Cisco IOS Firewall

Businesses face an increasingly hostile environment when data networks are connected to the public internet, and network borders are opened to business partners via VPN. Furthermore, the growing "inside" threat from malware such as worms, Trojan horses, unwanted application traffic and other malicious agents that can infiltrate a network, cause costly security disruptions, downtime, and unwanted bandwidth consumption.

Cisco IOS Firewall offers a threat control foundation to deploy secure access policies at all network interfaces: Internet perimeter, remote-site connectivity, business-partner access, and telecommuter connections.

- Application inspection and control builds on the existing state-full inspection infrastructure to offer comprehensive protection for industry-standard services, as well as a framework to configure custom protocol support to meet business requirements.
- Improvements to Cisco IOS Software's Zone-Based Policy Firewall provide innovative control capabilities for Instant Messaging and Peer-to-Peer applications, and granular application-level control for HTTP traffic, as well as firewall policy bandwidth-shaping and session limits.
- Performance enhancements bring Cisco IOS Firewall connection capacities and throughput capabilities in line with business requirements to integrate network threat control capabilities with other router features such as NAT, VPN, QoS, and dynamic routing:

Key Benefits

The Cisco IOS Firewall interoperates with other Cisco IOS Software components, providing outstanding value and benefits:

- Application Protection: Cisco IOS Firewall Application Inspection and Control minimizes threats on desirable network services like web traffic and mail protocols by enforcing protocol conformance and blocking unwanted application activity. Network bandwidth and employee time waste is limited by Cisco IOS Firewall blocking unwanted applications such as instant messaging traffic, peer-to-peer file-sharing traffic, and http-tunneling applications.
- Integrated Security: ICSA-certified and Common Criteria EAL4 certified firewall capability provides basic network protection through state-full inspection, blocking undesired network activity and allowing business-critical application traffic. Traffic controls block malicious efforts against vulnerable hosts such as fragmentation and replay attacks, and Denial-of-Service protection detects and mitigates unusual activity that characterizes network activity generated by worm-infected and zombie hosts.
- Compliance conformity: Facilitates conformance to audit and compliance requirements like PCI, HIPAA and SoX.

- Network Border Enforcement: Cisco IOS Firewall secures the front line of network connectivity when deployed at network access points. Left unguarded, connections to the public Internet, VPN and WAN access for remote sites, business-partner portals, and telecommuter VPN termination offer access points to sensitive resources. Cisco IOS Firewall offers a platform for application of secure network access policies to reduce the threat profile of connectivity points.
- Investment protection: Integrating firewall functionality into a multiprotocol router leverages an existing router investment, without the cost and learning curve associated with a new platform. Cisco IOS Firewall on Cisco IOS routers is an all-in-one, scalable solution that performs multiprotocol routing, perimeter security, intrusion detection, VPN functionality, and per-user authentication and authorization.
- Easy provisioning and management: Easy to use Cisco Router and Security Device Manager (SDM) enables rapid deployment of Cisco TAC approved default firewall policies and real-time monitoring of firewall logs. The Unified Firewall MIB provides an SNMP interface for monitoring firewall activity, and CS-MARS dynamically configures mitigation policies to counter network security threats.

