Cisco 7600 Series Routers Security Target

Revision 0.13

27 November, 2012

Table of Contents

List of Tables

DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco 7600 Series Routers running IOS 15.1(3)S3. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- Rationale [Section 7]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 4.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Table 1: ST and TOE Identification

ST Title	Cisco 7600 Series Routers Security Target
ST Version	0.13
Publication Date	27 November 2012
ST Author	Cisco Systems, Inc.
Developer of the TOE	Cisco Systems, Inc.
TOE Reference	Cisco 7600 Series Routers
TOE Hardware Models	Cisco 7600 Series (7613, 7609-S, 7606-S, 7604, and 7603-S) with RSP720 management cards (RSP720-3CXL-10GE, RSP720-3C-10GE, RSP720-3CXL-GE or RSP720-3C-GE), VPN IPSec SPA (ws-ipsec-3), and compatible line cards[1]
TOE Software Version	IOS 15.1(3)S3
ST Evaluation Status	In Evaluation
Keywords	Audit, Authentication, Encryption, Information Flow, Protection, Router, Traffic

1.2 Acronyms and Abbreviations

The following acronyms and abbreviations are used in this Security Target:

Table 2: Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
BGP	Border Gateway Protocol. An exterior gateway protocol. It performs routing between

[1] As listed in Annex B of this Security Target.

Acronyms / Abbreviations	Definition
	multiple autonomous systems and exchanges routing and reachability information with other BGP systems.
CBC	Cipher Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
DH	Diffie-Hellman
DRBG	Distributed Random Bit Generator
EAL	Evaluation Assurance Level
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Protocol
FIPS	Federal Information Processing Standard
HA	High Availability (device or component failover)
HMAC	Hashed Message Authentication Code
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IKEv1	Internet Key Exchange version 1
IOS	Cisco proprietary Internetwork Operating System
IP	Internet Protocol
IPSec	IP Security
IT	Information Technology
MAC	Media Access Control
MD5	Message Digest 5
NDPP	Network Device Protection Profile
NTP	Network Time Protocol
OS	Operating System
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.
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PVLAN	Private VLAN
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment
RIP	Routing Information Protocol
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SA	Security Association
SHA1	Secure Hashing Algorithm 1
SM	Service Module
SSH	Secure Shell
SSHv2	Secure Shell (version 2)
ST	Security Target
Sup2T	Cisco Supervisor Engine 2T (VS-S2T-10G or VS-S2T-10G-XL)
TACACS	Terminal Access Controller Access Control System
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDES	Triple Data Encryption Standard

Acronyms / Abbreviations	Definition
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User Datagram Protocol
VACL	VLAN ACL
VLAN	Virtual Local Area Network
VSS	Virtual Switching System

1.3 TOE Overview

The TOE is the Cisco 7600 Series w/ RSP720 (7613, 7609-S, 7606-S, 7604 and 7603-S) with an RSP720 management cards (RSP720-3CXL-10GE, RSP720-3C-10GE, RSP720-3CXL-GE or RSP720-3C-GE) running IOS 15.1(3)S3, a VPN IPSec SPA (ws-ipsec-3) plus any compatible line cards listed in Annex B of this Security Target (herein after referred to as the 7600, the router, or the TOE). The TOE is a purpose-built, routing platform with OSI Layer3 traffic filtering capabilities.

1.3.1 TOE Product Type

The TOE is a routing platform used to construct IP networks by interconnecting multiple smaller networks or network segments. As a Layer3 router, it supports routing of traffic based on tables identifying available routes, conditions, distance, and costs to determine the best route for a given packet. Routing protocols used by the TOE include BGP, RIPv2, and OSPFv2.

1.3.2 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 3: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
NTP Server	No	The TOE supports communications with an NTP server to receive clock updates.
Syslog server	No	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.
Authentication Server	No	The authentication server (RADIUS and TACACS+) is used to provide centralized authentication and related auditing for one or more distributed instances of the TOE.

1.4 TOE DESCRIPTION

Cisco IOS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing. Although IOS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 Logical Scope of the TOE below.

1.5 TOE Evaluated Configuration

The TOE consists of any one of a number of hardware configurations, each running the same version of IOS software. The 7600 chassis provides power, cooling, and backplane for the Supervisor Engine, line cards, and service modules. The Supervisor Engines run the IOS software. The evaluated configurations consist of the following:

Table 4: Evaluated Configurations

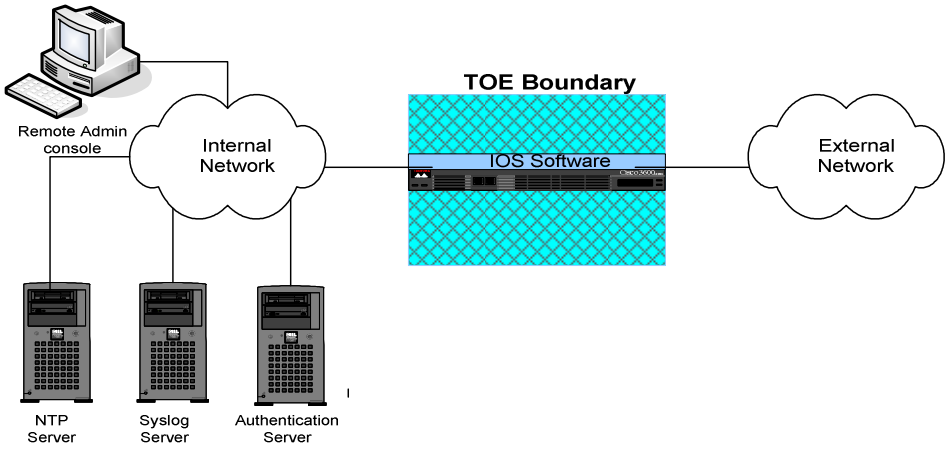
TOE	• One or more RSP720 Management Cards per chassis (Two Sup cards in one chassis provide Supervisor failover within the chassis.) • Each RSP720 running IOS 15.1(3)S3 (FIPS validated) • RSP720 cards installed into one or more 7613, 7609-S, 7606-S, 7604 or 7603-S (Two chassis can be configured together to support HA with VSS.)Each chassis with one VPN IPSec SPA (ws-ipsec-3)Line Card • With one or more compatible line cards. See Annex B for the list of compatible cards.

The TOE can optionally connect to an NTP server on its internal network for time services. A syslog server can also be used to store audit records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

If the TOE is to be remotely administered, SSHv2 must be used for that purpose. All administrative capabilities can be performed either remotely via SSHv2 or locally using the console port. Both methods access the same Command Line Interface (CLI) functionality.

