Cisco Systems Routers EAL3 Security Target

Release Date: February 29, 2008
Version: 1.8 Final

Table of Contents

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

List of Figures

List of Tables

Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

Identification

TOE Identification: Cisco Systems Routers (800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200, 7300, and 7400) running Cisco IOS Release 12.4(11)T2; 7600 running Cisco IOS Release 12.2(18)SXF8; 10000 and 12000 running 12.0(32)S7 and Cisco Secure ACS version 4.1.2.12

- ST Identification: Cisco Systems Routers EAL3 Security Target
- ST Version: 1.8 Final
- ST Publish Date: February 29, 2008
- ST Authors: Cisco Systems, Inc.

Overview

The TOE is Cisco Systems Routers (800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200, 7300, and 7400) running Cisco IOS Release 12.4(11)T2; 7600 running Cisco IOS Release 12.2(18)SXF8; 10000 and 12000 running 12.0(32)S7 running Cisco IOS and a Cisco Secure Access Control Server version 4.1.2.12 (hereafter referred to as 4.1). The versions of Cisco IOS under evaluation differ by router and are fully described in the “TOE Description” section on page 8. Routers are hardware devices used to construct IP networks by interconnecting multiple smaller networks or network segments. Cisco routers are highly scalable and flexible.

Cisco Secure Access Control Server provides a comprehensive identity-based access control solution for Cisco intelligent information networks. It is the integration and control layer for managing enterprise network users, administrators, and the resources of the network infrastructure.

Cisco IOS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing. Although Cisco IOS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself:

- Audit (Accounting)
- Identification & Authentication (Authentication)
- Access Control (Authorization)
- Traffic Filtering and Routing

- Security Management/ Access Control (Authorization)
- Protection of the TSF

The TOE does not address encryption (IPSec), VPNs, or Quality of Service (QoS).

CC Conformance Claim

The TOE is Common Criteria Version 2.2 (ISO/IEC 15408:2004) Part 2 and Part 3 conformant at EAL3. The TOE is also compliant with all International interpretations with effective dates on or before Feb 25, 2004.

The TOE does not conform to any Protection Profiles.

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.

Document Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations:

Assignment:	**indicated with bold text**
Selection:	indicated with underlined text
Refinement:	***indicated with bold text and italics***
Iteration:	indicated with typical CC requirement naming followed by a number in parentheses for each iteration (e.g., FMT_MSA.1(1))

Document Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. A subset of those definitions is included in the list below with supplemental definitions that are exclusive to Cisco products. They are listed here to aid the reader of the Security Target.

Acronym	Expansion or Definition
AAA	Authentication, Authorization, and Accounting. The framework which provides services a router needs for authenticating users, authorizing actions, and accounting.
ACS	The Cisco Secure Access Control Server (ACS) is a highly scalable, high-performance centralized user access control server controlling the AAA for all users in the TOE.
Assignment	The specification of an identified parameter in a component.
Assurance	Grounds for confidence that an entity meets its security objectives.
Attack Potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Acronym	Expansion or Definition
Audit Trail	In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
Authentication	To establish the validity of a claimed user or object.
Authorized Administrator	Generic term used for Network Administrators and Users that manage a TOE component; A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE. See FMT_SMR.1 and its footnote for applicability to the TOE.
Availability	Assuring information and communications services will be ready for use when expected.
BGP	Border Gateway Protocol. An exterior gateway protocol. It performs routing between multiple autonomous systems and exchanges routing and reachability information with other BGP systems.
Dependency	A relationship between requirements such that the requirements that is dependent upon must normally be satisfied for the other requirements to be able to meet their objectives.
EEPROM	Electrically erasable programmable read-only memory, specifically the memory in the router where the Cisco IOS is stored.
Guidance Documentation	Guidance documentation describes the delivery, installation, configuration, operation, management and use of the TOE as these activities apply to the users, administrators, and integrators of the TOE. The requirements on the scope and contents of guidance documents are defined in a PP or ST.
Identity	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
Interface Configuration	A command mode in Cisco IOS where a privileged administrator configures a hardware or virtual interface on the router. In order to access this mode a semi-privileged administrator must first access privileged EXEC mode.
IOS	Internetwork Operating System, the proprietary operating system developed by Cisco Systems.
NVRAM	Non-volatile random access memory, specifically the memory in the router where the configuration parameters are stored.
Network Administrator	The authorized user with access to the privileged exec mode (and other command modes) of the Cisco IOS router responsible for senior level administration of the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE

Acronym	Expansion or Definition
OSPF	Open Shortest Path First. An interior gateway protocol (routes within a single autonomous system). A link-state routing protocol which calculates the shortest path to each node.
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Privileged EXEC	A command mode in Cisco IOS that allows access to most management and troubleshooting functions, and from which the interface configuration mode is reached. Interfaces and sub-interfaces cannot be configured from this mode.
Refinement	The addition of details to a component.
RIP	Routing Information Protocol. An interior gateway protocol (routes within a single autonomous system). A distance-vector protocol that uses hop count as its metric.
ROM Monitor	A command mode in Cisco IOS that runs when the router is powered up or reset and helps to initialize the processor hardware and boot the operating system software. Privileged administrators can perform certain configuration tasks, such as recovering a lost password or downloading software over the console port, by using ROM monitor.
Secret	Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.
Security Attribute	Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.
Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy (SFP)	The security policy enforced by an SF.
Security Objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Strength of Function (SOF)	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.
SOF-Basic	A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.
Subinterface Configuration	A command mode in Cisco IOS where a privileged administrator configures a hardware or virtual sub-interface. In order to access this mode a privileged administrator must first access Interface Configuration mode.
TACACS+	Terminal Access Controller Access Control System. Part of AAA. Provides centralized user password authentication. Whenever a user requests some action, the router sends the user name and password to a central server. The server consults its access control database and either permits or denies the requested action.

Acronym	Expansion or Definition
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Functions Interface (TSFI)	A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
TSF Data	Data created by and for the TOE, which might affect the operation of the TOE.
User	The authorized user with access to the user command mode (and no other) of the Cisco IOS router responsible for first-level administration of the security parameters of the TOE. Such users are not subject to any access control requirements in user command mode once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE
User EXEC	A command mode in Cisco IOS which provides a semi-privileged administrator basic troubleshooting and management commands. It is the default operating mode.
Vulnerability	Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

TOE Description

The TOE is Cisco Systems Routers (800, 1700, 1800, 2600XM, 2800, 3700, 3800, 7200, 7300, 7400, 7600, 10000, 12000) running Cisco IOS and a Cisco Secure Access Control Server (ACS). A router is a device that determines the next network point to which a packet should be forwarded toward its destination. It is located at any gateway (where one network meets another). A router may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Routing protocols include BGP, RIP, and OSPF. IP packets are forwarded to the router over one or more of its 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.

Routers that support the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the routers (such as throughput and amount of storage) and therefore support security equivalency of the routers in terms of hardware:

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operations
- Flash memory (EEPROM), used to store the Cisco IOS image (binary program)
- USB slot, used to connect USB devices to the TOE (not relevant as none of the USB devices are included in the TOE)

- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs.
- Non-volatile random-access memory (NVRAM) is used to store router configuration parameters used to initialize the system at startup.
- Physical network interfaces (minimally two). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces.

Users of the TOE are router and ACS administrators, which will hereafter be referred to generically as authorized administrators or by the roles of privileged administrator (router), semi-privileged administrator (router), and authentication administrator (ACS). Privileged administrators configure the Cisco routers using the Global configuration commands to apply the features that affect the system as a whole. To initiate global configuration mode the privileged administrator enters the configure command at the privileged EXEC mode prompt. The user interface is run from either the console port on the router or by connecting to the router using secure shell. The user interface is a Command Line Interface (CLI) running the Command Interpreter (EXEC).

