Network Security Features for Cisco Integrated Services Routers Generation 2 Platform

This data sheet provides an overview of the network security features available on Cisco® Integrated Services Routers Generation 2 (ISR G2) platforms, including the Cisco 1900, 2900, and 3900 Series Integrated Services Routers.

Product Overview

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.

With routing performance and IP Security (IPSec) VPN and firewall acceleration up to five times that of previous integrated services routers with services enabled, the Cisco 1900, 2900, and 3900 Series Integrated Services Routers are ideal for small businesses and enterprise branch offices (Figure 1). The routers deliver a rich, integrated solution for connecting remote offices, teleworkers, 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 a cost-effective approach to meet the latest branch-office services requirement, accomplished while taking advantage of existing network designs and operational best practices.

Ultimate Experience

Protect your network from all threats while enhancing the branch-office experience:

- **Up to 5x performance increase** over previous generation routers
- **Secure collaboration and video networks:** Advanced VPN and Cisco IOS Firewall features deliver secure, high-quality voice and video and protect against call eavesdropping, toll fraud, and denial of service (DoS).
- **Secure mobility** with 802.11n wireless integration

Borderless Services

Through borderless services, you use the 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. 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. Recent highlights include:

- **Secure cloud computing services:** Group Encrypted Transport VPN gives you the tools to create secure clouds computing, enabling regulatory compliance—especially from the perspective of data in transit.
- **Secure unified mobile architecture:** This architecture provides an open framework for smart phones by using Cisco security, VPN, and public-key-infrastructure (PKI) technologies as enablers for provisioning, deploying, and managing mobile services. It provides a secure mobile infrastructure for a variety of different services such as voice, roaming, Wi-Fi, email messages, etc.

- **Cisco Virtual Office as a Service:** This service delivers advanced secure teleworking, enabling business resilience during disasters and pandemics.

Total Cost of Ownership

Router-based network security solutions reduce both capital expenditures (CapEx) and operating expenses (OpEx) by lowering the number of devices, training, manageability, power, and service contract costs. In addition, security bundles provide significant savings compared to buying the router and security features separately.

- **One-touch PSIRT update:** This router-based solution allows you to automatically download Product Security Incident Response Team (PSIRT) responses from Cisco.com. Optionally, the update allows you to implement the PSIRT recommendations.
- **Advanced instrumentation:** Router-based advanced instrumentation capabilities help you provision; monitor; maintain; make network performance measurements; collect and measure data; and troubleshoot the device, the network, and the services that are enabled.
- **Hardened foundational security:** You can safeguard your router and all entry points into your network to defend against attacks such as hacking and distributed DoS (DDoS) attacks.

Figure 1. Cisco 1900, 2900, and 3900 Series Integrated Services Router Portfolio

Security Features and Benefits of Cisco 1900, 2900, and 3900 Series Integrated Services Routers

New and improved software packaging has been introduced into Cisco IOS Software Release 15.0. A single universal image ships with Cisco 1900, 2900, and 3900 Series Integrated Services Routers. This single image contains the full suite of software functions previously available in several feature sets across eight different software images.

Three Cisco IOS Technology Package Licenses (Security, Unified Communications, and Data) are available as add-ons to the base image. Enabling the Security Technology Package, for example, requires purchasing and enabling a new license key. This key unlocks the security capabilities instantly, eliminating the need to download upgrades or to upgrade equipment in remote offices.

The preferred alternative would be to order a security bundle for the Cisco ISR G2, which includes the Security Technology Package License.

In addition to the Security Technology Package License, certain features require software activation Feature Licenses and Subscription Licenses. These features include Cisco IOS Secure Sockets Layer (SSL) VPN, Cisco IOS Intrusion Prevention System (IPS), and Cisco IOS Content Filtering.

Table 1 lists the features and corresponding feature licenses that provide entitlement for Cisco 1900, 2900, and 3900 Series Integrated Services Routers.