The TOE can optionally support any other line card or service module that is compatible with the supervisors and chassis models included in the TOE (See Annex B). These line cards and SMs are not security-relevant to the CC-evaluated security functional requirements.

The following figure provides a visual depiction of an example TOE deployment.



1.6 Physical Scope of the TOE

The TOE is a hardware and software solution that uses a combination of chassis, supervisor engine, IPSec Card, and line cards: the Cisco 7600 Series Routers (7613, 7609-S, 7606-S, 7604 and 7603-S) with Supervisor RSP720 (RSP720-3CXL-10GE, RSP720-3C-10GE, RSP720-3CXL-GE or RSP720-3C-GE), with Cisco IOS 15.1(3)S3 running on the Supervisor Engine, VPN IPSec SPA (ws-ipsec-3) line card, and any line cards listed in Annex B.

1.7 Logical Scope of the TOE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security audit
2. Cryptographic support
3. User data protection (Traffic Filtering / Traffic Flow Control)
4. Identification and authentication
5. Secure Management
6. Protection of the TSF
7. TOE access

These features are described in more detail in the subsections below.

1.7.1 Security Audit

The TOE generates audit messages that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: all use of the user identification mechanism; any use of the authentication mechanism; any

change in the configuration of the TOE; any matching of packets to access control entries in ACLs when traversing the TOE; and any failure of a packet to match an access control list (ACL) rule allowing traversal of the TOE. The TOE will write audit records to the local logging buffer by default and can be configured to send audit data via syslog to a remote audit server, or display to the CLI console.

1.7.2 Cryptographic Support

The TOE provides cryptography support for secure communications and protection of information when configured in FIPS mode. The crypto module is FIPS 140-2 SL2 validated, certificate number 1621. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; cryptographic hashing using SHA1; keyed-hash message authentication using HMAC-SHA1, and IPSec for authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE also implements SSHv2 for secure remote administration.

The TOE delivers VPN connections to remote entities using IPSEC. The VPN process includes remote device authentication, negotiation of specific cryptographic parameters for the session, and providing a secure connection to and from the remote device. For inbound or outbound connections with external IT entities that are capable of supporting VPN (e.g., a VPN Peer), the TOE will establish a secure connection. For other inbound or outbound traffic a secure connection will not be established.

1.7.3 Traffic Filtering (ACLs)

ACLs control whether routed IP packets are forwarded or blocked at the TOE interfaces that have been configured with IP addresses. The TOE examines each frame and packet to determine whether to forward or drop it, on the basis of criteria specified within the access lists applied to the interfaces through which the traffic would enter and leave the TOE. For those interfaces configured with Layer-3 addressing the ACLs can be configured to filter IP traffic using: the source address of the traffic; the destination address of the traffic; and the layer 3 and 4 protocol identifier. Use of Access Control Lists (ACLs) also allows restriction of remote administration connectivity to specific interfaces of the TOE so that sessions will only be accepted from approved management station addresses identified as specified by the administrator.

The TOE supports routing protocols including BGP, RIPv2, and OSPFv2 to maintain routing tables, or routing tables can configured and maintained manually. The security of the routing protocols is beyond the scope of this evaluation. Refer to the preparative procedures and operational guidance for the most secure configuration of the supported routing protocols. Since routing tables are used to determine which egress ACL is applied, the authority to modify the routing tables is restricted to authenticated administrators, and authenticated neighbor routers.

The TOE also ensures that packets transmitted from the TOE do not contain residual information from previous packets. Packets that are not the required length use zeros for padding so that residual data from previous traffic is never transmitted from the TOE.

The TOE allows VLAN connections to/from remote entities. The TOE provides the ability to identify the VLAN the network traffic is associated with. The TOE then permits or denies the network traffic based on the VLANs configured on the interface where the network traffic is received /destined. This policy is applied after the Firewall policy.

1.7.4 Identification & Authentication (Authentication)

The TOE performs authentication, using Cisco IOS platform authentication mechanisms, to authenticate access to user EXEC and privileged EXEC command modes. All users wanting to use TOE services are identified and authenticated prior to being allowed access to any of the services. Once a user attempts to access the management functionality of the TOE (via EXEC mode), the TOE prompts the user for a user name and password. Only after the administrative user presents the correct identification and authentication credentials will access to the TOE functionality be granted.

The TOE supports use of a remote AAA server (RADIUS and TACACS+) as the enforcement point for 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 RADIUS (note RADIUS only encrypts the password within the packet body, while TACACS+ encrypts the entire packet body except the header).

The TOE can be configured to display an advisory banner when administrators log in and also to terminate administrator sessions after a configured period of inactivity.

The TOE also supports authentication of other routers using router authentication supported by BGP, RIPv2, and OSPFv2. Each of these protocols supports authentication by transmission of MD5-hashed password strings, which each neighbor router uses to authenticate others.

The TOE also performs device-level authentication of the remote device (VPN peers). Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates itself. Device-level authentication is performed via IKE v1/IPSec v3 mutual authentication.

1.7.5 Security Management / Access Control (Authorization)

The TOE allows authorized administrators to add new administrators, create, modify, or delete configuration details such as interface parameters and ACLs, and to modify and set the time and date.

The TOE router platform maintains privileged and semi-privileged administrator roles. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15 (has all privileges on the box); and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. The term "authorized administrator" is used in this ST to refer to any user which has been assigned to a privilege level is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions.

The TOE also supports external IT entities. These external IT entities are peer routers that pass network control information (e.g., routing tables) to the TOE. Also included are any other VPN peers with whom the TOE exchanges information, including VPN clients and VPN gateways.

1.7.6 Protection of the TSF

The TOE provides secure transmission when TSF data is transmitted between separate parts of the TOE (encrypted sessions for remote administration (via SSHv2)). The TOE is also able to detect replay of information and/or operations. The detection applied to network packets that are terminated at the TOE, such as trusted communications between the administrators to TOE, IT entity (e.g., authentication server) to TOE. If replay is detected, the packets are discarded. In addition, the TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to TOE generated audit records. Alternatively, an NTP server can be used to synchronize the clock.

Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

1.7.7 TOE Access

The TOE can terminate inactive sessions after an authorized administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

1.8 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 5: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation on the router.	This mode of operation includes non-FIPS allowed operations.

The TOE provides VPN services in the evaluated configuration. However, only some aspects of VPN were subject to evaluation. Specifically, only IPsec features of the TOE were evaluated. (See FCS_IPSEC_EXT.1.)

