DATA SHEET

NETWORK SECURITY FEATURES ON THE CISCO INTEGRATED SERVICES ROUTERS

This data sheet provides an overview of the network security features on Cisco® 800, 1800, 2800 and 3800 series integrated services routers.

PRODUCT OVERVIEW

Cisco Systems® is redefining best-in-class routing with a new line of integrated services routers that are optimized for the secure delivery of concurrent data, voice, and video services. Founded on 20 years of leadership and innovation, the modular Cisco® 1800 Series, 2800 Series, and 3800 Series, and fixed-configuration Cisco® 800 Series and 1800 Series integrated services routers ship with the industry's most comprehensive security services, intelligently embedding data, security, voice, and wireless in the platform portfolio for fast, scalable delivery of mission-critical business applications. The Cisco 800, 1800, 2800, and 3800 series 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).

Cisco integrated services routers have been engineered to transparently interoperate with the Cisco 7200 Series, 7301, and 7600 Series headend security routers. The Cisco 7200 Series and 7301 aggregation routers, specifically, share the same innovative and comprehensive Cisco IOS® Software-based advanced security feature set as the integrated services routers, enabling customers to build a truly integrated and efficient intelligent network.

By combining proven Cisco IOS Software functions and industry-leading LAN/WAN connectivity with world-class network security features, integrated router security solutions provide customers the following benefits:

- "**Use What You Have**"—Takes full advantage of existing network infrastructure, enabling new security features on the router through Cisco IOS Software without deploying additional hardware
- "**Deploy Security Where You Need It Most**"—Provides the flexibility to apply security functionality, such as firewall, intrusion prevention system (IPS), and VPN, anywhere in the network to maximize security benefit
- "**Protect Your Gateways**"—Allows best-in-class security functions to be deployed at all entry points into the network
- "**Save Time and Money**"—Reduces the number of devices, lowering training and manageability costs
- "**Protect Your Infrastructure**"—Protects the router, defending against attacks that are targeted directly at the network infrastructure such as distributed denial-of-service (DDoS) attacks

TABLE OF CONTENTS

CISCO SELF-DEFENDING NETWORK

Cisco 800, 1800, 2800 and 3800 series integrated services routers and the Cisco 7200 Series and 7301 headend routers are integral components of the Cisco Self-Defending Network (SDN), a strategy to allow organizations to identify, prevent, and adapt to network security threats. With Cisco IOS Software-based VPN, firewall, and IPS, as well as optional enhanced VPN acceleration, intrusion detection system (IDS), and content-engine network modules (for the Cisco 2800 and 3800 Series), Cisco integrated services routers provide the industry's most robust and adaptable security solutions for the branch office with complementary support at the headend using the Cisco 7000 platforms.

The Cisco Self-Defending Network is built upon the pillars of Integrated Security, Collaborative Security Systems, and Adaptive Threat Defense, with Network Foundation Protection as an underlying support structure.

SDN Integrated Security revolutionized network security by making every network element a point of defense, including routers, switches, appliances and endpoints. The core elements of Integrated Security that enable routers to become key devices for securing the network include: Secure Connectivity, Threat Defense, and Trust & Identity.

- **Secure Connectivity**—Provides secure and scalable network connectivity, incorporating multiple types of traffic. Examples include VPN, Dynamic Multipoint VPN (DMVPN), Multi-Virtual Route Forwarding (VRF) and Multiprotocol Label Switching (MPLS) secure contexts, Voice and Video Enabled VPN (V3PN), and highly secure voice.
- **Threat Defense**—Prevents and responds to network attacks and threats using network services. Examples include Cisco IOS IPS and Cisco IOS Firewall.
- **Trust and Identity**—Allows the network to intelligently protect endpoints using technologies such as Authentication, Authorization, and Accounting (AAA), Public Key Infrastructure (PKI), and 802.1x.

With SDN Collaborative Security Systems, security becomes a network-wide system, including endpoints, network, and policies. Examples include solutions like Network Admission Control (NAC), where multiple services and devices work in coordination to thwart attacks with active management.

SDN Adaptive Threat Defense (ATD) further minimizes security risks by dynamically addressing threats at multiple layers, enabling tighter control of network traffic, endpoints, users, and applications. ATD also simplifies architectural designs while lowering operational costs by consolidating services onto fewer devices. This innovative approach combines secure, multilayer intelligence, application protection, network-wide control and threat containment within high-performance solutions. Key components of ATD include better coordinated threat mitigation through Anti-X Defenses, Application Security, and Network Control and Containment. Cisco continues to deliver on this next phase of the Self- Defending Network security strategy with the release of 12.3(14)T as detailed in the examples below.

- **Anti-X Defenses**—Prevent and respond to network threats through a combination of innovative traffic and content-oriented security services. Core security enforcement technologies include firewall, Intrusion Prevention System (IPS), and anomaly detection fused with application-inspection services such as network anti-virus, anti-spyware, anti-spam, anti-phishing, Distributed Denial of Service (DDoS) mitigation, and URL filtering. This convergence brings granular traffic inspection services to key network security enforcement points, thereby containing malicious traffic before it can be propagated across the network.

  Example: Protecting web servers against compromise with Advanced Application Inspection and Control – HTTP and Email inspection engines block access to write or place content on the web server.

- **Application Security**—Provide advanced business application protection through the use of application-level access controls, application inspection, and enforcement of appropriate application-use policies, web-application control, and transaction privacy.

  Example: Mitigate worms at the edge of the network with inline Intrution Prevention – signature customization and string engine support prevent worms at the edge (anti-spyware, malware, etc).

- **Network Control and Containment**—Network intelligence and the virtualization of security technologies provides the ability to layer sophisticated auditing and correlation capabilities to control and help protect any networked element or service such as Voice over IP (VoIP) with active management and mitigation capabilities.

  Example: Maximize security while maintaining business continuity with VRF-Aware Firewall—per context firewall policy allows users to customize security policies by department without workflow disruption.

Network Foundation Protection (NFP) is an integral and pervasive component of the Cisco Self-Defending Network that protects the network infrastructure from attacks and vulnerabilities, especially at the network level. Examples include control-plane policing, Network-Based Application Recognition (NBAR), and AutoSecure.

SECURITY FEATURES AND BENEFITS OF CISCO 800, 1800, 2800, AND 3800 INTEGRATED SERVICES ROUTERS

Engineered for delivering secure services, the integrated services routers offer a unique blending of both hardware and software security features. To enable network security features on the Cisco 800, 1800, 2800, and 3800 series routers, the following Cisco IOS Software feature sets are available:

- Advanced Enterprise Services
- Advanced IP Services
- Advanced Security

For more information about selecting the appropriate feature set, visit:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5460/prod_bulletin09186a00801af451.html

Table 1 lists select hardware security features of the Cisco 800, 1800, 2800, and 3800 series integrated services routers.