Figure 1. Defining Firewall Policies with SDM's Intuitive GUI

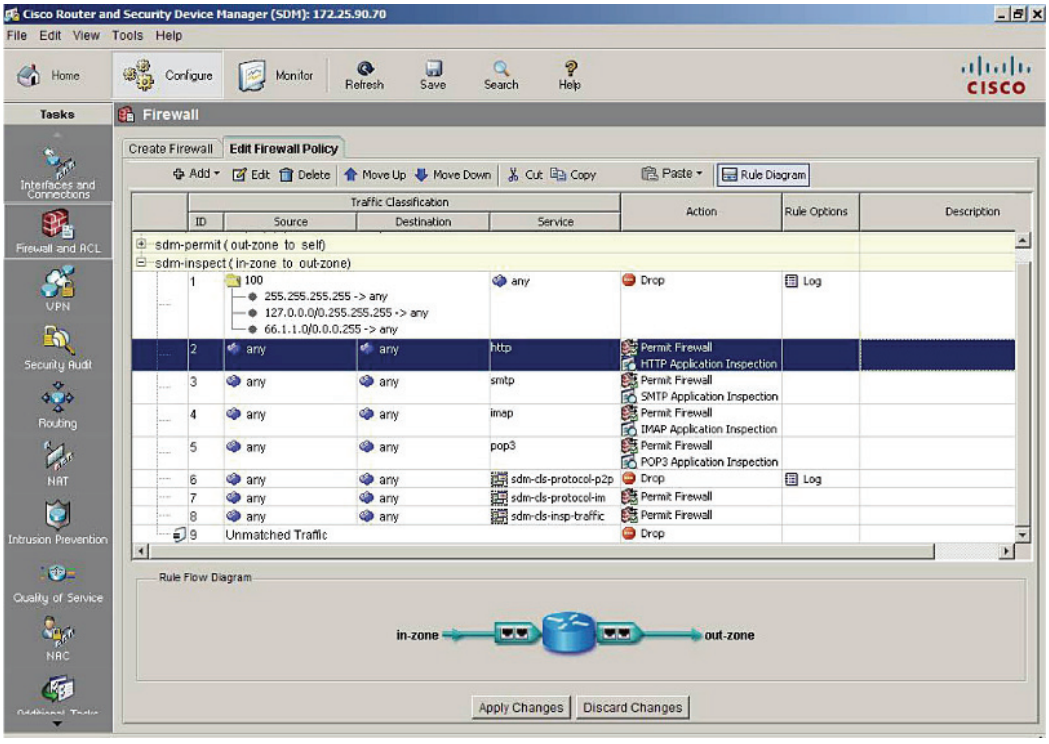
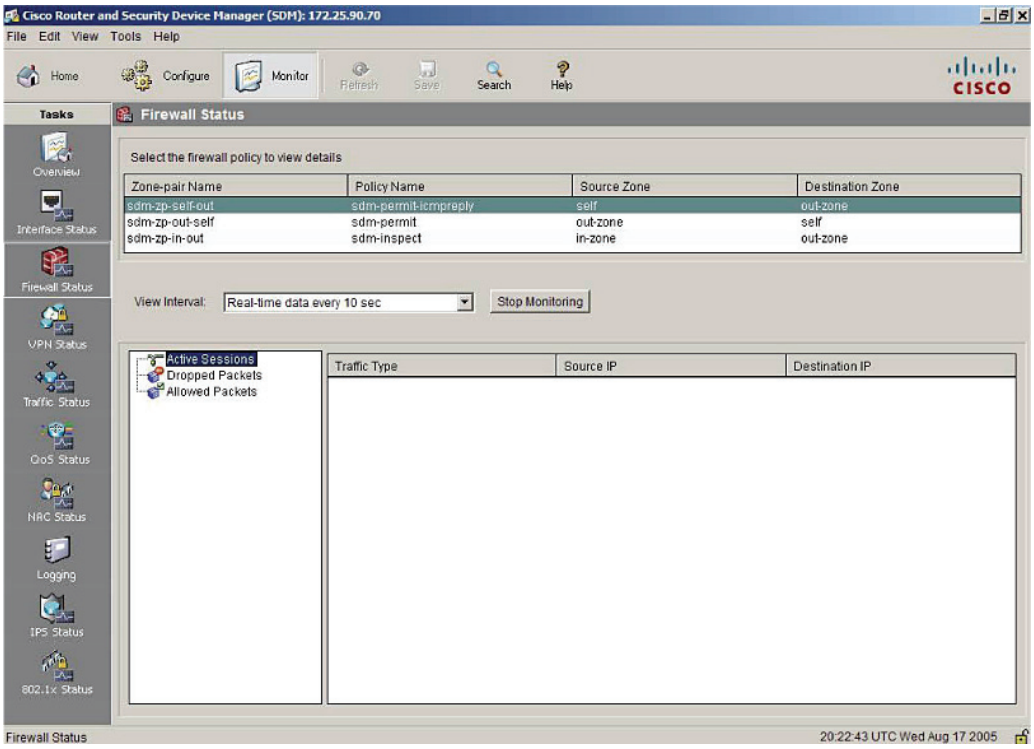


