

## The Value of Integrated Security

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. Today's network is the platform for business interactions across organizations and locations. At the same time, the threat environment is evolving such that the corporate perimeter is eroding, threats are increasingly difficult to detect and mitigate, and attacks are changing from broad to targeted.

Security breaches can attack a company from a wide range of sources, including the company's own networked PCs and servers. New worms and viruses also are targeting network endpoints, a situation that is of particular concern in small or branch offices with limited IT resources to combat these challenges. The resulting loss of data, regulatory or compliance repercussions for not protecting electronic assets, and lost revenue or productivity due to downtime "are pushing organizations to invest in security..."<sup>1</sup>

Today, the Cisco® Self-Defending Network builds on industry-leading network and endpoint defenses to incorporate innovative application security, content security, security monitoring technologies, and policy enforcement. The capabilities of the Cisco integrated security product portfolio, designed with a systems approach to information security, offer you a comprehensive solution for meeting today's security challenges.

Cisco helps organizations build self-defending networks that have pivotal capabilities to identify, prevent, and respond to threats. An important foundation of this framework is the Cisco integrated services router. These routers pioneered the delivery of secure, wire-speed data, voice, video, and other advanced services to small- and medium-sized businesses (SMBs) and enterprise branch offices.

This overview 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 innovative network security technology with more than 20 years of routing expertise to redefine network security and provide customers with end-to-end network protection.

---

<sup>1</sup> Infonetics Research, Network Security Appliances and Software, Quarterly Worldwide Market Share and Forecasts for 1Q08.

## The Arrival of More Insidious Threats

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

In today's environment, organizations are forced to address an array of their most challenging business security concerns yet, from preventing data leakage and loss to defending against botnets and meeting compliance requirements. Threats blending web and email traffic, malware, spyware, Internet worms, viruses, and Trojan horses spread across the world in minutes to multiple and regional networks, resulting in widespread intrusions and costly damage—not to mention lost productivity and the cost of downtime.

According to the 2008 CSI Computer Crime and Security Survey, financial fraud stemming from security breaches is the leading cause of financial loss for organizations at nearly \$500,000 per incident. Not far behind, malware and “bots” cost companies an average of nearly \$350,000. And loss of either proprietary information or customer/employee confidential data cost an average of \$250,000. It is clear that network attacks are not easing up. In this CSI study, they also found that<sup>2</sup>:

- Virus incidents occurred most frequently across organizations compared to all other types of threats
- Insider abuse of networks was the second-most frequently occurring, followed by theft of laptops and other mobile devices
- Attacks on Domain Name Systems (DNS) are up 2% from 2007, effecting 10% of all companies
- Targeted attacks (malware, bots, etc.) are on the rise, affecting 27% of companies
- Over 68% of companies are developing and implementing information security policies
- 50%+ believe that their losses were due to attacks from outside the organization

## Regulatory Compliance Necessitates Security Due Diligence

Today there is increased pressure to comply with industry regulations as well as state and federal regulations, created to enhance privacy, national security, and in many cases corporate accountability. Examples of these regulations include the Payment Card Industries (PCI) Data Security Standard, which affects all vendors who receive, store, or transmit cardholder data.

In the United States, other examples 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 to non-EU countries take place with only those organizations that provide acceptable levels of privacy protection.

Fines, penalties, lawsuits, and congressional hearings are just some of what a company may undergo if a security breach occurs and the company is out of compliance. The long-term effect of noncompliance is damage to the company's brand, or reputation, which sometimes never recovers.

---

<sup>2</sup> 2008 CSI Computer Crime and Security Survey

## Demand for Router Security Still Growing

The worldwide integrated security market continues to grow. “[G]rowth in this area can be attributed to sales of “branch, high-end, and router-based products; over time, we expect more branch revenue to transition from standalone appliances to routers with integrated security.”<sup>3</sup> Infonetics forecasts that the router market will grow well over the next four years, with the most price-banded categories losing overall appliance revenue share to routers. Products between \$1,500 and \$29,999 account for more than one-third of the revenue for integrated security appliances in early 2008, but much of this market is already losing some of its popularity to branch-office routers with integrated VPN and firewall.

Also according to Infonetics, “Many multiprotocol routers were purchased just prior to, and during, the Internet boom (1996–2001), and many of those routers are reaching the end of their lifecycle;” corporations looking to replace old multiprotocol routers with new routers will look for routers that support a wide range of IP services, specifically targeting IP Security (IPSec) VPN and security.

