexible and scalable way to implement security levels and advanced applications. The Cisco Secure Network Foundation is a core step in the Cisco Smart Business Roadmap, which provides a structured, planned evolution path to help organizations take advantage of today's business opportunities and maximize the long-term potential of their technology investments. Using the Cisco Smart Business Roadmap, businesses can work closely with Cisco and with Cisco partners to plan for future growth, simplify technology adoption, improve deployment time, and reduce overall costs.

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, simplifying operations
- Increase network security by minimizing the number of separate boxes that need to be secured
- 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 to reduce operating costs
- Take advantage of bundled packaging and service agreements to reduce capital costs

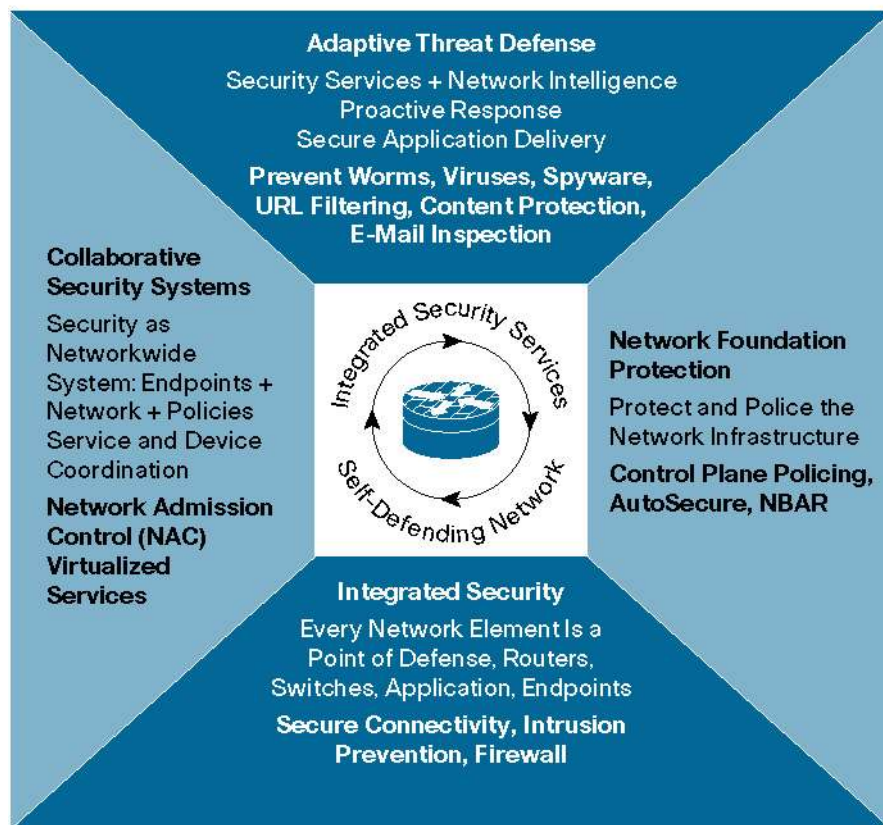
Distinguishing Security Features of the New Cisco Integrated Services Routers

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 incorporates security into every integrated services router by making hardware-based encryption a standard feature. This built-in, hardware-based encryption acceleration offloads 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 (Figure 3).

Figure 3.

Cisco Integrated Services Routers and the Self-Defending Network



Device Management

Cisco Router and Security Device Manager (SDM)

Every Cisco 800, 1800, 2800, and 3800 Series; Cisco 7200 Series; and Cisco 7301 Router comes with 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." It provides smart wizards to help enable security and routing features, Cisco Technical Assistance Center (TAC)-approved router configurations, and subject-related educational content.

Cisco Systems, Inc.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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 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.

NAC and other integrated security services can be enabled on Cisco 800, 1800, 2800, and 3800 Series; Cisco 7200 Series; and Cisco 7301 routers, with the Cisco IOS Software Advanced Security, Advanced IP Services, or Advanced Enterprise Services feature sets.

Authentication, Authorization, and Accounting

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

802.1x

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

Cisco integrated services routers were designed with integrated onboard USB 1.1 ports, which can be used to enable important security and storage capabilities. With these capabilities, the routers can 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 secures the network against attacks and vulnerabilities. Examples include Control Plane Policing, AutoSecure, and network-based application recognition (NBAR).