Table 1. Hardware Security Features of Cisco 800, 1800, 2800, and 3800 Series Routers

Feature	Cisco 3800	Cisco 2800	Cisco 1800	Cisco 800
Built-in VPN encryption acceleration (IPSec DES, 3DES, and AES 128, 192, and 256)	Comes standard with every model Also requires Cisco IOS Software Advanced Security or higher feature set to enable	Comes standard with every model Also requires Cisco IOS Software Advanced Security or higher feature set to enable	Comes standard with every model Also requires Cisco IOS Software Advanced Security or higher feature set to enable	Comes standard with every model Also requires Cisco IOS Software Advanced Security or higher feature set to enable
Advanced VPN encryption acceleration Hardware-assisted compression with IPPCP	Optional enhancement for additional performance and tunnel scalability (part numbers: Cisco 3825: AIM-VPN/EPII—PLUS Cisco 3845: AIM-VPN/HPII—PLUS)	Optional enhancement for additional performance and tunnel scalability (part number: AIM-VPN/EPII—PLUS)	Optional enhancement for additional performance and tunnel scalability on modular Cisco 1800s (part number: AIM-VPN/BPII—PLUS)	–

Feature	Cisco 3800	Cisco 2800	Cisco 1800	Cisco 800
IDS network module*	Optional enhancement through (part number NM-CIDS)	Optional enhancement through (part number NM-CIDS*)	–	–
Content-engine network module for content security*	Optional enhancement through Cisco Content Engine Network Module (part number CE-NM)	Optional enhancement through Cisco Content Engine Network Module (part number CE-NM*)	–	–

Table 2 provides integrated security features and benefits of the Cisco 800, 1800, 2800, and 3800 series. Many of these features are also available on the complementary Cisco 7000 headend routers. Hyperlinks to additional information in this document are included for most of the features listed.

Table 2. Primary Integrated Security Features and Benefits of Cisco 800, 1800, 2800, and 3800 Series Routers

Features	Benefits
CISCO IPSEC VPN	
MPLS VPN support	Branch-office optimized customer-edge (CE) functionality plus a mechanism to extend customers MPLS-VPN networks out to the CE with Multi-VRF-aware firewall, and IPSec.
DMVPN	Provides a scalable and flexible way to establish virtual full-meshed IPSec tunnels from branch to branch. Zero configuration at hub when adding new spokes.
Cisco Easy VPN remote and server support	This feature eases administration and management of point-to-point VPNs by actively pushing new security policies from a single headend to remote sites.
V3PN	Delivers cost-effective integrated voice, video, and data over VPN to any location.
Virtual Tunnel Interface (VTI)	Simplifies VPN configuration and design
Multi-VRF and MPLS secure contexts	Supports multiple independent contexts (addressing, routing and interfaces) at the branch location for separation of departments, subsidiaries, or customers. All contexts can share a single uplink connection to the core, (for example, IPSec VPN, or Frame Relay/ATM), while still maintaining secure separation between them.
Secure Provisioning/Digital Certificates	A simple, powerful mechanism for enrolling new remote-site devices in a secure network infrastructure
CISCO IOS FIREWALL AND INLINE INTRUSION PREVENTION (IPS)	
Cisco IOS Firewall	An ideal single-device security and routing solution for protecting the WAN entry point into the network. Now with IPv6 support.
Transparent Firewall	Segment existing network deployments into security trust zones without making address changes! Support for subinterfaces and VLAN trunks. Simultaneous transparent and Layer 3 firewall support.

Features	Benefits
Advanced Application Inspection and Control	Uses inspection engines to enforce protocol conformance and prevent malicious or unauthorized behavior such as port 80 tunneling or misuse of email connectivity
VRF-Aware Firewall	Firewall now included in the list of services available at the individual context level for VRF deployments
H.323	
Inline Intrusion prevention (IPS)	An in-line, deep-packet-inspection-based solution that works with Cisco IOS Software to effectively mitigate network attacks. IPS can drop traffic, send an alarm, locally shun, or reset the connection, enabling the router to respond immediately to security threats to protect the network.
Transparent IPS	
URL filtering (off-device)	Helps enable the Cisco IOS Firewall to interact with the Websense or N2H2 URL filtering software, thereby preventing users from accessing specified Websites on the basis of company security policies.
NETWORK FOUNDATION PROTECTION (NFP)	
Control Plane Policing	Reduces the success of a DoS attack by policing the incoming rate of traffic to the control plane, helping to maintain network availability even when under attack.
AutoSecure	Simplifies router security configuration and reduces the risk of configuration errors.
NBAR	This classification engine in Cisco IOS Software can recognize a wide variety of applications. When the application is recognized, the network can invoke specific services for that particular application, providing the proper level of control they need.
CPU/memory thresholding	By reserving CPU and memory, this feature allows the router to stay operational under high loads, such as those created by attacks.
SSHv2	
SNMPv3	
Role-Based CLI Access	Provides view-based access to CLI commands, allowing highly secure, logical separation of router between NetOps, SecOps, and end users.
NETWORK CONTROL AND CONTAINMENT	
NAC	Stems the spread of viruses and worms in the network by providing access only to trusted devices that match established access and security policies.
ADDITIONAL SECURITY FEATURES	
AAA	Allows administrators to dynamically configure the type of authentication and authorization they want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis.
Standard 802.1x support on integrated switching	Standard 802.1x applications require valid access credentials that make unauthorized access to protected information resources and deployment of unsecured wireless access points more difficult.

Features	Benefits
Cisco IOS Certificate Server and Client	Allows the router to act as a certificate authority on the network.
MANAGEMENT	
Secure management with Cisco SDM	This intuitive, easy-to-use, Web-based device management tool embedded within the Cisco IOS Software access routers can be accessed remotely using HTTPS and SSH.
Enterprise security management	Two tools are available for enterprise security deployments: CiscoWorks VMS is a comprehensive management tool for mid- to large-scale VPN deployments; it can configure both IPSec tunnels and firewall rules. Cisco IP Solution Center (ISC) 3.0 is a service provider MPLS IPSec management tool.