The Cisco Systems TOE hardware models are:

Table 1 TOE Router Hardware Models

Router Series	Router Model	Cisco IOS Version	Router Type
800 Series	831, 836, 837, 851, 857, 871, 876, 877, 878	12.4(11)T2	Ethernet, ADSL, SHDSL, and ISDN routers
1700 Series	1701, 1711, 1712, 1721, 1751, 1751-V, 1760	12.4(11)T2	Flexible, modular access routers
1800 Series	1801, 1802, 1803, 1811, 1812, 1841	12.4(11)T2	ADSL, SHDSL, ISDN, and Integrated Services routers
2600XM Series	2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, 2691	12.4(11)T2	Modular multiservice router and dial access server
2800 Series	2801, 2811, 2821, 2851	12.4(11)T2	Integrated Services router
3700 Series	3725, 3745	12.4(11)T2	Multiservice access routers
3800 Series	3825, 3845	12.4(11)T2	Integrated Services router
7200 Series	7204VXR, 7206VXR	12.4(11)T2	WAN-edge router for intelligent services, modularity, high performance, and scalability
7300 Series	7301	12.4(11)T2	WAN-edge router
7400 Series	7401	12.4(11)T2	Compact routers for application specific deployments
7600 Series	7603, 7606, 7609, 7613, Supervisor Engines: 7600-SUP2/MSFC2, 7600-SUP32/MSFC2A, 7600-SUP720/MSFC3	12.2(18)SXF8	High-end Services-enabled core and WAN aggregation router for voice, video, and data in enterprise and service provider applications
7600 Series	7600-CMM, 7600-MWAM	12.4(11)T2	High-end Services-enabled core and WAN aggregation router for voice, video, and data in enterprise and service provider applications

Table 1 TOE Router Hardware Models (continued)

Router Series	Router Model	Cisco IOS Version	Router Type
10000 Series	10700	12.0(32)S7	Edge-router for carriers deploying Broadband services
12000 Series	12006, 12008, 12010, 12012, 12016, 12404, 12406, 12410, 12416, 12810, 12816, Route Processor: PRP-1, PRP-2	12.0(32)S7	Gigabit Switch Routers (GSRs)

The TOE also includes ACS, which provides authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients, including routers.

Architecture Description

The TOE is the Cisco Routers running Cisco IOS. The network on which they reside, is part of the environment.

The following table lists the software, hardware and router operating system from Figure 1, below, and declares whether or not each is part of the TOE.

Table 2 TOE Boundary Description

Hardware	TOE?
Router	Yes
ACS Server hardware	No
OS	
Windows 2000 Server (ACS Server OS)	No
Software	
Cisco ACS Version 4.1.2.12	Yes
TACACS+ or RADIUS[1]	Yes
Cisco IOS (version listed in Table 1)	Yes

[1] Software installed with ACS: Includes TACACS+ protocol as defined by Cisco Systems in draft 1.78 and RADIUS as specified in RFC 2865. The versions of TACACS+ and RADIUS are dependent upon ACS, so they are the same for all of the Cisco IOS versions included in the TOE.

Physical Boundaries

The TOE consists of one or more physical devices: router(s) with Cisco IOS and ACS software. ACS software runs on a Windows 2000 Server. It should be noted that the Windows PC is not considered part of the TOE, only the ACS software operating on it. The Windows PC includes a firewall to protect the OS and the ACS. 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 are passed through the internetworking device and forwarded to their configured destination. Routing protocols used are RIP, OSPF, and BGP.

The ACS will be connected to the router either via a internal network (Figure 1) or via a crossover cable. The area inside the square on the figure below is the TOE Boundary which includes the router hardware, the Cisco IOS, and the ACS server software, but not the operating system of the server platform the ACS utilizes.

The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the Cisco IOS Router or ACS Server are to be remotely administered, then the management station must be connected to a internal network, SSH must be used to connect to the router, and SSL must be used to connect to the ACS. The ACS, remote management, and NTP boxes (if used) must all be attached to the internal (trusted) network.

Figure 1 TOE Boundary

Hardware/OS Components

Routers have two or more network interfaces. Routers are connected to at least one internal and one external network. The Cisco IOS configuration determines how packets are handled to and from the router's network interfaces.

Logical Boundaries

The TOE addresses the following features which are relevant to the secure configuration and operation of the router.

ACS provides the architectural framework for configuring a set of three independent security functions in a consistent manner. ACS provides a modular way of performing Authentication, Authorization and Accounting.

- Audit (Accounting)

  The router generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the router records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Audited events include; Modifications to the group of users that are part of the authorized administrator roles, all use of the user identification mechanism, any use of the authentication mechanism, any change in the configuration of the router or any failure of a packet to match an ACL rule allowing traversal of the router.

- Identification & Authentication (Authentication)

  The router performs authentication, using Cisco IOS platform authentication mechanisms, to authenticate access to user exec and privileged exec command modes.

Identification and Authentication provides the method of identifying and authenticating users, including login and password dialog, challenge and response, and messaging support. Encryption of the packet body is provided through the use of TACACS+ or RADIUS (note RADIUS only encrypts the password within the packet body).

Terminal Access Controller Access Control System (TACACS+) is part of AAA. TACACS+ provides ACS centralized user password authentication for all routers that the ACS manages and is an option that can be installed with ACS. Whenever a user requests some action, the router sends the user name and password to a central server located on the same server as the ACS. The server consults its access control database and either permits or denies the requested action.

- Traffic Filtering and Routing

  Restricts remote terminal connectivity, using the router's access-control list functionality, to specific interfaces of the TOE so that sessions will only be accepted from the management station(s) identified in the management session TOE security policy.

  Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. The router examines each packet to determine whether to forward or drop the packet, on the basis of the criteria you specified within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

  The router examines each packet to determine whether to forward or drop the packet, on the basis of the information contained within the routing tables.

  Routing algorithms fill routing tables with a variety of information. Destination/next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the next hop on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.

- Security Management / Access Control (Authorization)

  The ACS and Router allows authorized administrators to add new administrators, start-up and shutdown the device, create, modify, or delete configuration items, modify and set the time and date, and create, delete, empty, and review the audit trail. The ACS when using TACACS+ allows authentication administrators to modify and set the threshold for the number of permitted consecutive authentication attempt failures, restore authentication capabilities for users that have met or exceeded the threshold for permitted consecutive authentication attempt failures.

  The TOE router platform maintains privileged and semi-privileged administrator roles. The router performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged modes.

- Protection of the TSF

  The router protects against interference and tampering by untrusted subjects by implementing identification, authentication and access controls to limit configuration to privileged administrators. Additionally Cisco IOS is not a general purpose operating system and access to Cisco IOS memory space is restricted to only Cisco IOS functions.

  The ACS component protects against interference and tampering by untrusted subjects through its own interfaces by implementing identification, authentication, and roles.

  Both the router and ACS component ensure that when data is transmitted between them that security functions to protect the data from packet sniffing are invoked successfully before that data is transmitted.

The Cisco IOS contains a collection of features that build on the core components of the system. Those features that are not to be used on the TOE include the HTTP Server, the IEEE 802.11 Wireless Standards, MAC address filtering, SNMP, Telnet, and VPN.

Apart from these exceptions all types of network traffic through and to the TOE are within the scope of the evaluation.

Evaluated Cisco IOS Features

Table 3 lists the Cisco IOS features that are included or excluded in the TOE.

Table 3 Evaluated Cisco IOS Features

Feature	Description	Evaluated	Not Permitted	Not Evaluated
AAA	TACACS+ RADIUS (Remote Access Dial-In User Service)	X		
ACL	Access control lists.	X		
AES	Advanced Encryption Standard	X		
CEF	Cisco Express Forwarding	X		
Certificates and Certificate Server	Not permitted in the evaluated configuration.		X	X
DHCP	Dynamic Host Control Protocol (DHCP) enables you to automatically assign reusable IP addresses to DHCP clients.			X
Firewall	Firewall feature set: Not permitted in the evaluated configuration.		X	X
HSRP	Hot Standby Router Protocol (HSRP): Not permitted in the evaluated configuration.		X	X
HTTP Server	Not permitted in the evaluated configuration.		X	X
IEEE 802.11 Wireless Standards	Not permitted in the evaluated configuration.		X	X
IGMP	Not permitted in the evaluated configuration.		X	X
IPv6	Not permitted in the evaluated configuration.		X	X
MAC address filtering	Not permitted in the evaluated configuration.		X	X
Media Types (non-Ethernet)	Not evaluated: ADSL, ATM, Frame Relay, ISDN, MPLS, PPP, and PPPoE.			X
Mobile IP	Not permitted in the evaluated configuration.		X	X
NAC	Not permitted in the evaluated configuration.		X	X
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	Not evaluated.			X
QoS	Quality of Service features: Not evaluated.			X

Table 3 Evaluated Cisco IOS Features (continued)

Feature	Description	Evaluated	Not Permitted	Not Evaluated
Routing and Switching Protocols Disabled	Not permitted in the evaluated configuration: RIP version 1, EIGRP, and STP (Spanning tree protocol).		X	X
Routing Protocols Permitted	RIPv2: Routing Information Protocol (RIP) version 2 OSPF: Open Shortest Path First (OSPF) BGP: Border Gateway Protocol	X		
SSHv1	Not permitted in the evaluated configuration.		X	X
SSHv2	SSH version 2 client and server support.	X		
SLB	Server load balancing: Not evaluated.			X
SNMP	Simple Network Management Protocol (SNMP): Not permitted in the evaluated configuration.		X	X
SPAN	Switched Port Analyzer: Not evaluated.			X
Syslog	Configuration and delivery of SYSLOG messages.	X		
Telnet	Legacy unencrypted protocol for remote administration. Not permitted in the evaluated configuration.		X	X
VLAN	Not permitted in the evaluated configuration.		X	X
VoIP	Not permitted in the evaluated configuration: Voice over IP (VoIP), SIP (Session Initiation Protocol), and H.323.		X	X
VPN	Not permitted in the evaluated configuration: WebVPN, IPSec, IKE, EasyVPN, L2TP(Layer 2 Tunneling Protocol).		X	X

TOE Security Environment

This section describes the security environment in which the TOE is intended to be used.