Table 1. Security License Requirements for Cisco 1900, 2900, and 3900 Series Integrated Services Routers

Features	License Required
Authentication, authorization, and accounting (AAA), NetFlow, Network-Based Application Recognition (NBAR), access control lists (ACLs), Cisco IOS Flexible Packet Matching (FPM), 802.1x, and Cisco IOS Network Foundation Protection	None (available in base image)
Standard IP Security (IPSec), Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), Easy VPN and Enhanced Easy VPN, Virtual Tunnel Interface (VTI), Multi-Virtual Route Forwarding (VRF) Customer Edge (CE) (IPSec, firewall, and IPS), IPSec high availability, Cisco IOS Zone-Based Firewall, advanced application inspection and control, firewall for secure unified communications, VRF-aware firewall, firewall high availability, transparent firewall, Cisco IOS IPS, transparent IPS, VRF-aware IPS, secure provisioning and digital certificates, and Cisco IOS Certificate Server and Client	Security Technology Package License
Cisco IOS SSL VPN	Security Technology Package License + SSLVPN Feature License
Cisco IOS Content Filtering	Security Technology Package License + Content Filtering Subscription License
Cisco IOS IPS Subscription Service	Security Technology Package License + IPS Service

For more details about purchasing these licenses, refer to the “Ordering Information” section.

Table 2 lists integrated security features and benefits of Cisco 1900, 2900, and 3900 Series Integrated Services Routers. For more detailed information about these features, refer to the in-depth network security features data sheet at http://www.cisco.com/go/isrg2.

Table 2. Primary Integrated Security Features and Benefits of Cisco 1900, 2900, and 3900 Series Integrated Services Routers

Features	Description and Benefits
Secure Connectivity	
Standard IPSec	IPSec standards supported include Digital Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES; 128, 192, and 256) for encryption; Rivest, Shamir, Aldeman (RSA) algorithm signatures and Diffie-Hellman for authentication; and Secure Hash Algorithm 1 (SHA-1) or Message Digest Algorithm 5 (MD5) hashing algorithms for data integrity.
Group Encrypted Transport VPN	Group Encrypted Transport VPN eliminates the need for compromise between network intelligence and data privacy in private WAN environments. Service providers can finally offer managed encryption without provisioning and management difficulties because Group Encrypted Transport VPN simplifies the provisioning and management of VPN. Group Encrypted Transport VPN defines a new category of VPN, one that does not use tunnels.
DMVPN	This Cisco innovation for site-to-site VPNs provides a scalable and flexible way to establish virtual full-meshed IPSec connectivity between multiple locations. DMVPN features advanced spoke-to-spoke capabilities that enhance the performance of latency-sensitive voice applications. For the traditional hub-and-spoke model, DMVPN significantly reduces deployment complexity.
Easy VPN and Enhanced Easy VPN	Providing advanced value-add to IPSec standards, these features ease administration and management of point-to-point VPNs by actively pushing new security policies from the central headend router to remote sites. Enhanced Easy VPN features integrate with dynamic VTI for maximum ease of use and advanced per-user and tunnel-specific capabilities.
Cisco IOS SSL VPN	Cisco IOS SSL VPN provides secure remote-user access to corporate resources over the public Internet using only a web browser and its native SSL encryption.
VTI	You can configure these virtual interfaces directly with IPSec. VTI greatly simplifies VPN configuration and design over alternatives such as encapsulating IPSec inside generic routing encapsulation (GRE). It allows for per-user attributes and tunnel-specific features, offering administrators greater flexibility to respond to granular requirements. Both static and dynamic VTI are supported.
Multi-VRF and Multiprotocol Label Switching (MPLS) secure contexts	This feature supports multiple independent contexts (addressing, routing, and interfaces) at the branch-office 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 or ATM), while still maintaining secure separation between them.

