Q&A

MANAGED SERVICES: CISCO IOS FIREWALL

Cisco IOS Software-Based Technologies for Managed Services

The managed network services opportunity is projected to increase significantly in the coming years. A recent Cisco Systems® survey of 500 large corporations found substantial interest in managed IP services. At the top of the list were IP VPNs as a foundation for the integration of older networks and the addition of new services. Business customers—from the largest global corporations to midsize and smaller firms—are focusing on achieving cost efficiencies while adding new services. Recognizing the value of the network as a strategic tool, many companies are turning to service providers to manage their networks so they can focus more resources on their businesses. The IP VPN allows integration of older networks (such as ATM and Frame Relay) and provides a foundation for many new services. Examples include managed core services offerings and managed WAN and LAN services, which have been augmented by improved Web-based, user-friendly tools; service-level agreements (SLAs) and guarantees; and many newer IP-based applications, such as voice over IP (VoIP).

Cisco IOS® Software technologies make possible a secure, highly available, cost-effective managed services environment within an IP VPN. Partnering with Cisco®, service providers can streamline their infrastructures to avoid unnecessary overhead, offer more services more efficiently, and position these service offerings successfully with the established Cisco global enterprise customer base. Features such as Enhanced Interior Gateway Routing Protocol (EIGRP) make routing more efficient and turn IP/Multiprotocol Label Switching (MPLS) VPNs into a simpler, benefit-rich addition to customer networks.

Cisco IOS Software technologies for managed services environments serve as the foundation for high-speed routing and IP/MPLS, scalable IP VPNs, and robust network security, all integrated through a next-generation network management interface. These operate within several network topologies to fit the needs of different customers. Products in the Cisco IOS Software Family bring customizable networking solutions to headquarters, branch offices, and campuses, and extend full network capability to mobile workers, telecommuters, and remote data centers.

Cisco IOS Firewalls in Managed Services

More companies are realizing that the network is at the heart of their operations, and are making security a top priority. Small and medium-sized businesses (SMBs) are joining larger organizations to put appropriate safeguards in place. Service providers are taking up the security challenge, dedicating significant resources and personnel to selling managed security services. Cisco network security solutions that are embedded within IP VPNs allow service providers to meet the security requirements of a wide range of business customers. Integral to the Cisco security portfolio, Cisco IOS Firewall and Cisco IOS Intrusion Prevention give service providers comprehensive solutions to address growing security concerns.

Cisco IOS Firewall gives providers of managed services the ability to offer router-based advanced firewall capabilities and intrusion detection and authentication. Cisco IOS Firewall is supported on multiple Cisco router platforms. The Per-User Firewall feature of Cisco IOS Firewall allows service providers to offer a managed firewall solution through download of firewall, access control lists (ACLs), and other settings on a per-user basis, using a profile in the authentication, authorization, and accounting (AAA) server. AAA services streamline management of security solutions, for network and cost efficiencies.

These and other security features from Cisco offer service providers technologies that can generate ongoing managed services revenue while maintaining securely managed networks for large enterprises and smaller customers.

Q. What is a firewall?

A. A firewall is one or a group of mechanisms that protect networks by controlling and monitoring access entering and exiting the network. Because all traffic must traverse the firewall, it functions as a gatekeeper. It blocks access to specific protocols and data types, and inspects traffic flow for protocol adherence. This ensures that traffic continues to act in its original function. Although the method by which this process occurs is different in all implementations, the firewall generally performs several functions.