Assumptions

The assumptions are ordered into three groups: Personnel Assumptions, Physical Environment Assumptions, and Operational Assumptions.

Personnel Assumptions

A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error.
A.TRAIN_AUDIT	Administrators will be trained to periodically review audit logs to identify sources of concern
A.TRAIN_GUIDAN	Personnel will be trained in the appropriate use of the TOE to ensure security.

Physical Environment Assumptions

A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

Operational Assumptions

A.CONFIDENTIALITY	The hard copy documents that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to Authorized administrators.
A.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.
A.INTEROPERABILITY	The TOE will be able to function with the software and hardware of other router vendors on the network.
A.LOWEXP	The threat of malicious attacks aimed at exploiting the TOE is considered low.

Threats

The TOE or IT environment addresses the threats identified in the following sections. The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

T.AUDIT_REVIEW	Actions performed by users may not be known to the administrators due to actions not being recorded or the audit records not being reviewed prior to the machine shutting down.
T.MEDIATE	An unauthorized entity may send impermissible information through the TOE which results in the exploitation of resources on the network.
T.NOAUDIT	An unauthorized user modifies or destroys audit data.
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 to disrupt operations of the TOE.
T.NOMGT	The administrator is not able to easily manage the security functions of the TOE, resulting in the potential for the TOE configuration to compromise security objectives and policies.
T.UNAUTH_MGT_ACCESS	An unauthorized user gains management access to the TOE and views or changes the TOE security configuration.
T.TIME	An authorized administrator will not be able to determine the sequence of events in the audit trail because the audit records are not correctly time-stamped.

Security Objectives

This chapter describes the security objectives for the TOE and the TOE’s operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

O.ACCESS_CONTROL	The TOE will restrict access to the TOE Management functions to the privileged administrators and authentication administrators.
O.AUDIT_GEN	The TOE will generate audit records which will include the time that the event occurred and if applicable, the identity of the user performing the event.
O.AUDIT_VIEW	The TOE will provide the privileged administrators and authentication administrators the capability to review Audit data.
O.CFG_MANAGE	The TOE will provide management tools/applications to allow privileged administrators and authentication administrators to manage its security functions.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access.
O.MEDIATE	The TOE must mediate the flow of all information between hosts located on disparate internal and external networks governed by the TOE.
O.SELFPRO	The TOE (both router and ACS) must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.STARTUP_TEST	The router will perform initial startup tests upon bootup of the system.
O.TIME	The router will provide a reliable time stamp for its own use.

Security Objectives For The Environment

The following IT security objectives for the environment are to be addressed by the IT environment via technical means.

OE.ACS_PROTECT	The ACS software and related files will be partially protected by the host operating system on a properly secured and configured Windows Server host.
OE.ACS_TIME	The ACS will have access to a reliable time stamp from the environment.

The non-IT security objectives listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures:

OE.AUDIT_REVIEW Administrators will be trained to periodically review the audit logs to identify sources of concern.

OE.CONFIDENTIALITY The hard copy documents that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to Authorized administrators.

OE.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.

OE.INTEROPERABILITY The TOE will be able to function with the software and hardware of other vendors on the network.

OE.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

OE.LOWEXP The threat of malicious attacks aimed at exploiting the TOE is considered low.

OE.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error.

OE.TRAIN_GUIDAN Personnel will be trained in the appropriate use of the TOE to ensure security and will refer to all administrative guidance to ensure the correct operation of the TOE.

Rationale For Security Objectives For The TOE

This section provides the rationale that all security objectives are traced back to aspects of the addressed threats.

See the "Rationale For Threat Coverage" section on page 19 for a justification that the TOE security objectives counter the threats addressed by the TOE.

Table 4 Threats & IT Security Objectives Mappings

	T.AUDIT_REVIEW	T.MEDIATE	T.NOAUDIT	T.NOAUTH	T.NOMGT	T.UNAUTH_MGT_ACCESS	T.TIME
O.ACCESS_CONTROL						X	
O.AUDIT_GEN	X						
O.AUDIT_VIEW	X		X				

Table 4 Threats & IT Security Objectives Mappings (continued)

	T.AUDIT_REVIEW	T.MEDIATE	T.NOAUDIT	T.NOAUTH	T.NOMGT	T.UNAUTH_MGT_ACCESS	T.TIME
O.CFG_MANAGE					X		
O.IDAUTH						X	
O.MEDIATE		X					
O.SELFPRO			X	X		X	
O.STARTUP_TEST						X	
O.TIME							X

Rationale For Security Objectives For The Environment

This section provides the rationale that all security objectives for the environment are traced back to aspects of the addressed threats or assumptions.

See the "Rationale For Threat Coverage" section on page 19 for a justification that the security objectives for the environment counter the threats addressed by the operating environment.

See the "Rationale For Assumption Coverage" section on page 20 for a justification that the security objectives cover the assumptions.

Table 5 Threats & IT Security Objectives Mappings for the Environment

	A.NOEVIL	A.TRAIN_AUDIT	A.TRAIN_GUIDAN	A.LOCATE	A.CONFIDENTIALITY	A.GENPUR	A.INTEROPERABILITY	A.LOWEXP	T.AUDIT_REVIEW	T.NOAUTH	T.NOAUDIT	T.TIME	T.UNAUTH_MGT_ACCESS
OE.AUDIT_REVIEW		X							X				
OE.NOEVIL	X												
OE.TRAIN_GUIDAN			X										
OE.LOCATE				X									
OE.CONFIDENTIALITY					X								
OE.GENPUR						X							
OE.INTEROPERABILITY							X						

Table 5 Threats & IT Security Objectives Mappings for the Environment (continued)

	A.NOEVIL	A.TRAIN_AUDIT	A.TRAIN_GUIDAN	A.LOCATE	A.CONFIDENTIALITY	A.GENPUR	A.INTEROPERABILITY	A.LOWEXP	T.AUDIT_REVIEW	T.NOAUTH	T.NOAUDIT	T.TIME	T.UNAUTH_MGT_ACCESS
OE.LOWEXP								X					
OE.ACS_TIME												X	
OE.ACS_PROTECT										X	X		X

Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

T.AUDIT_REVIEW

Actions performed by users may not be known to the administrators due to actions not being recorded or the audit records not being reviewed prior to the machine shutting down.

The O.AUDIT_GEN objective requires that the TOE generate audit records. The O.AUDIT_VIEW requires the TOE to provide the Authorized administrator with the capability to view Audit data. These two objectives provide complete TOE coverage of the threat. The OE.AUDIT_REVIEW objective on the environment assists in covering this threat on the TOE by requiring that the administrator periodically check the audit record.

T.MEDIATE

An unauthorized entity may send impermissible information through the TOE which results in the exploitation of resources on the network.

The O.MEDIATE security objective requires that all information that passes through the network is mediated by the TOE.

T.NOAUDIT

An unauthorized user modifies or destroys audit data.

The O.AUDIT_VIEW objective requires that the TOE will provide the Authorized administrator the capability to review Audit data. The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. The OE.ACS_PROTECT objective requires that the host system assist the ACS with protecting itself from attempts to bypass, deactivate, or tamper with TOE security functions.

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 to disrupt operations of the TOE. The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. The OE.ACS_PROTECT objective requires that the host system the ACS is loaded on assist with this protection.
T.NOMGT	The administrator is not able to easily manage the security functions of the TOE, resulting in the potential for the TOE configuration to compromise security objectives and policies. The O.CFG_MANAGE objective requires that the TOE will provide management tools/applications for the administrator to manage its security functions, reducing the possibility for error.
T.UNAUTH_MGT_ACCESS	An unauthorized user gains management access to the TOE and views or changes the TOE security configuration. The O.ACCESS_CONTROL objective restricts access to the TOE management functions to authorized administrators. The O.IDAUTH objective requires a user to enter a unique identifier and authentication before management access is granted. The O.STARTUP_TEST objective perform initial tests upon system startup to ensure the integrity of the TOE security configuration. The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. OE.ACS_PROTECT objective requires that the host system assist the ACS in protecting itself from attempts to bypass, deactivate, or tamper with TOE security functions. This assistance is limited to ensuring file permissions are preserved on the operating system. ACS has its own discrete access control mechanisms covered under O.SELFPRO.
T.TIME	An authorized administrator will not be able to determine the sequence of events in the audit trail because the audit records are not correctly time-stamped. The O.TIME objective mitigates this threat by providing the accurate time to the TOE for use in the audit records. OE.ACS_TIME mitigates this threat for the ACS by ensuring that NTP is running on the host server.

