

# Cisco IOS Security Routers

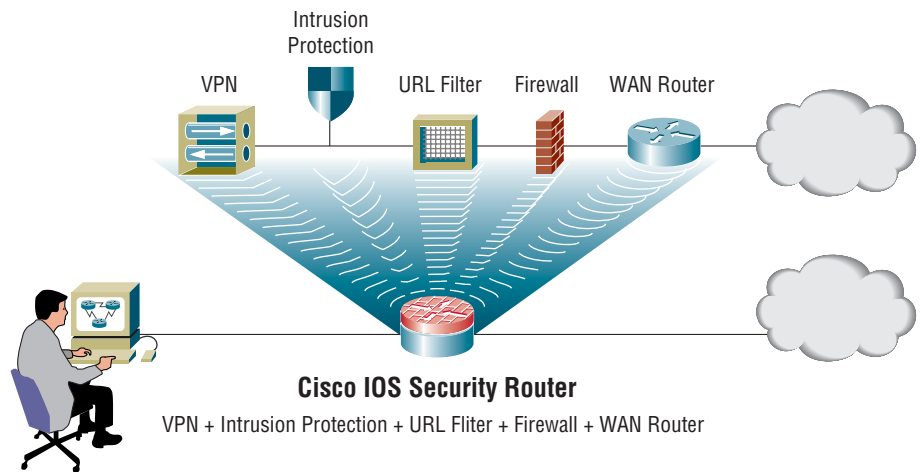
## Security **Embedded** within Your Network

Your investment in Cisco IOS® routers is a valuable asset that will help you achieve improved employee productivity while simultaneously reducing the cost of securing and managing the infrastructure.

### Integrated Security

Cisco IOS security routers combine security and network functions in a single device, independently delivering VPN, stateful firewall, intrusion protection and URL filtering in addition to the full-featured IP routing function.

Figure 1



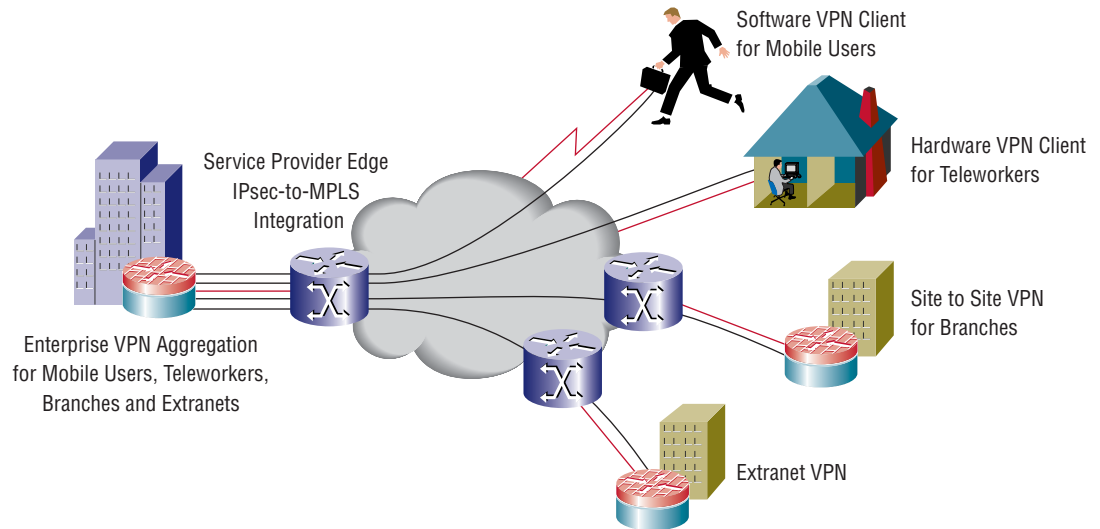
This integrated model is increasingly more relevant for remote branches and teleworkers where management of multiple devices from different vendors has become a challenging and expensive undertaking.