Q. What are the benefits of integrated Cisco IOS Firewall?

A. Along with other integrated security solutions, Cisco IOS Firewall:

- Takes advantage of existing network infrastructure, enabling new security features on the router through Cisco IOS Software without deploying additional hardware
- Provides the flexibility to apply firewall functions anywhere in the network to maximize security benefits
- Protects the router, defending against attacks targeted directly at the network infrastructure, such as distributed-denial-of-service (DDoS) attacks
- Allows deployment of best-in-breed security functions at all entry points into the network
- Reduces the number of devices, lowering training and manageability costs
- Simplifies network deployment (for example, customers do not have to “design around” non-EIGRP devices)
- Takes advantage of Cisco PIX® Firewall technology, combining robust Cisco IOS Software functions and industry-leading LAN and WAN connectivity with world-class stateful firewall functions

Q. When should I use Cisco IOS Firewall?

A. You can use Cisco IOS Firewall to:

- Protect the Internet link (most commercial requirements are in this category, for example split tunneling)
- Protect the spoke from the hub
- Protect the hub from the spoke (especially when potential threats exist inside the spoke, such as wireless access points)
- Protect from LAN to LAN
- Act as a bidirectional firewall for intelligent protection switching [CORRECT?] (IPS) (for example, protecting hub and spoke from each other simultaneously)

Q. What platforms support Cisco IOS Firewall?

A. Cisco IOS Firewall is currently supported on the Cisco 800, uBR900, 1700, 1800, 2600, 2800, 3600, 3700, 3800, 7100, 7200, and 7500 series routers, the Cisco 7301 Router, and Cisco Catalyst® 5000 and Catalyst 6000 series switches. This breadth of supports enables it to deliver important benefits, including multiservice integration (data, voice, video, and dial) and advanced security for dialup connections.

Q. Why use Cisco IOS Firewall in the branch?

A. Many networks have hub-and-spoke topologies that include branch offices, where the traffic aggregates into a larger corporate office (the hub). Although the hub is a common location to block and inspect traffic for attacks, it is not the only location to consider when deploying security. Branch offices also are an important location in your network to enable both firewall and IPS to address attacks as close to the entry point into the network as possible. By enabling Cisco IOS Software-based VPNs—site to site (IP Security [IPSec]) or IPSec with generic routing encapsulation (GRE) or Dynamic Multipoint VPNs (DMVPNs), with or without split tunneling; Cisco IOS IPS; and Cisco IOS Firewall—a Cisco router can perform encryption and decryption, tunnel termination, firewalling, and traffic inspection at the first point of entry into the network, an industry first. This reduces the number of additional devices needed to support the system and reduces operating and capital expenditure costs while enhancing security. Because it is an integrated solution, such a deployment does not require a separate device, thereby reducing network complexity and management. The net result is that Cisco IOS Firewall helps to stop attacking traffic at the point of origination, removing the unwanted traffic from the network as quickly as possible.

Q. Can I use an integrated services router as a firewall?
A. Yes. All Cisco 1800, 2800, and 3800 series integrated services routers can enable the Cisco IOS Firewall when purchased with the Cisco IOS Software Advanced Security or higher feature sets. The primary features of Cisco IOS Firewall include:

- Industrywide security-certified, stateful firewall
- 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