CISCO IPSEC VPN: VPN TUNNELING AND ENCRYPTION, DMVPN, EASY VPN, V3PN, VIRTUAL TUNNEL INTERFACE (VTI), MULTI-VRF CONTEXTS, AND SECURE PROVISIONING/DIGITAL CERTIFICATES

VPN Tunneling and Encryption

VPNs have been the fastest-growing form of network connectivity and Cisco takes it to a new standard by embedding VPN hardware into its integrated services routers. The Cisco 800, 1800, 2800, and 3800 series routers include built-in hardware-based encryption acceleration which offloads the Internet Protocol Security (IPSec), Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES)—encryption and VPN processes to provide increased VPN throughput with minimal impact to the router CPU. If additional VPN throughput or scalability is required, optional VPN encryption advanced integration modules (AIMs) are available on the modular Cisco 1800, 2800, and 3800 series. The result is increased VPN performance—up to four times faster than previous models—with lower overall router CPU usage. The optional AIM provides up to 10 times the encryption performance over previous models, as well as tunnel scalability. The primary features of both the built-in and AIM-based VPN accelerators include:

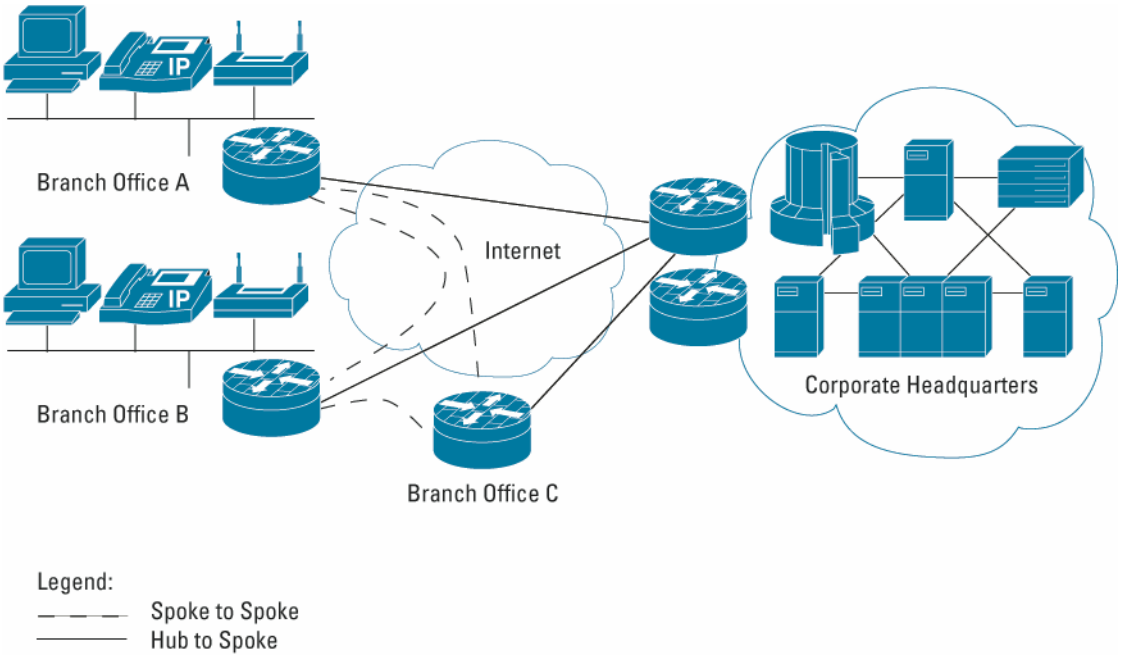
- Accelerates IPSec at speeds up to multiple, full-duplex T3/E3
- Accelerates hardware DES, 3DES, and AES (128, 192, and 256) encryption algorithms for all modules (both built-in and AIMs)
- Supports Rivest, Shamir, Aldeman (RSA) algorithm signatures and Diffie-Hellman for authentication
- Uses Secure Hash Algorithm 1 (SHA-1) or Message Digest Algorithm 5 (MD5) hashing algorithms for data integrity
- Supports Layer 3 (IP Payload Compression Protocol [IPPCP]) compression in hardware with the addition of the VPN encryption module

In addition to generic IPSec, the integrated services routers also can use an alternate tunneling technique that combines IPSec and generic routing encapsulation (GRE) protocols. The IPSec with GRE tunneling technique is a unique Cisco solution that helps enable dynamic routing protocols to be sent over the VPN, thus delivering greater network resiliency than IPSec-only solutions. In addition to providing a failover mechanism, GRE tunnels provide the ability to encrypt multicast and broadcast packets and non-IP protocols. By using GRE with IPSec, Cisco integrated services routers can support protocols, such as AppleTalk and Novell Internetwork Packet Exchange (IPX), as well as multicast and broadcast applications, such as video.

Dynamic Multipoint VPN (DMVPN)

Cisco leads the industry with the first routers to offer DMVPN functionality. Cisco DMVPN enables on-demand and scalable full-mesh VPN to reduce latency, conserve bandwidth, and simplify VPN deployments (See Figure 1). The DMVPN feature builds upon Cisco IPSec and routing expertise by enabling GRE tunnels, IPSec encryption, Next Hop Resolution Protocol (NHRP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP) to be dynamically configured. This dynamic configuration of VPN tunnels, combined with technologies such as quality of service (QoS) and IP Multicast, optimizes latency-sensitive applications such as voice and video. DMVPN also eases the administrative burden with zero configuration needed at the hub when adding new spokes or when setting up spoke-to-spoke connections.

Figure 1. Example of DMVPN



Easy VPN

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

Easy VPN offers the following benefits:

- Easy VPN supports both hardware (access routers) CPE and software remote access clients using the same central-site router. The Cisco VPN Client software can be installed on PCs, Macs, and UNIX systems to add remote access connectivity to the router-based VPN at no additional cost. Because a single technology (Easy VPN) is used for both the hardware CPE and software clients, total cost of ownership is reduced through simplification and unification of provisioning, monitoring, and AAA services.
- Easy VPN offers options of locally router-based and, centralized RADIUS and AAA authentication of both CPE routers and individual users. The 802.1x-based authentication also can be used to authenticate hosts at each CPE location.
- Easy VPN offers digital certificates, improving security over preshared keys.
- Load balancing for multiple central-site Easy VPN concentrators automatically distributes loads across multiple Easy VPN servers. Policy push of backup concentrator information to the CPEs allows companies to scale the solution without CPE reconfiguration.

- Virtualized Easy VPN Server allows service providers to offer VPN services to multiple customers using a single platform.
- Easy VPN offers full-feature integration, including dynamic QoS policy assignment, firewall and IPS, split tunneling, and Cisco Service Assurance Agent and NetFlow for performance monitoring.
- Cisco Router and Security Device Manager (SDM) allows wizard-based quick deployment of Easy VPN integrated with AAA and firewall, and real-time graphical monitoring of remote Easy VPN clients.
- Easy VPN is supported on all Cisco VPN service product lines: Cisco IOS Software, Cisco PIX Firewall, and Cisco VPN 3000 Series Concentrator

Voice and Video Enabled IPSec (V3PN)

The Cisco 800, 1800, 2800, and 3800 series and complementary Cisco 7000 headend solutions support V3PN. V3PN provides a VPN infrastructure capable of converged data, voice, and video across a highly secure, QoS-enabled IPSec network and allows customers to obtain the same performance for voice and video applications over an IP transport network as they would over an alternate WAN link—securely and effectively. Unlike many VPN devices on the market, Cisco integrated services routers accommodate the diverse network topology and traffic requirements that enable multiservice IPSec VPNs. The end-to-end network architecture of V3PN takes advantage of Cisco security-enabled routers with Cisco IOS Software to secure voice traffic.