Control Plane Policing

Even the most robust software and hardware architecture is vulnerable to DoS attacks, which attempt 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 core of the network, Cisco IOS Software includes policing functions that limit the rates of traffic destined for the control-plane processor. This feature, called Control Plane Policing, 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 helps reduce 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 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, the network can invoke services for that specific application. Cisco SDM includes an easy-to-use wizard to enable NBAR and also provides a graphical view of application traffic.

Secure Connectivity

Cisco integrated services routers provide secure and scalable network connectivity, incorporating multiple types of traffic. Examples include VPN tunneling and encryption, DMVPN, Easy VPN, V3PN, Virtual Tunnel Interface (VTI), Multivirtual Route Forwarding (VRF), Multiprotocol Label Switching (MPLS), and secure contexts.

VPN Tunneling and Encryption

VPNs are fast-growing forms of network connectivity. All Cisco 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. These AIMS help increase VPN performance while keeping the overall router CPU usage low. Each AIM provides up to 10 times the encryption performance over previous models, as well as tunnel scalability. Cisco 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, 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-Internet-based protocols.

Cisco IOS Web VPN

Secure Sockets Layer (SSL) VPN is compelling for remote-access security because it is transparent to the end user and easy to administer. With Cisco IOS Web VPN, available on Cisco integrated services routers, companies can extend their secure enterprise networks to any Internet-enabled location, including home computers, Internet kiosks, and wireless hotspots, enabling higher employee productivity and protecting corporate data while providing network access to partners and consultants.

Dynamic Multipoint VPN

DMVPN helps enable on-demand and scalable full-mesh VPNs to reduce latency, conserve bandwidth, and simplify deployment. DMVPN builds upon Cisco IPsec and routing expertise by supporting dynamic configuration of GRE tunnels, IPsec encryption, Next Hop Resolution Protocol (NHRP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP). Combined with technologies such as QoS and IP Multicast, this optimizes latency-sensitive applications such as voice and video. DMVPN also eases administration, requiring 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 Cisco integrated services routers help ensure 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.

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

Easy VPN

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

Voice- and Video-Enabled VPN

All Cisco 800, 1800, 2800, and 3800 Series; Cisco 7200 Series; and Cisco 7301 routers support V3PN. This provides customers with an infrastructure capable of converged data, voice, and video across a secure, QoS-enabled IPsec network. Customers can 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 available today, these Cisco routers accommodate the diverse network topology and traffic requirements of 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 customers can use 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 to 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 that helps ensure security and privacy as an organization’s traffic travels through a service 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

Cisco IOS Firewall is a stateful inspection firewall option available for Cisco routers. Taking advantage of the same stateful firewall technologies used in Cisco security appliances, Cisco IOS Firewall is supported on all integrated services routers with Advanced Security or higher Cisco IOS Software 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 place a firewall and inspect traffic for attacks, remote offices also are important to consider when deploying security.

Additional features within Cisco IOS Firewall provide an even greater level of security and enforcement. An application firewall gives Cisco IOS Firewall the intelligence to not only block non-HTTP traffic, but also to ensure that 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. Zone-based policy configuration provides a clear interface for configuring firewall policies that are aligned with traditional security policies. 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. These features give network administrators will have more granular control of applications passing through the firewall.

Cisco IOS Firewall not only helps enable a single point of protection at the perimeter of a network, but 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. Cisco IOS Firewall also allows organizations to use advanced QoS features in the same router.

Transparent Firewall

In addition to Layer 3 stateful firewalls, Cisco 800, 1800, 2800, and 3800 Series; Cisco 7200 Series; and Cisco 7301 routers support transparent firewalls, a feature that provides Layer 3 firewalls for Layer 2 connectivity on the same router. Transparent firewalls provide 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 (bidirectional) interfaces. Because it does not require IP subnet renumbering or IP addresses on the interfaces, a transparent firewall is an easy addition to existing networks.

Inline Intrusion Prevention

Cisco has developed the first routers to offer inline intrusion prevention functions. Cisco IOS IPS is an inline, deep-packet-inspection-based solution that helps Cisco IOS Software effectively mitigate network attacks. Used for intrusion prevention and event notification, Cisco IOS IPS takes advantage of technology from Cisco intrusion detection and prevention system (IDS/IPS) products, including Cisco IPS 4200 Series sensor appliances, the Cisco Catalyst® 6500 Series IDS Services Module, and network module IDS appliances.