The Cisco IOS contains a collection of features that build on the core components of the system.

Features enabled by default that must be disabled in the evaluated configuration:

- Telnet: Sends authentication data in plain text. This feature is enabled by default and must be disabled in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target.

Features disabled by default that must remain disabled in the evaluated configuration:

- SNMP does not enforce the required role privileges. This feature is disabled by default and cannot be configured for use in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target.
- HTTP Server for web user interface management: Sends authentication data in plain text and does not enforce the required role privileges. Not including this feature does not interfere with the management of TOE as defined in the Security Target.
- IEEE 802.11 Wireless Standards: The evaluated configuration of 7600 Routers as described is this Security Target does not support implementing wireless local area network. Use of this feature requires additional hardware beyond what is included in the evaluated configuration.
- MAC address filtering: The SFPs in the Security Target are defined as information flow polices, not access polices that allow access based on MAC address
- Flexible NetFlow: Used for a traffic analysis and optimization, and SFRs do not include performance/optimization features. Not including this feature does not interfere with the enforcement of the security policies as defined in the Security Target.
- The Network Assistant application and CiscoWorks LAN Management Solutions are separate licensed, separate products and are not included in the scope of this evaluation.

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

1.9 TOE Documentation

This section identifies the guidance documentation for the TOE:

- Preparative Procedures and Operational Guidance for the Common Criteria EAL2 Evaluated 7600 Series Routers with IOS 15.1(3)S3, and the public Cisco documentation referenced within.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The ST and the TOE it describes are conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009
  - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2 Augmented (ALC_FLR.2 and ALC_DVS.1)

2.2 Protection Profile Conformance

This ST and TOE it describes is not claiming conformance to any Protection Profile.

3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 6: TOE Assumptions

Assumptions (Personnel)	Assumption Definition
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.
Assumptions (Physical)	**Assumption Definition**
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
Assumptions (Operational)	**Assumption Definition**
A.CONFIDENTIALITY	Copies of TOE configuration data including representations of authentication data maintained off the TOE in hard-copy or soft-copy will be kept confidential and access will be limited to authorized administrators. Audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic.
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

Assumptions (Personnel)	Assumption Definition
	considered low.

3.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Basic.

Table 7: Threats

Threat	Threat Definition
T.AUDIT_REVIEW	Actions performed by users may not be known to the administrators due to actions not being recorded locally or remotely in a manner suitable for allow interpretation of the messages.
T.MEDIATE	An unauthorized entity may send impermissible information through the TOE which results in the exploitation of the recipient of the network traffic.
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 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	Evidence of a compromise or malfunction of the TOE may go unnoticed or not be properly traceable if recorded events are not properly sequenced through application of correct timestamps.
T.USER_DATA_REUSE	User data that is temporarily retained by the TOE in the course of processing network traffic could be inadvertently re-used in sending network traffic to a destination other than intended by the sender of the original network traffic.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

Table 8: Organizational Security Policies

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4 SECURITY OBJECTIVES

This Chapter identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

- This document identifies objectives of the TOE as O.objective with objective specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with objective specifying a unique name.

4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 9: Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
O.ACCESS_CONTROL	The TOE will restrict access to the TOE Management functions to the authorized 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 authorized administrators the capability to review audit data, and to configure the TOE to transmit audit messages to a remote syslog server.
O.CFG_MANAGE	The TOE will provide management tools/applications to allow authorized 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 must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.STARTUP_TEST	The TOE will perform initial startup tests upon bootup of the system.
O.TIME	The TOE will provide a reliable time stamp for its own use.

TOE Objective	TOE Security Objective Definition
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.

4.2 Security Objectives for the Environment

All of the assumptions stated in Section 3.1 are considered to be security objectives for the environment. The following are the non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 10: Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.AUDIT_REVIEW	Administrators will be trained to periodically review the audit logs to identify sources of concern, and will make a syslog server available for use by the TOE and TOE administrators.
OE.CONFIDENTIALITY	The hard copy documents and soft-copy representations 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. Audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic.
OE.INTEROPERABILITY	The TOE will be able to function with the software and hardware of other vendors on the network when the TOE administrators follow software and hardware interoperability guidance provided by the manufacturer.
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.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, dated: July 2009* and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [[***selected-assignment***]]).
- Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
- Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number placed at the end of the component. For example FCS_COP.1(1) and CFS_COP.1(2) indicate that the ST includes two iterations of the FCS_COP.1 requirement, (1) and (2).
- Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Extended Requirements (i.e., those not found in Part 2 of the CC) are identified with "_EXT" in of the functional class/name.
- Other sections of the ST use bolding to highlight text of special interest, such as captions.

5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 11: Security Functional Requirements

Functional Component	
Requirement Class	**Requirement Component**
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_STG.1: Protected audit trail storage
FCS: Cryptographic support	FCS_CKM.1(1): Cryptographic key generation - RSA

Functional Component	
	FCS_CKM.1(2): Cryptographic key generation - AES
	FCS_CKM.4: Cryptographic Key Destruction
	FCS_COP.1(1): Cryptographic operation (for RSA data encryption/decryption)
	FCS_COP.1(2): Cryptographic operation (for AES data encryption/decryption)
	FCS_COP.1(3): Cryptographic operation (for RNG)
	FCS_COP.1(4) Cryptographic operation (for MD5 hashing)
	FCS_COP.1(5): Cryptographic operation (for cryptographic hashing)
	FCS_COP.1(6): Cryptographic operation (for keyed-hash message authentication)
	FCS_IPSEC_EXT.1: IPSEC
	FCS_SSH_EXT.1: SSH
FDP: User data protection	FDP_IFC.1 Subset Information Flow Control - ACL
	FDP_IFF.1 Simple Security Attributes – ACL
	FDP_RIP.2: Full residual information protection
FIA: Identification and authentication	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UAU.5: Multiple Authentication Mechanisms
	FIA_UAU.7: Protected authentication feedback
	FIA_UID.2 User identification before any action
FMT: Security management	FMT_MOF.1 Management of Security Functions Behavior
	FMT_MSA.2 Secure 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: Protection of the TSF	FPT_RPL.1: Replay detection
	FPT_STM.1: Reliable time stamps
	FPT_TST_EXT.1: TSF testing
FTA: TOE Access	FTA_SSL.3: TSF-initiated termination
	FTA_TAB.1: Default TOE Access Banners

5.2.1 Security audit (FAU)

5.2.1.1 FAU_GEN.1: Audit data generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [***not specified***] level of audit **specified in Table 12**; and

c) [**no additional events**].