Rationale For Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the environment cover that assumption.

A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error. The OE.NOEVIL objective ensures that authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error.
A.TRAIN_GUIDAN	Personnel will be trained in the appropriate use of the TOE to ensure security and will refer to all administrative guidance to ensure the correct operation of the TOE. The OE.TRAIN_GUIDAN objective ensures that authorized administrators will be trained in the appropriate use of the TOE to ensure security and will refer to all administrative guidance to ensure the correct operation of the TOE.
A.TRAIN_AUDIT	Administrators will be trained to periodically review audit logs to identify sources of concern. The OE.AUDIT_REVIEW objective ensures that the authorized administrators are trained to periodically review audit logs to identify sources of concern.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.LOCATE objective ensures the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.CONFIDENTIALITY	The hard copy documents that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to Authorized administrators. The OE.CONFIDENTIALITY objective ensures the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to Authorized administrators.
A.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. The OE.GENPUR objective ensures there are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.INTEROPERABILITY	The TOE will be able to function with the software and hardware of other vendors on the network. The OE.INTEROPERABILITY objective ensures that the TOE will be able to function with the software and hardware of other vendors on the network.
A.LOWEXP	The threat of malicious attacks aimed at exploiting the TOE is considered low. The OE.LOWEXP objective ensures that the threat of a malicious attack in the intended environment is considered low.

IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, summarized in the following table. These security requirements are defined in the following sections.

Table 6 Functional Requirements

TOE Security Functional Requirements	
FAU_GEN.1(1) and (2)	Audit data generation (logging)
FAU_SAR.1(1)	Audit review on Router
FAU_SAR.1(2)	Audit review on ACS
FCS_CKM.1(1) and (2)	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1(1) and (2)	Cryptographic operation
FDP_IFC.1(1) and (2)	Subset Information Flow Control
FDP_IFF.1(1) and (2)	Simple Security Attributes
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MOF.1(1)	Management of security functions behavior on Router
FMT_MOF.1(2)	Management of security functions behavior on ACS
FMT_MSA.2	Static Attribute Initialization
FMT_MSA.3	Static Attribute Initialization
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RVM.1(1)	Non-bypassability of the TSP

Table 6 Functional Requirements (continued)

Explicitly Stated TOE Security Functional Requirements	
FPT_SEP_ EXP.1	Partial TSF domain separation
FPT_STM_RTR_EXP.1	Router Reliable time stamps
FPT_AMT_RTR_EXP.1	Router Abstract machine testing
IT Environment Security Functional Requirements	
FAU_STG.1	Protected audit trail storage
FPT_RVM.1(2)	Non-bypassability of the TSP
Explicitly Stated IT Environment Security Functional Requirements	
FPT_SEP_ENV_EXP.1	Partial Environment TSF domain separation
FPT_STM_ENV_EXP.1	Environment Reliable time stamps

TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

Security Audit (FAU)

FAU_GEN.1(1) Audit Data Generation – on All Cisco IOSVersions in Evaluation

FAU_GEN.1.1(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 ***specified in* Table 7**; and

c) no additional events.

FAU_GEN.1.2(1) 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, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, nformation **specified in the Additional Audit Record Contents column of Table 7**.

Table 7 FAU_GEN.1(1) Auditable Events

Functional Complete	Auditable Event	Additional Audit Record Contents
FDP_IFC.1.1	Any failure of a packet to match an ACL rule allowing traversal of the router.	The source, destination and protocol attributes of the traffic.

Application Note This iteration of FAU_GEN.1 applies to all Cisco IOS versions within the evaluation.

FAU_GEN.1(2) Audit Data Generation – on Cisco IOS Release 12.4(11)T2

FAU_GEN.1.1(2) 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 ***specified in* Table 8**; and

c) no additional events.

FAU_GEN.1.2(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, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information **specified in the Additional Audit Record Contents column of Table 8.**

Table 8 FAU_GEN.1(2) Auditable Events

Functional Complete	Auditable Event	Additional Audit Record Contents
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.2	All use of the user authentication mechanism.	The user identities provided to the TOE
FDP_IFC.1.1	Any failure of a packet to match an ACL rule allowing traversal of the router.	The source, destination and protocol attributes of the traffic.

Application Note This iteration of FAU_GEN.1 applies to only the following versions of the TOE: all router platforms running Cisco IOS Release 12.4(11)T2.

FAU_SAR.1(1) Audit Review on Router

FAU_SAR.1.1(1) The TSF shall provide **a privileged administrator and semi-privileged administrator** with the capability to read **all router audit trail data** from the audit records.

FAU_SAR.1.2(1) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.1(2) Audit Review on ACS

FAU_SAR.1.1(2) The TSF shall provide **an authentication administrator** with the capability to read **all ACS audit trail data** from the audit records.

FAU_SAR.1.2(2) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Cryptographic Support (FCS)

FCS_CKM.1(1) Cryptographic Key Generation – RSA

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **512, 1024, and 2048 bits** that meet the following: **PKCS #1**.

FCS_CKM.1(2) Cryptographic Key Generation – Diffie-Hellman

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Diffie-Hellman** and specified cryptographic key sizes **2048 bits** that meet the following: **none**.

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwrite** that meets the following: **no standard**.

FCS_COP.1(1) Cryptographic Operation – Remote Administration (SSH and SSL)

FCS_COP.1.1(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) or Advanced Encryption Standard (AES) as specified in FIPS PUB 197** and cryptographic key sizes **that are 192 or 128, 192, or 256 binary digits in length** that meet the following: **FIPS PUB 46-3 with Keying Option 1 and FIPS PUB 140-1 (Level 1) or FIPS 197**.

FCS_COP.1(2) Cryptographic Operation – Encryption

FCS_COP.1.1(2) The TSF shall perform **encryption of authentication data** in accordance with a specified cryptographic algorithm **MD5** and cryptographic key sizes **128 bit** that meet the following: **RFC 2403**.

User Data Protection (FDP)

FDP_IFC.1(1) Subset Information Flow Control - IP

FDP_IFC.1.1(1) The TSF shall enforce the **unauthenticated SFP** on:

a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another (acting as source and destination);

b) information: network packets (and data link frames with those packets);

c) operation: pass information by opening a relay connection through the TSF on behalf of the source subject to the destination subject, and with the TSF ensuring the following conditions:

- **the connection from the source subject is from a valid adjacent network,**
- **the new relay connection is established to the destination subject on a valid adjacent network.**

FDP_IFF.1(1) Simple Security Attributes - IP

FDP_IFF.1.1(1) The TSF shall enforce the **unauthenticated SFP** based on the following types of subject and information security attributes:

a) security subject attributes:

- **Presumed IP network address of source subject;**
- **presumed IP network address of destination subject;**
- **transport layer protocol and their flags and attributes (UDP, TCP);**
- **network layer protocol (IP, ICMP);**
- **TOE interface on which traffic arrives and departs;**

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) 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 IP address of the source subject, in the information, translates to an internal network address;**
- **and the presumed IP address of the destination subject, in the information, translates to an address on the other connected network.**

b) 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 IP address of the source subject, in the information, translates to an external network address;**
- **and the presumed IP address of the destination subject, in the information, translates to an address on the other connected network.**

FDP_IFF.1.3(1) The TSF shall enforce the **none**.

FDP_IFF.1.4(1) The TSF shall provide the following **none**.

FDP_IFF.1.5(1) The TSF shall explicitly authorize an information flow based on the following rules: **none**.

FDP_IFF.1.6(1) The TSF shall explicitly deny an information flow based on the following rules:

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed IP address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed IP address of the source

subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed IP address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed IP address of the source subject is an external IT entity on the loopback network.

e) The TOE shall drop requests in which the information received by the TOE does not correspond to an entry in the routing table.

Application Note These (IP) iterations of FDP_IFC.1 and FDP_IFF.1 apply to all versions of the TOE.