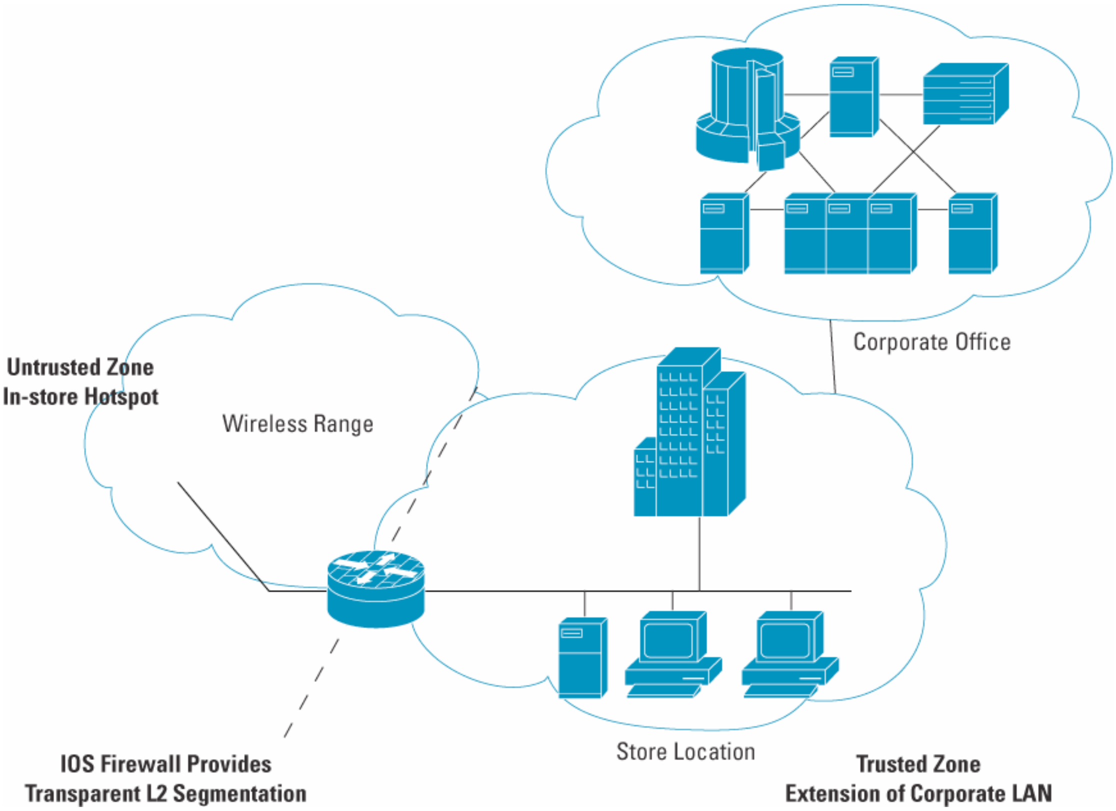
The Cisco IOS Firewall not only helps enable a single point of protection at the perimeter of a network, it also makes security policy enforcement an inherent component of the network itself. The flexibility and cost-effectiveness of both dedicated and integrated policy enforcement provides security 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 quality-of-service (QoS) features in the same router.

Q. Can Cisco integrated services routers support transparent firewalling? What are the benefits?
A. In addition to Layer 3 stateful firewalling, Cisco IOS Software routers can support transparent firewalling, which is the ability to provide Layer 3 firewalling for Layer 2 connectivity. The benefits of a transparent firewall follow:

- Easy addition of firewall to existing networks—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 all standard management tools
- Support for Dynamic Host Configuration Protocol (DHCP) pass-through to assign DHCP addresses on opposite interfaces (bidirectional)

Figure 1 shows an application of a transparent firewall.

Figure 1. Segment Existing Network Deployments into Security Trust Zones Without Making Address Changes: Cisco IOS Firewall Provides Transparent Layer 2 Segmentation [EDITS: cap s: Store; Cisco IOS…; Layer 2 (not L2)]



Q. Is Cisco IOS Firewall a stateful firewall?
A. Yes, it is a stateful firewall that uses the inherent stateful inspection engine of Cisco IOS Software for maintaining the detailed sessions database.

Q. What protocols or predefined services does Cisco IOS Firewall support?
A. Cisco IOS Firewall supports generic TCP regardless of the application layer protocol (sometimes called "single-channel" or "generic" TCP inspection), all User Datagram Protocol (UDP) features [CORRECT?] regardless of the application layer protocol (sometimes called single-channel or generic TCP [SHOULD THIS BE UDP?] inspection),CU-SeeMe, FTP, H.323v2, Session Initiation Protocol (SIP), Skinny Client Control Protocol (Skinny), HTTP (Java blocking), Internet Control Message Protocol (ICMP), Microsoft NetShow, UNIX R-commands (such as rlogin, rexec, and rsh), RealAudio, Real Time Streaming Protocol (RTSP), remote-procedure call (RPC), Simple Mail Transport Protocol (SMTP), SQL*Net, StreamWorks, Trivial File Transfer Protocol (TFTP), and VDOLive.

