Network Security Features for the Enterprise Headquarters

This data sheet provides an overview of the network security features available on the Cisco® 7301 Router and Cisco 7200 Series routers.

Executive Summary

Cisco integrated router security delivers the industry's most comprehensive and cost-effective security services, intelligently embedding routing and security functions for fast, scalable delivery of mission-critical business applications. With the Cisco 7301 and Cisco 7200 Series routers, enterprise customers can take advantage of this Cisco Systems® solution to evolve network foundations, increasing return on investment (ROI) and reducing operating expenses. And the solution offers the performance and scalability to support globally expanding networks.

By combining proven Cisco IOS® Software functions and industry-leading LAN and WAN connectivity with world-class network security features, Cisco 7301 and Cisco 7200 Series routers offer customers the following benefits:

- Aggregate site-to-site and remote-access VPNs in a single network platform, simplifying operations and reducing training costs
- Provide advanced security, including detection of and response to distributed denial-of-service (DDoS) attacks on corporate servers and other resources
- Build a high degree of resiliency into the network edge, keeping edge routers available if they are themselves targeted

Cisco integrated router security for enterprise headquarters incorporates a comprehensive suite of security services for securely extending business resources to remote sites, business partners, teleworkers, and mobile workers. Enterprise headquarters often have requirements for high-scale, high-performance solutions that simultaneously provide flexibility in business service offerings. Enterprise solutions must meet the critical up-time requirements of large, fast-paced environments.

Product Overview

The Cisco 7301 and Cisco 7200 Series routers are ideal for midsize to large enterprise organizations, delivering a rich, integrated security solution for connecting remote offices, mobile users, and partner extranets. Included as part of a Cisco 7200 security bundle, the Cisco VPN Services Adapter (VSA) provides the highest-performance encryption and key-generation services for IP Security (IPSec) VPN applications available in a midrange router. The VSA requires the Cisco 7200 Series NPE-G2 Network Processing Engine and fits in the I/O controller slot on the Cisco 7204VXR or 7206VXR chassis, conveniently conserving valuable slot density for other port adapters.

The Cisco 7301 and Cisco 7200 Series routers are designed for the enterprise headquarters, providing a combination of security features and advanced network services that offer a flexible, integrated approach to accommodate evolving network environments.

Cisco Self-Defending Network

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. Unlike point solution strategies, a network-based approach is a strategic approach; one that meets today's challenges with the flexibility to keep ahead of the curve.

Cisco Self-Defending Network is built upon the key principles of:

- Integration of security throughout existing infrastructure—built in, not bolted on
- Collaboration between security and network so they leverage each other and work in harmony together
- Adaptability: the ability of the network to intelligently evolve and adapt to emerging threats

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

Security Features and Benefits of Cisco 7301 and Cisco 7200 Series Routers

Engineered to deliver secure services, the Cisco 7301 and Cisco 7200 Series routers offer a unique blending of both hardware and software security features. Table 1 lists select hardware security features on these routers.

Table 1. Hardware Security Features of Cisco 7301 and Cisco 7200 Series Security Bundles

Feature	Cisco 7206 NPE-400 Security Bundle	Cisco 7206 NPE-G1 Security Bundle	Cisco 7206 NPE-G2 Security Bundle	Cisco 7301 Security Bundle
Advanced VPN Encryption Acceleration (IPSec Data Encryption Standard [DES], Triple DES [3DES], and Advanced Encryption Standard [AES] 128, 192, and 256)	VAM2+ (included)	VAM2+ (included)	VAM2+ or VSA (included), depending on the bundle	VAM2+ (included)

Cisco secure connectivity solutions protect the privacy and integrity of all information while cost-effectively creating a manageable communications infrastructure. Cisco threat control solutions protect against threats caused by Internet use, attacks and intrusions, and improper data access. Table 2 provides the integrated security features and benefits of the Cisco 7301 and Cisco 7200 Series routers. Many of these features are also available on the complementary Cisco 800 1800, 2800, and 3800 integrated services 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 7301 and Cisco 7200 Series Routers

Features	Benefits
Cisco VPN	
GET VPN	Revolutionary technology that provides IPsec encryption over private WAN connections without the use of tunnels.
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.
Easy VPN	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	Customer-edge (CE) and Provider-edge (PE) functionality plus a mechanism to extend customers MPLS-VPN networks out to the CE with Multi-VRF-aware firewall, and IPSec.