## Evolving Security Solutions from Cisco

Security solutions must evolve to meet changing security requirements, and Cisco continues to set the standard with innovative security solutions that address the ever-changing demands of enterprises in the real world. With Cisco Group Encrypted Transport (GET) VPN, Cisco IOS<sup>®</sup> Software content filtering, and Cisco IOS Firewall voice security enhancements, for example, your organization can focus on meeting today’s security demands while planning for future network needs.

We take a systems approach to information security, where measures taken to secure your resources must keep pace with your bandwidth requirements. As a result, Cisco embeds network security into the hardware of all integrated services routers and WAN aggregation routers.

## Value of Integrated Security Solutions on the Router

Integrating Cisco IOS Software security directly into the router offers many benefits. First, it takes full advantage of existing network infrastructure, enabling new security features on the router through Cisco IOS Software without deploying additional hardware. This scenario 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). For more information, read the white paper, ["Optimizing Branch Office Network Infrastructure TCO with Cisco ISR"](#).

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. Thus best-in-class security functions are deployed 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 scenario enables security capabilities to share information and

<sup>3</sup> Infonetics Research, Network Security Appliances and Software, Quarterly Worldwide Market Share and Forecasts for 1Q08.

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.

### **Go Green**

Local and global green initiatives are gaining serious commercial momentum in the marketplace. More and more, executives are talking about environmental concerns and raising their priority on corporate agendas. Multiple reports from the U.N. Intergovernmental Panel on Climate Change show increasing evidence that human activity—and particularly carbon dioxide output—is the main cause for global climate change. These trends are placing growing pressure on corporate policy makers to reduce their carbon footprint.

We think IT is critical in helping meet green-related challenges, which can vary, depending on company size. IT-related power demands, worker travel, and e-waste are all critical areas of concern in any organization's green efforts. Cisco is committed to being an industry leader in resource conservation.

One way to reduce power consumption and cooling requirements in the branch office is to consolidate features and functions onto fewer branch-office systems. Router security serves as a strong example of Cisco efforts to ensure that branch-office IT systems are both fully effective and resource-efficient. For more information, read the white paper, [“Reduce Power Consumption Through Integrated Services Delivery.”](#)

### **High Availability in the Branch Office**

Cisco offers a truly formidable suite of capabilities for maintaining high availability in the branch office. Designed from the beginning for always-accessible networking, the Cisco 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 solution for high availability in the branch office that minimizes network outages and ensures nonstop access to business-critical applications. The Cisco 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.”](#)

### **Performance**

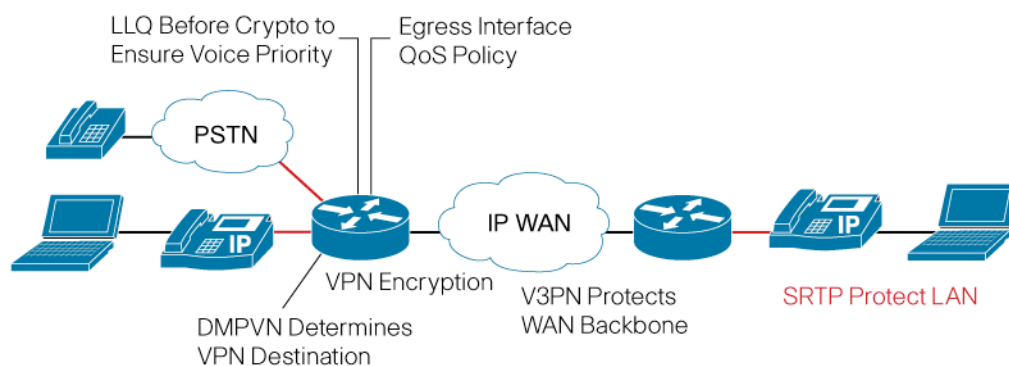
Using a systems approach, the Cisco integrated services routers are designed to provide appropriate WAN line-rate performance. That means if customers enable additional services such as voice or security, performance does not fall below the speed of the corresponding WAN interface. The integrated services 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 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 system (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. To access Miercom summary reports, visit <http://www.miercom.com>.