Q. What certifications are available for Cisco IOS Firewall?
A. On August 20, 2004, ICSA Labs announced that Cisco IOS Firewall was a certified product in its labs using the Cisco 2651XM Multiservice Router and the Cisco 3725 Multiservice Access Router. The Cisco 1841, 2811, and 3825 integrated services routers were certified in October, 2004. Recognizing that these validations are a critical component of its integrated security strategy, Cisco is dedicated to the ongoing pursuit of Federal Information Processing Standards (FIPS), Internet Computer Security Association (ICSA), and Common Criteria certifications.

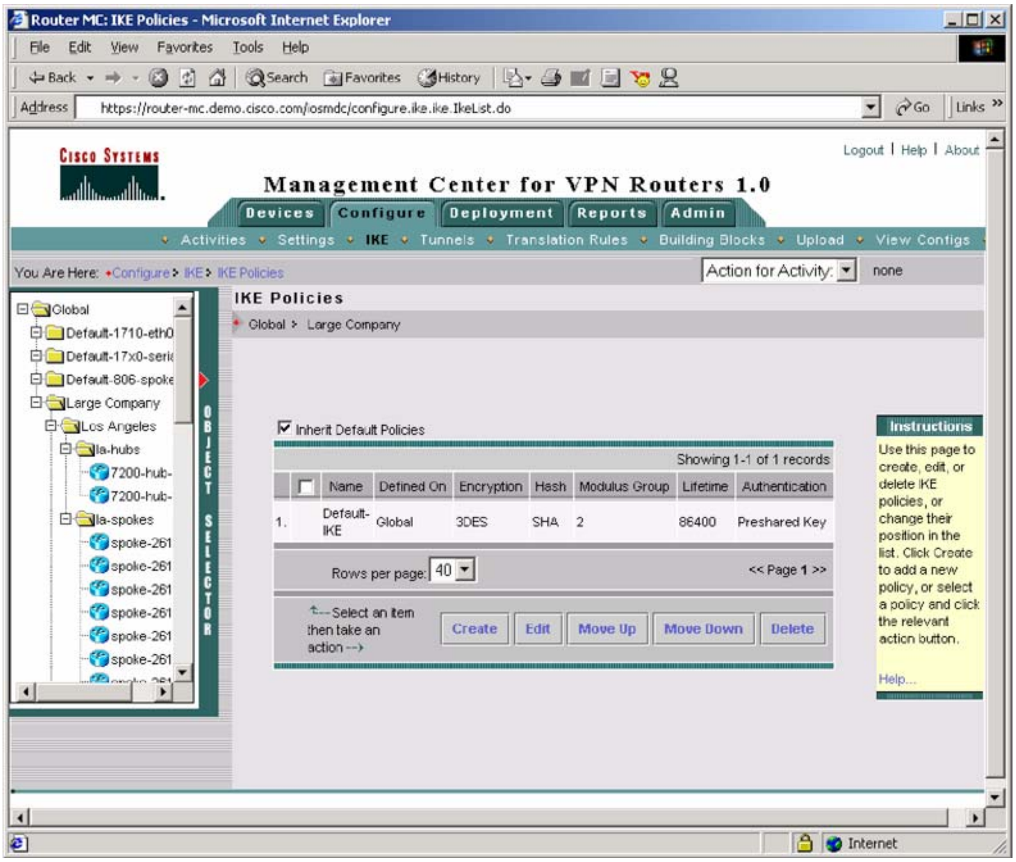
Q. What kind of performance can I expect from an integrated Cisco IOS Firewall?

A. In an independent test performed by Miercom, Cisco IOS Firewall performance was validated at up to 1.1 Gbps on the new Cisco 3800 Integrated Services Router.

Q. What tools are available to manage the Cisco IOS Firewall?
A. CiscoWorks VPN/Security Management Solution (VMS) and Cisco Router and Security Device Manager (SDM) are available to manage Cisco IOS Firewall. Cisco SDM offers both easy-to-use wizards for deployment and a graphical view to see how the firewall policies applied affect the traffic flow.