Delivering toll-quality voice and video over IPSec VPNs requires more than just encrypting traffic—it requires a blend of advanced multiservice and IPSec VPN technologies. 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 (VTI)

VPNs are increasingly being recognized as a mainstream solution for secure WAN connectivity. They replace or augment existing private networks that use leased lines, Frame Relay, or ATM to connect remote and branch offices and central sites more cost-effectively and with increased flexibility. This new status requires that VPN devices deliver higher performance, support for both LAN and WAN interfaces, and high network availability. Cisco IPSec virtual tunnel interfaces (VTI) are a new tool which can be used by customers to configure IPSec-based VPNs between site-to-site devices. IPSec VTI tunnels provide a designated pathway across the shared WAN and encapsulate traffic with new packet headers, which helps 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.

With IPSec VTIs delivered by Cisco, enterprises can take full advantage of cost-effective VPNs and continue to add voice and video to their data network without compromising quality and reliability. Cisco IPSec VTIs provide highly secure connectivity for site-to-site VPNs and can be combined with Cisco AVVID (Architecture for Voice, Video and Integrated Data) to deliver converged voice, video, and data over IP networks.

Multi-VRF and MPLS Secure Contexts for Service Providers

Multi-VRF, also referred to as VRF-Lite, provides the ability to configure and maintain more than one instance of a routing and forwarding table within the same physical router. Multi-VRF, in combination with Ethernet VLAN technologies and WAN VPN technologies such as Frame Relay, enables the provisioning of several logical services using one physical network, extending the privacy and security to a branch-office LAN.

One Cisco router with Multi-VRF can support multiple companies with overlapping IP addresses, while maintaining a separation of data, routing, and physical interfaces. For more information about Multi-VRF, visit the Product Bulletin.

Secure Provisioning and Digital Certificates

Secure Device Provisioning (SDP) offers a simple, powerful mechanism to enroll new remote-site devices in a secure network infrastructure. Relatively unskilled remote-site administrators can launch the SDP Web interface from SDM after configuring basic Internet connectivity. Using only their username, password, and the SDP Registration URL, the remote user can fully configure their site's router for any Cisco IOS-supported

IPsec options, or a basic bootstrap configuration can be applied to introduce the router to a more complex provisioning infrastructure. SDP leverages Cisco IOS' integrated Certification Authority Server to issue secure, scalable digital certificates to IPsec network devices. This combination of solutions positions Cisco IOS as an industry leader in integrated network security.

CISCO IOS FIREWALLAND INLINE INTRUSION PREVENTION

Cisco IOS Firewall

The Cisco IOS Firewall is a stateful-inspection firewall option available for Cisco routers. Built from market-leading PIX firewall technologies, Cisco IOS Firewall is supported on all the integrated services routers with the Cisco IOS Software Advanced Security or higher feature sets. Cisco IOS Firewall is an ideal single-box security and routing solution for protecting the WAN entry point into the network. While the hub is a common location to firewall and inspect traffic for attacks, it is not the only location to consider when deploying network security. Branch offices are also an important location in your network to both firewall and inspect traffic for attacks.

The primary features of Cisco IOS Firewall include:

- Stateful firewall including DoS protection
- Enhanced application, traffic, and user awareness to identify, inspect, and control applications
- Advanced protocol inspection for voice, video, and other applications
- Per-user, interface, or subinterface security policies
- Tightly integrated identity services to provide per-user authentication and authorization
- Ease of management through features such as Role-Based CLI Access views which allows secure, logical separation of router between NetOps, SecOps, and end users, and Firewall Policy View in Cisco SDM.

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

Cisco IOS Software supports IPv6 firewall, which enables deployment in mixed IPv4 and IPv6 environments. Cisco IOS Firewall IPv6 offers stateful protocol inspection (anomaly detection) of IPv6 packets and IPv6 DoS attack mitigation.

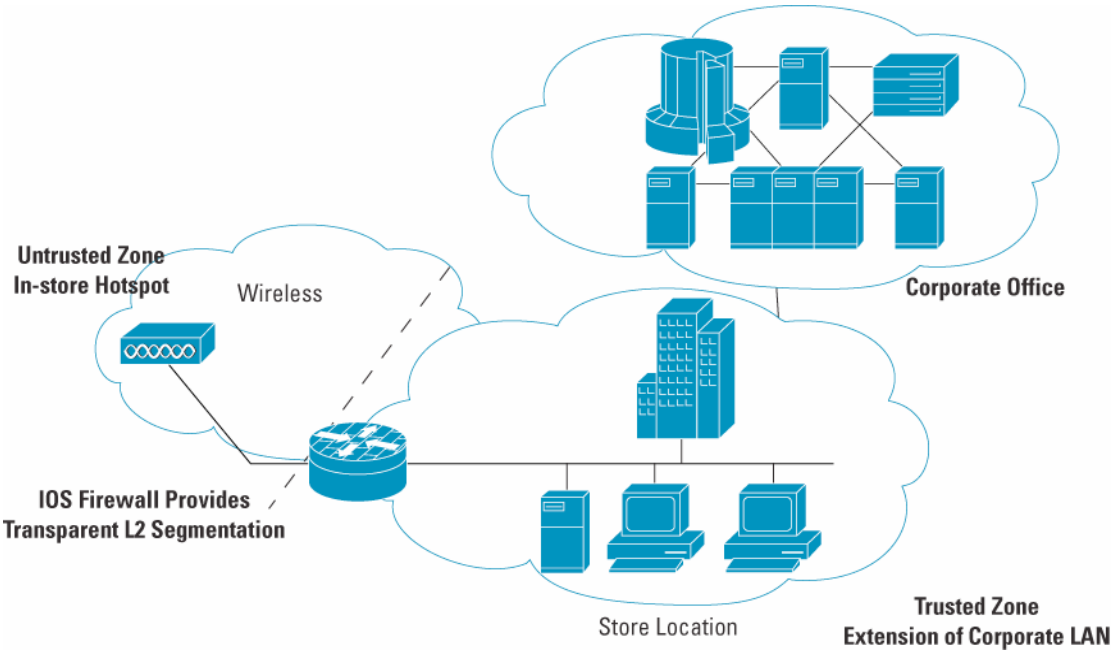
Transparent Firewall

In addition to Layer 3 stateful firewalling, the Cisco 800, 1800, 2800, and 3800 series integrated services routers and Cisco 7000 headend solutions can support transparent firewalling, which is the ability to provide Layer 3 firewalling for Layer 2 connectivity. The benefits of a transparent firewall include:

- Easy addition of firewall to existing networks with no IP subnet renumbering required
- Support for subinterfaces and VLAN trunks
- Spanning Tree Protocol support—Handles bridge-protocol-data-unit (BPDU) packets correctly per 802.1d, not just "pass or drop"
- Support for mixing Layer 2 and Layer 3 firewalling on the same router
- No need for IP addresses on the interfaces
- Support for Dynamic Host Configuration Protocol (DHCP) pass-through to assign DHCP addresses on opposite interfaces (bidirectional)

Figure 2 shows an application of Transparent Firewall.