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

a) Date* and time of the event, type of event, subject identity (if applicable), 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 12**].

Table 12: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_SAR.1	None.	
FCS_IPSEC _EXT.1	Failure to establish an IPSEC session Establishment/Termination of an IPSEC session	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_SSH_EXT.1	Failure to establish an SSH session Establishment/Termination of an SSH session	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_IFC.1	None	
FDP_IFF.1	All decisions on requests for information flow.	None.
FIA_UAU.2	All use of the authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.5	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UID.2	All use of the identification mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	None.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security attributes.	None.
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TST_EXT.1	Indication that TSF self-test was completed.	Any additional information generated by the tests beyond "success" or "failure".

5.2.1.2 FAU_GEN.2: User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [**the privileged administrator, and semi-privileged administrator with appropriate privileges**] with the capability to read [**all TOE audit trail data**] from the audit records.

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

5.2.1.4 FAU_STG.1 Protected audit trail storage

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

FAU_STG.1.2 The TSF shall be able to [***prevent***] ~~**unauthorized**~~ modifications to the stored audit records in the audit trail.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 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 [**1024-bits and 2048-bits**] that meet the following: [**FIPS 186-3**].

5.2.2.2 FCS_CKM.1(2) Cryptographic key generation – AES

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**DRBG using AES**] and specified cryptographic key sizes [**128-bits, 192-bits, 256-bits**] that meet the following: [**RNG as specified in FCS_COP.1(3)**].

5.2.2.3 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 [**cryptographic key zeroization**] that meets the following: [**FIPS 140-2 level 2**].

5.2.2.4 FCS_COP.1(1) Cryptographic operation (for RSA encryption/decryption)

FCS_COP.1.1(1) The TSF shall perform [**encryption and decryption of keying material**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**1024-bits and 2048-bits**] that meet the following: [**FIPS 140-2**].

5.2.2.5 FCS_COP.1(2) Cryptographic operation (for AES encryption/decryption)

FCS_COP.1.1(2) The TSF shall perform [**encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES operating in CBC mode**] and cryptographic key sizes [**128-bits, 192-bits, 256-bits**] that meets the following:[

- **FIPS PUB 197, "Advanced Encryption Standard (AES)";**
- **NIST SP 800-38A; and**
- **"AES KeyWrap Standard"**].

5.2.2.6 FCS_COP.1(3) Cryptographic operation (for RNG)

FCS_COP.1.1(3) The TSF shall perform [**Random Number Generation**] in accordance with a specified cryptographic algorithm [**RNG using AES**] and cryptographic key size [**256-bits**] that meet the following: [**SP 800-90 DRBG as specified in FIPS 140-2 Annex C**].

5.2.2.7 FCS_COP.1(4) Cryptographic operation (for MD5 hashing)

FCS_COP.1.1(4) The TSF shall perform [**secure hash (message digest)**] in accordance with a specified cryptographic algorithm: [**MD5**] and **message digest** sizes [**128-bit hash value**] that meet the following: [**RFC 1321**].

5.2.2.1 FCS_COP.1(5) Cryptographic operation (for cryptographic hashing)

FCS_COP.1.1(5) The TSF shall perform [**cryptographic hashing services**] in accordance with a specified cryptographic algorithm [**SHA-1]** and ~~**cryptographic key**~~ **message digest** sizes [**160 bits**] that meet the following: [**FIPS Pub 180-3 "Secure Hash Standard"**]

5.2.2.2 FCS_COP.1(6): Cryptographic operation (for keyed-hash message authentication)

FCS_COP.1.1(6) The TSF shall perform [**keyed-hash message authentication**] in accordance with a specified cryptographic algorithm [**HMAC-SHA-1**], and ~~**cryptographic key**~~ **resulting message digest** size [**160 bits**] that meet the following: [**FIPS Pub 198-1 "The Keyed-Hash Message Authentication Code", and FIPS PUB 180-3, "Secure Hash Standard."**]

5.2.2.3 FCS_IPSEC_EXT.1: IPSEC

FCS_IPSEC_EXT.1.1 The TSF shall implement IPSec using the ESP protocol as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), and using IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109, to establish the security association.

FCS_IPSEC_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

FCS_IPSEC_EXT.1.4 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to an administratively configurable number of kilobytes including the range from 100 - 200 MB of traffic for Phase 2 SAs.

FCS_IPSEC_EXT.1.5 The TSF shall ensure that all IKE protocols implement DH Groups 1, 2, and 5.

FCS_IPSEC_EXT.1.6 The TSF shall ensure that all IKE protocols implement Peer Authentication using the rDSA algorithm.

FCS_IPSEC_EXT.1.7 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its IPSec connections.

FCS_IPSEC_EXT.1.8 The TSF shall support the following:

- Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")");
- Pre-shared keys of 22 characters.

5.2.2.4 FCS_SSH_EXT.1 SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed upon request from the SSH client.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of 120 seconds, and provide a limit to the number of failed authentication attempts a client may perform in a single session to 3 attempts.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: password-based.

FCS_SSH_EXT.1.5 The TSF shall ensure that packets greater than 35,000 bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms AES-CBC-128, AES-CBC-256.

FCS_SSH_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH_RSA as its public key algorithm(s).

FCS_SSH_EXT.1.8 The TSF shall ensure that data integrity algorithms used in the SSH transport connection is hmac-sha1, hmac-sha1-96.

FCS_SSH_EXT.1.9 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.2.3 User data protection (FDP)

5.2.3.1 FDP_IFC.1 Subset Information Flow Control – ACL

FDP_IFC.1.1 The TSF shall enforce the [**ACL SFP**] on: [

a) **subjects: Layer 3 ports (i.e. any interface configured with an IP address including physical copper, fiber interface, or virtual interface)**
b) **information: IP packets**
c) **operation: forward or drop the packets**].

5.2.3.2 FDP_IFF.1 Simple Security Attributes - ACL

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

a) security subject attributes:

- **Interface ID (e.g. physical slot/port identifier, logical port-channel identifier, or VLAN identifier)**
- **IP address assigned to the interface**

b) security information attributes:

- **presumed IP address of the packet source;**
- **presumed IP address of the packet destination;**
- **transport layer protocol number (e.g. UDP, TCP);**
- **network layer protocol number (e.g. IPv4, IPv6, ICMPv4, ICMPv6, ESP, AH, etc.)**
- **ICMP type**
- **VLAN ID in Packet Header**].

