Cisco IOS®
Advanced Firewall
Integrated Threat Control for Router Security Solutions

http://www.cisco.com/go/iosfirewall
All-in-One Security for the WAN

Only Cisco® Security Routers Deliver All This

Secure Network Solutions
- Business Continuity
- Secure Voice
- Secure Mobility
- Compliance

Integrated Threat Control
- Advanced Firewall
- URL Filtering
- Intrusion Prevention
- Flexible Packet Matching
- Network Admission Control
- IEEE 802.1x
- Network Foundation Protection

Secure Connectivity
- GET VPN
- DMVPN
- Easy VPN
- SSL VPN

Management and Instrumentation
- SDM
- Role-Based Access
- NetFlow
- IP SLA
Integrated Threat Control Overview
Industry-Certified Security Embedded Within the Network

- Secure Internet access to the branch office without the need for additional devices
- Control worms, viruses, and adware and spyware right at the remote site; conserve WAN bandwidth
- Protect the router itself from hacking and DoS attacks
- Protect data, voice and video, wired and wireless, and WAN acceleration services

Router Protection
- Automated Router Lockdown
- Router Availability During DoS Attack

Worm and Virus Prevention
- Attain Distributed Defense and Rapid Response to Worms and Viruses
- Control Wired and Wireless User Access and Noncompliant Devices

Secure Internet
- Advanced Layer 3 to 7 Firewall
- P2P and IM Control
- Web Use Control
Cisco IOS® Firewall
Benefits

- Integrated perimeter and branch defense using proven Cisco® IOS Software routing, quality-of-service (QoS), voice, and wireless technologies
- Low total cost of ownership (TCO) through integration of firewall, IPS, and other security features on a popular networking platform
- Protection against network and application layer exploits and threats such as denial-of-service (DoS) attacks
- Compliance with requirements such as PCI, Sarbanes-Oxley, and HIPAA
- Ease of management and deployment
- Numerous WAN interface and density options on Cisco routers
- Green technology—reduced power consumption and footprint because the existing router is used
Cisco IOS® Firewall

Overview

**Stateful firewall:** Full Layer 3 through 7 deep packet inspection

**Flexible embedded application layer gateway (ALG):** Dynamic protocol and application engines for seamless granular control

**Application inspection and control:** Visibility into both control and data channels to help ensure protocol and application conformance

**Virtual firewall:** Separation between virtual contexts, addressing overlapping IP addresses

**Intuitive GUI management:** Easy policy setup and refinement with SDM and CSM

**Resiliency:** High availability for users and applications with stateful firewall failover

**WAN interfaces:** Most WAN and LAN interfaces

---

**Selected List of Recognized Protocols**

- HTTP, HTTPS, and JAVA
- E-mail: POP, SMTP, IMAP, and Lotus
- P2P and IM (AIM, MSN, and Yahoo!)
- FTP, TFTP, and Telnet
- Voice: H.323, SIP, and SCCP
- Database: Oracle, SQL, and MYSQL
- Citrix: ICA and CitrixImaClient
- Multimedia: Apple and RealAudio
- IPSec VPN: GDOI and ISAKMP
- Microsoft: MSSQL and NetBIOS
- Tunneling: L2TP and PPTP
SIP Protection for Secure Unified Communications
Enhance the Integrity and Availability of Cisco® Unified Communications

Session Initiation Protocol (SIP) (RFC 3261) inspection and granular access control for voice-over-IP (VoIP) traffic across branch networks

- Prevent unauthorized calls, call hijacking, any SIP protocol exploits, and related DoS attacks
- Remove malformed packets from reaching Cisco Unified Communications Manager at the head office
- Maintain high availability of mission-critical IP telephony calls while upholding high level of call experience
Cisco IOS® Firewall: Common Deployments Scenarios

- **Split tunnel:** Remote branch, retail store, and clinic
  - Division between VPN traffic to the LAN and direct public network connection for Internet traffic

- **Virtual firewall:**
  - **Retail chains**
    - Firewall between virtual contexts (VRFs) and to the WAN
    - Segregation of networks for photo and pharmacy with overlapping IP addresses
  - **Internet for partners: Co-location**
    - WAN connection sharing between business partners
    - Bank ATMs at retail store locations

- **Direct Internet connection:** Small office and managed firewall

- **Internal firewall:** International financial branches
  - Between international or untrusted locations or segments, often for compliance requirements
  - Transparent or routed environments
  - Wireless to wired segments
Cisco IOS® Firewall Deployment
Case Study: National Retailer