Features	Description and Benefits
IPSec high availability	With options such as IPSec Stateful Failover and Hot Standby Router Protocol (HSRP) with Reverse Route Injection (RRI), Cisco VPNs support numerous features for deploying redundancy and load balancing.
Integrated Threat Control	
Cisco IOS Firewall	Cisco IOS Firewall is an ideal single-device security and routing solution for protecting the WAN entry point into the network. Important features include zone-based policies; advanced application inspection and control for HTTP and email messages; firewall for secure unified communications; VRF-aware firewall, IPv6 support, and firewall high availability.
Cisco IOS IPS	Cisco IOS IPS offers an inline, deep-packet-inspection-based solution that works with Cisco IOS Software to effectively mitigate network attacks. It can drop traffic, send an alarm, or locally shun or reset the connection, helping the router respond immediately to security threats to protect the network. Important features include: inline function (can drop packets); ready-made “most-likely” signature file packages; Cisco Security Intelligence Operation (SIO) worldwide virus detection; customizable signatures; transparent IPS; and VRF-aware IPS.
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.
NetFlow	NetFlow provides anomaly-based detection of DDoS attacks and supplies data that aids in tracing the attack source and reacting to the attack in real time.
NBAR	This deep inspection mechanism provides control over a wide variety of applications by recognizing and classifying them. When an application is classified, the network can then provide specific services for that application.
FPM	FPM uses flexible and granular Layer 2–7 pattern matching deep within the packet header or payload to provide a rapid first line of defense against network threats and notable worms and viruses.
Trust and Identity	
PKI client (x.509 digital certificates)	Cisco IOS Software supports embedded PKI client functions that provide customers with a scalable and secure mechanism for distributing, managing, and revoking encryption and identity information. Advanced provisioning features provide powerful mechanisms to automate enrollment of new remote nodes into the network infrastructure with maximum security.
Cisco IOS certificate server	Cisco IOS Software includes an embedded scalable easy-to-manage certificate server, allowing the router to act as a certification authority on the network.
Standard 802.1x-based identity services	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.
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 Network Foundation Protection	
AutoSecure	AutoSecure offers a single command-line interface (CLI) command that instantly configures the security posture of routers and disables nonessential system processes and services, thereby eliminating potential security threats.
Control Plane Policing and Protection	This feature protects the route processor from unnecessary or malicious levels of traffic, including DoS attacks.
CPU and memory thresholding notification	This feature triggers a syslog notification when a specified percentage of CPU resources for a given process exceeds or falls below a certain threshold for a configured time period.
Routing protection	This feature validates routing peers, enhances routing stability, and provides overload protection by using MD5 peer authentication and redistribution protection.
ACL protection	These features protect the router from malicious traffic by restricting the legitimate traffic that can be sent to the router destination address.
Secure access mode (silent mode)	Secure access mode suppresses response messages from the router control plane, limiting network reconnaissance information available to hackers.
Raw IP traffic export	This feature allows copies of inbound and outbound packets to efficiently capture packets with analysis or intrusion-detection-system (IDS) tools by sending them out a LAN interface.
Source-based Remote-Triggered Black Holing (RTBH) filtering	This feature provides wire-rate, real-time defense against DDoS attacks using a combination of IP routing features.
Unicast Reverse Path Forwarding (uRPF)	uRPF helps mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.
Digital image signing	This feature provides SHA-512 hashing and RSA 2048-bit key encryption mechanisms to ensure the authenticity of all downloaded Cisco IOS Software images.
Cisco IOS Software login enhancements	These enhancements delay potential dictionary attacks and provide other methods of thwarting unwanted device access.
Role-based CLI access	This feature provides view-based access to CLI commands, allowing highly secure, logical separation of the router between network operations, security operations, and end users.

Features	Description and Benefits
Secure Shell (SSH) Protocol Version 2	SSHv2 enhances previous versions of SSH for remote network management by concealing password length, making dictionary attacks more difficult. It resolves SSHv1 vulnerability to man-in-the-middle attacks during user authentication.
Simple Network Management Protocol (SNMP) Version 3	SNMPv3 provides secure, standards-based management and control of devices for customer applications.

USB Port and Removable Credentials

The Cisco 1900, 2900, and 3900 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 you to store VPN credentials for deployment. USB flash memory allows you to store images and configurations.