## Total Business Connectivity

Cisco IOS security routers are unmatched in breadth and connectivity solutions, supporting mobile users, teleworkers, remote branches and Enterprise head-end aggregation over IP VPNs as well as traditional Layer 2 transports.

Figure 2

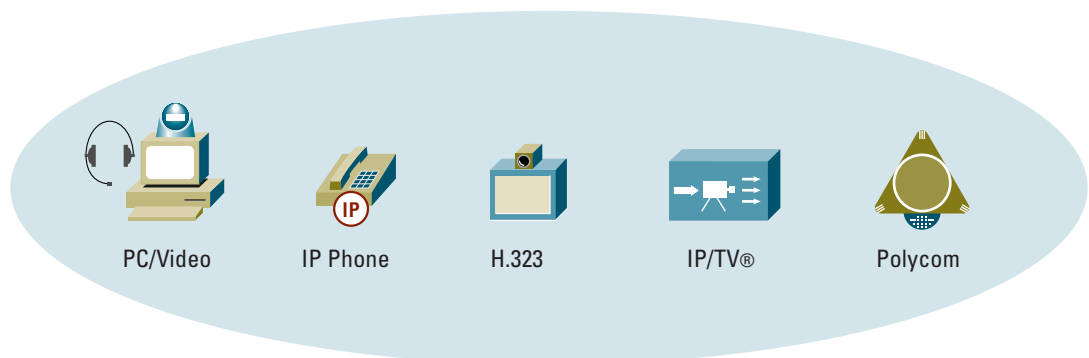


For Service Providers, Cisco IOS security routers serve as powerful edge devices marrying IPsec and Multiprotocol Label Switching (MPLS) protocols uniquely and provide carrier-class management tools.

## Consistent User Experience

Corporate employees need to be connected to their information securely from anywhere. Cisco IOS security routers allow employees to 'take' their work phone number with them and receive calls wherever in the world they may be. From their laptops they can do web conferencing, instant messaging, listen to corporate webcasts, use placeware and do e-learning—and have the same experience whether they are at home, headquarters, or a remote branch!

Figure 3



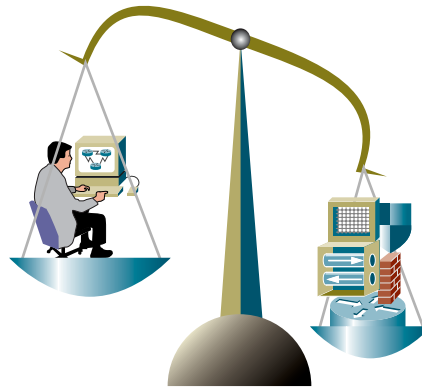
The key that makes this possible is the intelligence with which Cisco IOS integrates Security, VPN and IP networking services.



### **Reduced Cost of Ownership**

Your judicious investment in Cisco IOS gives you tremendous leverage to overcome the challenges of today's economy. You can extend the shelf life of your capital equipment purchases and extract value from operations skill sets and experience. Having a single device to learn and manage will undoubtedly increase administrator productivity and provide economies of scale.

**Figure 4**



For Service Providers, the Cisco IOS security router generates extra nimbleness in provisioning new services such as Enterprise Class Teleworking, Full Service Branch, and Dynamic VPNs into existing customer premises equipment reducing operating expenditures (OpEx) while simultaneously reducing capital expenditures (CapEx).



## Cisco IOS Security Routers—The Technology

Cisco IOS security routers combine comprehensive security services integrated with industry leading network services. A wide range of platforms and accelerator cards provide scalability and investment protection. The Cisco management software portfolio satisfies the needs of small businesses working with devices individually as well as enterprises and service providers mass deploying thousands of devices.

**Table 1**

Feature	Benefits
<b>Security Services</b>	
<b>Stateful firewall</b>	<p><b>Cisco IOS Stateful Firewall</b></p> <ul style="list-style-type: none"> <li>• Stateful firewall engine—Performs deep packet inspection maintaining state information per application</li> <li>• Threat detection and prevention—Denial-of-service detection and prevention, Java blocking, Simple Mail Transfer Protocol (SMTP) attack detection, IP fragmentation defense</li> <li>• URL filtering support—Web browsing control and auditing through URL filters including Content Engine Network Module, N2H2 and WebSense</li> <li>• Voice traversal—Firewall recognizes and secures multiple voice protocol traffic including H.323, Session Initiation Protocol (SIP) and Cisco Skinny Client Control Protocol</li> <li>• Multimedia application—VDO Live, RealAudio, InternetVideo Phone (H.323), NetMeeting (H.323), NetShow, CuSeeMe, Streamworks</li> <li>• Advanced applications—SQLNet, RPC, BSD R-cmds, ICMP, FTP, TFTP, SMTP and common TCP/UDP internet services</li> <li>• AAA Integration—Supports separate security policies per user, interface or sub-interface</li> </ul>
<b>Intrusion protection</b>	<p><b>Cisco IOS IDS</b></p> <ul style="list-style-type: none"> <li>• Over 100 signatures—Matches network traffic against malicious patterns</li> <li>• Enhanced performance—Combines with Cisco IOS Firewall to perform deep packet inspection with a single lookup</li> <li>• Inline operation (shunning)—Resets connections with malicious code attacks, providing protection to end users</li> <li>• Alarm management—Cisco Threat Response for false alarm minimization</li> </ul>
	<p><b>IDS Network Module</b></p> <ul style="list-style-type: none"> <li>• 45 Mbps. Separate processor, minimum impact on router performance</li> <li>• Full signature set (more than 850)</li> <li>• Response actions—Shunning, TCP resets, IP session logging</li> <li>• Alarm management—Cisco Threat Response for false alarm minimization</li> </ul>
	<p><b>Security Proxy (Content Engine Network Module)</b></p> <ul style="list-style-type: none"> <li>• Authentication, authorization, and accounting (AAA) support—Authenticates and authorizes end-users through an AAA server</li> <li>• Worm blocking—Rules-based pattern matching provides preliminary inspection of known malicious code with the ability to reset connections</li> <li>• Anti-virus proxy—Complements anti-virus software by caching the cleaned objects and using them in subsequent hits, thereby increasing anti-virus performance</li> </ul>
<b>URL filtering</b>	<p><b>Content Engine Network Module</b></p> <ul style="list-style-type: none"> <li>• Integrated SmartFilter URL filtering provides web surfing control and auditing, protecting against legal liabilities, preserving network bandwidth and improving productivity</li> <li>• Interoperability with N2H2 and WebSense URL filters</li> </ul>



**Table 1** (Continued)

Feature	Benefits
Trust and identity	<ul style="list-style-type: none"> <li>• CNS bootstrap call home—Forces newly provisioned remote routers to “call home” to management server, greatly simplifying large-scale deployments</li> <li>• Public key infrastructure (PKI) support—Digital certificates can be used to authenticate routers, providing greater scalability and security</li> <li>• Management tunnel—Allows periodic audit checks to ensure configurations have not been tampered with. Allows for a clean separation and outsourcing of management function</li> <li>• Secure RSA private key—Guards against router being stolen or misused, private key is erased if password recover attempted</li> <li>• PKI and AAA integration—Credentials stored centrally on an AAA server, allowing quick addition/deletion of devices with a single entry</li> <li>• DNS secured IP address assignment—Device-level protection against IP address hijacking</li> </ul>
<b>Network Integration</b>	
V3PN	<ul style="list-style-type: none"> <li>• Multiservice-centric quality of service (QoS)—Delivering toll-quality voice and video services requires QoS that addresses end-to-end transport quality. Low-latency queuing provides a foundation for prioritizing multiservice traffic and delivering specific bandwidth and latency guarantees. Cisco provides comprehensive low-latency queuing capabilities, including features specific to encrypted voice and video traversing the VPN. Furthermore, rich Cisco QoS features like traffic shaping to ensure quality on asymmetric link speeds and link fragmentation and interleaving (LFI) to control jitter in the presence of large packet transmissions like FTP are critical to ensuring voice and video quality on the VPN</li> <li>• Support for diverse traffic types—IP video traffic and voice traffic like hoot and holler and music on hold require support for multicast traffic across the VPN. Though IPSec is a unicast protocol, Cisco VPN routers, utilizing Cisco IOS software, accommodate multicast traffic and ensure the VPN infrastructure does not break multiservice applications</li> <li>• Support for multiservice network topologies—Because multiservice traffic is latency sensitive, network topologies must often be adapted to reduce network hops and minimize latency. Cisco VPN routers set the standard in delivering topology flexibility in network designs, accommodating topologies beyond basic hub-and-spoke designs to include hierarchical and fully meshed networks. Furthermore, Cisco VPN routers offer embedded software features such as Dynamic Multi-Point VPN that provide automated, dynamic provisioning of meshed networks for ease of deployment</li> <li>• Enhanced network failover capabilities—The Cisco V3PN solution provides comprehensive resiliency, addressing both VPN network transport and the IP telephony network. The full Layer 3 routing and stateful VPN failover capabilities of Cisco VPN routers provide network resiliency beyond the VPN device all the way to the network host, thereby eliminating network black holes. Survivable Remote Site Telephony (SRST) features for remote offices provide telephony-specific resiliency to ensure the voice network continues operating in the event of lost connectivity to the headquarters site</li> </ul>
Dynamic multipoint VPN (DMVPN)	<ul style="list-style-type: none"> <li>• Virtual full mesh—Allows IPsec with routing protocols to be dynamically configured</li> <li>• On-demand spoke-to-spoke tunnels—This industry-leading capability optimizes performance and reduces latency for real-time traffic</li> <li>• Dynamic discovery of spoke-to-hub tunnels—Minimizes hub configuration and ongoing updates when new spokes are added</li> <li>• QoS, Multicast support—Required for latency-sensitive applications e.g. Voice and Video</li> <li>• Tiered DMVPN—Allows preferential treatment of users, simplifies configuration</li> <li>• Enhanced Scalability—Load balancing doubles the performance compared to passive failover. Single hop to go from spoke to spoke reduces overhead on the system, Tiered DMVPN extends scalability</li> </ul>