FDP_IFC.1(2) Subset Information Flow Control - IPX

FDP_IFC.1.1(2) The TSF shall enforce the **unauthenticated SFP** on:

a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another (acting as source and destination);

b) information: network packets (and data link frames with those packets);

c) operation: pass information by opening a relay connection through the TSF on behalf of the source subject to the destination subject, and with the TSF ensuring the following conditions:

- **the connection from the source subject is from a valid adjacent network,**
- **the new relay connection is established to the destination subject on a valid adjacent network.**

FDP_IFF.1(2) Simple Security Attributes - IPX

FDP_IFF.1.1(2) The TSF shall enforce the **unauthenticated SFP** based on the following types of subject and information security attributes:

a) security subject attributes:

- **presumed IPX network address of source subject;**
- **presumed IPX network address of destination subject;**
- **transport layer protocol and their flags and attributes (SPX);**
- **network layer protocol (IPX);**
- **TOE interface on which traffic arrives and departs**;

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) 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 IPX address of the source subject, in the information, translates to an internal network address;**
- **and the presumed IPX address of the destination subject, in the information, translates to an address on the other connected network.**

b) 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 IPX address of the source subject, in the information, translates to an external network address;**
- **and the presumed IPX address of the destination subject, in the information, translates to an address on the other connected network.**

FDP_IFF.1.3(2) The TSF shall enforce the **none**.

FDP_IFF.1.4(2) The TSF shall provide the following **none**.

FDP_IFF.1.5(2) The TSF shall explicitly authorize an information flow based on the following rules: **none**.

FDP_IFF.1.6(2) The TSF shall explicitly deny an information flow based on the following rules:

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed IPX address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed IPX address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed IPX address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed IPX address of the source subject is an external IT entity on the loopback network.

e) The TOE shall drop requests in which the information received by the TOE does not correspond to an entry in the routing table.

Application Note These (IPX) iterations of FDP_IFC.1 and FDP_IFF.1 apply to only the following versions of the TOE: the 1700 series (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), the 1800 series (1801, 1802, 1803, 1811, 1812, 1841), the 2600XM series (2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, 2691), the 2800 series (2801, 2811, 2821, 2851), the 3700 series (3725, 3745), the 3800 series (3825, 3845), the 7200 series (7204VXR, 7206VXR), the 7301, the 7401, the 7600 series (only 7603, 7606, 7609, 7613, Supervisor Engines: 7600-SUP2/MSFC2, 7600-SUP32/MSFC2A, 7600-SUP720/MSFC3), and the 12000 series (12006, 12008, 12010, 12012, 12016, 12404, 12406, 12410, 12416, 12810, 12816, Route Processor: PRP-1, PRP-2).

Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within **one and five** unsuccessful authentication attempts occur related to **login**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **lock the account until the authentication administrator re-enables it**.

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) authentication data (e.g., password).

FIA_UAU.2 User Authentication Before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user

FIA_UID.2 User Identification Before Any Action

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.

Security Management (FMT)

FMT_MOF.1(1) Management of Security Functions Behavior on Router

FMT_MOF.1.1(1) The TSF shall restrict the ability to determine the behavior of the functions **listed below** to **the privileged administrator**:

a) start-up and shutdown;

b) create, modify, or delete configuration items;

c) modify and set the time and date;

d) create, delete, empty, and review the router audit trail;

e) create, delete, modify, and view filtering rules;

and the semi-privileged administrator:

a) review the router audit trail.

FMT_MOF.1(2) Management of Security Functions Behavior on ACS

FMT_MOF.1.1(2) The TSF shall restrict the ability to determine the behavior of the functions **listed below** to **the authentication administrator**:

a) modify and set the threshold for the number of permitted consecutive authentication attempt failures;

b) restore authentication capabilities for users that have met or exceeded the threshold for permitted consecutive authentication attempt failures;

c) create, delete, empty, and review the ACS audit trail;

FMT_MSA.2 Static Attribute Initialization

FMT_MSA.2.1 The TSF shall ensure that only secure values are acceptable for security attributes.

FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the **unauthenticated SFP** to provide <u>permissive</u> default values for 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.

FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to <u>modify</u> **all router TOE data and all ACS TOE data** to **privileged administrators and authentication administrators, respectively**.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1 The TSF shall be capable of performing the following security management functions:

a) start-up and shutdown;

b) create, modify, or delete configuration items;

c) modify and set the time and date;

d) create, delete, empty, and review the audit trail;

e) create, delete, modify, and view filtering rules.

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: **privileged administrator, semi-privileged administrator and authentication administrator**[1]

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from <u>disclosure</u> when it is transmitted between separate parts of the TOE.

[1] The term “authorized administrators” is still used generically in some places in the ST. Where used clarification will follow if it does not refer to all three roles.

FPT_RVM.1(1) Non-bypassability of the TSP

FPT_RVM.1.1(1) The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Explicitly Stated TOE Security Functional Requirements

The SFRs defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

Protection of TSF (FPT)

FPT_SEP_ EXP.1 Partial TSF Domain Separation

FPT_SEP_ EXP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_ EXP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM_RTR_EXP.1 Router Reliable Time Stamps

FPT_STM_RTR_EXP.1.1The TSF component shall be able to provide reliable time stamps for the router component's use.

FPT_AMT_RTR_EXP.1 Router Abstract Machine Testing

FPT_AMT_RTR_EXP.1.1The TSF shall run a suite of tests at the request of the authorized user to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF for the router TOE component.

IT Environment Security Requirements

Security Audit (FAU)

FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The ***IT environment*** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The IT environment shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

FPT_RVM.1(2) Non-bypassability of the TSP

FPT_RVM.1.1(2) The ***IT environment*** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Explicitly Stated IT Environment Security Functional Requirements

The SFRs on the IT environment defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

Protection of TSF (FPT)

FPT_SEP_ENV_EXP.1 Partial Environment TSF Domain Separation

FPT_SEP_ENV_EXP.1.1The IT environment shall maintain a security domain for the TOE's execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP_ENV_EXP.1.2The IT environment shall enforce separation between the security domains of subjects in the TSC.

FPT_STM_ENV_EXP.1 Environment Reliable Time Stamps

FPT_STM_ENV_EXP.1.1The IT environment shall be able to provide reliable time stamps for the ACS component's use.

TOE Strength of Function Claim

The only probabilistic or permutational mechanisms in the product are the password mechanism used to authenticate users and the cryptographic mechanisms. Strength of cryptographic algorithms is outside the scope of the Common Criteria.

The minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism is SOF-basic. For a rationale for this selected level, see section Rationale For Strength of Function Claim.

Specific strength of function metrics are defined for the following requirements:

FIA_UAU.2 Strength of Function shall be demonstrated such that the probability that authentication data can be guessed is no greater than one in one million (000001).

TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 (EAL3) as defined by the CC and additionally meets the ALC_FLR.1 assurance requirement. The assurance components are summarized in Table 9.

Table 9 Assurance Requirements: EAL3

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_CAP.3	Authorization controls
	ACM_SCP.1	TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures

Table 9 Assurance Requirements: EAL3

Assurance Class	Assurance Components	
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC: Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Basic Flaw Remediation
ATE: 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
AVA: Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

ACM_CAP.3 Authorization Controls

Developer action elements:

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a CM system.

ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.XC The configuration list shall uniquely identify all configuration items that comprise the TOE. (Interpretation 003)

ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.3.7C The CM plan shall describe how the CM system is used.

ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

Evaluator action elements:

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.1 TOE CM Coverage

Developer action elements: (Interpretation 004)

ACM_SCP.1.1D The developer shall provide a list of configuration items for the TOE.

Content and presentation of evidence elements: (Interpretations 004 and 038)

ACM_SCP.1.1C The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements:

ACM_SCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_DEL.1 Delivery Procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, Generation, and Start-up Procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE. (Interpretation 051)

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

ADV_FSP.1 Informal Functional Specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

ADV_HLD.2 Security Enforcing High-level Design

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security requirements.