Q. What system management tools are available for configuration and monitoring of security on Cisco routers?
A. For management of firewall and VPN features, the CiscoWorks VMS management bundle is available (Figure 2). For more information about the CiscoWorks VMS, visit: http://www.cisco.com/go/vms.

Figure 2. CiscoWorks VMS Screenshot


Router MC: IKE Policies - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://router-mc.demo.cisco.com/iosmdc/configure.ike.ike.IkeList.do
Go Links
Cisco Systems
Logout | Help | About
Management Center for VPN Routers 1.0
Devices Configure Deployment Reports Admin
Activities Settings IKE Tunnels Translation Rules Building Blocks Upload View Configs
You Are Here: Configure > IKE > IKE Policies
Action for Activity: none
Global
Default-1710-eth0
Default-17x0-seri
Default-806-spoke
Large Company
Los Angeles
la-hubs
7200-hub-
7200-hub-
la-spokes
spoke-261
spoke-261
spoke-261
spoke-261
spoke-261
spoke-261
OBJECT SELECTOR
Internet

IKE Policies

Global > Large Company

☑ Inherit Default Policies

Showing 1-1 of 1 records

	□	Name	Defined On	Encryption	Hash	Modulus Group	Lifetime	Authentication
1.		Default-IKE	Global	3DES	SHA	2	86400	Preshared Key

Rows per page: 40 << Page 1 >>

←--Select an item then take an action -->

Create
Edit
Move Up
Move Down
Delete

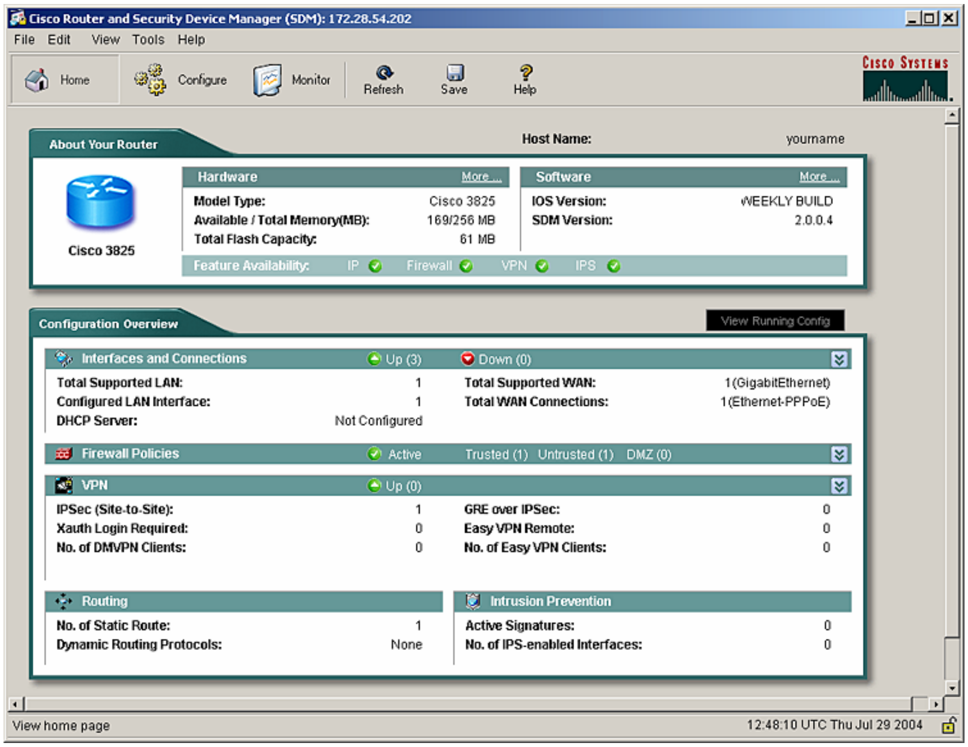
Instructions

Use this page to create, edit, or delete IKE policies, or change their position in the list. Click Create to add a new policy, or select a policy and click the relevant action button.

Help...

