

# Cisco IOS Software Release 12.1 for Catalyst 5000/RSM

*Cisco Secure Integrated Software (formerly known as Cisco IOS Firewall) for Catalyst 5000/RSM*

## Introduction

Cisco IOS® Release 12.1 for the Catalyst® 5000 Route Switch Module (RSM) brings firewall security features into the campus-switching environment. As security makes inroads from the edge to inside of the network, Cisco Secure Integrated Software (formerly known as Cisco IOS Firewall Feature Set) on Route Switch Module helps in implementing campus-wide enterprise security policy. The old security notion of bad guys outside and good guys inside has been replaced with the new notion of security everywhere. In fact security on the global Internet and on internal corporate intranets has become a significant concern for enterprises wishing to extend connectivity beyond closed private networks.

While there is an increasing need to provide customers, vendors, and ever more mobile employees access to a broader range of corporate information using public networks, confidential data and company resources across the whole network must be protected. In addition, the potential for online transactions and e-commerce will be realized only when a secure network infrastructure is in place and can be relied upon. As larger volumes of information are exchanged and as financial transactions begin to be conducted over these networks, a great deal needs to be secured. The loss of assets such as confidential company data is an obvious area of concern and needs protection with the help of technologies like RSM based firewall.

For the purposes of security on networks of computers or computing devices, security can be defined more specifically by three basic concepts. These are privacy (or confidentiality), authentication, and data integrity. These basic concepts transcend all the technologies, applications, and implementations related to network security and manifest themselves as corporate security policy. Security is an area of extreme importance to corporate users. Given the wide range of requirements, technologies, and implementations, as well as the ever changing nature of the complete security landscape on the Internet, enterprise network managers must implement a flexible but encompassing security infrastructure.

Cisco Secure Integrated Software not only helps in designing a comprehensive security policy in protecting the valuable internal resources but can respond to the threats in real time. Using trunking, virtual LANS (VLANs) can extend from the wiring closets to data center where RSM module can be located to provide the highly secure multiprotocol connectivity. Most of the port adapters, supported for Cisco 7500 and Cisco 7200 are supported for Cisco Secure Integrated Software on RSM.

The key firewall security features for Route Switch Module include:

- Context-based Access Control (CBAC)
- Intrusion Detection (59 signatures)
- Authentication Proxy—Dynamic per user authentication and authorization supporting both TACACS+ and RADIUS.
- Java Blocking
- Real-time alerts and audit trail
- Dynamic port mapping (PAM)
- Configurable alerts and audit trail
- Simple Mail Transfer Protocol (SMTP) attack detection and prevention
- MS Netshow support
- IPSec encryption
- Tunneling Protocols

## **Key Benefits**

### **Proven IOS Software**

The major benefits of including firewall feature set in RSM entails the flexibility and robustness of the existing IOS feature sets along with the investment protection for the hardware. Cisco IOS Firewall as a software solution is ideal with its robust security features, low footprint requirement, and cost effectiveness.

### **Intranet Security with Policy Enforcement**

Provides security infrastructure for enforcing a Enterprise-wide security policy for connections within an organization as well as between the organization and the rest of the corporate network. Cisco IOS software supports Terminal Access Controller Access Control System (TACACS+), Remote Access Dial-In User Service (RADIUS), IP Security (IPSec), Message Digest 5 (MD5), secure hash algorithm (SHA), Rivest, Shamir Aldeman algorithm (RSA), Data Encryption Standard (DES), Digital Signature Standard (DSS), Cisco encryption technology, and Kerberos.

### **Active Defense Against Distributed Denial of Service Attacks**

Integrated Intrusion Detection system provides real time protection, interception, monitoring and reporting of the most common denial of service attacks. The Cisco IOS software-based intrusion-detection capabilities are an ideal complement to a full, Cisco Secure IDS as it provides additional visibility into the network on Cisco IOS software-based devices and communicates with the CSIDS Director security management system.

### **End to End Security**

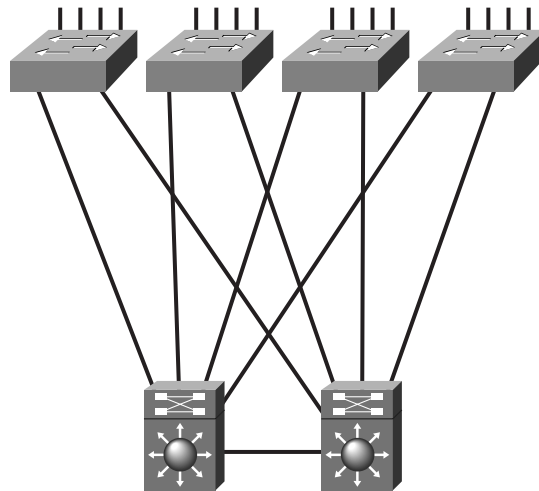
Cisco Secure Integrated Software helps in bringing intelligent network services for both Enterprise and Service providers from an End to End perspective. The security features like IPSec, Stateful Firewalling, Intrusion Detection, Network Address Translation, SSH, Application based user Authentication and Authorization secure the network along with delivering services like QoS, policy networking etc.

## Functional Description

### Context-Based Access Control (CBAC)

CBAC is a per-application control mechanism for IP traffic, including standard Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) Internet applications, multimedia applications (including H.323 and other video applications), and Oracle databases. CBAC inspects TCP and UDP packets and tracks their “state,” or connection status. The Cisco IOS Firewall CBAC engine provides secure, per-application access control across network perimeters. CBAC enhances security for TCP and user datagram protocol (UDP) applications that use well-known ports by scrutinizing source and destination addresses. CBAC allows network administrators to implement firewall intelligence as part of an integrated, single-box solution.

Figure 1 Catalyst 5000 with RSM and Integrated IOS Firewall



CBAC adds inspection intelligence to access control list (ACL) capabilities by reading the entire packet for application status information. Using this information, CBAC creates a temporary, session-specific ACL entry, permitting return traffic into the trusted network. This temporary ACL effectively opens a door in the firewall. When a session times out or ends, the ACL entry is deleted and the door closes to additional traffic. Standard and extended ACLs cannot create temporary ACL entries, so, until now, administrators have been forced to weigh security risks against information access requirements. Advanced applications that select from multiple channels for return traffic have been difficult to secure using standard or extended ACLs.

### Intrusion Detection System (IDS)

The Cisco Secure Integrated Software’s IDS identifies 59 of the most common attacks using signatures to detect patterns of misuse in network traffic. The intrusion-detection signatures included in the new release of the Cisco Secure Integrated Software were chosen from a broad cross section of intrusion-detection signatures. The signatures represent suspicious packets and the most common network attacks and information-gathering scans.

### Authentication Proxy

Network administrators can create specific security policies for each user with Cisco Secure Integrated Software per-user authentication and authorization. Previously, user identity and related authorized access was determined by a user’s fixed IP address, or a single security policy had to be applied to an entire user group or subnet. Now, per-user policy can be downloaded dynamically to the router from a TACACS+ or RADIUS authentication server.

## Ordering Information

Cisco IOS Release 12.1 for the Catalyst 5000 RSM is available immediately.

## For More Information

To find out more about Cisco IOS security and the Cisco IOS Firewall feature set, please visit the Cisco Web site at:

<http://www.cisco.com/warp/customer/cc/cisco/mkt/security/>

<http://www.cisco.com/warp/customer/cc/cisco/mkt/security/iosfw/prodlit/>

For the list of the supported port adapters, please refer to:

[http://www.cisco.com/warp/customer/cc/cisco/mkt/switch/cat/c5000/prodlit/694\\_pp.htm](http://www.cisco.com/warp/customer/cc/cisco/mkt/switch/cat/c5000/prodlit/694_pp.htm)

White paper on Cisco Secure Integrated Software

[http://www.cisco.com/warp/customer/cc/cisco/mkt/security/iosfw/tech/firew\\_wp.htm](http://www.cisco.com/warp/customer/cc/cisco/mkt/security/iosfw/tech/firew_wp.htm)

Distributed Denial of Service News Flash:

<http://www.cisco.com/warp/customer/707/newsflash.html>

Enterprise Network Security:

<http://www.cisco.com/warp/customer/779/largeent/issues/security/>

## Marketing Contacts

<b>Andy Gallagher</b>	408 526-7845	agallagh@cisco.com
<b>Randy Hall</b>	703 484-5557	rhall@cisco.com
<b>John Lopez</b>	408 853-6756	johlopez@cisco.com
<b>Jocelyne Okrent</b>	408 527-2041	jokrent@cisco.com
<b>Ajay Gupta</b>	408 525-3788	ajgupta@cisco.com



### 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

Copyright © 2000 Cisco Systems, Inc. All rights reserved. Printed in the USA. SMARTnet is a trademark; Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9912R) 02/00 BW5962