ADV_RCR.1 Informal Correspondence Demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ADM.1 Administrator Guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the authorized administrators of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the authorized administrators, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the authorized administrators.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User Guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1Identification of Security Measures

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_FLR.1 Basic Flaw Remediation

Developer action elements:

ALC_FLR.1.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

Content and presentation of evidence elements:

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Evaluator action elements:

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_COV.2 Analysis of Coverage

Developer action elements:

ATE_COV.2.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Testing: High-level Design

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional Testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent Testing - Sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer’s functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA_MSU.1 Examination of Guidance

Developer action elements:

AVA_MSU.1.1D The developer shall provide guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements:

AVA_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_SOF.1 Strength of TOE Security Function Evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.1 Developer Vulnerability Analysis

Developer action elements: (Interpretation 051)

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements: (Interpretation 051)

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

Rationale For TOE Security Requirements

TOE Security Functional Requirements

Table 10 SFR to Security Objectives Mapping

	O.ACCESS_CONTROL	O.AUDIT_GEN	O.AUDIT_VIEW	O.CFG_MANAGE	O.IDAUTH	O.MEDIATE	O.SELFPRO	O.STARTUP_TEST	O.TIME
FAU_GEN.1(1) and (2)		X							
FAU_SAR.1(1) and (2)			X						
FCS_COP.1(1) and (2)							X		
FCS_CKM.1(1) and (2)							X		
FCS_CKM.4							X		
FDP_IFC.1(1) and (2)						X			
FDP_IFF.1(1) and (2)						X			
FIA_AFL.1					X				
FIA_ATD.1					X				
FIA_UAU.2					X				
FIA_UID.2					X				
FMT_MOF.1(1) and (2)	X			X					
FMT_MSA.2							X		
FMT_MSA.3	X			X		X			
FMT_MTD.1	X								
FMT_SMF.1				X					
FMT_SMR.1	X			X					
FPT_ITT.1							X		

Table 10 SFR to Security Objectives Mapping (continued)

	O.ACCESS_CONTROL	O.AUDIT_GEN	O.AUDIT_VIEW	O.CFG_MANAGE	O.IDAUTH	O.MEDIATE	O.SELFPRO	O.STARTUP_TEST	O.TIME
FPT_RVM.1(1)							X		
FPT_SEP_ EXP.1							X		
FPT_STM_RTR_EXP.1									X
FPT_AMT_RTR_EXP.1								X	

O.ACCESS_CONTROLThe TOE will restrict access to the TOE Management functions to the Authorized administrators.

The TOE is required to provide the ability to restrict the use of TOE management/administration/security functions to authorized administrators of the TOE. These functions are divided between the router (privileged administrator) and the ACS (authentication administrator) [FMT_MOF.1(1) and (2)]. Only authorized administrators of the TOE may modify TOE data [FMT_MTD.1]. The TOE must be able to recognize the administrative role that exists for the TOE [FMT_SMR.1]. The TOE must allow the privileged administrator to specify alternate initial values when an object is created [FMT_MSA.3]. The TOE ensures that all user actions resulting in the access to TOE security functions and configuration data are controlled. The TOE ensures that access to TOE security functions and configuration data is based on the assigned user role.

O.AUDIT_GEN The TOE will generate audit records which will include the time that the event occurred and if applicable, the identity of the user performing the event.

Security relevant events must be defined and auditable for the TOE [FAU_GEN.1(1) and (2)]. Timestamps associated with the audit record must be reliable [FPT_STM.1].

O.AUDIT_VIEW The TOE will provide the privileged administrators and authentication administrators the capability to review Audit data.

Security relevant events must be available for review by authorized administrators (both privileged administrators and authentication administrators) [FAU_SAR.1(1) and (2)].

O.CFG_MANAGE The TOE will provide management tools/applications to allow privileged administrators and authentication administrators to manage its security functions.

The TOE is required to provide the ability to for authorized administrators (both privileged administrators and authentication administrators) to perform management/administration/security [FMT_MOF.1(1) and (2)]. The TOE is capable of performing numerous management functions including startup, shutdown, and creating/modifying/deleting configuration items [FMT_SMF.1]. The TOE must be able to recognize the administrative role that exist for the TOE [FMT_SMR.1]. The TOE must allow the privileged administrator to specify alternate initial values when an object is created [FMT_MSA.3]. The TOE requires that all users, switches, devices and hosts actions resulting in the access to TOE security functions and configuration data are controlled to prevent unauthorized activity. The TOE ensures that access to TOE security functions and configuration data is done in accordance with the rules of the access control policy.

O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access.

The TOE is required to provide users with security attributes to enforce the authentication policy of the TOE and to associate security attributes with users [FIA_ATD.1]. Users authorized to access the TOE must be defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. Before anything occurs on behalf of the user, the user’s identity is identified to the TOE [FIA_UID.2]. Multiple consecutive unsuccessful attempts to authenticate using ACS result in locking of the account until the authentication administrator re-enables it [FIA_AFL.1].

O.MEDIATE The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.

The TOE is required to identify the entities involved in the unauthenticated information flow control SFP [FDP_IFC.1(1) and (2), FDP_IFC.1(1) and (2)] and to identify the attributes of the users sending and receiving the information in the unauthenticated SFP [FDP_IFF.1(1) and (2)]. The policy is defined by saying under what conditions information is permitted to flow [FDP_IFF.1(1) and (2)]. Information that is permitted to flow will then be routed according to the information in the routing table [FDP_IFF.1(1) and (2)]. The TOE ensures that there is a default deny policy for the information flow control security rules [FMT_MSA.3].

O.SELFPRO The TOE (both router and ACS) must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

The router component of the TOE ensures that the TSF has a domain of execution that is separate and that cannot be violated by unauthorized users [FPT_SEP _EXP.1]. The ACS component provides a domain that protects itself from untrusted users and from interference through its own interfaces that would prevent it from performing its functions [FPT_SEP _EXP.1] The TOE ensures that the TSP enforcement functions cannot be bypassed [FPT_RVM.1(1)].

The router component of the TOE provides an encrypted (SSH) mechanism for remote management of the TOE and for protection of authentication data transferred between the router and ACS (MD5). [FCS_COP.1(1) and (2), FCS_CKM.1(1) and (2), FCS_CKM.4, FMT_MSA.2, FPT_ITT.1]

O.STARTUP_TEST The TOE will perform initial startup tests upon bootup of the system.

The TOE is required to demonstrate the correct operation of the security assumptions on startup by running initialization tests [FPT_AMT_RTR_EXP.1].

O.TIME The TSF will provide a reliable time stamp for its own use.

The router is required to provide reliable timestamps for use with the audit record. [FPT_STM_RTR_EXP.1].

TOE Security Assurance Requirements

EAL3 augmented with ALC_FLR.1 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws. Including the assurance requirement ALC_FLR.1 is to allow for future assurance maintenance activities.

Rationale For IT Environment Security Requirements

Table 11 Environmental Security Requirements Mapping

	OE.ACS_PROTECT	OE.ACS_TIME
FAU_STG.1	X	
FPT_RVM.1(2)	X	
FPT_SEP_ENV_EXP.1	X	
FPT_STM_ENV_EXP.1		X

OE.ACS_PROTECT The Windows Server Host must protect the ACS against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions through attacking the Windows operating system.

The ACS ensures that the TSF has a domain of execution that is separate and that cannot be violated by unauthorized users [FPT_SEP_ENV_EXP.1] through its independent system of authentication. The Windows Server host ensures that the TSP enforcement functions cannot be bypassed [FPT_RVM.1(2)]. The Windows Server host also protects stored audit records from unauthorized deletion [FAU_STG.1].

OE.ACS_TIME The Windows Server Host will provide a reliable time stamp for use.

The Windows Server Host is required to provide reliable timestamps for use with the audit record. [FPT_STM ENV_EXP.1]. This in turn is taken by the ACS to satisfy O.AUDIT_GEN for events internal to the ACS.

Rationale for Explicitly Stated Security Requirements

Table 12 presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Table 12 Explicitly Stated Requirement Rationale

Explicit Requirement	Identifier	Rationale
FPT_SEP_ EXP.1.1	Partial TSF Domain Separation	This requirement is necessary because the domain separation on the TOE is partially met by the TOE and partially met on the IT environment.
FPT_STM_RTR_EXP.1.1	Router Reliable Time Stamps	This requirement is necessary because the CC version of FPT_STM.1 does not specify portions of the TOE. This is specific to the router component. This requirement is split between the TOE and the environment.
FPT_SEP_ENV_EXP.1.1	Partial Environment TSF Domain Separation	This requirement is necessary because a separate version of the CC requirement FPT_SEP.1 is needed for the environment of the TOE.
FPT_STM_ENV_EXP.1.1	Environment Reliable Time Stamps	This requirement is necessary because the CC version of FPT_STM.1 does not allow the time stamp source to be split. This is specific to the TOE environment. This requirement is split between the TOE and the environment.

Rationale For IT Security Requirement Dependencies

This section includes a table of the requirements are their dependencies and a rationale for any dependencies that are not satisfied.

