Network Security Features on the Cisco Integrated Services Routers

Product Overview

This data sheet provides an overview of the hardware and software security features available on Cisco® 800, 1800, 2800, and 3800 Series Integrated Services Routers.

Cisco 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 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).

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

- Use existing infrastructure to secure branch-office connections: You can take full advantage of your existing network infrastructure to control security threats at remote sites and conserve WAN bandwidth—without deploying additional hardware.
- Protect gateways and network infrastructure: You can safeguard your router and all entry points into your network to defend against attacks such as hacking and distributed denial-of-service (DDoS) attacks.
- Offer perimeterwide security: You have the flexibility to apply security functions, such as firewall, intrusion prevention system (IPS), content filtering, and VPN, anywhere in your network to maximize security benefits.
- Secure voice and video networks: Advanced VPN and IOS Firewall features deliver secure, high-quality voice and video and protect against call eavesdropping, toll fraud, and denial of service (DoS).
- Enable advanced teleworking: The solutions provide secure teleworking capabilities, enabling business resilience during disasters and pandemics.
- Cost-effective with both capital expenditures (CapEx) and operating expenses (OpEx): The solutions reduce the number of devices, lowering training, manageability, power, and service contract costs. In addition, security bundles provide significant savings compared to buying the router and security features separately.

Cisco Self-Defending Network

Cisco 800, 1800, 2800, and 3800 Series Integrated Services Routers and the Cisco ASR 1000 Series Aggregation Services Routers, Cisco 7200 Series Routers, and Cisco 7301 Routers are integral components of the Cisco Self-Defending Network (SDN), an architectural solution designed for the evolving security landscape. Security is integrated everywhere, and with the help of a lifecycle services approach, your enterprise can design, implement, operate, and optimize network platforms that defend critical business processes against attack and disruption, protect

privacy, and support policy and regulatory compliance controls. With Cisco IOS IP Security (IPsec) and Secure Sockets Layer (SSL) VPN, firewall, content filtering, and IPS, as well as options for additional hardware acceleration for many of those security features, Cisco integrated services routers provide a robust and adaptable security solution for the branch office.

Cisco SDN Integrated Security revolutionized network security by making every network element a point of defense, including routers, switches, appliances, and endpoints. For more information about the Cisco Self-Defending Network, visit http://www.cisco.com/go/sdn.

Security Features and Benefits of Cisco 800, 1800, 2800, and 3800 Series Integrated Services Routers

Engineered for delivering secure services, the integrated services routers offer an innovative blending of both hardware-accelerated and software security features. Available in a variety of configurations, router security bundles provide a valuable and easy way to protect the network foundation as security becomes an integral and fundamental network capability. Table 1 describes the security bundles on the Cisco 800, 1800, 2800, and 3800 Series routers.

Note: Security bundle components are subject to change.

Table 1. Cisco Integrated Services Router Security Bundles

Router Security Bundle	Description	Hardware Acceleration	Cisco IOS Software Feature Set	Cisco IOS Software Release
SEC Bundles	Base security bundle	Standard onboard hardware acceleration for IPsec	Advanced Security	12.4(3) Mainline
HSEC Bundles	Premium security bundle	IPsec advanced integration module (AIM) included for optimal IPsec and SSL performance; SSL VPN user license	Advanced Security	12.4(9)T
VSEC Bundles	Base voice and security bundle	Standard onboard hardware acceleration for IPsec and Packet Voice DSP Module (PVDM)	Advanced IP Services	12.4(9)T
HVSEC Bundles	Premium voice and security bundle	IPsec AIM module included for optimal IPsec and SSL performance	Advanced IP Services	12.4(9)T

Table 2 lists the available Cisco IOS Software feature sets to enable network security features on the Cisco 800, 1800, 2800, and 3800 Series routers.

Table 2. Cisco IOS Software Feature Sets with Security for Cisco 800, 1800, 2800, and 3800 Series Routers

Feature Set	Description
Advanced Security	IP Base plus Cisco IOS Firewall, IPS, Content Filtering, and IPsec VPN
Advanced IP Services	Advanced Security plus IP Voice, Multiprotocol Label Switching (MPLS), and IPv6
Advanced Enterprise Services	Full Cisco IOS Software

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

Table 3 lists the 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 ASR 1000 Series, Cisco 7200 Series, and Cisco 7301 Routers. For additional details about these security features, please reference Cisco Network Security Features for the Enterprise Headquarters.