- Photo kiosk a potential security threat at the store—media card slots
- Support needed for overlapping address space
  Multiple partners co-located at the store
- Direct Internet access needed for partners
- PCI compliance requires retail stores to firewall wired and wireless and Packet-over-SONET (PoS) segments
  Inter-VRF routing + firewall may be enabled for wired VPN Routing and Forwarding (VRF) and wireless VRF
  Cisco has its retail design guide certified through a third party (CyberTrust)
## Cisco® Security Router Certifications

<table>
<thead>
<tr>
<th>Routers</th>
<th>FIPS</th>
<th>Common Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>140-2, Level 2</td>
<td>IPSec (EAL4)</td>
</tr>
<tr>
<td>Cisco 870 Series</td>
<td>✓</td>
<td>In progress</td>
</tr>
<tr>
<td>Cisco 1800 Series</td>
<td>✓</td>
<td>In progress</td>
</tr>
<tr>
<td>Cisco 2800 Series</td>
<td>✓</td>
<td>In progress</td>
</tr>
<tr>
<td>Cisco 3800 Series</td>
<td>✓</td>
<td>In progress</td>
</tr>
<tr>
<td>Cisco 7200 Series VAM2+</td>
<td>✓</td>
<td>In progress</td>
</tr>
<tr>
<td>Cisco 7200 Series VSA</td>
<td>✓</td>
<td>In progress</td>
</tr>
<tr>
<td>Cisco 7301 VAM2+</td>
<td>✓</td>
<td>In progress</td>
</tr>
<tr>
<td>Cisco 7600 Series IPSec VPN SPA</td>
<td>✓</td>
<td>In progress</td>
</tr>
<tr>
<td>Cisco Catalyst® 6500 Series IPSec VPN SPA</td>
<td>✓</td>
<td>In progress</td>
</tr>
<tr>
<td>Cisco 7600 Series</td>
<td>✓</td>
<td>In progress</td>
</tr>
</tbody>
</table>

[cisco.com/go/securitycert]
Management and Instrumentation
Overview

**Cisco® Security Device Manager**
- Quickest way to set up a device
- Wizards to configure firewall, IPS, VPN, QoS, and wireless
- Ships with device

**Cisco Security Manager**
- New solution for configuring routers, appliances, and switches
- New user-centered design
- New levels of scalability

**Cisco Security Monitoring, Analysis and Response System (MARS)**
- Solution for monitoring and mitigation
- Uses control capabilities within infrastructure to eliminate attacks
- Visualizes attack paths

**Cisco IOS® Instrumentation**
- Industry leadership in instrumentation
- Feeds into Cisco Security MARS
- Partitioned access for network and security operations teams
Cisco® Router and Security Device Manager (SDM)

- **Web-based device management tool** for Cisco routers that simplifies router deployments and helps troubleshoot complex network and VPN connectivity problems
- **Zone-based firewall** for granular policy control between virtual zones
- **Application control and URL filtering** unique on a per-rule basis
Cisco® Security Manager

- State-of-the-art user interface
- Multiple views to suit administrator preferences
  - Device, policy, and topology views
- Unified management of multiple security services
  - Firewall, VPN, and intrusion prevention system (IPS)
- Supports Cisco Integrated Services Routers, ASA, PIX®, IPS Sensors, and Catalyst® Service Modules
Cisco® Security Monitoring, Analysis and Response System (MARS)

- Cisco Security MARS “Know the battlefield”: Mitigation and response turnkey system
- Gain network intelligence
  - Use the network you have; correlate router’s NetFlow (WAN data) with firewall, intrusion detection system (IDS), and switch data
  - Build topology and traffic-flow model
  - Know device configuration and enforcement abilities
- ContextCorrelation™
  - Correlates, reduces, and categorizes events and validates incidents
- Allows for response
Cisco Services and Support

Cisco and its partners provide a broad portfolio of security services that help you to:

• Protect privacy and integrity of information
• Achieve and maintain regulatory compliance,
• Protect your network investment,
• Optimize network operations, and
• Extend the power of your business by preparing your network for new applications

Cisco IOS® Firewall

Summary

- Fundamental building block for defense-in-depth approach (Layers 3 to 7)
- Widely deployed fully stateful firewall
- Common criteria (EAL4) certified
- Low TCO
  - Use network investment to deploy firewall at the branches
  - Available as part of security bundles on Cisco Integrated Services Routers
- Critical for compliance conformity to PCI, Sarbanes-Oxley, and HIPAA