### 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 1.

**Figure 1.** Secure, Toll-Quality IP Telephony Using DMVPN and V3PN



#### Requirements

- Mesh configuration, hub & spoke simplicity
- Wire-speed encryption
- Voice and video prioritization
- Bandwidth conservation
- Concurrent services VPN
- Secure RTP

#### Benefits

- Ease of management, configuration
- Traffic throughput with encryption
- Toll-quality, jitter-free voice and video
- Setup of DMVPN tunnel when needed
- WAN hacker security, lower costs
- LAN hacker security

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 quality of service (QoS) for voice, video, and data traffic; and high network availability and thus increased productivity. With this approach, you can:

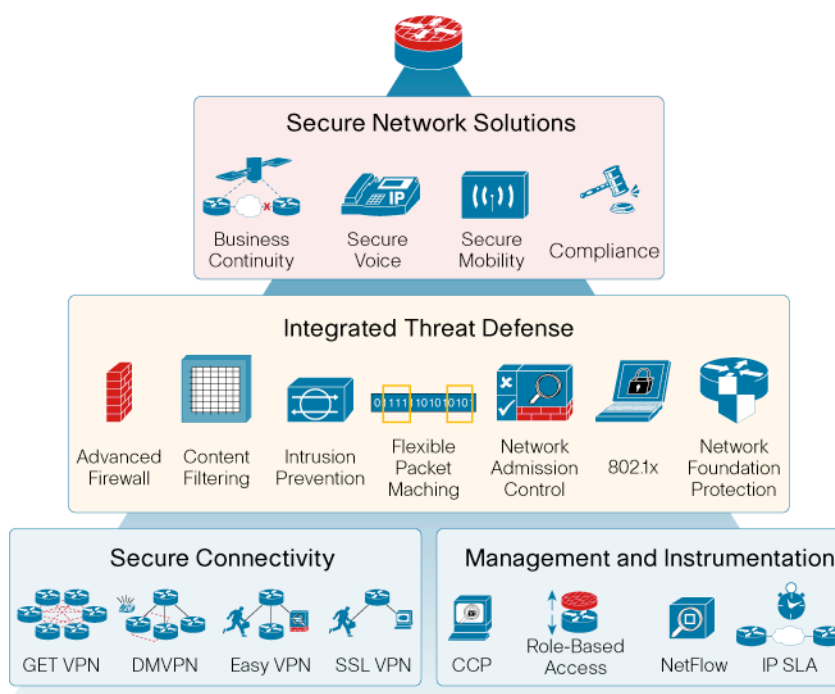
- More quickly deploy basic and advanced services
- Manage these services using common tools and interfaces for simplicity in operations
- Increase network security by minimizing the number of separate boxes that need to be locked down
- Take advantage of existing and future interfaces and network modules 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 expenditures

## Distinguishing Router Security Features

Founded on 20 years of leadership and innovation, Cisco integrated services routers and aggregation services routers ship with comprehensive security services, intelligently embedding data, security, and voice into a single, resilient system for fast, scalable delivery of mission-critical business applications.

The Integrated Services Router and aggregation services router families were designed with security as a fundamental component, 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 effect on the router CPU. If additional VPN throughput or scalability (for example, more VPN tunnels) is required, optional VPN encryption advanced integration modules (AIMs) are available. Router security encompasses much more than just VPN, however. Cisco IOS Software offers a suite of integrated threat-control technologies as well as other features to mitigate threats and secure your business (refer to Figure 2).

**Figure 2.** Router Security Technologies



### VPN for Secure Communications

“Most end-users are still moving from a model of centralized Internet connectivity to distributed connectivity, which will continue for at least the next five years; low cost Internet bandwidth is widely available, and it makes sense to take advantage of the cost savings and security offered by VPNs and distributed Internet connectivity.”<sup>4</sup>

<sup>4</sup> Infonetics Research, Network Security Appliances and Software, Quarterly Worldwide Market Share and Forecasts for 1Q08.

And ensuring the privacy and integrity of all information is vital to your business. As your company uses the flexibility and cost-effectiveness of the Internet to extend its network to branch offices, telecommuters, customers, and partners, security is paramount. Creating a secure, manageable, and cost-effective communications infrastructure will:

- Improve productivity
- Enhance business efficiency
- Help ensure compliance with information privacy regulations

### Cisco VPN Tunneling and Encryption

VPNs have been the fastest-growing form 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 effect on the router CPU. This feature supports IPSec, Advanced Encryption Standard (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 ten times the encryption performance over previous models, as well as tunnel scalability.