Figure 2. Segment Existing Network Deployments into Security Trust Zones Without Making Address Change; Cisco IOS Firewall Provides Transparent Layer 2 Segmentation



Advanced Application Inspection and Control

Cisco IOS Firewall has been enhanced with the introduction of Advanced Application Inspection and Control, which currently includes HTTP and several email inspection engines. Companies may decide to permit some common applications, such as Web browsing, through their firewalls. Unfortunately, such access can result in non-HTTP applications, such as instant messaging (IM), attempting to exploit hosts behind this opening in the firewall. While traditional firewall enforcement blocks traffic based on source and destination addresses and protocol and port numbers, the Cisco IOS Firewall HTTP Inspection Engine enforces protocol conformance and prevents malicious or unauthorized behavior such as port 80 tunneling, malformed packets, and Trojans from passing through. The HTTP Inspection Engine provides Cisco IOS Firewall the intelligence to not only block non-HTTP traffic, but to help ensure traffic that is assumed to be HTTP is legitimate Web browsing and not IM or similar traffic trying to gain access through the firewall. The net result is that network administrators will have more granular control of applications passing through the firewall. Some benefits include:

- Ability to define and enforce security policies for port 80
- Control misuse of port 80 by rogue applications that tunnel traffic inside HTTP and use port 80 to avoid scrutiny
- Perform protocol anomaly detection services
- HTTP Inspection Engine
  - Detects misuse of HTTP/Web connectivity
  - Prevents protocol masquerading
  - Strict RFC compliance enforcement
  - RFC command control (for example, get or put)
  - URL- or header-length policy enforcement
  - Supports real-time alarms and audit-trail messages
  - MIME-type filtering and content validation

- Email Inspection Engine
  - SMTP/ESMTP/POP3/IMAP
  - Detects misuse of Email connectivity
  - Prevents protocol masquerading
  - Strict RFC compliance enforcement

VRF Aware Firewall

Cisco IOS Firewall is now included in the list of services available at the individual context level for VRF deployments. VRF Aware Firewall allows customers to use the power of Cisco VRF technology:

- Provides per-network VRF-aware firewall solution
- Supports current global parameters on a per-VRF basis
- Tags Syslog messages with VRF information
- Supports the ability to limit the number of firewall sessions per VRF

H.323 Support

The Cisco IOS Firewall supports H.323 Version 1 and 2 inspections. H.323 V2 provides additional options over H.323 V1, including a “fast start” option. The fast start option minimizes the delay between a user-initiated connection and receipt of the data (voice, video). H.323 V2 inspection is compatible with H.323 V1.

With H.323 V1, a separate channel for media control (H.245 channel) is opened after a TCP connection is established between the client and server (H.225 channel). Multimedia channels for audio and video are further negotiated through this channel.

The H.323 V2 client opens a connection to server, which is listening on port 1720. The data channel between the client and the server is dynamically negotiated using any of the high UDP ports (1024 to 65536).

The firewall uses this port information, along with connection information from the client, to create dynamic ACL entries in the firewall. As TCP or UDP connections are terminated, the firewall removes these dynamic entries from the appropriate ACLs.

Intrusion Prevention System (IPS)

Cisco leads the industry with the first routers to offer IPS functionality. Cisco IOS IPS is an in-line, deep-packet-inspection-based solution that helps 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 IDS Family, including Cisco IDS 4200 Series sensors, Cisco Catalyst 6500 Series IDS Services Module, and network module hardware IDS appliances. Because Cisco IOS Software IPS is in-line, it can drop traffic, enabling the router to respond immediately to security threats and protect the network.

While it is common practice to deploy an IPS system to inspect traffic for attacks at the headend, protecting branch offices is also important to help ensure that malicious traffic is stopped as close to the entry point into the network as possible. By using Cisco IOS IPS at the branch, the branch-connected routers can drop traffic, send an alarm, locally shun, or reset the connection as needed to stop attacking traffic at the point of origination and remove it from the network as quickly as possible. These actions can be configured per signature. Although IT professionals agree to this defense approach, it has always been cost-prohibitive to deploy an IPS system at every access point. Now, with an IPS solution integrated into the existing access router, it is possible to implement this best practice throughout the network with no expense beyond the router required.

Benefits:

- Provides the ability to load and enable selected IPS signatures in the same manner as Cisco IDS sensor appliances
- Supports an ever-increasing number of signatures from which to choose; currently more than 1200 of the signatures supported by Cisco IDS sensor platforms
- Allows users to modify an existing signature or create a new signature to address newly discovered threats (each signature action can be enabled individually)
- Takes advantage of worldwide virus detection ability from Trend Micro, a Cisco AVVID Partner

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

Transparent IPS

In addition to Layer 3 IPS, as of 12.4(1st)T, the Cisco 800, 1800, 2800, and 3800 series integrated services routers and Cisco 7000 headend solutions will support transparent IPS, which is the ability to provide Layer 3 IPS for Layer 2 connectivity. The benefits of a transparent IPS include:

- Easy addition of IPS to existing networks with no IP subnet renumbering required
- Support for subinterfaces and VLAN trunks
- Spanning Tree Protocol support—Handles bridge-protocol-data-unit (BPDU) packets correctly per 802.1d, not just "pass or drop"
- Support for mixing Layer 2 and Layer 3 IPS on the same router
- No need for IP addresses on the interfaces
- Support for Dynamic Host Configuration Protocol (DHCP) pass-through to assign DHCP addresses on opposite interfaces (bidirectional)

URL Filtering

Cisco has URL filtering (off-device or on-device optional) to support the Cisco IOS Firewall. This allows a customer to use either Websense or N2H2 URL filtering products with Cisco routers. The Websense URL Filtering feature helps your Cisco IOS Firewall to interact with the Websense or N2H2 URL filtering software running on a separate server, thereby allowing you to prevent users from accessing specified Websites on the basis of your security policy. The Cisco IOS Firewall works with the Websense and N2H2 server to know whether a particular URL should be allowed or denied (blocked). Refer also to the Content Engine Network Module for URL filtering capabilities on the Cisco 2800 and 3800 series for complete on-device URL filtering and content security.