Q. What device management tools are available for deploying security on Cisco routers?
A. The new Cisco 1800, 2800, and 3800 series routers come with factory-installed Cisco SDM. Cisco SDM is an intuitive, Web-based device manager (GUI) for deployment and management of Cisco IOS Software-based routers (Figure 3). Cisco SDM helps enable easy router configuration and monitoring through the use of a startup wizard for quick deployment and lock-down, smart wizards to help enable security and routing features, Cisco Technical Assistance Center (TAC)-approved router configurations, and subject-related educational content (Figure 3).

Figure 3. Cisco SDM 2.0



Host Name: yourname

Hardware

Model Type: Cisco 3825
Available / Total Memory(MB): 169/256 MB
Total Flash Capacity: 61 MB

Software

IOS Version: WEEKLY BUILD
SDM Version: 2.0.0.4

Feature Availability: IP ✓ Firewall ✓ VPN ✓ IPS ✓

Interfaces and Connections ● Up (3) ● Down (0)

Total Supported LAN: 1
Configured LAN Interface: 1
DHCP Server: Not Configured
Total Supported WAN: 1(GigabitEthernet)
Total WAN Connections: 1(Ethernet-PPPoE)

Firewall Policies ✓ Active Trusted (1) Untrusted (1) DMZ (0)

VPN ● Up (0)

IPSec (Site-to-Site): 1
Xauth Login Required: 0
No. of DMVPN Clients: 0
GRE over IPSec: 0
Easy VPN Remote: 0
No. of Easy VPN Clients: 0

Routing

No. of Static Route: 1
Dynamic Routing Protocols: None

Intrusion Prevention

Active Signatures: 0
No. of IPS-enabled Interfaces: 0

12:48:10 UTC Thu Jul 29 2004

Cisco SDM 2.0 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 status, and reduce their operational costs.

Cisco SDM 2.0 includes support for the following new features:

- Inline IPS with dynamic signature update and signature customization
- Role-based router access support
- Easy VPN server and AAA
- Digital certificates for IPSec VPNs
- VPN and WAN connection troubleshooting
- QoS policy configuration and network-based application recognition (NBAR)-based application traffic monitoring

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

Q. Can the switching interfaces on the integrated services routers be used with Transparent Cisco IOS Firewall?
A. Yes. This is easily done by creating VLAN interfaces and then applying the firewall to these interfaces.

Q. Do the integrated services routers support URL filtering?
A. URL filtering has become increasingly important within companies because of increased liability from inappropriate material in the workplace; it also is a tool to increase productivity while using corporate assets. URL

filtering is offered two ways for integrated services routers—either within Cisco IOS Firewall or through the content-engine network module.

Cisco IOS Firewall as a URL filter supports Websense and N2H2 Web filtering clients and works with external Websense and N2H2 servers. As a user requests a URL, the traffic is sent to the Websense or N2H2 server to check the link. If the link is appropriate, the page is loaded.

The content-engine network module is available for Cisco 2800 (excluding the Cisco 2801) and Cisco 3800 integrated services routers, which act as an Internet proxy cache and an "on-box" URL filtering application server. On-box filtering preserves WAN bandwidth because the traffic does not traverse over the network to a remote server. Preloaded filtering applications from original equipment manufacturers (OEMs) Websense and Smartfilter provide features such as Application Use Policy, Traffic Logging and Reporting, and Anti-Virus Gateway (Internet Content Adaption Protocol (ICAP) to scan, clean, and cache Web content.

Q. What are the benefits of integrated security?
A. Integrated security solutions take advantage of Cisco PIX Firewall and IDS sensor technologies, combining robust Cisco IOS Software functions and industry-leading LAN and WAN connectivity with world-class security functions.

Integrating Cisco IOS Software security into the router offers many benefits:

- Use what you have—Takes advantage of existing network infrastructure, helping enable 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 functions, such as firewall, IPS, and VPN, anywhere in the network to maximize security benefits
- Protect your gateways—Allows best-in-breed 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 targeted directly at the network infrastructure, such as DDoS attacks

the Cisco Web site at www.cisco.com/go/offices.