Cisco routers support a variety of VPN solutions to meet the unique needs of organizations today, including:

- **Standards-Based IPSec:** Supports “no-frills,” site-to-site connectivity for connecting remote locations to headquarters, where there are no requirements for features such as dynamic routing or QoS
- **Easy VPN:** Offers high-scale hub-and-spoke topologies, using a “policy-push” technology to simplify provisioning and management while retaining feature richness and policy control
- **DMVPN:** Enables on-demand and scalable full-mesh VPN to conserve bandwidth and simplify VPN deployment
- **Group Encrypted Transport VPN:** Provides easy-to-manage encryption for private WANs, using a common security methodology, not point-to-point IPSec tunnels

### Secure Voice and Video

Media authentication and encryption features on the integrated services routers 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. 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.

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 enable Cisco V3PN include multiservice-centric QoS, support for diverse traffic types, support for multiservice network topologies, and enhanced network failover capabilities.

### Multi-VRF and MPLS Secure Contexts for Service Providers

Multi-Virtual Route Forwarding (VRF) is an extension of site-to-site IPsec VPN. Your business 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 segregation is particularly critical when deploying to multiple branch offices. Multi-VRF is designed to preserve privacy between segments in a graceful and affordable way.

For more information about Cisco IOS VPN, visit <http://www.cisco.com/go/vpn>.

### Managing Threats

Cisco integrated threat control offers comprehensive network protection through simplified policy control and proactive system protection. It works to:

- Protect network, servers, endpoints, and information
- Regulate network access, isolate infected systems, prevent intrusions, and protect critical business assets
- Counteract malicious traffic such as worms, viruses, and malware before they affect your business

### Cisco IOS Firewall

The Cisco IOS Firewall, certified by Common Criteria (EAL4), is a stateful inspection firewall available on Cisco routers. Taking advantage of the same stateful firewall technologies used in the Cisco PIX<sup>®</sup> Firewall and Cisco adaptive security appliances (ASA), it helps ensure network availability and the security of company assets by protecting the network infrastructure against network and application layer attacks, viruses, and worms. Cisco IOS Firewall not only enables a single point of protection at the perimeter of a network, it also makes security policy enforcement an inherent component of the network itself. It protects unified communications by guarding Session Initiation Protocol (SIP) endpoints and call-control resources. Cisco IOS Firewall supports:

- **Application Firewall:** Blocks non-HTTP traffic and ensures 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
- **Transparent Firewall:** Offers Layer 3 firewalling for Layer 2 connectivity on the same router
- **Zone-Based Policy Firewall:** Provides a clear interface for configuring granular firewall policies aligned with your businesses' information security policies by tightly controlling network service access and enforcement

For more information about Cisco IOS Firewall, visit <http://www.cisco.com/go/iosfw>.

### Cisco IOS Intrusion Prevention System

Cisco is the first to offer inline IPS functions on routers. Cisco IOS IPS is an inline, deep packet inspection-based solution that enables 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 Prevention System (IPS) sensor products, including Cisco IPS 4200 Series Sensors and the Cisco Catalyst<sup>®</sup> 6500 Intrusion Detection System Module.

Because Cisco IOS IPS is in line, it can drop traffic, send an alarm, or reset the connection, enabling the router to respond immediately to security threats and protect the network. Through collaboration with IPsec VPN, generic routing encapsulation (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. For more information about Cisco IOS IPS, visit <http://www.cisco.com/go/iosips>.

### **Cisco IOS Content Filtering**

Cisco IOS Content Filtering can help your organization protect itself from known and new Internet threats, improve employee productivity, and enforce business policies for regulatory compliance. It:

- Monitors and regulates all Internet activities by blocking or restricting access to certain websites
- Provides protection from malicious sites that are known to give out malware, adware, spyware, and phishing
- Helps your organization better manage network resources with simple and easy deployment

### **Additional Security Features**

- Cisco IOS Software offers additional security technologies that can help your network intelligently protect endpoints: Network Admission Control (NAC); identity services; and authentication, authorization, and accounting (AAA).
- Network Admission Control is an industry-wide 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.
- AAA provides the primary framework to set up access control on a router or access server.
- The 802.1x standard makes 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.
- 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).
- Flexible Packet Matching complements Cisco IOS IPS by supporting custom filters that can be defined and deployed more rapidly than IPS signatures or antivirus patterns can be updated. It gives network security administrators powerful tools to identify miscreant traffic and immediately drop or log it for audit purposes.