Cisco Intrusion Prevention System Network Module

You can deploy the Cisco Intrusion Prevention System Network Module (IPS NME), which brings hardware-based intrusion prevention to branch offices and small businesses, within Cisco 1900, 2900, and 3900 Series Integrated Services Routers. 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 NME can monitor up to 75 Mbps of traffic, and is suitable for multiple T1/E1 and T3 environments. Cisco IPS NME interoperates with a variety of Cisco IOS Software security features.

For more information about the Cisco IPS NME, visit http://www.cisco.com/en/US/products/ps8395/index.html.

Cisco NAC Network Module

You can use the Cisco Network Access Control (NAC) Network Module, which adds the feature-rich Cisco NAC Appliance Server capabilities, with Cisco 2900 and 3900 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.

For more information about the Cisco NAC Network Module, visit http://www.cisco.com/en/US/products/ps8788/index.html.

Security Management

Cisco Configuration Professional

Cisco Configuration Professional is a valuable, productivity-enhancing embedded management tool for network administrators and channel partners deploying routers in medium-sized businesses and enterprise branch offices. The application allows you to implement router, unified communications, security, and wireless network configurations with reduced cost and increased confidence and ease. Cisco Configuration Professional configurations have been approved by the Cisco Technical Assistance Center (TAC). Cisco Configuration

Professional also helps you avoid potential network problems 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, quality of service (QoS), and NAC policy features. The application assumes a general understanding of networking technologies and terms but assists individuals unfamiliar with the Cisco CLI.

Cisco Security Management Suite

The Cisco Security Management Suite is a framework of products and technologies designed for scalable policy administration and enforcement for the Cisco Self-Defending Network. This integrated solution can simplify and automate the tasks associated with security management operations, including configuration, monitoring, analysis, and response. The main components of this suite follow:

- **Cisco Security Monitoring, Analysis and Response System (MARS):** This appliance-based, all-inclusive solution allows network and security administrators to monitor, identify, isolate, and counter security threats.
- **Cisco Security Manager:** This enterprise-class management application is designed to configure firewall, VPN, and IPS security services on Cisco network and security devices. You can use this application in networks of all sizes—from small networks to large networks consisting of thousands of devices—by using policy-based management techniques. Cisco Security Manager Release 3.3.1 adds support for the Cisco 1900, 2900, and 3900 Series Integrated Services Routers.

These applications are integrated to allow you to continuously monitor and improve the security of your network as threats arise.

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 our integrated security strategy and are dedicated to the ongoing pursuit of Federal Information Processing Standards (FIPS) and Common Criteria certifications.

For more information, visit http://www.cisco.com/go/securitycert.

Ordering Information

To place an order, visit the Cisco Ordering Homepage.

Security bundles include the Security Technology Package License, which offers you significant ROI through price reductions, versus adding security later. A comprehensive list of the Cisco 1900, 2900, and 3900 Series Integrated Services Router security bundles is available at http://www.cisco.com/go/securitybundles.

Security Technology Package Licenses are required to upgrade routers that are not part of security bundles. Paper licenses are delivered by mail (in paper form). E-delivery licenses are delivered immediately in an email message. Table 3 provides a list of Security Technology Package License part numbers.

Table 3. Security Technology Package License Part Numbers for Cisco 1900, 2900, and 3900 Series Integrated Services Routers

License	Description
SL-19-SEC-K9(=)	Security License (Paper) for Cisco 1941
SL-29-SEC-K9(=)	Security License (Paper) for Cisco 2901-2951
SL-39-SEC-K9(=)	Security License (Paper) for Cisco 3925/3945

License	Description
L-SL-19-SEC-K9=	Security License (E-Delivery) for Cisco 1941
L-SL-29-SEC-K9=	Security License (E-Delivery) for Cisco 2901-2951
L-SL-39-SEC-K9=	Security License (E-Delivery) for Cisco 3925/3945

Additionally, Feature and Subscription Licenses are required for certain features. Refer to Tables 4-5 for the list of available part numbers.