Table 3. Primary Integrated Security Features and Benefits of Cisco 800, 1800, 2800, and 3800 Series Routers

Features	Benefits
Cisco VPN	
Group Encrypted Transport VPN	Group Encrypted Transport VPN offers IPsec encryption over private WAN connections without the use of tunnels. This security model introduces the concept of "trusted" group member routers that use a common security methodology that is independent of any point-to-point relationship. This solution is ideally suited for full-mesh branch-office deployments.
Dynamic Multipoint VPN (DMVPN)	DMVPN provides a scalable and flexible way to establish virtual full-meshed IPsec tunnels from branch office to branch office. No configuration is necessary at the hub when adding new spokes.
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.
MPLS VPN support	This feature offers branch office-optimized customer edge functions plus a mechanism to extend customers' MPLS VPN networks out to the customer edge with Multi-Virtual Route Forwarding (VRF)-aware firewall and IPsec.
Multi-VRF and MPLS secure contexts	The multi-VRF feature supports multiple independent contexts (addressing, routing, and interfaces) at the branch office for separation of departments, subsidiaries, or customers. All contexts can share a single uplink connection to the core (for example, IPsec VPN, Frame Relay, or ATM), while still maintaining secure separation between them.
Secure Provisioning and Digital Certificates	This simple, powerful mechanism enrolls new remote-site devices in a secure network infrastructure.
Voice and Video Enabled VPN (V3PN)	V3PN delivers cost-effective integrated voice, video, and data over VPN to any location.
Virtual Tunnel Interface (VTI)	VTI simplifies VPN configuration and design.
SSL VPN	SSL VPN provides VPN remote-access connectivity from almost any Internet-enabled location using only a web browser and its native SSL VPN encryption.
Cisco IOS Firewall	
Cisco IOS Firewall	This single-device security and routing solution protects the WAN entry point into the network. It offers IPv6 support and zone-based policy mapping for easier administration.
Advanced application inspection and control (Application Firewall)	This feature uses inspection engines to enforce protocol conformance and prevent malicious or unauthorized behavior such as port 80 tunneling or misuse of email connectivity.
Transparent Firewall	This feature segments existing network deployments into security trust zones without making address changes. It supports subinterfaces and VLAN trunks as well as simultaneous transparent and Layer 3 firewall.
VRF-Aware Firewall	A firewall is included in the list of services available at the individual context level for VRF deployments.
Firewall for secure unified communications	Cisco IOS Firewall transparently supports voice traffic, including application-level conformance of media protocol call flow and the associated open channels. It supports voice protocols such as H.323v2, v3, and v4; Skinny Client Control Protocol (SCCP); and Session Initiation Protocol (SIP) and assures protection of unified communications components such as Cisco Unified Communications Manager, Cisco Unified Border Element, and their endpoints.
Cisco IOS Intrusion Prevention (IPS)	
Inline intrusion prevention system (IPS)	This inline, deep packet inspection-based feature works to effectively mitigate network attacks. IPS can drop traffic, send an alarm, locally shun, or reset the connection, allowing the router to respond immediately to security threats to protect the network.
Transparent IPS	This feature provides Layer 3 IPS for Layer 2 connectivity.
Flexible Packet Matching (FPM)	This feature complements Cisco IOS IPS by supporting custom filters that can be defined and deployed more rapidly, before IPS signatures or antivirus patterns are updated.
Cisco Network Foundation Protection (NFP)	
AutoSecure	AutoSecure simplifies router security configuration and allows for rapid implementation of security policies with a "one-touch" device-lockdown process.
Control Plane Policing	This feature protects against a DoS attack by policing the incoming rate of traffic to the control plane, helping to maintain network availability even when under attack.
CPU or memory thresholding	By reserving CPU and memory, this feature allows the router to stay operational under high loads, such as those created by attacks.
Network-Based Application Recognition (NBAR)	This classification engine in Cisco IOS Software can recognize a wide variety of applications. When the network recognizes an application, it can invoke specific services for that particular application, providing the proper level of control it needs.

Features	Benefits
NetFlow	NetFlow technology efficiently provides the metering base for a critical set of applications, including network traffic accounting, usage-based network billing, network planning, and DoS monitoring and network monitoring capabilities. Cisco NetFlow applications collect NetFlow export data, perform data volume reduction, perform postprocessing, and give end-user applications easy access to NetFlow data.
Role-based command-line interface (CLI) access	This feature provides role-based access to CLI commands, allowing highly secure, logical separation of the router between network operations groups, security operations groups, and end users.
Secure Shell (SSH) Protocol Version 2	SSHv2 provides powerful new authentication and encryption capabilities with options for tunneling additional types of traffic over the encrypted connection, including file-copy and email protocols.
Simple Network Management Protocol Version 3 (SNMPv3)	This interoperable standards-based protocol for network management provides secure access to devices by authenticating and encrypting packets over the network.
Cisco Network Admission Control (NAC)	
NAC	NAC stops the spread of viruses and worms in the network by providing access to only trusted devices that match established access and security policies.
Additional Security Features	
Authentication, authorization, and accounting (AAA)	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, Internetwork Packet Exchange [IPX], or virtual private dialup network [VPDN]) basis.
Cisco IOS Certificate Server and Client	This feature allows the router to act as a certificate authority on the network.
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.
Cisco IOS Content Filtering	Cisco IOS Content Filtering offers category-based productivity and security ratings for small and medium-sized businesses (SMBs) and midmarket companies. Content-aware security ratings protect against malware, malicious code, phishing attacks, and spyware. URL and keyword blocking help to ensure that employees are productive when accessing the Internet. This subscription-based hosted solution takes advantage of an in-the-cloud threat database, and is closely integrated with Cisco IOS Software.
Secure Management	
Cisco Configuration Professional	This web-based device management tool simplifies router, security, unified communications, wireless, WAN, and basic LAN configuration through easy-to-use wizards.
Enterprise Security Management	• Cisco Security Manager is a powerful but easy-to-use solution to centrally provision all aspects of device configuration and security policies for Cisco firewalls, VPNs, and IPSs. • Cisco Security Monitoring, Analysis and Response System (CS-MARS) is an integrated security-event manager. • Cisco IP Solution Center (ISC) 3.0 is a service provider MPLS IPsSec management tool.

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

Built-in VPN encryption acceleration comes standard on the Cisco 800, 1800, 2800, and 3800 Series Integrated Services Routers, but requires a Cisco IOS Software Advanced Security or higher feature set to enable it. IPsec Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES) 128, 192, and 256 are supported.

USB Port and Removable Credentials

The Cisco 800, 1800, 2800, and 3800 Series Integrated Services Routers were designed with onboard USB 1.1 ports, enabling important security and storage capabilities. These capabilities help to secure user authentication, store removable credentials for establishing secure VPN connections, securely distribute configuration files, and provide bulk flash memory storage for files and configuration.

Taking advantage of these USB ports, USB E-Tokens can provide secure configuration distribution and allow users to store VPN credentials for deployment. USB flash memory allows users to store images and configurations.

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, SMBs, Wi-Fi hotspots, and teleworker locations.

Benefits include the following:

- Integrated wireless LAN access point option (802.11n, 802.11b/g, or 802.11a/b/g) available across the entire portfolio of integrated services routers
- Extensive wireless security, including support for Wi-Fi Protected Access (WPA) and a variety of authentication types, and survivable local authentication for wireless clients at remote sites
- Access-zone routing and customizable subscriber services for secure public access at Wi-Fi hotspots
- Mobile IP services for mobility across wireless LAN and third-generation (3G) wireless WAN networks

Cisco Security Modules: Additional Security Options for Cisco 1841 and Cisco 2800 and 3800 Series Routers

For customers seeking additional hardware-based acceleration, several security-based modules are available for the Cisco 1841 and Cisco 2800 and 3800 Series routers.

Cisco IPsec VPN Advanced Integration Module

The VPN AIM for the Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers optimizes VPN performance for both IPsec and SSL VPN deployments. It provides up to 40 percent better performance for IPsec VPN over the built-in IPsec encryption, and up to twice the performance for Cisco IOS SSL VPN encryption.