Table 13 SFR Dependencies

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FCS_CKM.1	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	YES
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2	YES
FSC_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	YES
FDP_IFC.1	FDP_IFF.1	YES
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	YES YES
FIA_AFL.1	FIA_UAU.1	YES, via FIA_UAU.2
FIA_ATD.1	none	N/A
FIA_UAU.2	FIA_UID.1	YES, via FIA_UID.2
FIA_UID.2	none	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	YES YES

Table 13 SFR Dependencies (continued)

Functional Component	Dependency	Included
FMT_MSA.2	FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	YES No, see rational below. YES
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	No, see rationale below. YES
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	YES YES
FMT_SMF.1	none	N/A
FMT_SMR.1	FIA_UID.1	YES
FPT_ITT.1	none	N/A
FPT_RVM.1	none	N/A
FPT_SEP_ EXP.1	none	N/A
FPT_STM_RTR_EXP.1	none	N/A
FPT_AMT_RTR_EXP.1	none	N/A

Functional component FMT_MSA.3 depends on functional component FMT_MSA.1 Management of security attributes. In an effort to place all the management requirements in a central place, FMT_MOF.1 was used. Therefore FMT_MOF.1a more than adequately satisfies the concerns of leaving FMT_MSA.1 out of this Security Target.

Rationale For Internal Consistency and Mutually Supportive

The ST includes all the functional security requirements to address security functionality provided by the TOE. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies or providing an acceptable rationale for not satisfying the dependency as demonstrated in Section Rationale For IT Security Requirement Dependencies
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section TOE Security Functional Requirements
- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely.

Rationale For Strength of Function Claim

The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. The security objectives imply probabilistic or permutational security mechanism and the TOE password constraints satisfy the minimal “industry” accepted constraints that should be good enough for SOF-Basic.

TOE Summary Specification

TOE Security Functions

Audit (Accounting)

The router and the ACS provide basic data logging and security auditing. Audit data is stored in memory on the router. Although the data may be reviewed, it is not persistent and will be deleted upon system reboot. Permanent audit data is stored by the ACS either in a CSV file on the server or in a SQL database on the server

Audit data generation: FAU_GEN.1(1) and (2).

Audit data is generated by Cisco IOS. Audit data includes audit records for each of the auditable events specified in Table 7.

Audit records include the date and time of the event, the type of event, subject identity, and if the record addresses a success or a failure. Additional data collected for specific audit events are provided in Table 7.

Security Audit review and restricted review: FAU_SAR.1(1) and (2)

Both the ACS and the router provide the ability for authorized administrators to read audit information. The authentication administrator can read audit information on ACS, and the privileged administrator can read audit information on the router. Semi-privileged administrators can also read audit information on the router by default.

Reliable Time Stamps: FPT_STM_RTR_EXP.1

The router clock provides reliable time stamps for use by the router component of the TOE. 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. The reliable time stamp for the ACS portion of the TOE is provided by the underlying Windows OS (FPT_STM_ENV_EXP.1).

Identification & Authentication (Authentication)

Identification and Authentication for logging on to the Router can be provided either locally on the router or through the ACS using TACACS+. Authorized administrators (all roles) of the TOE must be identified and authenticated prior to using the system. Username/Password combinations will be set to enter privileged administrative modes (Privileged Exec, User) as well as access to auxiliary, console, and connecting to the router using SSH.

User attribute definition: FIA_ATD.1(1)

The user security attributes for both the router and ACS are identity and password.

Timing of Identification and authentication: FIA_UAU.2(1), FIA_UID.2(1).

It is possible for a privileged or semi-privileged administrator to log directly into Cisco IOS on the router by connecting directly to the console port. These administrators log into Cisco IOS to perform local maintenance, diagnostics, or debugging. Identification and authentication must take place before any other actions can be performed.

The authentication mechanism is the only security function realized by a probabilistic or permutational security mechanism. The minimum password length for users and administrators is 8 characters (with a character set of at least 80 characters), which meets the SOF claim of SOF-basic.

Identification and Authentication for logging on to the ACS checks its internal user database. If the user exists in the internal user database (that is, is a known or discovered user), ACS tries to authenticate the user with the specified password type against the specified database. Authentication for that user either passes or fails, depending on other procedures in the normal authentication process.

Failure handling: FIA_AFL.1.

All versions of the TOE rely on ACS for account lockout of ACS-authenticated sessions. The authentication administrator configures the ACS server to lockout accounts after one to five consecutive failed authentication attempts. This results in users that reach that limit having their accounts locked until the authentication administrator unlocks them. Routers running Cisco IOS version 12.4(11)T2 also allow the ability to lockout user accounts using local authentication on the router.

Traffic Filtering and Routing

Information Flow and Security Attributes: FDP_IFC.1(1) and (2), FDP_IFF.1(1) and (2)

The router supports routing of the traffic that is permitted by the information flow policies. All traffic passing through the router is processed by the ACL attached to the interface/protocol. The ACL is processed top-down, with processing continuing until the first match is made.

All traffic that successfully clears the ACLs is processed by the routing tables. The routing table is processed top-down, with processing continuing until the first match is made. The routing table may be statically updated by a privileged administrator or dynamically through routing protocols.

Security Management / Access Control (Authorization)

The TOE allows administrators to add new administrators, start-up and shutdown the device, create, modify, or delete configuration items, modify and set the threshold for the number of permitted authentication attempt failures, restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures, modify and set the time and date, and create, delete, empty, and review the audit trail.

Management and specification of security functions: FMT_MOF.1(1) and (2), FMT_SMF.1

The following functions are specified for the TOE and are restricted to authentication administrators and privileged administrators:

a. start-up and shutdown (privileged administrators only);

b. create, modify, or delete configuration items (both privileged administrators and authentication administrators);

c. modify and set the time and date (privileged administrators only);

d. modify and set the threshold for the number of permitted consecutive authentication attempt failures (authentication administrators only);

e. restore authentication capabilities for users that have met or exceeded the threshold for permitted consecutive authentication attempt failures (authentication administrators only);

f. create, delete, empty, and review the audit trail (both privileged administrators and authentication administrators);

g. create, delete, modify, and view filtering rules (privileged administrators only).

Static Attribute Initialization: FMT_MSA.3

By default, the TOE allows information flow with the unauthenticated SP (i.e., the TOE allows all data to pass through). The administrator is instructed in administrator guidance how to set default attribute values in a secure manner.

Management of TSF data: FMT_MTD.1

This requirement states that TOE data can only be queried and modified by a privileged administrator.

Security Roles: FMT_SMR.1.

The TOE maintains the roles of the privileged administrator, semi-privileged administrator and authentication administrator.

The router maintains all Cisco IOS administrator roles (privileged and semi-privileged administrators). 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 TOE also maintains the ACS administrator (authentication administrator).

Protection of the TSF

Abstract Machine Testing: FPT_AMT_RTR_EXP.1

The router initiates a suite of tests upon startup to ensure proper operation of the underlying abstract machine that underlies the TOE. The router plus the Cisco IOS image is considered the abstract machine.

The router is required to demonstrate the correct operation of the security assumptions at the request of the authorized administrator by generating a one-way MD5 hash of the running Cisco IOS image to demonstrate if the file has been corrupted. The administrator can match this MD5 hash to one on the Cisco download website to ensure integrity of the file. Alternately the administrator can enter the expected hash at the command line and the router can verify that the value matches the one of the running image.

Internal data transfer: FPT_ITT.1

The TOE protects data transferred between the router and the ACS server from disclosure by using the RADIUS and TACACS+ protocols. RADIUS uses MD5 hashes derived from a shared secret to protect passwords being transmitted between the router and the ACS. TACACS+ uses MD5 hashes derived from a shared secret to protect the entire data transmission.

Non-bypassability of the TSP: FPT_RVM.1(1)

The TOE protects its management functions by isolating them through identification and authentication of administrative users.

TSF domain separation: FPT_SEP _EXP.1.

The router component of the TOE protects itself from interference and tampering by untrusted subjects by implementing authentication and access controls to limit configuration to privileged administrators. Cisco IOS is not a general purpose operating system and access to Cisco IOS memory space is restricted to Cisco IOS functions. Additionally, Cisco IOS is the only software running on the routers in the TOE.

The external interfaces to the ACS component of the TOE ensure that users must login prior to accessing administrative ACS functions and resources. In addition, the external interfaces to the ACS ensure that users must login prior to accessing other ACS resources. Protection of the ACS component of the TOE from physical and logical tampering from other methods is ensured by the physical security assumptions and by the domain separation requirements on the ACS hardware and operating system in the environment.

The protection of the security domain for the ACS component's execution is provided by the underlying Windows OS (FPT_SEP_ENV_EXP.1), which implements port filtering to protect itself and the ACS component.

Remote Management: FCS_COP.1(1) and (2), FCS_CKM.1(1) and (2), FCS_CKM.4, and FMT_MSA.2

The TOE implements Secure Shell (SSH) using RSA key generation and 192 bit 3DES or 128, 192, or 256 bit AES encryption for the purposes of remote management of the router. 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). Implementation of the various cryptographic standards ensure that only appropriate secure values are used for the cryptographic functions performed.