### **Offload Security to Cisco Router Security Modules**

For customers seeking additional performance, optional security hardware acceleration modules are available for the Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers: the Cisco IPSec VPN Advanced Integration Module (AIM), the Cisco Intrusion Prevention System (IPS) AIM (also available in a network module form factor), and the Cisco NAC Network Module.

### **Router Security Management**

For a small number of devices, embedded Cisco GUI device managers—Cisco Router and Security Device Manager (SDM) and Cisco Configuration Professional—combine routing and security services management with ease of use, smart wizards, and in-depth troubleshooting capabilities to provide a tool that supports the benefits of integrating services onto the router. Customers can synchronize routing and security policies throughout the network, have a more comprehensive view of their router services status, and reduce their operating expenses.

For enterprise-wide management of firewall and VPN features, the Cisco Security Management Suite is an integrated security-event manager that includes the new Cisco Security Manager and Cisco Security Monitoring, Analysis and Response System (MARS). For more information about the Cisco Security Manager and Cisco Security MARS, visit <http://www.cisco.com/go/mars>.

### **Strong Market Interest for Router-Integrated Services**

Market interest for integrated services continues to be strong, from small businesses to large enterprises.

ValueClick, Inc. is one of the largest online marketing companies in the world, serving more than 1 billion ads per day from 16 offices across the world. With so many customers and partners relying on ValueClick's Internet-enabled services, the company requires the strongest possible protection against viruses, malware, and other Internet-based threats, while adhering to compliance requirements.

Using Cisco IOS security threat-control services, ValueClick can manage a firewall, an IPS, and VPN connectivity at each company location using the same Cisco platform that terminates the WAN and Internet connection—without deploying multiple dedicated appliances. Because these powerful defense capabilities are fully integrated into the core functions of the Cisco routers, ValueClick can take advantage of advanced threat protection and rich management features without having to compromise simplicity.

### **Dedicated Security Appliances or Integrated Security Router?**

Cisco offers 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 and Branch Offices**

As much of the industry market research suggests, 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 or data center with a standalone appliance 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 concerns 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 functions 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 content filtering, as well as optional hardware encryption and IPS 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 employ Cisco IOS Firewall on its existing routers.

### **Company Preferences**

Choosing integrated security or dedicated-purpose security solutions also may be influenced by 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 or simply turning on Cisco IOS Software security and VPN modules—is a cost-effective option for extending the deployment life of an infrastructure. This scenario 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 Cisco security appliances into Cisco IOS Software-based security software, the feature sets have become increasingly similar. That being said, there are technology-specific differences. It is important for an organization to understand its security and performance needs before making any decision.

## Summary

The security industry is rapidly evolving because of new threats, so it is difficult to predict exactly what will happen in the coming years, but “we do believe in one thing when it comes to security: users will always consume security functionality in a wide variety of form factors, and while spending may shift between categories and form factors, the basic growth trends don’t change.”<sup>5</sup>

The reality of security threats keeps network security high on the list of priorities for IT managers. As security requirements evolve, with 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 Cisco integrated services routers integrate VPN, firewall, inline IPS services, and content filtering across the Cisco router portfolio, delivering the industry’s most comprehensive and adaptable security solutions. These routers address the needs of branch 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 a wide array of LAN and WAN connectivity options with innovative 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 simply “turn on” security features on their routers and apply those security functions anywhere in the network.

## 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:

- Cisco Self-Defending Network Brochure  
[http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/net\\_brochure0900aec800efd71.pdf](http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/net_brochure0900aec800efd71.pdf)
- Security Features on the Cisco Integrated Services Routers  
[http://www.cisco.com/en/US/products/ps5854/products\\_data\\_sheet0900aec80169b0a.html](http://www.cisco.com/en/US/products/ps5854/products_data_sheet0900aec80169b0a.html)

For additional router security solutions and product collateral, visit <http://www.cisco.com/go/routersecurity>.

<sup>5</sup> Infonetics Research, Network Security Appliances and Software, Quarterly Worldwide Market Share and Forecasts for 1Q08.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0809R)