Cisco Intrusion Prevention System Advanced Integration Module and Network Module

The Cisco Intrusion Prevention System Advanced Integration Module (IPS AIM) and IPS Network Module (IPS NME) for the Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers brings hardware-based intrusion prevention to branch offices and small businesses. With the ever-increasing complexity and sophistication of security threats, every point of the network can be at risk. Cisco IPS can accurately identify, classify, and stop malicious traffic, including worms, spyware, malware, adware, network viruses, and application abuse. Vigilant protection helps ensure business continuity and minimizes the effect of costly intrusions. Running Cisco IPS Sensor Software, the Cisco IPS AIM can monitor up to 45 Mbps of traffic and is suitable for T1/E1 and T3 environments. Cisco IPS AIM interoperates with a variety of Cisco IOS Software security features.

Cisco NAC Network Module

The Cisco NAC Network Module brings the feature-rich Cisco NAC Appliance Server capabilities to Cisco 2800 and 3800 Series Integrated Services Routers. The Cisco NAC Appliance (formerly Cisco Clean Access Server) is a rapidly deployable NAC product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network.

The integration of Cisco NAC Appliance Server capabilities into a network module for integrated services routers allows network administrators to manage a single device in a branch office for data, voice, and security requirements, reducing network complexity, IT staff training, equipment sparing requirements, and maintenance costs.

Embedded Services Management

Cisco Configuration Professional (CCP)

Cisco Configuration Professional is a valuable, productivity-enhancing tool for network administrator and channel partners deploying routers in medium-sized businesses and enterprise branch offices. Cisco Configuration Professional allows them to implement router, unified communications, security, and wireless network configurations with reduced cost and increased confidence and ease. Futher, Cisco Configuration Professional configurations have been approved by the Cisco Technical Assistance Center (TAC). Cisco Configuration Professional also helps customers avoid potential network issues by proactively monitoring router performance statistics, system logs, and security logs in real time.

Cisco Configuration Professional offers smart wizards and advanced configuration support for Cisco LAN and WAN interfaces, Network Address Translation (NAT), stateful and application firewall policy, IPS, IPsec VPN, QoS, and NAC policy features. Cisco Configuration Professional assumes a general understanding of networking technologies and terms but assists individuals unfamiliar with the Cisco CLI.

For more information about the Cisco Configuration Professional, visit http://www.cisco.com/go/ccp.

Cisco Security Manager and Cisco Security MARS

For enterprisewide management of firewalls and VPN features, the Cisco Security Management Suite is an integrated security-event manager that includes the new Cisco Security Manager and Cisco Security MARS. For more information about the Cisco Security Manager and Cisco Security MARS, visit http://www.cisco.com/go/mars.

Certifications

Cisco is committed to maintaining an active product security certification and evaluation program for customers worldwide. We recognize that these validations are a critical component of its integrated security strategy and are dedicated to the ongoing pursuit of Federal Information Processing Standards (FIPS), International Computer Security Association (ICSA), and Common Criteria certifications. For more information, please visit: http://www.cisco.com/go/securitycert.

FIPS

The National Institute of Standards and Technology (NIST) is a nonregulatory federal agency within the U.S. Commerce Department's Technology Administration that develops and promotes measurement, standards, and technology. The Cisco 800, 1800, 2800, and 3800 Series routers are designed to meet NIST's FIPS certification.

Common Criteria

Common Criteria is an international standard for evaluating IT security developed by a consortium of countries to replace numerous existing country-specific security assessment processes. It 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 been evaluated under the Australasian Information Security Evaluation Program (AISEP) against the Information Technology Security Evaluation Criteria (ITSEC) or the Common Criteria.

Ordering Information

To place an order, visit the Cisco Ordering Home Page. Security bundles offer you significant return on investment (ROI) through sizable price reductions, versus adding security later. Ordering details for the Cisco 800, 1800, 2800, and 3800 Series router security bundles are available at the following link http://www.cisco.com/go/securitybundles.

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 can 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 ASR 1000 Series and Cisco 7000 Series headend security solutions, visit http://www.cisco.com/go/routersecurity or contact your local Cisco account representative.

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.

Printed in USA C78-502073-00 10/08