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

When combined with Cisco integrated services routers, Cisco IOS IPS can load and help enable selected IPS signatures in the same manner as Cisco IPS sensor appliances, allowing customers to choose from more than 1200 of the signatures supported by Cisco IDS/IPS platforms. Companies can modify an existing signature or create a new signature to address newly discovered threats. For maximum 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. Cisco SDM configures the router appropriately for these signatures.

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

Cisco offers URL filtering to support 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 either Websense or N2H2 URL filtering software to prevent users from accessing specified Websites on the basis of their security policy. Cisco IOS Firewall works with the Websense and N2H2 servers to determine whether to allow or deny (block) a particular URL.

Advanced Security Network Modules (for the Cisco 2800 and 3800 Series)

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

The Cisco IDS Network Module helps enable a complete IDS/IPS system that works in concert with other IDS/IPS components to efficiently protect the data and information infrastructure. The Cisco IDS Network Module 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.

Pep Boys

Pep Boys, a leading automotive aftermarket and service chain in the United States with nearly 600 stores in the United States and Puerto Rico, is one example. To connect its retail locations and provide access to inventory, point-of-sale, and corporate applications, the automotive retailer decided to perform an infrastructure upgrade to ensure high network resiliency and availability. Pep Boys chose Cisco routers with integrated encryption, IPsec VPN, Network Admission Control (NAC), and intrusion prevention. These secure routers help Pep Boys meet their business needs, including the need to continuously maintain a strong security posture. Another company goal is to continue to ensure that customers have the best possible experience in a Pep Boys store with a high-performance network that delivers maximum uptime.

Fresenius Medical Care (FMCNA)

FMCNA, the largest integrated provider of products and services for individuals with chronic kidney failure, operates 1140 dialysis clinics in North America with over 28,000 employees. The company replaced its Frame Relay network and implemented a medical-grade network. FMCNA now has high-speed access to patient information and workflow applications using Cisco routers with embedded encryption acceleration, IPsec VPN, firewall, inline intrusion prevention, and Network Admission Control (NAC). With the rate of growth of new clinics, the dynamic multipoint VPN (DMVPN) capability made it easier to scale VPN services to over one thousand sites. The Cisco IOS Firewall helps the company maintain a robust security posture for complying with the Health Insurance Portability and Accounting Act (HIPAA) and Sarbanes-Oxley regulations.

Dedicated Security Appliances or Integrated Security Router?

Customers deploying firewalls can choose either a Cisco best-in-class, dedicated Cisco ASA security appliance or a Cisco Integrated Services Router with security features. The router-integrated security features take advantage of security technologies developed on the appliances and combines those capabilities 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 and Medium-Sized Businesses

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 headends with standalone appliances and their data centers with switch-based firewall services modules, 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 face many of the same security issues that large corporate 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 their support model. Integrating multiple devices into one centrally managed platform can ease the troubleshooting and maintenance concerns in these smaller offices, while lowering TCO.

Cisco integrated services routers are ideal for small businesses, 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 capabilities, as well as optional enhanced VPN acceleration, IDS, and content-engine network modules, Cisco offers the industry's most robust and adaptable security solution for small and medium-sized offices.

Company Preferences

Choosing integrated or dedicated-purpose network 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 ASA 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 ASA security appliance typically offers new security features before they are provided as options for the Cisco IOS Firewall.

Summary

Network security remains a priority 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, Cisco integrated services routers integrate Cisco IOS VPN, firewall, and inline IPS services across the Cisco router portfolio, delivering the industry's most comprehensive and adaptable security solutions. The integrated services 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 companies take advantage of their 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. Cisco integrated services routers protect all entry points into the network, and defend against attacks targeted directly at the network infrastructure. By deploying Cisco integrated services routers as part of the Cisco Smart Business Roadmap, technical decision makers can be confident that their immediate technology investments will scale to support their long-term network goals.

For More Information

For more information about integrated security features of the modular Cisco 800, 1800, 2800, and 3800 Series integrated services routers, refer to the following documents:

Data Sheet

Security Features on Cisco Integrated Services Routers

http://www.cisco.com/application/pdf/en/us/guest/products/ps5854/c1650/cdccont_0900aecd80169b0a.pdf

Q&A

Security Features on Cisco Integrated Services Routers

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

Miercom Lab Testing Summary Reports

Cisco integrated services routers

<http://www.miercom.com>

Network Admission Control

http://www.cisco.com/en/US/netsol/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>

Technology Information

To learn more about WebVPN and other security technologies, visit:

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



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 © 2006 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, PIX, and SMARTnet 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. (0601R) DB/LW10727 05/06

Printed in the USA