The TOE implements SSL using RSA or Diffie-Hellman key generation and 128 bit AES encryption for the purposes of remote management of the ACS. Implementation of the various cryptographic standards ensure that only appropriate secure values are used for the cryptographic functions performed.

Encryption is implemented using 128 bit MD5 hashing for purposes of protecting authentication data transferred between the router and the ACS server from disclosure.

Key overwriting is done upon creation of new cryptographic keys, and the new key is written over the old one in NVRAM.

Remote management of the router via SSH provides full access to the CLI command set. Remote management of the ACS via SSL provides full access to the ACS GUI.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

Security Assurance Measures

Table 14 Assurance Requirements: EAL3

Assurance Requirement	Assurance Components
ACM_CAP.3	The description of the configuration items and controls used to prevent unauthorized modification is provided in Cisco's Configuration Management Plan and Delivery Procedure.
ACM_SCP.1	The description of the scope of control for configuration items is provided in Cisco's Configuration Management Plan and Delivery Procedure.
ADO_DEL.1	The description of the delivery procedures is provided in Cisco's Configuration Management Plan and Delivery Procedure.
ADO_IGS.1	The installation, generation, and start-up procedures are provided in Installation and Configuration for Common Criteria EAL3 Evaluated Cisco IOS/AAA Routers.

Table 14 Assurance Requirements: EAL3 (continued)

Assurance Requirement	Assurance Components
ADV_FSP.1	The informal functional specification is provided in Cisco IOS / AAA Functional Specification EAL3.
ADV_HLD.2	The security enforcing high-level design is provided in Cisco IOS / AAA High Level Design EAL3.
ADV_RCR.1	The informal correspondence demonstration is provided in Cisco IOS / AAA Functional Specification EAL3.
AGD_ADM.1	The administrator guidance is provided in the following documents: Installation and Configuration for Common Criteria EAL3 Evaluated Cisco IOS/AAA Routers and documents referenced therein.
AGD_USR.1	See AGD_ADM.1
ALC_DVS.1	The life cycle measures are described in Cisco Systems Development Security for Cisco IOS.
ALC_FLR.1	The flaw remediation measures are described in Cisco Systems Development Security for Cisco IOS.
ATE_COV.2	The analysis of coverage is provided in Cisco IOS Routers EAL3 Detailed Test Plan
ATE_DPT.1	The depth of testing analysis is provided in Cisco IOS Routers EAL3 Detailed Test Plan
ATE_FUN.1	The functional testing description is provided in Cisco IOS Routers EAL3 Detailed Test Plan
ATE_IND.2	The TOE and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_MSU.1	The following documentation is free from misleading, unreasonable and conflicting guidance: IOS / AAA Vulnerability, Misuse and Strength of Function, EAL 3
AVA_SOF.1	The strength of function analysis performed is provided in IOS / AAA Vulnerability, Misuse and Strength of Function, EAL 3,
AVA_VLA.1	The vulnerability analysis performed is provided in IOS / AAA Vulnerability, Misuse and Strength of Function, EAL 3, Version: 0-

Rationale for TOE Security Functions

This section contains a table which relates the security functional requirements to the TOE security functions. The rationale that the security functions cover the security functional requirements is in Section TOE Security Functions.

Table 15 SFR to Security Functions Mapping

	Audit (Accounting)	Authentication (Authentication)	Traffic Filtering and Routing	Security Management / Access Control	Protection of the TSF
FAU_GEN.1(1) and (2)	X				
FAU_SAR.1(1) and (2)	X				
FCS_COP.1(1) and (2)					X
FCS_CKM.1(1) and (2)					X
FCS_CKM.4					X
FDP_IFC.1(1) and (2)			X		
FDP_IFF.1(1) and (2)			X		
FIA_AFL.1		X			
FIA_ATD.1		X			
FIA_UAU.2		X			
FIA_UID.2		X			
FMT_MOF.1(1) and (2)				X	
FMT_MSA.2					X
FMT_MSA.3				X	
FMT_MTD.1				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FPT_ITT.1					X
FPT_RVM.1(1)					X
FPT_SEP_EXP.1					X
FPT_STM_RTR_EXP.1	X				
FPT_AMT_RTR_EXP.1					X

Appropriate Strength of Function Claim

The "Rationale For Strength of Function Claim" section on page 46 contains a justification for the claim of SOF-basic.

The password authentication mechanism implemented by FIA_UAU.2 meet the strength of function claim of SOF-basic by requiring, through guidance, a password of at least 8 characters with a character set of at least 80 characters.

Security Assurance Measures & Rationale

The assurance documentation listed below was developed to meet the developer action and content and presentation of evidence elements for each assurance requirement defined in the CC.

Table 16 Assurance Measure Rationale: EAL3

Assurance Requirement	Assurance Measures	Assurance Rationale
ACM_CAP.3 ACM_SCP.1	Cisco's Configuration Management Plan and Delivery Procedure v0-9, April 2007 Cisco AAA Configuration Items v0-6, October 2007	The configuration management document defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE.
ADO_DEL.1	Cisco's Configuration Management Plan and Delivery Procedure v0-9, April 2007	The delivery document describes the steps performed to ensure consistent, dependable delivery of the TOE to the customer.
ADO_IGS.1	Installation and Configuration for Common Criteria EAL3 Evaluated Cisco IOS/AAA Routers and the documents referenced therein, October 2007, v0-9.	The installation document describes the steps necessary for secure installation, generation and start-up of the TOE.
ADV_FSP.1	Cisco IOS / AAA Functional Specification EAL3, October 31, 2007, v0-11	The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.
ADV_HLD.2	Cisco IOS / AAA High Level Design EAL3, October 31, 2007, v0-10	The security enforcing high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.
ADV_RCR.1	Cisco IOS / AAA Functional Specification EAL3, October 31, 2007, v0-11	The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD.
AGD_ADM.1	Installation and Configuration for Common Criteria EAL3 Evaluated Cisco IOS/AAA Routers and the documents referenced therein, October 2007, v0-9.	The administrator guidance document provides complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	N/A	Because the TOE is transparent to non-administrative users and all operations are administrative in nature and are performed by solely by authorized administrators, there is no guidance documentation available for non-administrative functions.
ALC_DVS.1	Cisco Systems Development Security for Cisco IOS, February 2005, v0-2	Documentation on the security of the development environment describing all physical, procedural, personnel, and other security measures, that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_FLR.1	Cisco's Configuration Management Plan and Delivery Procedure v0-9, April 2007	Documentation on the security of the development environment describing the handling of all product defects and how they are tracked.

Table 16 Assurance Measure Rationale: EAL3 (continued)

Assurance Requirement	Assurance Measures	Assurance Rationale
ATE_COV.2	Cisco IOS Routers EAL3 Detailed Test Plan, September 28, 2007, v1.8	The test coverage document provides a mapping of the test cases performed against the TSF.
ATE_DPT.1	Cisco IOS Routers EAL3 Detailed Test Plan, September 28, 2007, v1.8	The depth of testing document.
ATE_FUN.1	Cisco IOS Routers EAL3 Detailed Test Plan, September 28, 2007, v1.8	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	The TOE and testing documentation will be made available to the CC testing laboratory for independent testing.	The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_MSU.1	Refer to AGD_ADM.1 and ADO_IGS.1 assurance measures Cisco IOS / AAA Vulnerability, Misuse and Strength of Function, EAL 3, Version: 0-6, Date: 8/22/2007.	The guidance documentation provided is complete and clear. Correct use of the guidance will result in the prevention and/or detection of insecure TOE states.
AVA_SOF.1	Cisco IOS / AAA Vulnerability, Misuse and Strength of Function, EAL 3, Version: 0-6 Date: 8/22/2007.	The strength of function analysis document provides the SOF argument for the passwords used for administrator login to the TOE.
AVA_VLA.1	Cisco IOS / AAA Vulnerability, Misuse and Strength of Function, EAL 3, Version: 0-6, Date: 8/22/2007.	The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

Protection Profile Modifications

This Security Target does not claim conformance to any Protection Profiles.

Protection Profile Additions

This Security Target does not claim conformance to any Protection Profiles.

Rationale

Security Objectives Rationale

Sections Rationale For Security Objectives For The TOE, page 17 through Rationale For Assumption Coverage, page 20 provide the security objectives rationale.

Security Requirements Rationale

Sections Rationale For TOE Security Requirements, page 41 through Rationale For Strength of Function Claim, page 46 provides the security requirements rationale.

TOE Summary Specification Rationale

Sections Rationale for TOE Security Functions, page 51 through Security Assurance Measures & Rationale, page 53 provides the TSS rationale.

Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html