Figure 2. Monitoring Cisco IOS Firewall sessions with SDM



Cisco IOS Firewall Features

Table 1. Cisco IOS Firewall Features and Capabilities

Capability	Feature	Description
Advanced Application Inspection and Control	Instant Messenger Blocking	Offers per-service control to block or allow MSN Messenger, Yahoo! Messenger, and AOL Instant Messenger. Allows service restriction to text-chat only, blocking voice and video chat and file transfer.
	Peer-to-Peer Control	Individually blocks access to BitTorrent, Gnutella, KaZaA, and eDonkey file-sharing networks. Service-specific improvements were made available in 12.4(9)T to limit certain activities supported by certain Peer-to-Peer networks.
	Protocol Conformance Checking	Enforces protocol conformance for HTTP, Simple Mail Transfer Protocol (SMTP), Extended SMTP (ESMTP), Internet Mail Access Protocol (IMAP), and Post Office Protocol 3 (POP3). Enables detection and prevention of unwanted traffic on desired applications' service ports. HTTP inspection offers Java Applet filtering to block malicious content in http traffic. Cisco IOS Software Version 12.4(9)T introduced capabilities to configure Regular Expression matching for policy enforcement, as well a granular application inspection and control of various HTTP objects, such as HTTP methods, URLs/URIs , and header names, and values such as maximum URI length, maximum header length, maximum number of headers, maximum header-line length, non-ascii headers, or duplicate header fields. This allows the ability to limit buffer overflows, HTTP header vulnerabilities, binary or non-ascii character injections, exploits like SQL injection, cross site scripting and worm attacks. HTTP inspection also offers Java Applet filtering to block malicious content in http traffic.
Stateful Inspection	Zone Based Policy Firewall	Improved firewall policy configuration provides a clear interface for configuring firewall policies aligned with businesses' information security policies. Modular, granular firewall policies improve security by tightly controlling network service access and enforcement. New configuration model changes router firewall behavior to an appliance-like default "deny-all" policy, removing dependence on Access-Control Lists. Supports Transparent (Bump-In-The Wire) operation and multiple VRF-aware virtual firewalls per device.
	Transparent Firewall	Transparent Firewall enables insertion of a stateful Layer 2 firewall within an existing network, without readdressing statically defined devices. Provides the same Layer 3-7 filtering as "routed" mode, but offers the simplicity of "bump-in-the-wire" deployment.

Capability	Feature	Description
	Firewall for Secure Unified Communications	Supports voice traffic including application-level conformance of the media protocol as to call flow and the associated open channels. It supports voice protocols such as H.323v2, SCCP, and Session Initiation Protocol (SIP) and assures protection of Unified Communications components like Cisco UCM (Unified Communications Manager), Cisco CUBE (Cisco Unified Border Element) and their endpoints.
	Virtual (VRF-aware) Firewall	VRF-Aware firewall functions offers virtual firewalls for isolated route space and overlapping addresses.
	Destination URL Policy Management	Offers URL filtering support of Websense and N2H2 services, as well as a local black- or white-list in router configuration.
	Authentication Proxy	Network administrators can authenticate and authorize each user's access to network resources with Cisco IOS Firewall Authentication Proxy, using HTTP, Telnet, FTP and HTTPS interfaces.
Management Provisioning Alerts/Logging	Cisco SDM	Web-based device management tool improves network and security manager productivity, simplifies router security deployment, and monitors device status.
	Cisco CS-MARS	Collects statistics and correlates event activity, using audit-trail and event logging activity carried in syslog and snmp.
	Cisco Security Manager (CSM)	CSM is capable of managing multiple security devices across the network infrastructure and scales to 1000s of devices.
	Audit Trail and Logging	Records time stamp, source host, destination host, ports, duration, and total number of bytes transmitted for detailed reporting. Security events are logged according to severity level, providing details for forensics or debugging.
	Unified Firewall MIB	Simplifies monitoring using any SNMP based management system. Shares object definitions with other Cisco firewall products, so a uniform monitoring policy can be applied on all Cisco firewall devices.
Application Traffic Rate and Session Control	Policy-Map Policing	Applies rate limits to firewall policies to control network bandwidth utilization. Session policing limits connection rates to network hosts and helps protect against DoS attacks
High Availability	Stateful Failover	Active/standby failover between two routers for most TCP-based services. Firewall session state is maintained such that active sessions continue even during a router or circuit failure*.

* Current support for Cisco 1841, 2800, 3700, 3800, 7200 and 7301 router families

Platform Support

Cisco IOS Firewall is available in Advanced Security, Advanced Enterprise, and Advanced IP Services software Images for all currently-supported access router platforms, 7200 Series Routers, and the 7301. The default Security Router Bundle includes the appropriate software image, along with enough memory and storage to support firewall features and other threat defense capabilities.

Table 2. Feature Availability

Product Family	Platforms Supported
800	831, 836, 837, 851, 857, 871, 876, 877, 878
1700	1701, 1702, 1711, 1712, 1721, 1751, 1751-V, 1760
1800	1801, 1802,1803,1811,1812,1841
2600	2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, 2691
2800	2801, 2811,2821,2851
3600	3660
3700	3725, 3745
3800	3825,3845
7200	7204VXR,7206VXR
7300	7301

Additional Resources

- ICSA Certification: http://newlabs.icsalabs.com/icsa/product.php?tid=fghhf456fgh
- Router Firewall Web Page: http://www.cisco.com/go/iosfirewall
- Router Security Web Page: http://www.cisco.com/go/routersecurity/

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 C78-60014-04 03/08