NETWORK FOUNDATION PROTECTION (NFP) (CISCO IOS SOFTWARE, INCLUDED IN IP BASE AND HIGHER): CONTROL PLANE POLICING, AUTOSECURE, NBAR, CPU/MEMORY THRESHOLDING, SSHV2, SNMP AND ROLE-BASED CLI ACCESS

Control Plane Policing

Even the most robust software implementation and hardware architecture is vulnerable to a DoS attack. DoS attacks are malicious acts designed to paralyze a network infrastructure by flooding it with worthless traffic, camouflaged as specific types of control packets directed at the control plane processor. To block this and similar threats directed toward the heart of the network, Cisco IOS Software includes programmable policing functionality on routers that limits the rates of, or "polices," traffic destined for the control plane. 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

AutoSecure, a feature of Cisco IOS Software, simplifies router security configuration and reduces the risk of configuration errors. The interactive mode, suited for experienced users, prompts users to customize security settings and router services, providing greater control over the router's security functions. If an untrained user needs to quickly secure a router without much human intervention, AutoSecure's non-interactive mode is available. This mode automatically enables router security functions based on defaults set by Cisco Systems. A single command instantly configures the security posture of routers and disables nonessential system processes and services, eliminating potential network security threats.

NBAR

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 that use dynamic TCP/UDP port assignments. NBAR, when used in a security context, can detect worms based on payload signatures. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR also helps ensure that network bandwidth is used efficiently by working with QoS features to provide guaranteed bandwidth, bandwidth limits, traffic shaping, and packet coloring. SDM (see Cisco Router and Security Device Manager below) has an easy-to-use wizard to enable NBAR and also provides a graphical view of application traffic.

CPU/Memory Thresholding

Cisco IOS Software allows the ability to set global memory thresholds on memory utilization of the router and generate notifications when the thresholds are hit. By reserving CPU and memory, this feature allows the router to stay operational under high loads, such as those created by attacks.

Secure Shell Version 2

Secure Shell Protocol version 2 (SSHv2) provides powerful new authentication and encryption capabilities. More options are now available for tunneling additional types of traffic over the encrypted connection, including file-copy and e-mail protocols. Network security is enhanced by a greater breadth of authentication functionality, including digital certificates and more two-factor authentication options.

Simple Network Management Protocol Version 3 (SNMPv3)

Simple Network Management Protocol version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:

- **Message Integrity**—Helping to ensure that a packet has not been tampered with in transit.
- **Authentication**—Determining that the message is from a valid source.
- **Encryption**—Scrambling the contents of a packet to prevent it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

Role-Based CLI Access

The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS Software. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information and can define what commands are accepted and what configuration information is visible. Applications of Role-Based CLI Access include network administrators providing security personnel access to specific functions. In addition, service providers can use this feature to grant limited access to end customers to aid in troubleshooting the network. Cisco SDM ships with factory default access profiles for

administrators, read-only (for end users), firewall policy, and Easy VPN remote. Users logging into Cisco SDM with a particular role-based access can view GUI screens specific to their roles only.

NETWORK CONTROL AND CONTAINMENT: NAC

Network Admission Control (NAC)

Network Admission Control (NAC) is an industrywide collaboration effort led by Cisco Systems to help ensure that every endpoint complies with network security policies before being granted network access to limit damage caused by viruses and worms. NAC controls network access by interrogating devices connecting to the network to see if they comply with network security policies.

NAC allows networks to identify vulnerable systems and enforce effective network admission controls by allowing only trusted endpoint devices that comply with the latest corporate antivirus and operating system patch policies to access 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 sources or targets of worm and virus infections.

NAC can be enabled on the Cisco 800, 1800, 2800, and 3800 series with the Cisco IOS Software Advanced Security, Advanced IP Services, or Advanced Enterprise Services feature sets. NAC is also available on the Cisco 7000 headend routers.

NAC offers the following benefits:

- **Broad span of control**—Common access methods that hosts use to connect to the network, such as router WAN links, IPSec remote access, and dialup, are covered.
- **Multivendor solution**—Led by Cisco, NAC is the result of a multivendor collaboration with the leading antivirus vendors, including Network Associates, Symantec, and Trend Micro.
- **Extension of existing technologies and standards**—NAC extends the use of existing communication protocols and network security technologies, such as Extensible Authentication Protocol (EAP), 802.1x, and RADIUS services.
- **Extension of existing network and antivirus investments**—NAC ties together existing investments in network infrastructure and antivirus technology to provide admission control facilities.

ADDITIONAL SECURITY FEATURES

Authentication, Authorization, and Accounting (AAA)

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

802.1x

802.1x applications make unauthorized access to protected information resources more difficult through the requirement of valid access credentials. By deploying 802.1x applications, network administrators can also effectively eliminate the possibility of users deploying unsecured wireless access points, addressing one of the greatest concerns of easy-to-deploy WLAN equipment.

Cisco IOS Certificate Server and Client

The Cisco IOS Certificate Server embeds a certificate server into Cisco IOS Software, allowing the router to act as a certificate authority on the network.

Cisco Certificate Server allows for the issuing and revoking of digital certificates. Traditionally, it has been difficult to generate and manage cryptography information as VPN installations grow in size. The Cisco Certificate Server addresses these challenges with a simple, scalable, easy-to-manage certification authority built onto the same hardware supporting IPsec VPN. The Cisco IOS Certificate Server provides an important alternative to simple symmetric key deployments.

Cisco IOS also supports embedded PKI Client functionality, which interoperates with the Certificate Server and third party certificate authorities. The features of the PKI Client include:

- Support for on-box ACLs to accept/reject certificates based on certificate fields
- Integration with AAA for authorization of certificates based on username and other attributes
- Support for Online Certificate Status Protocol (OCSP)
- Support for Certification Revocation Lists and Automatic re-enrollment

HARDWARE SECURITY FEATURES OF CISCO 800, 1800, 2800, AND 3800 SERIES ROUTERS

USB Port/Removable Credentials

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

Two new features are available to take advantage of these USB ports are USB E-Token and USB Flash support. The USB E-Token feature and USB Flash feature enable Cisco routers with built-in USB ports to support E-Tokens and USB Flash memory. The USB E-Token feature provides secure configuration distribution and allows users to store VPN credentials for deployment. The USB Flash feature allows users to store images and configurations using USB Flash memory.

Secure Wireless LAN Services

The modular Cisco 1800, 2800, and 3800 series, as well as the fixed-configuration Cisco 850, 870, and 1800 Series integrated services routers offer a comprehensive suite of secure, enterprise-class wireless services to enable productivity enhancements at wireless enterprise branch offices, small and medium-sized businesses, Wi-Fi hotspots, and teleworker locations.