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

a) External entities 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 (Cisco IOS IP ACLs), 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) External entities 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 (Cisco IOS IP ACLs), 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**

c) **There is no previous matching rule in the access list that denies the flow**

d) **For VLANS: if the receiving VLAN interface is configured to be in the same VLAN as the transmitting VLAN interface; or**

e) **For VLANS: the frames have been received into the VLAN through traffic flow controls enforced at Layer 3 as defined in a, b, and c above and have the appropriate VLAN ID included in the traffic header**].

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

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [**none**].

FDP_IFF.1.5 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**].

5.2.3.3 FDP_RIP.2: Full residual information protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] all objects.

5.2.4 Identification and authentication (FIA)

5.2.4.1 FIA_ATD.1 User Attribute Definition

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

For interactive users:

a) **user identity;**

b) **privilege levels; and**

c) password.

For neighbor routers:

d) IP address; and

e) password

For VPN peers:

f) subject identity (IP address/Host Name);

g) IKE Security Attributes (IPaddress of destination, receiving/transmitting interface, transport protocol].

5.2.4.2 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

5.2.4.3 FIA_UAU.5: Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide a [**local password-based authentication mechanism, support remote password-based authentication via RADIUS and TACACS+, and device-level authentication with a trusted peer via IKE/IPSEC**] to perform user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**administratively-defined sequence in which authentication mechanisms should be used**].

5.2.4.4 FIA_UAU.7: Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide ~~only~~ [**no feedback, nor any locally visible representation of the user-entered password**] to the user while the authentication is in progress.

5.2.4.5 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.

5.2.5 Security management (FMT)

5.2.5.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [***determine the behavior of, enable, disable, and modify the behavior of***] the functions [

a) Audit trail (create, delete, empty, review)

b) Network traffic (information flow) rules (create, delete, modify, and view)
c) Routing tables (create, modify, delete)
d) Session inactivity (set, modify threshold limits)
e) Time determination (set, change date/timestamp)
f) TSF self test (TOE and cryptographic module)
g) IPSec and SSH configurations (create, modify, delete)] to [**privileged administrator, and semi-privileged administrator with appropriate privileges**].

5.2.5.2 FMT_MSA.2 Secure Attribute Initialization

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [**security attributes that are considered in the ACL SFP**].

5.2.5.3 FMT_MSA.3 Static Attribute Initialization

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

FMT_MSA.3.2 The TSF shall allow the [**privileged administrator, and semi-privileged administrator with appropriate privileges**] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [***modify***] the [**all TOE data**] to [**the privileged administrator, and semi-privileged administrator with appropriate privileges**].

5.2.5.5 FMT_SMF.1 Specification of Management Functions

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

a) Ability to manage the cryptographic functionality
b) Ability to manage the audit logs and functions
c) Ability to manage information flow control attributes
d) Ability to manage routing tables
e) Ability to manage security attributes belonging to individual users
f) Ability to manage the default values of the security attributes
g) Ability to manage the warning banner message and content
h) Ability to manage the time limits of session inactivity
i) Ability to manage the date and timestamp
j) Ability to run cryptographic self-tests

k) Ability to manage VLAN configuration].

5.2.5.6 FMT_SMR.1 Security Roles

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

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

Application note: The term "authorized administrator" is used in this ST to refer to any user which has been granted rights equivalent to a privileged administrator or semi-privileged administrator.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 FPT_RPL.1: Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [**network packets terminated at the TOE**].

FPT_RPL.1.2 The TSF shall perform [**reject the data**] when replay is detected.

5.2.6.2 FPT_STM.1: Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.6.3 FPT_TST_EXT.1: TSF testing

FPT_TST_EXT.1.1 The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

5.2.7 TOE Access (FTA)

5.2.7.1 FTA_SSL.3: TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**authorized-administrator-configurable time interval of session inactivity**].

5.2.7.2 FTA_TAB.1: Default TOE Access Banners

FTA_TAB.1.1 Before establishing a **local or remote ~~user~~ administrator** session the TSF shall display an **authorized-administrator-specified** advisory **notice and consent** warning message regarding unauthorized use of the TOE.

5.3 Extended Components Definition

This Security Target includes Security Functional Requirements (SFR) that are not drawn from existing CC Part 2. The Extended SFRs are identified by having a label '_EXT' after the requirement name for TOE SFRs. The structure of the extended SFRs is modeled after the SFRs included in CC Part 2. The structure is as follows:

A. Class – The extended SFRs included in this ST are part of the identified classes of requirements.

B. Family – The extended SFRs included in this ST are part of several SFR families

C. Component – The extended SFRs are not hierarchical to any other components, though they may have identifiers terminating on other than "1". The dependencies for each extended component are identified in the TOE SFR Dependencies section of this ST below.

D. The management requirements, if any, associated with the extended SFRs are incorporated into the Security management SFRs defined in this ST.

E. The audit requirements, if any, associated with the extended SFRs are incorporated into the Security audit SFRs defined in this ST.

F. The dependency requirements, if any, associated with the extended SFRs are identified in the dependency rationale and mapping section of the ST (Table 13).

Extended Requirements Rationale:

FCS_IPSEC_EXT.1: This SFR was modeled from the NDPP – where it is defined as a requirement specific to IPSEC protocol supported by the TOE. The IPSec protocol is used to secure communications between the TOE and the endpoints; mainly remote administration. Securing the communication channel provides interoperability and resistance to cryptographic attack by means of two-way authentication of each endpoint. Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's implementation of the protocol as well as the specifics detailed in the NDPP. Given that this is a validated US Government Protection Profile the rationale for use of this extended requirement is deemed acceptable.

FCS_SSH_EXT.1: This SFR was modeled from NDPP – where it is defined as a requirement specific to SSH protocol supported by the TOE. The SSH protocol is used to secure communications between the TOE and the endpoints; mainly remote administration. Securing the communication channel provides interoperability and resistance to cryptographic attack by means of two-way authentication of each endpoint. Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's implementation of the protocol as well as the specifics detailed in the NDPP. Given that this is a validated US Government Protection Profile the rationale for use of this extended requirement is deemed acceptable.

FPT_TST_EXT.1: This SFR was modeled from NDPP – where it is defined as a requirement for TSF self tests of the TOE during initialization (on bootup) that allows for the detection of failures of the underlying security mechanisms prior to the TOE becoming operational. Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's comprehensive set of self tests. Given this is a validated US Government Protection Profile the rationale for use of this extended requirement is deemed acceptable.

5.4 TOE SFR Dependencies Rationale

Table 13: SFR Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Met by FAU_GEN. Met by FIA_UID.2
FAU_SAR.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_STG.1	FAU_GEN.1	Met by FAU_GEN.1
FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Met by FCS_COP.1(1) Met by FCS_CKM.4
FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Met by FCS_COP.1(2) Met by FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Met by FCS_CKM.1
FCS_COP.1(1)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Met by FCS_CKM.1(1) and FCS_CKM.4
FCS_COP.1(2)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	Met by FCS_CKM.1(2) and FCS_CKM.4
FCS_COP.1(3)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	See rationale below for FCS_COP.(3) FCS_CKM.4
FCS_COP.1(4)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	See rationale below for FCS_COP.(4) FCS_CKM.4
FCS_COP.1(5)	FDP_ITC.1 or 2 or FCS_CKM.1 FCS_CKM.4	See rationale below for FCS_COP.(5) FCS_CKM.4
FCS_COP.1(6)	FDP_ITC.1 or 2 or	See rationale below for FCS_COP.(6)

SFR	Dependency	Rationale
	FCS_CKM.1 FCS_CKM.4	FCS_CKM.4
FCS_IPSEC_EXT.1	FCS_COP.1	Met by FCS_COP.1(1), (2), (3), (5), and (6)
FCS_SSH_EXT.1	FCS_COP.1	Met by FCS_COP.1(1), (2), (3), (5), and (6)
FDP_IFC.1	FDP_IFF.1	Met by FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1 and FMT_MSA.3
FDP_RIP.2	No dependencies	N/A
FIA_ATD.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1	Met by FIA_UID.2
FIA_UAU.5	No dependencies	N/A
FIA_UAU.7	FIA_UAU.1	Met by FIA_UAU.2
FIA_UID.2	No dependencies	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Met by SMT_SMF.1 and FMT_SMR.1
FMT_MSA.2	FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	Met by FDP_IFC.1 FMT_SMR.1 See rationale below regarding FMT_MSA.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Met by FMT_SMR.1 See rationale below regarding FMT_MSA.1
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Met by FMT_SMF.1 Met by FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	Met by FIA_UID.2
FPT_RPL.1	No dependencies	N/A
FPT_STM.1	No dependencies	N/A
FPT_TST_EXT.1	No dependencies	N/A
FTA_SSL.3	No dependencies	N/A
FTA_TAB.1	No dependencies	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.1 more than adequately satisfies the concerns of leaving FMT_MSA.1 out of this Security Target.

Functional components FCS_COP.1(3) (RNG), FCS_COP.1(4) (MD5), FCS_COP.1(5) (cryptographic hashing), and FCS_COP.1(6) (keyed-hash message

authentication), do not require the dependency on FCS_CKM.1 because their cryptographic operations do not require key generation.

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

The TOE assurance requirements for this ST are EAL2 Augmented with ALC_FLR.2 and ALC_DVS.1 derived from Common Criteria Version 3.1, Revision 3. The assurance requirements are summarized in the table below.

Table 14: Assurance Measures

Assurance Class	Components	Components Description
DEVELOPMENT	ADV_ARC.1	Security Architectural Description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
GUIDANCE DOCUMENTS	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
LIFE CYCLE SUPPORT	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw remediation procedures
TESTS	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
VULNERABILITY ASSESSMENT	AVA_VAN.2	Vulnerability analysis

5.5.2 Security Assurance Requirements Rationale

This Security Target claims conformance to EAL2 Augmented with ALC_FLR.2 and ALC_DVS.1. This target was chosen to ensure that the TOE has a moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks. Augmentation was chosen to address secure design practices for the TOE and having flaw remediation procedures and correcting security flaws as they are reported.

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

Table 15: Assurance Measures

Component	How requirement will be met
ADV_ARC.1	The architecture description provides the justification how the security functional requirements are enforced, how the security features (functions) cannot be bypassed, and how the TOE protects itself from tampering by untrusted active entities. The architecture description also identifies the system initialization components and the processing that occurs when the TOE is brought into a secure state (e.g. transition form a down state to the initial secure state (operational)).

Component	How requirement will be met
ADV_FSP.2	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
ADV_TDS.1	The TOE design describes the TOE security functional (TSF) boundary and how the TSF implements the security functional requirements. The design description includes the decomposition of the TOE into subsystems and/or modules, thus providing the purpose of the subsystem/module, the behavior of the subsystem/module and the actions the subsystem/module performs. The description also identifies the subsystem/module as SFR (security function requirement) enforcing, SFR supporting, or SFR non-interfering; thus identifying the interfaces as described in the functional specification. In addition, the TOE design describes the interactions among or between the subsystems/modules; thus providing a description of what the TOE is doing and how.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.2 ALC_CMS.2	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ALC_DEL.1	The Delivery document describes the delivery procedures for the TOE to include the procedure on how to download certain components of the TOE from the Cisco website and how certain components of the TOE are physically delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components.
ALC_DVS.1 ALC_FLR.2	The Lifecycle document(s) describes the security measures and controls that are in place at the development site(s), the security measures and controls that are in place regarding employees, and the security measures and controls that are in place during the development and maintenance of the TOE. These procedures also include the flaw remediation and reporting procedures so that security flaw reports from TOE users can be appropriately acted upon, and TOE users can understand how to submit security flaw reports to the developer.
ATE_COV.1 ATE_FUN.1	The Test document(s) consist of a test plan describes the test configuration, the approach to testing, and how the TSFI (TOE security function interfaces) has been tested against its functional specification as described in the TOE design and the security architecture description. The test document(s) also include the test cases/procedures that show the test steps and expected results, specify the actions and parameters that were applied to the interfaces, as well as how the expected results should be verified and what they are. Actual results are also included in the set of Test documents.
ATE_IND.2	Cisco will provide the TOE for testing.
AVA_VAN.2	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

This section identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 16: How TOE SFRs are Met

TOE SFRs	How the SFR is Met
FAU_GEN.1	The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include events related to the enforcement of information flow policies, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table"). Each of the events is specified in the audit record is in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited. The audit trail consist of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. As noted above, the information includes [at least] all of the required information. Additional information can be configured and included if desired. Refer to the Guidance documentation for configuration syntax and information. The logging buffer size can be configured from a range of 4096 (default) to 2147483647 bytes. It is noted, not make the buffer size too large because the router could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the router. However, this value is the maximum available, and the buffer size should not be set to this amount. Refer to the Guidance documentation for configuration syntax and information. The administrator can also configure a 'configuration logger' to keep track of configuration changes made with the command-line interface (CLI). The administrator can configure the size of the configuration log from 1 to 1000 entries (the default is 100). Refer to the Guidance documentation for configuration syntax and information. The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc; all of which are described in the Guidance documents and IOS CLI. The logs can be saved to flash memory so records are not lost in case of failures or restarts. Refer to the Guidance documentation for configuration syntax and information. The administrator can set the level of the audit records to be displayed on the console or sent to the syslog server. For instance all emergency, alerts, critical, errors, and warning message can be sent to the console as an immediate indicator

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>of a generated syslog event. All notifications and information type message can be sent to the syslog server, as message is only for information; router functionality is not affected. Note that audit records are transmitted in the clear to the syslog server, though it is stated the syslog server is attached to the internal (isolated and protected) network.

<table>
<tr><th>Auditable Event</th><th>Rationale</th></tr>
<tr><td>All use of the user identification mechanism.</td><td>Events will be generated for attempted identification/ authentication, and the username attempting to authenticate and source address or interface will be included in the log record.</td></tr>
<tr><td>Any use of the authentication mechanism.</td><td>Events will be generated for attempted identification/ authentication, and the username attempting to authenticate will be included in the log record, along with the origin or source of the attempt.</td></tr>
<tr><td>Management functions</td><td>The use of the security management functions is logged; modifications of the behavior of the functions in the TSF and modifications of default settings.</td></tr>
<tr><td>Changes to the time.</td><td>Changes to the time are logged.</td></tr>
<tr><td>Failure to establish and/or establishment/failure of an IPSEC session</td><td>Attempts to establish an IPSEC session or the failure of an established IPSEC tunnel is logged.</td></tr>
<tr><td>Failure to establish and/or establishment/failure of an SSH session</td><td>Attempts to establish an SSH session or the failure of an established SSH is logged.</td></tr>
<tr><td>All decisions on requests for information flow.</td><td>The use of access lists with logging keywords results in the logging of all access requests that match that acl.</td></tr>
<tr><td>Indication that TSF self-test was completed.</td><td>During bootup, if the self test fails, the failure is logged.</td></tr>
</table></td></tr>
<tr><td>FAU_GEN.2</td><td>The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. For example a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. Refer to the Guidance documentation for configuration syntax and information.</td></tr>
<tr><td>FAU_SAR.1</td><td>The TOE provides the interface for the authorized administrator to read all of the TOE audit records. The records include the information described in FAU_GEN.1 above. Refer to the Guidance documentation for commands,</td></tr>
</table>

TOE SFRs	How the SFR is Met
	configuration syntax and information related to viewing of the audit log files.
FAU_STG.1	Through the TOE CLI administrative interface, the TOE provides the ability for privileged administrators to delete audit records stored within the TOE. The TOE provides dedicated CLI commands that are only available to the privileged administrator to facilitate the deletion of audit records. The local events cannot be altered by any users or mechanisms.
FCS_CKM.1(1) FCS_COP.1(1)	The TOE generates RSA key establishment schemes conformant with FIPS 186-3 (Refer to FIPS 140-2 certificate #1621). RSA keys are used for encryption and decryption of keying material in SSHv2 used for remote administration of the TOE.
FCS_CKM.1(2) FCS_COP.1(2) FCS_COP.1(3)	AES is used for RADIUS KeyWrap. The TOE provides key generation for AES 128-bit and 256-bit keys using a Random Number Generator that meets NIST SP 800-90 DRBG as specified in FIPS 140-2 Annex C. The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128, 192, 256 bits) as described in FIPS PUB 197, "Advanced Encryption Standard (AES)" and NIST SP 800-38A. (Refer to FIPS 140-2 certificate #1621)
FCS_CKM.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys through the module securely administering both cryptographic keys and other critical security parameters (CSPs) such as passwords. (Refer to FIPS 140-2 certificate #1621).
FCS_COP.1(4)	The TOE provides MD5 hashing as specified in RFC 1321 for authentication of neighbor routers via BGP, RIPv2, and OSPFv2 with shared passwords.
FCS_COP.1(5)	The TOE provides cryptographic hashing services using SHA-1that meets FIPS Pub 180-3 "Secure Hash Standard".
FCS_COP.1(6)	The TOE uses HMAC-SHA1 message authentication that meets FIPS Pub 198-1 "The Keyed-Hash Message Authentication Code", and FIPS PUB 180-3, "Secure Hash Standard".
FCS_IPSEC_EXT.1	The TOE implements IPSec (on both IPv4 and IPv6) to provide authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE implementation of the IPSec standard (in accordance with the RFCs noted in the SFR) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services. IPSec Internet Key Exchange, also called ISAKMP, is the negotiation protocol that lets two peers agree on how to build an IPSec SA. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPSec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPSec peers that is also used to manage IPSec connections, including: • The negotiation of mutually acceptable IPSec options between peers, • The establishment of additional Security Associations to protect packets flows using ESP, and • The agreement of secure bulk data encryption AES (128 and 256 bit) keys for use with ESP. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation.

TOE SFRs	How the SFR is Met
FCS_SSH_EXT.1	The TOE implements SSHv2 (telnet is disabled in the evaluated configuration). SSHv2 sessions are limited to a configurable session timeout period of 120 seconds, a maximum number of failed authentication attempts limited to 3, and will be rekeyed upon request from the SSH client. SSH connections will be dropped if the TOE receives a packet larger than 35,000 bytes. The TOE's implementation of SSHv2 supports hashing algorithms hmac-sha1, and hmac-sha1-96.
FDP_IFC.1 FDP_IFF.1	The TOE controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator in the IP flow control policies. Within an ACL, the first entry in the ACL that matches the inspected traffic is the rule that's applied. ACLs can be applied inbound to an interface an/or outbound from an interface. All ACLs applicable to a traffic flow through the TOE applied in the order in which they're encountered, i.e. any inbound ACL is applied to the traffic flow when the packet is received and any outbound ACL is applied before the packet is transmitted. For routed traffic, the outbound interface is determined by the routing table. Use of routing protocols specified as permitted in the TOE description (BGP, OSPF, and RIPv2), does not interfere with the inspection of packets and proper enforcement of rules defined in FDP_IFF.1. Use of the routing table is required to determine the proper egress port for IP traffic flows, and thus which, if any, outbound ACL will be applied to the traffic flow, and static or dynamic updates to the routing table are expected and consistent with proper enforcement of traffic flow controls for Layer 3 traffic. Since routing tables are used to determine which egress ACL is applied, the authority to modify the routing tables is restricted to authenticated administrators, and authenticated neighbor routers. After the inbound Firewall rules are implemented, the VLAN rules are enforced. This means that if a packet is dropped based on the configured firewall rule set, then the packet will be dropped before undergoing VLAN processing. The TOE facilitates VLAN connections with other connected devices by supporting VLANs and VLAN configuration on TOE interfaces. When network traffic is received by a TOE interface that has been made part of a VLAN, the TOE verifies the VLAN ID included in the traffic header. If the VLAN ID in the traffic header matches the receiving TOE interface VLAN ID, then the traffic is permitted. If the VLAN ID in the packet header does not match the VLAN ID on the TOE receiving interface, the traffic is not permitted. Packets are only forwarded if the VLANs match the configured VLANs. For example, if interface A is part of vlan 100 but received traffic that was tagged for vlan 200, if would not be permitted. If the traffic matches the VLAN ID, it is sent on to the destination interface that is also part of the VLAN. There the VLAN tag is removed and the traffic passes on for egress firewall rule enforcement. Traffic arriving directly at a VLAN configured interface without a VLAN tag is tagged with the VLAN ID assigned to the port and passed into the VLAN, and traffic leaving via a VLAN configured (non-trunk) interface has the VLAN tag stripped and is sent on for egress firewall processing. The exception for both inbound and outbound traffic is a TOE interface that is a trunk port that links a VLAN across networking devices. In this case, for traffic arriving, the interface can be configured to accept multiple vlan tags and pass them on to the appropriate vlan internally for further processing as described above. For outbound traffic at the trunk, the vlan header is retained for parsing on