Table 4. SSL VPN Feature License Part Numbers for Cisco 1900, 2900, and 3900 Series Integrated Services Routers

License	Description
FL-SSLVPN10-K9(=)	Cisco SSLVPN Clientless Feature license PAK (Paper) – 10 Clientless Users
FL-SSLVPN25-K9(=)	Cisco SSLVPN Clientless Feature license PAK (Paper) – 25 Clientless Users
FL-SSLVPN100-K9(=)	Cisco SSLVPN Clientless Feature license PAK (Paper) – 100 Clientless Users
L-FL-SSLVPN10-K9(=)	Cisco SSLVPN Clientless Feature license PAK (E-Delivery) – 10 Clientless Users
L-FL-SSLVPN25-K9(=)	Cisco SSLVPN Clientless Feature license PAK (E-Delivery) – 25 Clientless Users
L-FL-SSLVPN100-K9(=)	Cisco SSLVPN Clientless Feature license PAK (E-Delivery) – 100 Clientless Users

Table 5. Content Filtering Subscription License Part Numbers for Cisco 1900, 2900, and 3900 Series Integrated Services Routers

License	Description
FL-19-CNFIL-1Y(=)	IOS Content Filtering 1 YR Subscription License PAK (Paper) for Cisco 1941-1941W
FL-29-CNFIL-1Y(=)	IOS Content Filtering 1 YR Subscription License PAK (Paper) for Cisco 2901-2951
FL-39-CNFIL-1Y(=)	IOS Content Filtering 1 YR Subscription License PAK (Paper) for Cisco 3925-3945
L-FL-19-CNFIL-1Y(=)	IOS Content Filtering 1 YR Subscription License PAK (E-Delivery) for Cisco 1941-1941W
L-FL-29-CNFIL-1Y(=)	IOS Content Filtering 1 YR Subscription License PAK (E-Delivery) for Cisco 2901-2951
L-FL-39-CNFIL-1Y(=)	IOS Content Filtering 1 YR Subscription License PAK (E-Delivery) for Cisco 3925-3945

Cisco Services for IPS provides signature file updates, Cisco Intellishield search access and threat defense bulletins, along with hardware advanced and onsite parts replacement options, operating system updates, and 24 x 7 x 365 TAC support. Table 6 provides a list of Cisco Services for IPS part numbers for Cisco IOS IPS and Cisco IPS NME respectively.

Table 6. Cisco Services for IPS Part Numbers for Cisco 1900, 2900, and 3900 Series Integrated Services Routers

License	Description
CON-SU1-XXXXXXXX*	CISCO SERVICES FOR IPS 8X5XNBD Cisco IPS For 19xx, 29xx or 39xx
CON-SU2-XXXXXXXX*	CISCO SERVICES FOR IPS 8X5X4 Cisco IPS For 19xx, 29xx or 39xx
CON-SU3-XXXXXXXX*	CISCO SERVICES FOR IPS 24x7x4 Cisco IPS For 19xx, 29xx or 39xx
CON-SU4-XXXXXXXX*	CISCO SERVICES FOR IPS 24x7x2 Cisco IPS For 19xx, 29xx or 39xx
CON-SUO1-XXXXXXXX*	CISCO SERVICES FOR IPS ONSITE 8X5XNBD Cisco IPS For 19xx, 29xx or 39xx
CON-SUO2-XXXXXXXX*	CISCO SERVICES FOR IPS ONSITE 8X5X4 Cisco IPS For 19xx, 29xx or 39xx
CON-SUO3-XXXXXXXX*	CISCO SERVICES FOR IPS ONSITE 24x7x4 Cisco IPS For 19xx, 29xx or 39xx
CON-SUO4-XXXXXXXX*	CISCO SERVICES FOR IPS ONSITE 24x7x2 Cisco IPS For 19xx, 29xx or 39xx

*xxxxxxxx-suffix specific to Cisco 1900, 2900 or 3900 Series product identification

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a

clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies.

For More Information

For more information about network security on Cisco 1900, 2900, and 3900 Series Integrated Services Routers, 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 C78-556151-00 09/09