**Table 1** (Continued)

Feature	Benefits
<b>IPsec-to-MPLS integration</b>	<ul style="list-style-type: none"> <li>• VRF-aware IPsec—Terminates multiple customer edge IPsec tunnels onto a single provider edge VRF interface, reducing CapEx</li> </ul>
<b>IPsec NAT transparency</b>	<ul style="list-style-type: none"> <li>• Allows encrypted IPsec traffic to traverse Network Address Translation (NAT) or Port Address Translation (PAT) devices by wrapping IPsec within User Datagram Protocol (UDP), simplifying VPN design and deployment</li> </ul>
<b>High availability</b>	<ul style="list-style-type: none"> <li>• IPsec stateful failover—Provides subsecond failover that provides reliability for mission-critical applications like Systems Network Architecture (SNA), voice and databases. Scales to thousands of remotes. Less help desk calls from end-users in the event of a head-end failure</li> <li>• DMVPN load balancing and self-healing—Doubles the performance compared to passive failover, while providing resiliency. Reroutes around link failures, maximizes uptime</li> <li>• Easy VPN failover—Ability to failover to multiple backup peers successively</li> </ul>
<b>Management</b>	
<b>IP Solutions Center (ISC)</b>	<ul style="list-style-type: none"> <li>• Policy-based management, scales from 50 to 20,000 devices</li> <li>• Multiple VPN deployments—site-to-site VPN, remote access VPN, DMVPN, Easy VPN</li> <li>• PKI-based end-to-end authentication and audit checks</li> <li>• Device abstraction layer—Allows policy rules to be created independent of devices and later pushed to different device implementations such as PIX® and Cisco IOS firewall</li> <li>• Bootstrap call home—Forces newly provisioned routers to call home to management server, get authenticated and receive their digital certificates and policies</li> <li>• Hub-and-spoke, full and partial mesh topologies</li> <li>• Design and deploy complex firewall rules</li> <li>• Cisco IOS IDS provisioning and tuning</li> <li>• Integrated routing— Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP)</li> <li>• Automate provisioning of failover and load balancing</li> <li>• QoS provisioning</li> <li>• Massive NAT configuration deployment</li> <li>• Service provisioning—Network-based IPsec, MPLS, managed firewall, managed IDS</li> </ul>
<b>CiscoWorks VPN/ Security Management System (VMS)</b>	<ul style="list-style-type: none"> <li>• Policy-based management—for small to large enterprises (up to 700 devices)</li> <li>• Combines web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network and host-based IDS</li> <li>• Device hierarchy and policy inheritance</li> <li>• Industry-leading auto update feature—allows a large number of firewalls to pull security configurations and update themselves easily and quickly.</li> <li>• Centralized role-based access control enables different groups to have different access rights across different devices and applications</li> <li>• Integrated monitoring of Cisco PIX and Cisco IOS syslogs, and events from network and host-based IDS, along with event correlation</li> </ul>



**Table 1** (Continued)

Feature	Benefits
<b>Security Device Manager (SDM)</b>	<ul style="list-style-type: none"><li>• Single device management, suitable for a handful of devices</li><li>• Security Audit—ICSA, TAC approved security configuration</li><li>• Intelligent wizards—Autodetect mis-configurations and propose fixes e.g. punches hole through firewall for DHCP if WAN interface is DHCP-addressed</li><li>• 1-step router lockdown through AutoSecure</li><li>• 1-step VPN—site-to-site VPN and Easy VPN</li><li>• Tools for expert users—ACL editor, VPN tunnel quality monitoring</li><li>• Granular monitoring of router, interface, firewall, VPN and logging status</li></ul>
<b>Easy VPN</b>	<ul style="list-style-type: none"><li>• Easy VPN client—Cisco IOS security routers act as remote VPN clients, typically useful for small branches and teleworkers. Configured automatically by policy push from head-end</li><li>• Easy VPN server—Cisco IOS security routers act as remote access head-ends, terminating software as well as hardware VPN clients</li></ul>
<b>Secure access</b>	<ul style="list-style-type: none"><li>• Authentication—PKI, AAA, command authorization</li><li>• Encrypted access—Secure Sockets Layer (SSL), Secure Shell (SSH), encrypted communications with management applications</li><li>• Out-of-band management—Ensure access despite DoS attacks, congestion or line protocol drops</li><li>• Audit trails—Console logging and syslogs, audit checks through management tunnel</li><li>• Unicast reverse path forwarding (uRPF)—Anti-spoofing by verifying the source address</li></ul>
<b>AutoSecure</b>	<ul style="list-style-type: none"><li>• Transform security posture of Cisco IOS routers—Quick way to implement router security best practices to safeguard the network</li><li>• Disable non-essential services—Eliminate DoS attacks based on fake requests to router services, disable mechanisms that could be used to exploit security holes, prevent attackers from knowing packets have been dropped</li><li>• Enforce secure access—Enforce enhanced security in accessing device, enhanced security logs</li><li>• Secure forwarding plane—Protect against SYN attacks, anti-spoofing, defend against man-in-the-middle attacks, enforce stateful firewall configuration on external interfaces for firewall images, enable NetFlow on software forwarding platforms</li></ul>



**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.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
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 Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)