

Announcing Cisco IOS Firewall Feature Set for the Cisco 7200 Series

Introduction

The Cisco IOS® Firewall Feature set, which adds sophisticated firewall capabilities to the existing security services of Cisco IOS software, is now available for the Cisco 7200 series. Customers can now take advantage of high-performance firewall services integrated with the performance, flexibility, and cost-effectiveness of the Cisco 7200 platform. These services are of particular benefit for users deploying virtual private network (VPN) applications.

The Cisco IOS Firewall Feature set is available for the Cisco 7200 series beginning with Cisco IOS Release 12.0(3)T and subsequent releases of 12.0T. The Firewall Feature set is included with specific IP, desktop, and enterprise software images.

Cisco IOS Firewall Benefits

The Cisco IOS Firewall enhances existing Cisco IOS security capabilities such as authentication and encryption with firewall capability. This includes stateful, application-based filtering, Java blocking, defense against network attacks such as SYN flooding, port scans, and packet injection, and support for VPNs based on the Internet Protocol Security (IPSec) standard.

Benefits of the Cisco IOS Firewall feature set include:

- *VPN Support*—using Cisco IOS Firewall with other Cisco IOS encryption and quality of service (QoS) features enables secure, low-cost transmission over public networks, reduces implementation and management costs for remote branch offices and extranets, and ensures mission-critical application traffic receives high-priority delivery. Cisco IOS supports multiple tunneling protocols, including Generic Routing Encapsulation (GRE), Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPSec) with both 56-bit (DES) and 168-bit (3DES) encryption.
- *Flexibility*—this all-in-one solution can perform routing, provide protected Internet connectivity, and apply distinct security characteristics according to a user-defined policy to each interface on a per-user or per-application basis.
- *Investment protection*—integrating firewall functionality into a multiprotocol router leverages an existing router investment. Routers are usually deployed to separate sensitive network segments and manage private/public network interfaces. The addition of Cisco IOS Firewall saves costs and management training associated with learning a new platform.
- *Ease of management*—with remote management capabilities, a network administrator can implement security features from a central console over the network.

Cisco IOS Firewall Features

Feature	Description
Context-Based Access Control (CBAC)	<ul style="list-style-type: none"> Provides internal users secure, per-application-based access control for all traffic across perimeters, for example between private enterprise networks and the Internet
Java Blocking	<ul style="list-style-type: none"> Protects against unidentified, malicious Java applets
Denial of Service Detection/Prevention	<ul style="list-style-type: none"> Defends and protects router resources against common attacks; checks packet headers and drops suspicious packets
Audit Trail	<ul style="list-style-type: none"> Details transactions. Records time stamp, source host, destination host, ports, duration, and total number of bytes transmitted for detailed reporting
Real-Time Alerts	<ul style="list-style-type: none"> Logs alerts in case of denial-of-service attacks or other pre-configured conditions

Related Cisco IOS Security Features

Feature	Description
Basic and Advanced Traffic Filtering	<ul style="list-style-type: none"> Standard and extended access control lists (ACLs) apply controls over access to specific network segments and define which traffic passes through a network segment Lock and key—dynamic ACLs grant temporary access through firewalls upon user identification (username/password)
Policy-Based Multiple Interface Support	<ul style="list-style-type: none"> Controls user access by IP address and interface as determined by security policy
Peer Router Authentication	<ul style="list-style-type: none"> Ensures that routers receive reliable routing information from trusted sources
Event Logging	<ul style="list-style-type: none"> Allows administrators to track potential security breaches or other nonstandard activities on a real-time basis by logging output from system error messages to a console terminal or syslog server, setting severity levels, and recording other parameters

Availability and Ordering

Cisco IOS Firewall is available for the Cisco 7200 series with Cisco IOS Release 12.0(3)T and subsequent 12.0T releases. IP-only, Desktop/IBM, and Enterprise images with two levels of encryption (IPSec 56 and IPSec 3DES) can be ordered with the Cisco IOS Firewall option.

Cisco IOS Firewall is also available for Cisco 1600, 1720, 2500, 2600, and 3600 series routers.

Additional Information

Additional information about the Cisco IOS Firewall Feature Set can be found at: <http://www.cisco.com/warp/customer/778/security/firewall/>.

Please contact Mark Jansen, product manager, Enterprise WAN Software Products, at mjansen@cisco.com or Jocelyne Okrent, product manager, Cisco IOS Firewall Feature Set, at jokrent@cisco.com for additional details.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
<http://www.europe.cisco.com>
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

Americas
Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at <http://www.cisco.com/offices>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela