Security Target For Cisco IOS Firewall Versions 12.3(14)T and 12.4(4)T

October 2006
Version: 1.0

Conventions

The notation, formatting, and conventions used in this Security Target document are largely consistent with the conventions used in Version 2.1 of the Common Criteria (CC) document. Selected presentation choices are discussed here to aid the Security Target reader. The CC allows several operations to be performed on functional requirements; refinement, selection, assignment and iteration are defined in Section 2.1.4 of Part 2 of the CC. Refinements are indicated by **bold text** and ~~strike through~~. Selections are denoted by underlined, *italicized text*, and assignments are enclosed in [square brackets]. Iterations are denoted by showing the iteration number in parenthesis, numbered in sequence, as appropriate.

Terminology

In the CC document, many terms are defined in Section 2.3 of Part 1. The terms listed in Table 1 The are a subset of those definitions, and are listed here to aid the user of the Security Target.

Table 1 Common Criteria Acronyms and Expansions

Acronym	Expansion Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function

Corporate Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

Table 1 Common Criteria Acronyms and Expansions (continued)

Acronym	Expansion Definition
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
TTP	Trusted Third Party

The terminology in Table 2 is specific to the TOE and its environment; these definitions are also provided to aid the user of the Security Target.

Table 2 TOE Definitions

Term	Definition
Assets	Data transmitted over a network
End System	A client or server system with an IP address
Extranet	The interconnection of two or more intranets interconnected with an untrusted network using internetworking devices compliant with the TOE to protect packet flows between the intranets.
Internetworking_Device	A device that interconnects two or more network segments and forwards IP traffic between the end systems connected to the attached network segments (for example, a router or firewall).
Intranet	An organization's internal network, constructed from trusted networks (typically LAN's) interconnected with untrusted networks or network segments using internetworking devices
Network	A single network segment or two or more network segments interconnected by internetworking devices
Network Segment	A single physical segment to which end systems are connected
Packet Flow	A unicast flow of IP packets identified by some combination of source/destination IP address, source/destination TCP/UDP port number, TOS field and input interface

Table 2 TOE Definitions (continued)

Term	Definition
Replay Attack	An attempt by an eavesdropper to capture some portion of a transmission and retransmit it at a later time to gain authorized access to the receiver or to spoof the security functions of the receiver.
Router	A network component (hardware or software) that determines the next network point to which a packet should be forwarded toward its destination on a packet switched network.
Unicast	Communication between a single sender and a single receiver over a network.
User	A human that interacts with the TOE to configure and operate the TOE, such as an administrator. End users (clients) do not interact with the TOE.

Table 3 lists abbreviations that are used when referring to Cisco routers.

Table 3 Cisco Router Terms

Term	Definition
CLI	Command-line Interface
E	Ethernet
Cisco IOS	Cisco Internetwork Operating System
PA	Port Adapter (a large, high-performance, modular network interface)
WIC	Wide Area Network (WAN) Interface Card (a small modular network interface for WANs)

Document Organization

Section 1 provides the introductory material for the security target.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively, that must be satisfied by the TOE.

Section 6 presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

Section 7 provides the Protection Profile claims made by this Security Target.

Section 8 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

Section 8 also provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the requirements.

Section 1: Introduction

1.1 Identification

Title:	Security Target for Cisco IOS/Firewall Version 1.0
Authors:	Cisco Systems, Inc.
Last Updated:	4 October, 2006
CC Version:	2.2
Keywords:	Firewall, Router
TOE:	Cisco IOS/Firewall Versions 12.3(14)T and 12.4(4)T

1.2 Security Target Overview

The TOE is the implementation of the Firewall functionality of Cisco IOS running on Cisco Systems routers. Routers are used to construct IP networks by interconnecting multiple smaller networks or network segments. The Cisco IOS Firewall functionality controls the flow of internet protocol (IP) traffic between network interfaces.

The TOE is called Cisco IOS Firewall.

The TOE meets all the security requirements of the U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, version 1.4, May 1, 2000 with the exception of AVA_VLA.3. This ST does not claim compliance with the referenced Traffic Filter Firewall Protection Profile for Medium Robustness Environments. The assurance class ALC_FLR.1 has been added in order to allow for assurance maintenance to be performed at a later date in order to update the certified products.

The specific versions of the Cisco IOS Firewall hardware and software included in this evaluation are listed in Table 4.

The TOE consists of a Cisco router and Cisco IOS software matching the various models and version information shown in Table 4, the TOE also includes the PIX Firewall Syslog Server which operates on a Windows 2000 platform (see section 2.3.2 Physical for version information). This software has been included to perform viewing, searching and sorting of audit data. The windows 2000 platform has been included under the Common Criteria Evaluation and Validation Scheme (CCEVS) Precedent PD-0113 which allows for the use of the third party product in completion of the functionality for the protection of stored audit data as specified in the SFR FAU_STG.1.

Routers are dedicated hardware devices with purpose written software, which performs many networking functions. The TOE only addresses the following:

- The Firewall function
- Functions relevant to the secure configuration and operation of the Firewall function, such as the authentication and configuration of TOE administrator, configuration of packet filter rules and the searching and sorting of audit data.
- The remote administration of the Cisco IOS router via SSH connections to the routers command line interface.

The Cisco IOS Firewall enhances existing Cisco IOS security capabilities with many features including authentication and encryption, and with state-of-the-art security features, such as stateful packet filtering, defence against network attacks, per user authentication and authorization, and real-time alerts.

1.3 CC Conformance Claim

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, January 2004, CCIMB-2004-01-002.
- Common Criteria for Information Technology Security Evaluation Part 3: Evaluation Assurance Level 4 (EAL4), Version 2.2, Revision 256, January 2004, CCIMB-2004-01-003.
- Common Criteria for Information Technology Security Evaluation Final Interpretation RI# 137, 30 January 2004.

All Common Criteria for Information Technology Security Evaluation Final Interpretations from January 2004 through to the start of the evaluation of this TOE (September 30, 2004) have been included.

This TOE uses the CCEVS Precedents PD-0113 to allow for the inclusion of Windows 2000 in order to satisfy the SFR FAU_STG.1, and PD-0115 to allow for authentication services to be provided by the TOE environment by the use of the RADIUS and TACACS+ protocols. This allows for compliance with interpretation I-0463.

2.0 TOE Description

This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

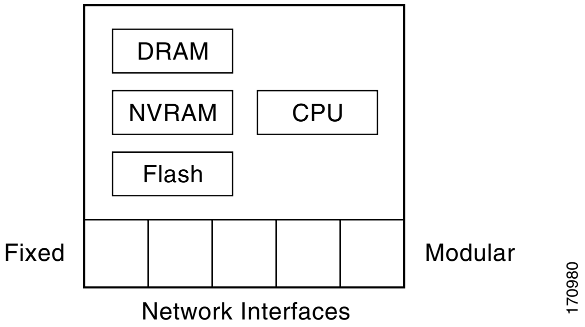
2.1 Product Type

The TOE is comprised of Cisco routers running the Cisco Internetwork Operating System (IOS) as listed in Table 4, and operating in the capacity of a firewall.

Routers that support the TOE have a number of common hardware characteristics.

- Central processor that supports all system operations, such as an Intel Pentium, PowerPC, MIPS
- Dynamic memory, used by the central processor for all system operations
- Flash memory, used to store the operating system image
- Non-volatile memory, which stores configuration parameters used to initialize the system at system startup
- Multiple physical network interfaces (minimally two). Some models will have a fixed number and type of interfaces; some models will have slots that accept additional network interfaces.

Figure 1 Common Hardware Components of a Cisco Router



The basic operation of a router is as follows:

1. The operating system reads the configuration parameters from non-volatile memory, builds the necessary data structures in dynamic memory and commences operation.
2. IP packets are forwarded to the router over one or more of it's physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the router. This processing typically results in the IP packets being forwarded out of the router over another interface, or dropped in accordance with a configured policy.
3. The operating system employs packet filtering of the routed packets resulting in the packet flow being permitted or dropped, and logged in accordance with the configured policy. Packet filtering relies upon the basic routing functionality in order to function.

2.1.1 Cisco IOS Routers

Routers forward packets from one network segment to another based on network layer information (such as an IP address). Interconnected routers will exchange information to determine the optimal path along which network traffic should be forwarded. The primary function of a router is to provide connectivity between networks of end systems. Routers can also filter packets to permit or deny packet flows.

All Cisco routers use common operating system software called the Internetwork Operating Systems (IOS). For a Cisco router to be compliant with the TOE, it must be equipped with the appropriate version of the Cisco IOS software that includes the Firewall function and configured in accordance with the TOE. The TOE-compliant routers and Cisco IOS software versions are identified in Table 4.

2.2 General TOE Functionality

The primary security function of the TOE is the use of Firewall functionality to provide controlled and audited access to services between networks by permitting or denying the flow of IP traffic traversing the firewall. Other functions of the TOE support this primary function.

This section describes Firewall options which are supported by the TOE.

2.2.1 Packet Filtering

Packet Filtering is the primary functionality implemented by the TOE; for example, TOE internetworking devices are deployed at the edges of untrusted networks (such as the Internet), in order to provide controlled communications between two networks that are physically separated. When a packet flow reaches the TOE, the TOE applies an information flow security policy in the form of access control lists and stateful inspection to the traffic before forwarding it into the remote network. Packet flows arriving at a network interface of the TOE are checked to ensure that they conform with the configured packet filter policy, this may include checking attributes such as the presumed source or destination IP address, the protocol used, the network interface the packet flow was received on, and source or destination UDP/TCP port numbers. Packet flows not matching the configured packet filter policy are dropped.

2.2.2 Auditing

The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, the affected subject identity and the outcome of the event. Audited events include; all configuration changes, user attribute changes, successful or failed authentication attempts, information flow events, success or failure of cryptographic operations, changes to system time and the use of audit functions.

The TOE uses TCP syslog for the reliable transport of audit data to the PIX firewall syslog server. The TOE has been configured to limit the loss of audit data in the event of failure of the TCP syslog connection or syslog server. The TOE allows for the searching and sorting of audit log data in a user friendly manner.

2.2.3 Administration

Since the Firewall function is embedded within the router operating system software, configuration, management and operation of the firewall must be undertaken through the normal IOS administrative interfaces provided by the router (console, SSH, syslog, etc). The administration of the TOE takes place by entering text based commands through the routers command-line interface (CLI). To ensure that only authorized administrator can gain secure access to these interfaces, the security target specifies that administration of the TOE may be conducted locally via the console port or remotely via an SSH connection to the TOE-enabled router provided an external AAA service capable of single-use mechanisms is used.

Management of the TOE router using SNMP, HTTP or Telnet is not included in the target of evaluation.

2.3 Scope and Boundaries

2.3.1 Logical

The TOE is a software function within Cisco routers. Routers are dedicated hardware devices with purpose written software that perform many networking functions. The TOE is a subset of the entire router functionality and only addresses:

- The Firewall function (see section 2.2.1 Packet Filtering)
- The Audit function (see section 2.2.2 Auditing)
- Functions relevant to the secure configuration and operation of the firewall function (see section 2.2.3 Administration)
- The remote administration of the Cisco IOS router via SSH connections to the routers command line interface (see section 2.2.3 Administration)

2.3.2 Physical

The TOE consists of two physical devices: the router with operating system (Cisco IOS) and firewall software, and the PIX Firewall Syslog Server (PFSS) software running on a Windows 2000 PC (referred to as the PIX Firewall Syslog Server). It should be noted that the Windows 2000 operating system is included in the TOE scope and that the Windows PC is in its evaluated configuration as specified by the Windows 2000 Security Target, Version 2.0, 18 October 2002. When the TOE-enabled router is in use, at least two of the network interfaces of the internetworking device will be attached to different networks. The router configuration will determine how packet flows received on an interface will be handled. Typically, packet flows that are permitted to be passed through the internetworking device will be forwarded to their configured destination, and all other packet flows dropped.

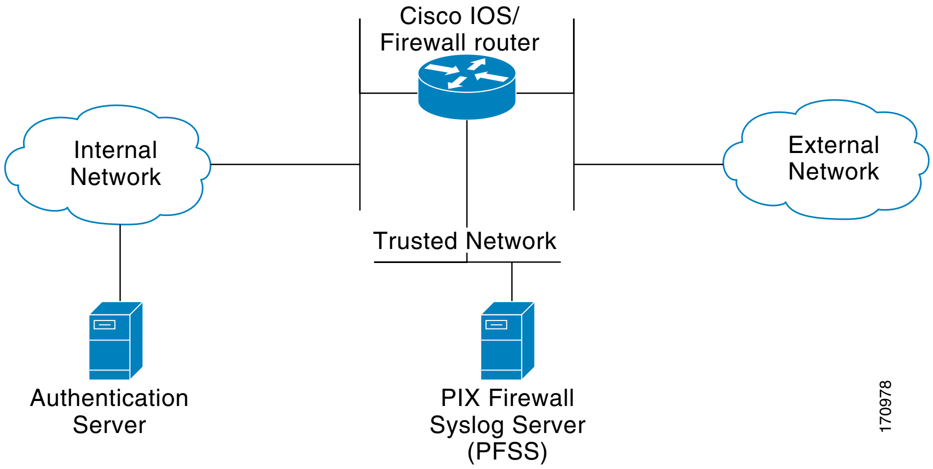
The PIX Firewall Syslog Server (PFSS) is to be physically connected to a trusted interface of the Cisco IOS Firewall directly or indirectly via an attached trusted network as shown in Figure 2

It should be noted that more than one untrusted network may be connected to the Cisco IOS Firewall via separate interface, and that an untrusted network may be considered internal or external, this allows for the use of the firewall to filter packet flows between two or more untrusted networks. In this situation the PFSS must still be connected via an additional trusted network.

The Authentication Server shown in Figure 2 is part of the TOE environment and may provides remote authentication services via the RADIUS or TACACS+ protocols. The remote authentication must be a single-use mechanism.

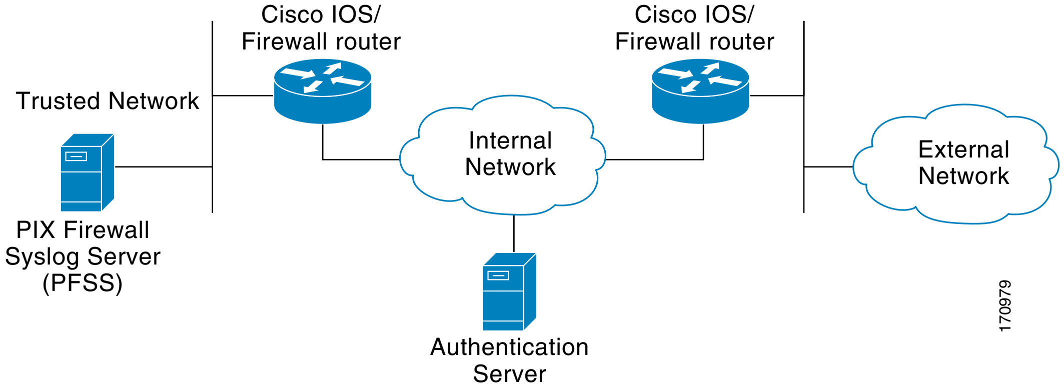
The 28xx, 38xx and 72/73xx series of routers are modular and include at least two Fast Ethernet interfaces. When the TOE consists of one of these series, a third interface is required to connect to the Trusted Network.

Figure 2 Typical Configuration for 28xx, 38xx, and 72/72xx



The 87x and 18xx series of routers are fixed configuration with a maximum of two Fast Ethernet interfaces. When the TOE consists of one of these series, a second instance of the TOE is required to protect access to the Trusted Network.

Figure 3 Typical Configuration for 87xx and 18xx



The scope of evaluation includes all of the Router makes, models, and corresponding Cisco IOS versions listed in Table 4.

Table 4 TOE Router Platforms and OS version information

Model Family	Model	Cisco IOS Software Version
8xx	c871, c876, c877,c878	12.4(4)T
18xx	c1841	12.3(14)T
	c1811, c1812	12.4(4)T
	c1801, c1802, c1803	
28xx	c2801, c2851, c2821, c2811	12.3(14)T

Table 4 TOE Router Platforms and OS version information (continued)

Model Family	Model	Cisco IOS Software Version
38xx	c3845, c3825	12.3(14)T
72xx, 73xx	7206VXR, 7204VXR, CISCO7301	12.3(14)T

The Cisco IOS binary image files are included in the TOE in their entirety.

The TOE also includes the PIX Firewall Syslog Server version 5.1(3). This software has been included to perform viewing, searching and sorting of audit data.

The scope of evaluation includes the network interface modules listed in the following table. These network interfaces have been confirmed to zeroize all data buffers used for the padding of transmissions. Note that the interfaces are listed by router families and models due to the differences between platform architecture.

Table 5 TOE Router Platforms and Network Interfaces

Model Family	Model	Network Interface Type
8xx	c871, c876, c877,c878	10/100 Ethernet, ATM, FE switch, ISDN, xDSL
18xx	c1841	HWIC-4ESW 10/100 Ethernet On-board fast ethernet
	c1801, c1802, c1803, c1811, c1812	10/100 Ethernet, FE switch
28xx	c2851, c2821, c2811	10/100 Ethernet, ATM, Frame, Serial
	c2801	HWIC-4ESW 10/100 Ethernet HWIC-D-9ESW 10/100 Ethernet On-board fast ethernet
38xx	c3845, c3825	10/100/1000 Ethernet, ATM, Channelized, DSL, Frame Relay, ISDN, Serial
72xx, 73xx	7206VXR, 7204VXR, CISCO7301	10/100/1000 Ethernet, ATM, ISDN, POS Interface, Serial and Multichannel

The PFSS resides on a Windows 2000 platform. The Syslog server has been included because of its ability to perform reliable Syslog functions using TCP/IP and provide for the viewing, searching, and sorting of audit log data. The PFSS is designed so that multiple Cisco IOS Routers may transfer audit logs to a single PFSS. In the evaluated configuration the PFSS must be on a trusted network directly connected to the TOE as shown in Figure 2.

Cisco IOS software contains a collection of features that build on the core components of the system. Table 6 categorizes the features as included in the evaluated configuration ("Included"), excluded and therefore not available in the evaluated configuration ("Not to be Used"), and trusted to not interfere with the TSF ("Trusted").

Note Apart from the exceptions listed in Table 6, all types of network traffic through and to the TOE are within the scope of the evaluation.

Table 6 Collection of Cisco IOS Features

Feature	**Description**	**Included**	**Not to be Used**	**Trusted**
AAA	Authentication, Authorization and Accounting support TACACS+: TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router, switch or network access server. RADIUS: Support for Remote Access Dial-In User Service (RADIUS)	X		
AES	Advanced Encryption Standard	X		
CEF	Cisco Express Forwarding	X		
Certificates and Certificate Server	The Certificate Server offers a secure facility for deploying encryption key information through compliance with the x.509v3 standards for digital certificate generation and distribution.			X
DHCP	Dynamic Host Control Protocol (DHCP) enables you to automatically assign reusable IP addresses to DHCP clients.			X
Firewall	Firewall: Tracking the state and context of network connections to provide enhanced perimeter security. Application Firewall: Application firewall services for IOS ACL: Access Control List	X		
HSRP	Hot Standby Router Protocol (HSRP) provides automatic router backup			X
HTTP Server	Emweb HTTP Core, HTTP 1.1 Server integration with Cisco IOS		X	

Table 6 Collection of Cisco IOS Features (continued)

Feature	Description	Included	Not to be Used	Trusted
IEEE 802.11 Wireless Standards	This support enables interoperability under 802.11 specifications for network architecture, wireless association, and radio management. Support for 802.11 standards allows you to set the access point mode of operation (root or repeater), Service Set Identifier (SSID), authentication type, channel selection, transmission rates, power-save mode, and security based on wired equivalent privacy (WEP), and other configurable fields		X	
IGMP	Internet Group Management Protocol, version 3			X
IPv6	IPv6 (Internet Protocol Version 6) has also been called "IPng" (IP Next Generation). Formally, IPv6 is a set of specifications from the Internet Engineering Task Force (IETF). IPv6 was designed as an evolutionary set of improvements to the current IP Version 4. The most obvious difference between IPv6 and IPv4 is that IP addresses are lengthened from 32 bits to 128 bits.			X
Media Types	ISDN: ISDN involves the digitalization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone. Frame Relay: Frame Relay switching is a means of switching packets based on the DLCI, which can be considered the Frame Relay equivalent of a MAC address. You perform switching by configuring your Cisco router or access server into a Frame Relay network. There are two parts to a Frame Relay network: Frame Relay DTE (the router or access server) and Frame Relay DCE switch. ATM: ATM media types. ADSL: Asynchronous Digital Subscriber Line PPP: PPP provides a method for transmitting datagrams over serial point-to-point links. PPPoE: PPP over Ethernet client to allow the router (CPE) to act as the client in a PPPoE scenario			X
Mobile IP	Allows nodes in an IP network to roam to remote networks and remain in contact with their home network.			X
NAC	Network Admission Control provides a way to limit access to the network to only those hosts having compliant software as defined by the administrator.			X

Table 6 Collection of Cisco IOS Features (continued)

Feature	Description	Included	Not to be Used	Trusted
NAT	Network Address Translation is used by a device (firewall, router or computer) that sits between an internal network and the rest of the world.			X
NetFlow	The Cisco IOS NetFlow feature tracks the IP traffic that is routed by your Cisco device by using a built-in cache. Tracked information can be retrieved and viewed on-screen using “show” commands, or exported and printed in reports, which enables you to analyze the IP traffic data for a specific time period. Using the NetFlow feature, you can review traffic, trend, billing, and other traffic-related data.			X
QoS	Quality of Service			X
Routing Protocols	OSPF: Open Shortest Path First (OSPF) is a routing protocol developed for Internet Protocol (IP) networks by the interior gateway protocol (IGP) working group of the Internet Engineering Task Force (IETF). RIP: Routing Information Protocol (RIP) is a distance-vector protocol that uses hop count as its metric. EIGRP: Enhanced Interior Gateway Routing Protocol BGP: Border Gateway Protocol STP: Spanning tree algorithms provide path redundancy by defining a tree that spans all of the switches in an extended network and then force certain redundant data paths into a standby (blocked) state.			X
SSH	SSHv2 client and server support	X		
SLB	Server load balancing			X
SNMP	The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.		X	
SPAN	Switch Port Analyzer			X
Syslog	Configuration and delivery of SYSLOG messages	X		
Telnet	Legacy unencrypted protocol for administration		X	

Table 6 Collection of Cisco IOS Features (continued)

Feature	Description	Included	Not to be Used	Trusted
VoIP	Voice over IP enables Cisco routers to carry voice traffic (for example, telephone calls and faxes) over an IP network. In Voice over IP, the digital signal processor segments the voice signal into frames, which are then coupled in groups of two and stored in voice packets. Call Manager Express SIP: Session Initiation Protocol H.323 Version 2 Support upgrades Cisco IOS software to comply with the mandatory requirements and several of the optional features of the version 2 specification.			X
VPN	WebVPN: This feature enables secure remote access through SSLVPN on Cisco IOS routers. IPSec: IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”), such as Cisco routers. IKE: The Internet Key Exchange (IKE) protocol is a key management protocol standard which is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. EasyVPN: This feature provides enhanced VPN functionality and policy management for Cisco VPN remote access clients. L2TP: Layer 2 Tunneling Protocol MPLS: Multiprotocol label switching, MPLS (or Tag Switching), combines the performance and capabilities of Layer 2 (data link layer) switching with the proven scalability of Layer 3 (network layer) routing. MPLS enables service providers to meet the challenges of explosive growth in network utilization while providing the opportunity to differentiate services without sacrificing the existing network infrastructure. The MPLS architecture is flexible and can be employed in any combination of Layer 2 technologies. MPLS support is offered for all Layer 3 protocols.		X	

3. TOE Security Environment

To clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and of the manner for which the TOE is intended.
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.

3.1 Secure Usage Assumptions

Table 7 lists assumptions that are made in relation to the operation of TOE.

Table 7 Secure Usage Assumptions

Name	Description
A.PHYSEC	The TOE is physically secure.
A.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
A.GENPUR	There is no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.REMACC	Authorized administrator may access the TOE remotely from the internal and external networks.
A.PROTECTIF	The PFSS is to be connected to the Cisco IOS Firewall enabled router such that the network interface of the PFSS is only accessible by the TSF. This may be achieved by either directly connecting the PFSS to the router, or indirectly over the trusted network. This protection of the PFSS network interface is required by PD-0113.

3.2 Threats to Security

This ST identifies the threat agents against the TOE as attackers with expertise, resources, and motivation that combines to be a moderate attack potential.

3.2.1 Threats Addressed by the TOE

TOE addresses threats listed in Table 8.

Table 8 Threats Addressed by the TOE

Name	Description
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (for example, spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.

Table 8 Threats Addressed by the TOE (continued)

Name	Description
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.
T.MODEXP	A skilled attacker with moderate attack potential may attempt to bypass the TSF to gain access to the TOE or the assets it protects.
T.TUSAGE	The TOE may be inadvertently configured, used and administered in a insecure manner by either authorized or unauthorized persons

3.2.3 Organization Security Policies

Table 9 describes the organizational security policies relevant to the operation of the TOE.

Table 9 Organizational Security Policies

Name	Description
P.CRYPTO	Triple DES and AES encryption (as specified in FIPS 46-3 [3]) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1).

4. Security Objectives

The security objectives are a high-level statement of the intended response to the security problem. These objectives indicate how the security problem, as characterized in the “Security Environment” section of the ST (see the section “3. TOE Security Environment”), is to be addressed.

Table 10 describes security objectives for the TOE, while Table 11 describes objectives for the environment.

The environmental objective O.IDAUTH(env) is an iteration of the TOE Objective O.IDAUTH, and has been added in order to allow for remote authentication services to be provided by the environment.

The Security Objectives for the Environment (see section 4.2 Security Objectives for the Environment) are considered Non-IT.

4.1 Security Objective for the TOE

Table 10 Security Objectives for the TOE

Name	Description
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.
O.MEDIAT	The TOE must mediate the flow of all information between users on an internal network connected to the TOE and users on an external network connected to the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

Table 10 Security Objectives for the TOE (continued)

Name	Description
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
O.EAL	The TOE must be tested and shown to be resistant to attackers possessing moderate attack potential.

4.2 Security Objectives for the Environment

Table 11 Security Objectives for the Environment

Name	Description
O.PHYSEC	The TOE is physically secure.
O.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
O.GENPUR	There are no general-purpose computing capabilities (for example, the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
O.PUBLIC	The TOE does not host public data.
O.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
O.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.

Table 11 Security Objectives for the Environment (continued)

Name	Description
O.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (for example, a console port) if the connection is part of the TOE.
O.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
O.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
O.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
O.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
O.IDAUTH (env)	The TOE environment must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions

5. IT Security Requirements

5.1 TOE Security Functional Requirements

This section contains the functional requirements for the TOE, drawn from part two of the Common Criteria.

5.1.1. FMT_SMR.1 Security roles

FMT_SMR.1.1 - The TSF shall maintain the role~~s~~ [privileged administrator, semi-privileged administrator and audit administrator].

FMT_SMR.1.2 - The TSF shall be able to associate **human** users with t**he privileged administrator, semi-privileged administrator and audit administrator** roles.

5.1.2. FIA_ATD.1 User attribute definition

FIA_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to individual users:

a. [identity

b. association of a human user with the authorized administrator role

c. the privilege level of a user role.]

5.1.3. FIA_UID.2 User identification before any action (1)

FIA_UID.2.1 - The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.4. FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 - The TSF shall detect when [**a non-zero number determined by the authorized administrator] of** unsuccessful authentication attempts occur related to [authorized TOE administrator access or authorized TOE IT entity access].

FIA_AFL.1.2 - When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending external IT entity from successfully authenticating until an authorized administrator takes some action to make authentication possible for the external IT entity in question].

5.1.5. FIA_UAU.5 Multiple authentication mechanisms (1)

FIA_UAU.5.1 - The TSF shall provide [a password mechanism] to support user authentication.

FIA_UAU.5.2 - The TSF shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules:

a. ~~single-use authentication mechanism shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator.~~

b. ~~single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity.~~[1]

c. reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator].

5.1.6. FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 - The TSF shall enforce the [UNAUTHENTICATED_SFP] on the following:

a. [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another

b. information: traffic sent through the TOE from one subject to another

c. operation: pass information]

5.1.7. FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 - The TSF shall enforce the [UNAUTHENTICATED_SFP] based on the following types of subject and information security attributes:

1. [subject security attributes:
   - Presumed address
   - No additional attributes
2. Information security attributes:
   - presumed address of source subject
   - presumed address of destination subject
   - transport layer protocol
   - TOE interface on which traffic arrives and departs
   - Service
   - No additional attributes]

[1] Parts a and b of FIA_UAU5.2(1) is performed by the TOE environment and hence have been removed from FIAA_UAU.5.2(1) and included in the environmental iteration of this requirement (FIA_UAU.5.2(2)).

FDP_IFF.1.2 - The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

1. [Subjects on an internal network can cause information to flow through the TOE to another connected network if:
    - All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator
    - The presumed address of the source subject, in the information, translates to an internal network address
    - The presumed address of the destination subject, in the information, translates to an address on the other connected network
2. Subjects on the external network can cause information to flow through the TOE to another connected network if:
    - All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator
    - The presumed address of the source subject, in the information, translates to an external network address
    - The presumed address of the destination subject, in the information, translates to an address on the other connected network]

FDP_IFF.1.3 - The TSF shall enforce the [none].

FDP_IFF.1.4 - The TSF shall provide the following [none].

FDP_IFF.1.5 -The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules:

1. [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network.
2. The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network.
3. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network.
4. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network].

5.1.8. FMT_MSA.1 Management of security attributes (1)

FMT_MSA.1.1 (1) - The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule and add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(1)] to [the privileged administrator].

5.1.9. FMT_MSA.1 Management of security attributes (2)

FMT_MSA.1.1 (2) - The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to *delete* **and** [create] the security attributes [information flow rules described in FDP_IFF.1(1)] to [the privileged administrator].

5.1.10. FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 - The TSF shall enforce the [UNAUTHENTICATED_SFP] to provide *restrictive* default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2 - The TSF shall allow the [privileged administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.11. FMT_MTD.1 Management of TSF data (1)

FMT_MTD.1.1(1) - The TSF shall restrict the ability to *query*, *modify*, *delete*, [and assign] the [user attributes defined in FIA_ATD.1.1] to [the privileged administrator].

5.1.12. FMT_MTD.1 Management of TSF data (2)

FMT_MTD.1.1(2) - The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1.1] to [the privileged administrator].

5.1.13. FMT_MTD.2 Management of limits on TSF data

FMT_MTD.2.1 - The TSF shall restrict the specification of the limits for [the number of authentication failures] to [the privileged administrator].

FMT_MTD.2.2 - The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [actions specified in FIA_AFL.1.2].

5.1.13. FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 - The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following objects: [resources that are used by the subjects of the TOE to communicate through the TOE to other subjects].

5.1.15. FCS_COP.1 Cryptographic operation

FCS_COP.1.1 - The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with a specified cryptographic algorithm: [Triple Data Encryption Standard (DES) as specified in FIPS PUB 46-3 and implementing any mode of operation specified in FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys)] and cryptographic key sizes [that are 192 binary digits in length and Advanced Encryption Standard (AES) as specified in FIPS PUB 197 and cryptographic key sizes [that are 128 binary digits in length] that meet the following: [FIPS PUB 46-3 with Keying Option 1 and FIPS PUB 140-1 (Level 1)].

5.1.16. FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 - The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.17. FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 - The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 - The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.18. FPT_STM.1 Reliable time stamps

FPT_STM.1.1 - The TSF shall be able to provide reliable time stamps for its own use.

5.1.19. FAU_GEN.1 Audit data generation

FAU_GEN.1.1 - The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions
b. All auditable events for the *not specified* level of audit
c. [the events in Table 12].

FAU_GEN.1.2 - The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity, outcome (success or failure) of the event
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 12].

Table 12 Auditable Events

Functional Component	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Modifications to the group of users that are part of **the privileged administrator, semi-privileged and audit administrator** roles.	The identity of the privileged administrator performing the modification and the user identity being associated with the privileged administrator role.
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE.
FIA_UAU.5	All use of the user identification mechanism.	The user identities provided to the TOE.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the privileged administrator of the users capability to authenticate.**	The identity of the offending user and the privileged administrator
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.

Table 12 Auditable Events (continued)

Functional Component	Auditable Event	Additional Audit Record Contents
FCS_COP.1	Success and failure, and the type of cryptographic operation.	The identity of the external IT entity attempting to perform the cryptographic operation.
FPT_STM.1	Changes to the time.	The identity of the privileged administrator performing the operation.
FMT.MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the privileged administrator performing the operation.

5.1.20. FAU_SAR.1 Audit review

FAU_SAR.1.1 - The TSF shall provide [an audit administrator] with the capability to read [all audit trail data] from the audit records.

FAU_SAR.1.2 - The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.21. FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 - The TSF shall provide the ability to perform *searches* ***and*** *sorting* of audit data based on:

a. [presumed subject address

b. ranges of dates

c. ranges of times

d. ranges of addresses]

5.1.22. FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 - The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 - The TSF shall be able to *prevent* unauthorized modifications to the audit records.

5.1.23. FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 - The TSF shall *prevent auditable events, except those taken by the privileged* ***administrator*** and [shall limit the number of audit records lost] if the audit trail is full.

5.1.24. FMT_MOF.1 Management of security functions behavior (1)

FMT_MOF.1.1 (1) - The TSF shall restrict the ability to *enable*, *disable* the functions:

a. operation of the TOE

b. single-use authentication function described in FIA_UAU.5]

to [a privileged administrator].

5.1.25. FMT_MOF.1 Management of security functions behavior (2)

FMT_MOF.1.1(2) - The TSF shall restrict the ability to *enable, disable, determine and modify the behavior* of the functions:

a. [audit trail management and backup / restore for audit trail data to [an audit administrator]

b. backup and restore for TSF data, information flow rules, and audit trail data

c. communication of authorized external IT entities with the TOE]

to [a privileged administrator].

5.1.26. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 - The TSF shall be capable of performing the following security management functions:

a. [create, delete, modify, and view information flows rules that permit or deny information flows

b. enable or disable the operation of the TOE

c. configure the single-use authentication function described in FIA_UAU.5

d. configure audit trail management

e. backup and restore TSF data, information flow rules, and audit trail data

f. enable or disable communication of authorized external IT entities with the TOE].

5.2 Environmental Security Functional Requirements

The following environmental SFRs have been included to allow for remote authentication services to be provided by the environment.

5.2.1. FIA_UID.2 User identification before any action (2)

FIA_UID.2.1 - The **TOE Environment** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.2. FIA_UAU.5 Multiple authentication mechanisms (2)

FIA_UAU.5.1 - The **TOE Environment** shall provide [a single-use password mechanism and single-use authentication mechanisms] to support user authentication.

FIA_UAU.5.2 - The **TOE Environment** shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules:

a. single-use authentication mechanism shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator.

b. single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity.

c. ~~reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator.[1]]~~

5.3 TOE Security Assurance Requirements

The TOE meets all the Assurance Requirements prescribed by EAL4 in Part 3 of the CC and additionally meets the ALC_FLR.1 assurance requirement. Assurance components are summarized by Assurance Class in Table 13.

Table 13 Assurance Requirements: EAL4 Augmented

Assurance Class	Assurance Components	
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Basic Flaw Remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

[1] Part c of FIA_UAU5.2 (2) is performed by the TOE and has been removed from the environmental iteration of this requirement.

6. TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

For specific information of TOE functions met by permutational or probabilistic mechanisms and their associated Strength of Function claims, see section 8.2.5 of this document.

6.1 IT Security Functions

This section presents the security functions performed by the TOE. Security Functional Requirements that are satisfied by a Security Function are identified in Table 14.

6.1.1 Packet Filtering

PACKETFILTER.1 - Packet Filtering

The TOE performs packet filtering by applying an information flow security policy (UNAUTHENTICATED_SFP), in the form of access control lists and stateful inspection, to specific interfaces of the TOE-enabled router. The access-control list and stateful firewall can include presumed source/destination IP address, protocol, interface and source/destination UDP/TCP port number. The TOE shall permit an information flow between controlled subjects if all information security attributes are permitted by the information flow security policy. Packets not matching the information flow security policy are logged and discarded by the router. The TOE rejects requests for access or services where the information arrives on a network interface, and the presumed address of the source subject is an external IT entity on a different network interface, this includes broadcast and loopback networks. This allows for traffic from known spoofed addresses, broadcasts and loopbacks to be blocked. By implementing this form of policy enforcement, the TOE ensures that the TSP cannot be bypassed as long as the TOE is correctly configured.

6.1.2 Configuration and Management

CONFIG.1 - Management Interfaces

The router can be configured, managed and operated using the command-line interface (CLI) either via direct local connection to a physical console port, or remotely via an in-band network connection. No management interfaces other than that provided via the console port are available in the Cisco IOS default configuration. The remote management connection to the CLI via SSH must be explicitly enabled to be used and all other remote management connections that Cisco IOS is capable of using, such as telnet, are disallowed in the evaluated configuration. The management interface presented at the console port is always enabled. Access to the CLI requires valid authentication.

The router maintains all Cisco IOS administrator roles. The Router can and shall be configured to authenticate both unprivileged and privileged access to the command line interface using a username and password. Privileged access is defined by any privilege level entering an enable password after their individual login. The router restricts the ability to create, modify and delete user accounts to authorized administrators (those with privileged access). No router CLI functions are accessible to an unauthenticated user, with the exception of the authentication functions. Additionally unprivileged access restricts the administrator from accessing any CLI commands that modify the security configuration of the TOE.

Both successful and unsuccessful authentication attempts are logged. After a number of unsuccessful authentication attempts, as configured by the administrator, the user account is locked and may no longer authenticate to the TOE until the user account is unlocked by an authorized administrator.

The privileged administrator has control over all router functions, attributes, and data, either by executing commands, viewing status and configuration, or editing the router configuration settings. The default configuration will be secure so that packet flows will not occur. The privileged administrator has the right to change from the default to allow packet flows.

The TOE security function CONFIG.1 uses access control to limit access to the audit log data whilst on the router to authorized administrators. To ensure that Audit data cannot be modified, functionality to allow for the modification of audit logs has not been implemented in the TOE. The PFSS is solely for the viewing of audit logs and does not have the ability to change the security configuration of the router.

CONFIG.2 - Management of Time

The router maintains real time using a reliable software clock that interfaces to an internal hardware clock. The router restricts the ability to change the system time to an authorized administrator. Hardware clocks are not available in the 800 series of routers, in this situation the administrator is required to update the software clock in the event of power failure or system restart.

6.1.3 Audit

AUDIT.1 - System Messages

The TOE generates audit messages that identify specific TOE operations – For each event, the TSF shall record the date and time of each event, the type of event, the subject identity, the affected subject identity and the outcome of the event. Audited events include; all configuration changes, user attribute changes, successful or failed authentication attempts, information flow events, success or failure of cryptographic operations, changes to system time and the use of audit functions. For more information on auditable events see section 5.1.19. FAU_GEN.1 Audit data generation.

TCP syslog is used to transmit data to the PIX Firewall Syslog Server (PFSS). In the event of audit storage failure on the PFSS, the reliable syslog connection will close causing the router to perform a series of reconnection attempts. If the router is continually unable to connect to the syslog server for a TCP retry period of nine minutes the router will fail close, disallowing all new connection attempts with the exception of connections to the administration interface. The router will remain in this state until the connection to the PFSS is made available and TCP Syslog configuration is re-established. In this case, the only audit data that will be lost is that of events occurring within the nine minute window in which the syslog connection is down, and the administration events generated afterwards.

AUDIT.2 – Audit Review

The review of audit logs is conducted using the PFSS. The PFSS receives reliable syslog transmissions from an IOS/Firewall enabled router as described in AUDIT.1. The PFSS stores audit data to the local hard disk. The audit logs can be viewed, searched and sorted using the purpose built Cisco software included with the PFSS. If the PFSS audit logs fill to their maximum allowed capacity, the TCP syslog connection will be closed.

The PFSS uses the Windows 2000 operating system to provide protection of the stored audit records.

6.1.4 Management and Resources

RESOURCE.1 - Management of Resources

The TOE prevents a subjects information resources from being available to other subjects by zeroising all memory used for the padding of transmissions prior to the construction of the individual packets to be sent by the interface. This functionality is implemented by the interface driver, and has been implemented in all network interface modules provided in this evaluation (see section 2.3.2 Physical for a full list of network interfaces included in the scope of this evaluation).

This function is designed to prevent data from previous transmissions being accidentally present in transmission padding (etherleak).

6.1.5 Protection of TSC

PROTECT.1 – Protection of TSC

To enforce the protection of the TOE configuration through the distinction and separation of information flows. The TOE protects itself from interference and tampering by untrusted subjects by implementing authentication and access controls to limit configuration to authorized administrators. Cisco IOS is not a general purpose operating system and access to Cisco IOS memory space is restricted to only Cisco IOS functions. Additionally, Cisco IOS is the only software running on the TOE enabled routers.

6.1.6 Remote Management

REMOTE.1 – Remote Management

The TOE implements Secure Shell (SSH) using 192-bit 3DES and 128-bit AES encryption for the purposes of remote management. The implementation of SSH provides an integrated single use mechanism in that the transport protocol provides a unique session identifier that is bound to the key exchange process. This is used by higher level protocols to bind data to a given session and prevent replay of data from prior sessions. See section 9.2.3 *Replay* of the SSH Protocol Architecture internetworking draft for more information on the SSH protocol (http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-21.txt).

The use of SSH for remote management requires the use of the external authentication server for the purposes of one time authentication.

Remote management via SSH provides full access to the CLI command set.

Table 14 Mapping Security Functions to Functional Requirements

TSS Reference	IT Security Function	Functional Component	Functional Requirement
PACKETFILTER.1	Packet Filtering	FDP_IFF.1 FDP_IFC.1 FPT_RVM.1	Simple security attributes Subset information flow control Non-bypassability of the TSP

CONFIG.1	Management Interfaces	FIA_UAU.5(1)
		FIA_UID.2(1)
		FIA_AFL.1
		FMT_MTD.2
		FMT_SMR.1
		FMT_MOF.1(1)
		FMT_MOF.1(2)
		FMT_MSA.1(1)
		FMT_MSA.1(2)
		FMT_MSA.3
		FIA_ATD.1
		FMT_MTD.1(1)
		FMT_MTD.1(2)
		FMT_SMF.1
			Multiple authentication mechanisms
			User identification before any action
			Authentication failure handling
			Management of limits on TSF data
			Security roles
			Management of security functions behavior
			Management of security functions behavior
			Management of security attributes
			Management of security attributes
			Static attribute initialization
			User attribute definition
			Management of TSF data
			Management of TSF data
			Specification of Management Functions

CONFIG.2	Management of Time	FPT_STM.1 FMT_MTD.1(2)	Reliable time stamps Management of TSF data
AUDIT.1	System Messages	FAU_GEN.1 FAU_STG.4	Audit data generation Prevention of audit data loss
AUDIT.2	Audit Review	FAU_SAR.1 FAU_SAR.3 FAU_STG.1 FAU_STG.4	Security Audit Review Selectable Audit Review Protected audit trail storage Prevention of audit data loss

Table 14 Mapping Security Functions to Functional Requirements (continued)

TSS Reference	IT Security Function	Functional Component	Functional Requirement

REMOTE.1	Remote Management	FCS_COP.1
		FIA_UAU.5(2)
		FIA_UID.2(2)
			Cryptographic Operation (encryption)
			Multiple authentication mechanisms
			User identification before any action

RESOURCE.1	Management of Resources	FDP_RIP.1	Subset residual information protection
PROTECT.1	Protection of the TSC	FPT_SEP.1	TSF domain separation

6.2 Assurance Measures

The purpose of this section is to show that the identified assurance measures are appropriate to meet the assurance requirements by mapping the identified assurance measures onto the assurance requirements.

The Assurance Measures that demonstrate the correct implementation and use of the Security Functions of the TOE are as follows:

- Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS/Firewall (ADM), version 1-0, October 2006.
- Functional Specification for Cisco IOS/Firewall (FSP), version A.20, 28 July 2006.
- TOE Security Policy Model for Cisco IOS/Firewall (SPM), version A.13, 24 August 2005.
- High Level Design for Cisco IOS/Firewall (HLD), version A.14, 30 June 2006.
- Low Level Design for Cisco IOS/Firewall (LLD), version 1-5, 28 June 2006.
- Cisco's Configuration Management Plan and Delivery Procedures (CMP), version 0-8, 7 August 2006.
- Cisco IOS Firewall Specific Configuration Items List and Delivery Procedures (CL), version 0-9, 30 June 2006.
- Development Security for Cisco IOS (DEVSEC), version 0-3, September 2005.
- IOSFirewall-EAL4-COV-DPT spreadsheet (ATE), version 0-11,June 2006.
- Misuse Analysis for Cisco IOS/Firewall (MSU), version 0-3, August 2005.
- Vulnerability Analysis/Strength of Function Analysis for Cisco IOS/Firewall (VLA-SOF), version 0-8 April 2006.
- Representational Correspondence Demonstration for Cisco IOS/Firewall (RCR), version A.10, 30 June 2006.
- TOE Source Code

Table Table 15 demonstrates that the identified assurance measures completely meet the assurance requirements by showing that all requirements are mapped to an assurance measure.

Table 15 Mapping of Assurance Measures to Assurance Requirements

CC Assurance Component		Assurance Measure
ACM_AUT.1	Partial CM automation	CMP
ACM_CAP.4	Generation support and acceptance procedures	CMP
ACM_SCP.2	Problem tracking CM coverage	CMP
ADO_DEL.2	Detection of modification	CMP, CL
ADO_IGS.1	Installation, generation, and start-up procedures	ADM
ADV_FSP.2	Fully defined external interfaces	FSP
ADV_HLD.2	Security enforcing high-level design	HLD
ADV_IMP.1	Subset of the implementation of the TSF	TOE Source Code
ADV_LLD.1	Descriptive low-level design	LLD
ADV_RCR.1	Informal correspondence demonstration	FSP, HLD, LLD, RCR
ADV_SPM.1	Informal TOE security policy model	SPM
AGD_ADM.1	Administrator guidance	ADM
AGD_USR.1	User guidance	ADM
ALC_DVS.1	Identification of security measures	DEVSEC
ALC_FLR.1	Basic Flaw Remediation	CMP
ALC_LCD.1	Developer defined life-cycle model	CMP
ALC_TAT.1	Well-defined development tools	CMP
ATE_COV.2	Analysis of coverage	ATE
ATE_DPT.1	Testing: high-level design	ATE
ATE_FUN.1	Functional testing	ATE
ATE_IND.2	Independent testing - sample	ATE, TOE
AVA_MSU.2	Validation of analysis	MSU
AVA_SOF.1	Strength of TOE security function evaluation	VLA-SOF
AVA_VLA.2	Independent vulnerability analysis	VLA-SOF

The assurance measures documents have been specifically written to meet the assurance requirements and are structured as follows:

Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS/Firewall (ADM)

Since non-administrative users have no direct interaction with the TOE, no non-administrative user guidance is required. Therefore the assurance requirement AGD_USR.1 does not apply to this evaluation. The User Guidance document provides the following information:

- Guidance for TOE administrators with procedural information on installation, configuration and management of the TOE. (AGD_ADM.1)
- Describes procedures for the installation, generation, and start-up of the TOE. (ADO_IGS.1)
- Detailed syntax information on the external interfaces used for such interaction with the TOE. (ADV_FSP.2)

Functional Specification for Cisco IOS/Firewall (FSP)

- Describes the security functionality of the TOE. (ADV_FSP.2)
- Defines the external interfaces to the TOE. (ADV_FSP.2)

TOE Security Policy Model for Cisco IOS/Firewall (SPM)

- Describes the security policy implemented by the TOE (ADV_SPM.1)

High Level Design for Cisco IOS/Firewall (HLD)

- Describes the relationship between TOE sub-systems, their interfaces and the sequence of events in response to stimulus at those interfaces. (ADV_HLD.2)

Low Level Design for Cisco IOS/Firewall (LLD)

- Describes the TOE sub-systems, their interfaces and the sequence of events in response to stimulus at those interfaces (ADV_LLD.1)· A source code representation of the TOE. (ADV_IMP.1)

Cisco's Configuration Management Plan and Delivery Procedures (CMP)

- Describes the development life-cycle model. (ALC_LCD.1)
- Describes the development tools. (ALC_TAT.1)
- Describes the CM model (ACM_AUT.1) and how problem tracking and flaw remediation is undertaken. (ALC_FLR.1 and ACM_SCP.2)
- Description of TOE generation and acceptance procedures. (ACM_CAP.4)
- Describes the delivery procedures and how they provide for the detection of modification. (ADO_DEL.2)
- Describes additional development tools. (ALC_TAT.1)

Development Security for Cisco IOS (DEVSEC)

- Describes the security measures for the development site (ALC_DVS.1).

IOSFirewall-EAL4-COV-DPT spreadsheet (ATE)

- Describes the testing undertaken of the TOE and the implementation of the functionality specified in the ST and the design documentation. (ATE_DPT.1)
- Describes coverage of the testing. (ATE_COV.2)

- Describes the testing of security functionality. (ATE_FUN.1)
- The TOE will be provided to the evaluators. (ATE_IND.2)

Misuse Analysis for Cisco IOS/Firewall (MSU)

- Describes vulnerability analysis undertaken. (AVA_MSU.2)

Vulnerability Analysis/Strength of Function Analysis for Cisco IOS/Firewall (VLA-SOF)

- Strength of TOE security function evaluation. (AVA_SOF.1)
- Demonstrates that a systematic search for vulnerabilities has been conducted and provides an analysis showing that these vulnerabilities are not exploitable in the environment defined by this ST. (AVA_VLA.2)

Representational Correspondence Demonstration for Cisco IOS/Firewall (RCR)

- Demonstrates correspondence between ST, HLD, LLD and TOE Source Code. (ADV_RCR.1)

7. PP Claims

This Security Target does not make any claim of PP compliance. The Security Functional Requirements, TOE Security Environment and Objectives are based upon the U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, version 1.4, May 1, 2000 but do not claim compliance with it.

8. Rationale

8.1 Rationale for IT Security Objectives

O.IDAUTH

This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.

O.SINUSE

This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.

O.MEDIAT

This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

O.SECSTA

This security objective ensures that no information is compromised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

O.ENCRYP

This security objective is necessary to counter the threats and policy: T.NOAUTH, T.PROCOM and P.CRYPTO by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely.

O.SELPRO

This security objective is necessary to counter the threats: T.SELPRO, T.NOAUTH, and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC

This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

O.ACCOUN

This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

O.SECFUN

This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

O.LIMEXT This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.

O.EAL This security objective is necessary to counter the threat: T.MODEXP because it requires that the TOE is resistant to penetration attacks performed by an attacker possessing moderate attack potential.

Table 16 Summary of Mappings Between Threats, Policies, and IT Security Objectives

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T. MODEXPO	P. CRYPTO
O.IDAUTH	X											
O.SINUSE		X	X									
O.MEDIAT				X	X	X						
O.SECSTA	X								X			
O.ENCRYP	X						X					X
O.SELPRO	X								X	X		
O.AUDREC								X				
O.ACCOUN								X				
O.SECFUN	X		X							X		
O.LIMEXT	X											
O.EAL											X	

O.PHYSEC The TOE is physically secure and the network interface of the PFSS is only accessible by the TSF.

O.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

O.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

O.PUBLIC The TOE does not host public data.

O.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

O.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

O.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (for example, a console port) if the connection is part of the TOE

O.NOREMO

Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks

O.REMACC

Authorized administrators may access the TOE remotely from the internal and external networks.

O.GUIDAN

This non-IT security objective is necessary to counter the threat: T.TUSAGE and T.AUDACC because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

O.ADMTRA

This non-IT security objective is necessary to counter the threat: T.TUSAGE and T.AUDACC because it ensures that authorized administrators receive the proper training.

O.IDAUTH(env)

The environmental objective O.IDAUTH(env) has been specified in addition to the objectives specified for the TOE. The rational for this objective is that O.IDAUTH(env) is necessary to counter the threat T.NOAUTH as it requires that users be uniquely identified before accessing the TOE. This objective allows for the use of external authentication services provided by the TOE environment.

	T.TUSAGE	T.AUDACC	T.NOAUTH	A.PROTECTIF
O.GUIDAN	X	X		
O.ADMTRA	X	X		
O.IDAUTH(env)			X	
O.PHYSEC				X

Since the rest of the security objectives for the environment are, in part, a restatement of the security assumptions, those security objectives trace to all aspects of the assumptions.

8.2 Security Requirements Rationale

The functional and assurance requirements presented in this Security Target are mutually supportive and their combination meets the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria. This section illustrates the mapping between the security requirements and the security objectives. Section 8.1 demonstrates the relationship between the threats, policies and IT security objectives. Together these tables demonstrate the completeness and sufficiency of the requirements.

The rationale for the SOF is based on the moderate attack potential identified in this Security Target. The security objectives imply the need for probable or permutational security mechanisms. The metrics defined in this Security Target are acceptable (such as passwords) metrics to protect information in DoD Mission-Critical Categories.

FMT_SMR.1 Security roles

Each of the CC class FMT components in this Protection Profile depend on this component. It requires the PP/ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA_ATD.1 User attribute definition

This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of a user, the users identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_AFL.1 Authentication failure handling

This component ensures that human users who are not authorized administrators can not endlessly attempt to authenticate. After some number of failures that the authorized administrator decides, that must not be zero, the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.

FIA_UAU.5 Multiple authentication mechanisms

This component was chosen to ensure that multiple authentication mechanism are used appropriately in all attempts to authenticate at the TOE from an internal or external network. An additional SOF metric for this requirement is defined in section 5.1.1 to ensure that the mechanism is of adequate cryptologic strength. This component traces back to and aids in meeting the following objective: O.SINUSE and O.IDAUTH.

FDP_IFC.1 Subset information flow control

This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (for example, users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes

This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FMT_MSA.1 Management of security attributes (1)

This component ensures the TSF enforces from TOE start-up the UNAUTHENTICATED_SFP to restrict the ability to add, delete and modify specified security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (2)

This component ensures the TSF enforces from TOE start-up the UNAUTHENTICATED_SFP to restrict the ability to create or delete specified security attributes that are listed in information flow rules in FDP_IFF.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.3 Static attribute initialization

This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MTD.1 Management of TSF data (1)

This component ensures that the TSF restrict abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.1 Management of TSF data (2)

This component ensures that the TSF restrict abilities to set the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.2 Management of limits on TSF data

This component ensures that the TSF restrict the specification of limits of the number of unauthenticated failures to the authorized administrator and specifies the action be taken if limits on the TSF data are reached or exceeded. This component traces back to and aids in meeting the following objective: O.SECFUN.

FDP_RIP.1 Subset residual information protection

This component ensures that neither information that had flown through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FCS_COP.1 Cryptographic operation

This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that DES is used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP.

FPT_RVM.1 Non-bypassability of the TSP

This component ensures that the TSF are always invoked from initial start-up. This component traces back to and aids in meeting the following objective: O.SELPRO and O.SECSTA.

FPT_SEP.1 TSF domain separation

This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_GEN.1 Audit data generation

This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review

This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

This component is chosen to ensure that the audit trail is always (for example, from initial start-up) protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SELPRO. and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full and resources will not be compromised upon recovery. This component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SELPRO andO.SECFUN.

FMT_MOF.1 Management of security functions behavior (1)

This component was to ensure the TSF restricts the ability of the TOE start up and shut down operation and single-use authentication function (described in FIA_UAU.5) to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN and O.LIMEXT.

FMT_MOF.1 Management of security functions behavior (2)

This component was to ensure the TSF restricts the ability to modify the behavior of functions such as audit trail management, back and restore for TSF data, and communication of authorized external IT entities with the TOE to an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN and O.LIMEXT.

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FMT_SMR.1									X	
FIA_ATD.1	X	X								
FIA_UID.2	X							X		
FIA_AFL.1						X				
FIA_UAU.5	X	X								
FDP_IFC.1			X							
FDP_IFF.1			X							
FMT_MSA.1 (1)			X	X					X	

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FMT_MSA.1 (2)			X	X					X	
FMT_MSA.3			X	X					X	
FMT_MTD.1 (1)									X	
FMT_MTD.1 (2)									X	
FMT_MTD.2									X	
FDP_RIP.1			X							
FCS_COP.1					X					
FPT_RVM.1				X		X				
FPT_SEP.1					X					
FPT_STM.1							X			
FAU_GEN.1							X	X		
FAU_SAR.1							X			
FAU_SAR.3							X			
FAU_STG.1				X		X			X	
FAU_STG.4				X		X			X	
FMT_MOF.1 (1)				X					X	X
FMT_MOF.1 (2)				X					X	X

The environmental SFRs FIA_UAU.5(2), and FIA_UID.2(2) were chosen to ensure that multiple authentication mechanism are used appropriately in all attempts to authenticate at the TOE from an internal or external network. These requirements trace back to and aid in meeting the objective O.IDAUTH(env).

FMT_SMF.1 Specification of Management Functions requires that a defined set of security management functions are made available so that an administrator can manage the security configuration of the TOE. This security functional requirement directly provides support for the security objective O.SECFUN.

The requirement FMT_SMF.1 was included in this ST in addition to the SFRs to satisfy a dependency of FMT_MOF.1. This dependency was introduced in International Interpretation RI#65 which has since been incorporated into version 2.2 of part 2 of the Common Criteria.

To allow for authentication services to be provided by the TOE environment by the use of the RADIUS and TACACS+ protocols, the SFRs iterations FIA_UAU.5(2), and FIA_UID.2(2) have been included as environmental SFRs. And the original SFRs have been renamed as iterations FIA_UAU.5(1), and FIA_UID.2(1).

8.2.1 Suitability of TOE Security Functions to Meet Security Requirements

Table 17 maps each SFR to the TSF that implements the requirement in the TOE. The table shows the completeness of the TOE, since all SFRs are met by TSFs.

Table 17 SFR to TSF Cross Reference

TSF SFR	REMOTE.1	PACKET FILTER.1	CONFIG.1	CONFIG.2	AUDIT.1	AUDIT.2	RESOURCE.1	PROTECT.1
FCS_COP.1	X							
FIA_UAU.5 (1)			X					
FDP_IFF.1		X						
FDP_IFC.1		X						
FPT_RVM.1		X						
FAU_GEN.1					X			
FAU_STG.4					X	X		
FAU_SAR.1						X		
FAU_SAR.3						X		
FIA_UID.2 (1)			X					
FIA_AFL.1			X					
FMT.MTD.2			X					
FMT_SMR.1			X					
FMT_MOF.1(1)			X					
FMT_MOF.1(2)			X					
FMT_MSA.1 (1)			X					
FMT_MSA.1 (2)			X					
FMT_MSA.3			X					
FIA_ATD.1			X					
FMT_MTD.1 (1)			X					
FMT_MTD.1 (2)			X	X				
FMT_SMF.1			X					
FAU_STG.1						X		
FPT_STM.1				X				
FDP_RIP.1							X	
FPT_SEP.1								X

FCS_COP.1

The TSF REMOTE.1 satisfies this requirement by providing192bit 3DES and 128 bit AES encryption, as specified in FIPS PUB 46-3, for SSH based remote administrative functions.

FIA_UAU.5(1)

The TSF CONFIG.1 satisfies this requirement by requiring a username and password for user authentication, and an “enable” password for privileged administrator authentication.

FIA_UAU.5(2)

The TSFs REMOTE.1 and CONFIG.1 satisfy this requirement as they both require a username and password for user authentication when remote authentication services are used. The use of remote authentication services over RADIUS or TACACS+ protocols for Secure Shell (SSH) remote management sessions, satisfies the requirement for one time authentication.

FDP_IFF.1

The TSF PACKETFILTER.1 satisfies this requirement by permitting or denying a packet flow based on its presumed source/destination IP address, protocol, interface and source/destination UDP/TCP port number. The packet filter function is applied to TOE interfaces to implement the UNAUTHENTICATED SPF which defines the rules for packet filtering.

FDP_IFC.1

The TSF PACKETFILTER.1 satisfies this requirement by examining the attributes of each packet flow and applying the information flow control policy UNAUTHENTICATED SPF to it. See section 6.1.1 Packet Filtering for a full list of packet flow attributes.

FPT_RVM.1

The TSFs PACKETFILTER.1 and CONFIG.1 ensures that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The TSP cannot be bypassed provided the TOE is correctly configured. Packets are unable to pass through the TOE until the information flow control policy has been configured.

FAU_GEN.1

The TSF AUDIT.1 satisfies this requirement by generating audit logs in accordance with the requirement.

FAU_STG.4

The TSFs AUDIT.1 and AUDIT.2 satisfy this requirement by limiting the potential for the loss of audit data through reliable transfer to an external source and by limiting the functions of the TOE should the local audit logs reach their maximum capacity.

FAU_SAR.1

The TSF AUDIT.2 satisfies this requirement by enabling the ability for authorized users to review the audit logs.

FAU_SAR.3

The TSF AUDIT.2 satisfies this requirement by providing the means to select, search and sort audit data on the PIX Firewall Syslog Server.

FIA_UID.2(1)

The TSF CONFIG.1 satisfies this requirement by requiring users to undergo identification before access to its management interfaces is granted.

FIA_UID.2(2)

The TSFs REMOTE.1 and CONFIG.1 satisfy this requirement by requiring users to undergo identification before access to its management interfaces is granted when using either local or remote authentication services.

FIA_AFL.1

The TSF CONFIG.1 satisfies this requirement by detecting unsuccessful authentication attempts, and locking a user from authenticated access to the TOE when the number of consecutive unsuccessful authentication attempts reaches a limit set by an authorized administrator. The account then requires unlocking by an authorized administrator before the user can be authenticated.

FMT_MTD.2

The TSF CONFIG.1 satisfies this requirement by allowing an authorized administrator to set the threshold of unsuccessful authentication attempts required before a user account is locked. The TSF then enforces the requirements of FIA_AFL.1 should this occur.

FMT_SMR.1

The TSF CONFIG.1 satisfies this requirement by maintaining the role of authorized administrator. The TSF is able to associate users with this role.

FMT_MOF.1(1)

The TSF CONFIG.1 satisfies this requirement by allowing only the authorized administrators the right to manage the operation and single use authentication functions of the TOE.

FMT_MOF.1(2)

The TSF CONFIG.1 satisfies this requirement by allowing only the authorized administrators the right to manage the configuration of the TOE security functions including those that implement the UNAUTHENTICATED_SFP.

FMT_MSA.1(1)

The TSF CONFIG.1 satisfies this requirement by allowing only the authorized administrators the right to manage the configuration that enforces the UNAUTHENTICATED_SFP.

FMT_MSA.1(2)

The TSF CONFIG.1 satisfies this requirement by allowing only the authorized administrators the right to manage the configuration that enforces the UNAUTHENTICATED_SFP.

FMT_MSA.3

The TSF CONFIG.1 satisfies this requirement by ensuring that restrictive default values are allocated to security attributes for the UNAUTHENTICATED_SFP, and allowing the authorized administrator to alter the values from the default.

FIA_ATD.1

The TSF CONFIG.1 satisfies this requirement by maintaining all required security attributes belonging to individual users.

FMT_MTD.1(1)

The TSF CONFIG.1 satisfies this requirement by only allowing the authorized administrator to alter the TSF configuration.

FMT_MTD.1(2)

The TSFs CONFIG.1 and CONFIG.2 satisfy this requirement by only allowing the authorized administrator to alter the system time.

FMT_SMF.1

The TSF CONFIG.1 satisfies this requirement by implementing the functionality to work as follows:

- Create, delete, modify, and view information flows rules
- Enable or disable the operation of the router
- Configure SSH for remote management
- Configure audit trail management
- Allow for the backup and restoration of TSF data, information flow rules, and audit trail data; and
- Enable or disable communication of authorized external IT entities with the TOE by applying information flow rules.

FAU_STG.1

The TSF AUDIT.2 satisfies this requirement by protecting the stored audit records from unauthorized deletion and disallowing all modification whilst stored on the PFSS.

FPT_STM.1

The TSF CONFIG.2 satisfies this requirement by maintaining the system time and using the timestamp in audit records.

FDP_RIP.1

The TSF RESOURCE.1 satisfies this requirement by ensuring that all network interfaces used by the router use zeroised data for the purposes of padding transmissions.

FPT_SEP.1

The TSF PROTECT.1 satisfies this requirement because Cisco IOS runs on its own specific hardware and is not a general purpose OS. Additionally, Cisco IOS management functions are isolated by authentication, no programming interface is provided and only Cisco IOS functions are carried out on a Cisco IOS router.

8.2.2. SFR Dependency Rationale

With the exception of the functional component FCS_COP.1, all dependencies are contained in this Security Target. Functional component FCS_COP.1 depends on the following functional components: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction and FMT_MSA.2 Secure Security Attributes. Cryptographic modules must be FIPS PUB 140-1 compliant. If the cryptographic module is indeed compliant with this FIPS PUB, then the dependencies of key generation, key destruction and secure key values will have been satisfied in becoming FIPS PUB 140-1 compliant.

This Security Target includes the additional SFR FMT_SMF.1 with has been included to satisfy the dependency of the FMT_MOF.1 SFR. The inclusion of this SFR does not introduce any additional unsupported dependencies.

The SFRs FIA_UAU.5(1) and FIA_UAU.5(2) has been included to ensure that multiple authentication mechanisms used by the TOE are used appropriately. Both iterations of the SFR FIA_UAU.5 have been included in the ST in place of FIA_UAU.1 and are considered sufficient to satisfy the dependency of FIA_AFL.1.

8.2.3. Assurance Security Requirements Rationale

EAL4 Augmented was chosen to ensure a moderate level of security for protecting information in DoD Mission-Critical Categories. Mission-Critical Categories of information is assumed, by nature, to have a greater threat for disclosure and/or corruption by unauthorized parties by the assumption A.MODEXP.

As an indirect dependency of vulnerability analysis, tools and techniques used to develop, analyze and implement the TOE must be identified and documented. This is supported by the requirement ALC_TAT.1. Since the threat to Mission-Critical Categories of information is greater, more detailed product information is required as indicated by requirements ADV_HLD.2, ADV_IMP.1, and ADV_LLD.1 in this Protection Profile. The chosen assurance level as supported by O.EAL is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone vulnerability analysis by the developer and independent penetration testing by the evaluator.

8.2.4. Mutually Supportive Security Requirements

The mutually supportive security requirements rationale is presented in section 8.2 Security Requirements Rationale.

The additional security functional requirement FMT_SMF.1 directly supports FMT_MOF.1(1) and FMT_MOF.1(2) by providing a specific set of management functions with which to manage the security configuration of the TOE.

8.2.5. Strength of Function Claims

The TOE cryptographic components of the TOE are FIPS PUB 140-1 compliant, and therefore do not require a claim of strength for cryptographic algorithms to be made.

Cisco Systems has completed FIPS PUB 140-2 validations for the 8xx family (Certificate #707), 18xx fixed card family (Certificate #702), 1841/2801 (Certificate #620), 2800 family (Certificates #617,#619), 3800 family (Certificate #618), 7204VXR and 7301 (Certificate #673). The FIPS validated versions of software do not match exactly with this evaluation. Cisco Systems asserts that the versions of software included in this evaluation meet the requirements of FIPS PUB 140-2.

The SFR FIA_UAU.5(1) is implemented by the TSF CONFIG.1 which utilizes probabilistic mechanisms in order to accurately authenticate users via a username and password (CONFIG.1).

For the SFR FIA_UAU.5(1) the strength of function claim is SOF-medium. A strength of function claim of SOF-medium is also made for IT Security Function CONFIG.1. A SOF claim is not required for REMOTE.1 as it uses the TOE’s cryptographic algorithms.

Identification and Authentication functions performed by the Windows 2000 platform also have a strength of function claim of SOF-medium as specified in the section 8.2.6 of the Windows 2000 Security Target, Version 2.0, 18 October 2002. The Windows 2000 platform Identification and Authentication functionality is in direct support of the SFR FAU_STG.1 and the TSF AUDIT.2 which protect the audit data stored on the PFSS.

The TOE claims a minimum strength of function of SOF-medium for the TOE security functional requirements and the TOE as a whole.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.