Features	Benefits
Multi-VRF and MPLS secure contexts	Supports multiple independent contexts (addressing, routing and interfaces) 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
V3PN	Delivers cost-effective integrated voice, video, and data over VPN to any location.
Virtual Tunnel Interface (VTI)	Simplifies VPN configuration and design
SSL VPN	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	An ideal single-device security and routing solution for protecting the WAN entry point into the network. Now with IPv6 support and Zone-based policy mapping for easier administration.
Advanced Application Inspection and Control (Application Firewall)	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	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.
VRF-Aware Firewall	Firewall now included in the list of services available at the individual context level for VRF deployments
Cisco IOS Intrusion Prevention (IPS)	
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	Provides Layer 3 IPS for Layer 2 connectivity
Network Foundation Protection (NFP)	
Flexible Packet Matching	Cisco IOS Flexible Packet Matching (FPM) is the next-generation Access Control List (ACL) technology that provides rapid first line of defense against malicious traffic at the entry point into the network. It features powerful custom pattern matching deep within packet header or payload, minimizing inadvertent blocking of legitimate business traffic.
AutoSecure	Simplifies router security configuration and enables rapid implementation of security policies with a “one touch" device lockdown process .
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.
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.
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.
Netflow	NetFlow technology efficiently provides the metering base for a key set of applications including network traffic accounting, usage-based network billing, network planning, as well as Denial Services monitoring, and network monitoring capabilities. Cisco NetFlow applications collect NetFlow export data, perform data volume reduction, post-processing, and provide to end-user applications easy access to NetFlow data.
Role-Based CLI Access	Provides view-based access to CLI commands, allowing highly secure, logical separation of router between NetOps, SecOps, and end users.
Source-based Remotely Triggered Blackholes (RTBH) Filtering	This feature provides wire-rate, real-time defense against DDoS attacks using a combination of IP routing features.
SSHv2	Provides powerful new authentication and encryption capabilities with options for tunneling additional types of traffic over the encrypted connection, including file-copy and e-mail protocols
SNMPv3	An interoperable standards-based protocol for network management that provides secure access to devices by a combination of authenticating and encrypting packets over the network
Network Admission Control (NAC)	
Network Admission Control (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	

Features	Benefits
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.
Cisco IOS Certificate Server and Client	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.
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.
Management	
Single device secure management	Cisco Router and Security Device Manager (SDM) is an intuitive, easy-to-use, Web-based device management tool embedded within the Cisco IOS Software of Cisco routers that can be accessed remotely using HTTPS and SSH.
Enterprise security management	Three tools are available for enterprise security deployments: • Cisco Security Management Suite (CSMS), an integrated security-event manager that includes the new Cisco Security Manager, and Cisco Security Monitoring, Analysis, and Response System (MARS). • Cisco IP Solution Center (ISC) 3.0 is a service provider MPLS IPSec management tool.

Additional Features

High Availability and Load Balancing for the Headquarters

Critical for the Enterprise headquarters, Cisco VPNs support numerous features for deploying redundancy and load balancing. For smaller-scale headend IPSec deployments, HSRP and RRI can be used to provide redundancy, whereas for larger deployments Cisco server load balancing (SLB) can be used to provide redundancy as well as load balancing:

- IPSec Stateful Failover-IPSec Stateful Failover allows customers to employ a backup IPSec server to continue processing and forwarding IPSec packets after a planned or unplanned outage occurs. The backup (secondary) IPSec server automatically takes over the tasks of the active (primary) router, without losing secure connections with its peers if the active router loses connectivity for any reason. This process is transparent to the end user and does not require adjustment or reconfiguration of any remote peer. IPSec Stateful Failover is designed to work in conjunction with stateful switchover (SSO) and HSRP. HSRP provides network redundancy for IP networks, helping ensure that user traffic immediately and transparently recovers from failures in network edge devices or access circuits. IPSec Stateful Failover provides protection for IPSec tunnels, IPSec with GRE, and Cisco IOS Easy VPN traffic.
- HSRP and RRI-RRI works with both dynamic and static cryptography maps to simplify network designs for VPNs requiring either high availability or load balancing. Routes are created for each remote network or host on the headend device to allow for dynamic route propagation. HSRP and IPSec dynamically reroute traffic to provide maximum availability of services. For hosts that do not have the ability to switch to another router if a primary router failure occurs, HSRP provides continuous network access. In this case, the HSRP virtual IP address is used as the VPN tunnel endpoint to provide continuous availability for stateless failover of IPSec.
- SLB-Virtual servers can be defined to represent a group of physical servers in a cluster of network servers (a server farm). When a client initiates a connection to the virtual server, the Cisco IOS Software chooses a physical server for the connection based on a configured load-balancing algorithm. In case of a failure of a physical server, SLB

dynamically reroutes all the incoming new IPSec sessions to the other server, thus providing redundancy.

Security Management

Embedded Services Management: Cisco Router and Security Device Manager (SDM)

Every Cisco 7301 and Cisco 7200 Series router security bundle comes with factory-installed Cisco SDM. An intuitive, Web-based device manager (GUI) for deployment and management of Cisco routers, SDM helps enable 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.

SDM features include:

- In-line IPS with updatable signatures and customizable dynamic signature update and signature customization (see IPS)
- Role-based router access
- Integrated Cisco IOS SSLVPN Management
- 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.

Cisco Security Management Suite (CSMS)

Cisco Security Manager is a policy-based configuration management system designed to efficiently provision small to large scale Cisco firewall, VPN, and Intrusion Prevention System deployments. Cisco Security MARS delivers sophisticated monitoring. analysis, and mitigation functionality for multi-vendor networks.

For more information about the Cisco Security Manager and Cisco MARS, visit http://www.cisco.com/go/mars.

Certifications

Cisco is committed to maintaining an active product certification and evaluation program for customers worldwide. Cisco IOS VPN has achieved Federal Information Processing Standards (FIPS) 140-2, and Cisco IOS Firewall has achieved Internet Computer Security Association (ICSA) certification; 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 the Cisco 7301 and Cisco 7200 Series. For more information, visit http://www.cisco.com/go/securitycert.

FIPS

The Cisco 7301 and 7200 Series routers 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 certification.

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 Information Technology

Security Evaluation Criteria (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 7301 and Cisco 7200 Series router 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 7301 and Cisco 7200 Series Routers

Bundle Part Number	Bundle Description
7206VXRG1/2+VPNK9	Cisco 7206VXR chassis, Cisco NPE-G1 processor with 512 MB of system memory, three onboard 100/1000 Ethernet ports, VAM2+, AC power, and Cisco IOS IP Firewall with IPS IPSec 3DES Software
7206VXRG2/2+VPNK9	Cisco 7206VXR chassis, Cisco NPE-G2 processor with 1 GB of system memory, three onboard 100/1000 Ethernet ports, VAM2+, AC power, and Cisco IOS Advanced Security Software
7206VXRG2/VSAVPNK9	Cisco 7206VXR chassis, Cisco NPE-G2 processor with 1 GB of system memory, three onboard 100/1000 Ethernet ports, VPN Services Adapter, AC power, and Cisco IOS Advanced Security Software
CISCO7301/2+VPNK9	Cisco 7301 chassis with three onboard 100/1000 Ethernet ports, VAM2+, 512 MB of system memory, AC power, and Cisco IOS IP Firewall with IPSec 3DES Software

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 7301 and Cisco 7200 Series routers and the complementary Cisco 800, 1800, 2800, and 3800 series branch router 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 C78-341104-01 03/08