Benefits:

- Integrated wireless LAN access point option (802.11b/g or 802.11a/b/g) available across the entire portfolio of integrated services routers
- Extensive wireless security including support for WiFi Protected Access (WPA) and a variety of authentication types, and survivable local authentication for wireless clients at remote sites
- Access Zone Routing and Service Selection Gateway services for secure public access at WiFi hotspots
- Mobile IP services for mobility across wireless LAN and cellular networks
- Customized guest access solutions for large enterprises with Cisco Service Selection Gateway (SSG) and Cisco Subscriber Edge Services Manager (SESM)

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

For customers seeking a dedicated, hardware-based solution for IDS and content security, two network security modules are available for the Cisco 2800 and 3800 series routers.

Intrusion Detection Network Module

When the Cisco IDS Network Module (part number NM-CIDS) is added to the Cisco 2800 or 3800 series routers, it helps enable a complete IDS system as part of the Cisco IDS sensor portfolio. These IDS sensors work in concert with the other IDS components, including Cisco IDS Management Console, the CiscoWorks VPN/Security Management Solution (VMS), and Cisco IDS Device Manager, to efficiently protect customers' 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 1200 IPS signatures supported. Through collaboration with IPSec VPN and GRE traffic, this module can allow decryption, tunnel termination, and traffic inspection at the first point of entry into the network—an industry first. This reduces the need for any additional devices typically required to support the system, lowering operating expenses and capital expenditures while enhancing network security.

Content Security Network Module

For an on-device content security and URL filtering solution from Cisco, the Content Engine Network Module (NM-CE) for the Cisco 2800 or 3800 series routers operates as an integrated, fully functional Internet proxy cache and URL filtering server for Websense or SmartFilter, and can eliminate the need for separate standalone Web filtering servers. Eliminating the standalone servers can generate a significant savings

EMBEDDED SERVICES MANAGEMENT: CISCO ROUTER AND SECURITY DEVICE MANAGER (SDM)

Cisco Router and Security Device Manager (SDM)

Every Cisco 800, 1800, 2800, and 3800 series router comes with factory-installed Cisco Router and Security Device Manager (SDM) and it is also available on the Cisco 7000 headend platforms. Cisco SDM is an intuitive, Web-based device manager (GUI) for deployment and management of Cisco routers (See Figure 3). Cisco SDM enables easy router configuration and monitoring through the use of a startup wizard for quick deployment and router lock-down, smart wizards to help enable security and routing features, Cisco Technical Assistance Center (TAC)-approved router configurations, and subject-related educational content.

Cisco SDM combines 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 now synchronize the routing and security policies throughout the network, have a more comprehensive view of their router services status, and reduce their operating expenses.

Main new features in Cisco SDM 2.1.1 include support for:

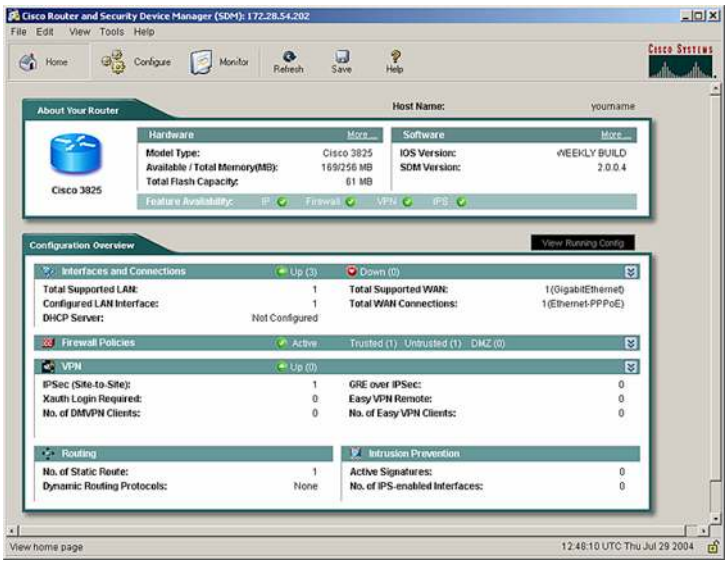
- Fixed-configuration Cisco 800 Series and 1800 Series integrated services routers
- Integrated wireless management
- Quick and easy router deployment wizard—Express Setup
- PC-based SDM (no SDM files required on router flash)
- Point-to-Point Protocol over ATM (PPPoA) configuration
- Japanese language Windows OS support
- SDM user interface translated in Japanese, Simplified Chinese, French, German, Italian, and Spanish languages [*Available by June 2005*]

Primary features in Cisco SDM 2.0 include:

- In-line IPS with updatable signatures and customizable dynamic signature update and signature customization (see IPS)
- Role-based router access
- Easy VPN server and AAA
- Digital certificates for IPSec VPNs
- VPN and WAN connection troubleshooting
- QoS policy configuration and NBAR-based application traffic monitoring

For more information about the Cisco SDM, visit http://www.cisco.com/go/sdm.

Figure 3. Cisco Router and Security Device Manager



For management of firewall and VPN features, the CiscoWorks VPN/Security Management Solution (VMS) management bundle is available. For more information about the CiscoWorks VMS, visit http://www.cisco.com/go/vms.

CERTIFICATIONS

Cisco is committed to maintaining an active product certification and evaluation program for customers worldwide. Cisco IOS VPN has achieved FIPS 140-2, Cisco IOS Firewall has achieved ICSA certification and Common Criteria EAL4+ certification is pending. Cisco recognizes that these validations are a critical component of its integrated security strategy and is dedicated to the ongoing pursuit of FIPS, ICSA, and Common Criteria certifications. For more information, please visit http://www.cisco.com/go/securitycert.

FIPS

The Cisco 800, 1800, 2800, and 3800 series have been designed to meet FIPS 140-1 Level 2 security. The NIST has upgraded FIPS 140-1 to FIPS 140-2. Cisco will now be submitting many of its routers for FIPS 140-2, Level 2.

ICSA

ICSA is a commercial security certification body that offers ICSA IPSec and ICSA Firewall Certification for various types of security products. Cisco participates in ICSA's IPSec program as well as its Firewall program.

Common Criteria

Common Criteria is an international standard for evaluating IT security. It was developed by a consortium of countries to replace numerous existing country-specific security assessment processes, and was intended to establish a single standard for international use. Currently, 14 countries officially recognize the Common Criteria. Several versions of Cisco IOS Software IPSec and Cisco routers have now been evaluated under the Australasian Information Security Evaluation Program (AISEP) against the ITSEC or the Common Criteria.

ORDERING INFORMATION

To place an order, visit the Cisco Ordering Home Page. Table 3 gives ordering information for the Cisco 800, 1800, 2800, and 3800 series routers security bundles. The breadth of Cisco's access and headend security bundles can be found at http://www.cisco.com/go/securitybundles.

Table 3. Ordering Information for Cisco 800, 1800, 2800, and 3800 Series Routers

Product Name	Part Number
Cisco 851 Secure Ethernet Router	CISCO851-K9
Cisco 876 Security Bundle with Plus ISDN Feature Set	CISCO876-SEC-I-K9
Cisco 876 Security Bundle with Plus Feature Set	CISCO876-SEC-K9
Cisco 877 Security Bundle with Plus Feature Set	CISCO877-SEC-K9
Cisco 878 Security Bundle with Plus Feature Set	CISCO878-SEC-K9
Cisco 871 Secure Ethernet Router	CISCO871-K9
Dual Ethernet Security Router with V.92 Modem Backup	CISCO1811/K9
Dual Ethernet Security Router with ISDN S/T Backup	CISCO1812/K9
Cisco 1841 Security Bundle with Advanced Security Cisco IOS Software	CISCO1841-SEC/K9
Cisco 2801 Security Bundle with Advanced Security Cisco IOS Software	CISCO2801-SEC/K9
Cisco 2811 Security Bundle with Advanced Security Cisco IOS Software	CISCO2811-SEC/K9
Cisco 2821 Security Bundle with Advanced Security Cisco IOS Software	CISCO2821-SEC/K9
Cisco 2851 Security Bundle with Advanced Security Cisco IOS Software	CISCO2851-SEC/K9
Cisco 3825 Security Bundle with Advanced Security Cisco IOS Software	CISCO3825-SEC/K9
Cisco 3845 Security Bundle with Advanced Security Cisco IOS Software	CISCO3845-SEC/K9
Cisco 1841 Enhanced Security Bundle with AIM-VPN BPII-PLUS, Advanced IP Cisco IOS Software	CISCO1841-HSEC/K9
Cisco 2801 Enhanced Security Bundle with AIM-VPN EPII-PLUS, Advanced IP Cisco IOS Software	CISCO2801-HSEC/K9
Cisco 2811 Enhanced Security Bundle with AIM-VPN EPII-PLUS, Advanced IP Cisco IOS Software	CISCO2811-HSEC/K9
Cisco 2821 Enhanced Security Bundle with AIM-VPN EPII-PLUS, Advanced IP Cisco IOS Software	CISCO2821-HSEC/K9
Cisco 2851 Enhanced Security Bundle with AIM-VPN EPII-PLUS, Advanced IP Cisco IOS Software	CISCO2851-HSEC/K9
Cisco 3825 Enhanced Security Bundle with AIM-VPN EPII-PLUS, Advanced IP Cisco IOS Software	CISCO3825-HSEC/K9
Cisco 3845 Enhanced Security Bundle with AIM-VPN HPII-PLUS, Advanced IP Cisco IOS Software	CISCO3845-HSEC/K9
Cisco 2801 V3PN Bundle with AIM-VPN EPII-PLUS, PVDM2-8, Advanced IP Cisco IOS Software, 64 MB Flash, 256 DRAM	CISCO2801-V3PN/K9

Product Name	Part Number
Cisco 2811 V3PN Bundle with AIM-VPN EPII-PLUS, PVDM2-16, Advanced IP Cisco IOS Software, FL-SRST-36, 64 MB Flash, 256 DRAM	CISCO2811-V3PN/K9
Cisco 2821 V3PN Bundle with AIM-VPN EPII-PLUS, PVDM2-32, Advanced IP Cisco IOS Software, FL-SRST-48, 64 MB Flash, 256 DRAM	CISCO2821-V3PN/K9
Cisco 2851 V3PN Bundle with AIM-VPN EPII-PLUS, PVDM2-48, Advanced IP Cisco IOS Software, FL-SRST-72, 64 MB Flash, 256 DRAM	CISCO2851-V3PN/K9
Cisco 3825 V3PN Bundle with AIM-VPN HPII-PLUS, PVDM2-64, FL-SRST-168, Advanced IP Cisco IOS Software, 64 MB Flash, 256 DRAM	CISCO3825-V3PN/K9
Cisco 3845 V3PN Bundle with AIM-VPN HPII-PLUS, PVDM2-64, FL-SRST-240, Advanced IP Cisco IOS Software, 64 MB Flash, 256 DRAM	CISCO3845-V3PN/K9
Enhanced Performance DES, 3DES, and AES VPN Encryption and Compression for Cisco 1800	AIM-VPN/BPII-PLUS
Enhanced Performance DES, 3DES, and AES VPN Encryption and Compression for Cisco 2800	AIM-VPN/EPII-PLUS
Enhanced Performance DES, 3DES, and AES VPN Encryption and Compression for Cisco 3800	AIM-VPN/HPII-PLUS
Cisco 1841 Advanced Security (Cisco IOS Software)	c184x-advsecurityk9
Cisco 2801 Advanced Security (Cisco IOS Software)	S28NASK9
Cisco 2800 Advanced Security (Cisco IOS Software)	S28NASK9
Cisco 3825 Advanced Security (Cisco IOS Software)	S382ASK9
Cisco 3845 Advanced Security (Cisco IOS Software)	S384ASK9
Cisco 1841 Advanced IP Services (Cisco IOS Software)	c184x-advipservicesk9-mz
Cisco 2801 Advanced IP Services (Cisco IOS Software)	S28AISK9
Cisco 2800 Advanced IP Services (Cisco IOS Software)	S28AISK9
Cisco 3825 Advanced IP Services (Cisco IOS Software)	S382AISK9
Cisco 3845 Advanced IP Services (Cisco IOS Software)	S384AISK9
Cisco 1841 Advanced Enterprise Services (Cisco IOS Software)	c184x-adventerprisek9-mz
Cisco 2801 Advanced Enterprise Services (Cisco IOS Software)	S28AESK9
Cisco 2800 Advanced Enterprise Services (Cisco IOS Software)	S28NAESK9
Cisco 3825 Advanced Enterprise Services (Cisco IOS Software)	S382AESK9
Cisco 3845 Advanced IP Services (Cisco IOS Software)	S384AESK9
Intrusion Detection System Network Module	NM-CIDS-K9

Product Name	Part Number
Content Engine NM—Basic Performance—20 GB	NM-CE-BP-20G-K9
Content Engine NM—Basic Performance—40 GB	NM-CE-BP-40G-K9
Content Engine NM—Basic Performance—80 GB	NM-CE-BP-80G-K9

SERVICE AND SUPPORT

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, refer to Cisco Technical Support Services or Cisco Advanced Services.

FOR MORE INFORMATION

For more information about network security on the Cisco 800, 1800, 2800, and 3800 series integrated services routers and the complementary Cisco 7000 headend security solutions, visit http://www.cisco.com/go/routersecurity or contact your local Cisco account representative.

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

205240.O_ETMG_JR_4.05

Printed in the USA