TOE SFRs	How the SFR is Met
	the receiving system.
FDP_RIP.2	The TOE ensures that packets transmitted from the TOE do not contain residual information from previous packets. Packets that are not the required length use zeros for padding. Residual data is never transmitted from the TOE. Once packet handling is completed its content is overwritten before memory buffer which previously contained the packet is reused. This applies to traffic destined to or through the TOE.
FIA_ATD.1	The TOE maintains and manages the following user security attributes; user identity, privilege levels (roles), and password. The user name and password are used by the TOE to identify and authenticate an administrator wishing to gain access to the TOE management functionality. The role is used by the TOE to allow an authenticated user to assume a predefined TOE role and perform specific management functions. For neighbor routers, which do not have access to the interactive admin interface, the attributes maintained are IP address and password, which are used to authenticate the remote router for exchange of routing table information. For each vpn peer, the TOE maintains the identity of the vpn peer and its IKE security attributes.
FIA_UAU.2 FIA_UID.2	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through the TOE's CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE through either a directly connected console or remotely through an SSHv2 connection, the TOE prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. The TOE stores all passwords in encrypted format using AES. In addition, all pre-shared and symmetric keys are stored in encrypted form using AES encryption to prevent access. This functionality is configured on the TOE using the 'service password-encryption' command. For neighbor routers, which do not have access to the CLI, the neighbor router must present the correct hashed password prior to exchanging routing table updates with the TOE. The TOE authenticates the neighbor router using its supplied password hash, and the source IP address from the IP packet header.
FIA_UAU.5	The TOE can be configured to require local authentication and/or remote authentication via a RADIUS or TACACS+ server as defined in the authentication policy. Administrators can be authenticated to the local user database, or be redirected to a remote authentication server. Interfaces can be configured to try one or more remote authentication servers, then fail back to the local user database if the remote authentication servers are inaccessible. Neighbor routers are authenticated only to passwords stored locally. All TOE passwords are stored encrypted on the TOE. When RADIUS and/or

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>TACACS+ are used for authentication, then the RADIUS and/or TACACS+ clients and servers are responsible for protecting the user passwords. When RADIUS and/or TACACS+ is enabled, the router prompts for a username and password, then verifies the username and password with a RADIUS and/or TACACS+ server. For both the RADIUS and TACACS+ a hash of the password is securely stored on the RADIUS and TACACS+ servers. When a user logs in via RADIUS and/or TACACS+, the hash value of the password is sent encrypted to the RADIUS and/or TACACS+ servers to be verified. If the hash values match, then the user is allowed to login. TACACS+ encrypts the entire payload including the username and password when communicating between the client and the server.

The TOE performs device-level authentication of the remote device (VPN peers) via IKE/IPSEC. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates itself. Device-level authentication is performed via IKE v1/IPSec v3 mutual authentication.</td></tr>
<tr><td>FIA_UAU.7</td><td>When a user enters their password at the local console or via SSH, the TOE does not echo any characters of the password or any representation of the characters.</td></tr>
<tr><td>FMT_MOF.1</td><td>The TOE provides the authorized administrator the ability to perform the actions required to control the TOE, including: audit trail (create, delete, empty, review) management, network traffic (information flow) rules (create, delete, modify, and view), routing tables (create, modify, delete), session inactivity time period (set, modify threshold limits), time determination (set, change date/timestamp), TSF self test (TOE and cryptographic module), and IPSec and SSH configurations. Refer to the Guidance documentation for configuration syntax, commands, and information related to each of the functions. Some of the functions are restricted to a specific administrative role and/or to an authorized administrator with the proper permissions (level).</td></tr>
<tr><td>FMT_MSA.2</td><td>The TOE inspects the headers of incoming frames and packets to ensure that the headers and the security-relevant information they contain, such as VLAN tags and addresses, is appropriately structured, and malformed frames and packets are discarded.

The TOE’s administrative interfaces only permit valid values to be specified within administratively-defined rules for the ACL SFP. For the ACL SFP, the administrative interfaces will ensure that the administrator will only be able to associate valid (configured) VLANs with valid (configured) Layer 2 interfaces. For example, VLAN parameters such as VLAN ID, name, and type must be specified within an acceptable range.

<table><tr><td>Parameter</td><td>Default</td><td>Range</td></tr><tr><td>VLAN ID</td><td>1</td><td>1–4094</td></tr></table>
In addition, the administrative interfaces will ensure that the administrator will only be able to associate a single outbound IP ACL, and/or a single inbound IP ACL on any one Layer 3 interface. Further, the administrative interface will ensure that only valid values are permitted for security relevant information and subject attributes in ACLs, including valid IP address formats, masks, protocol identifiers, and port numbers.</td></tr>
<tr><td>FMT_MSA.3</td><td>The default TOE SFP is restrictive within the TOE. The flow control policies must be administratively configured to be restrictive. When no ACLs have been</td></tr>
</table>

TOE SFRs	How the SFR is Met
	explicitly created and applied to interfaces, IP traffic is allowed to flow between subnets as defined in the routing table. The TOE only permits the authorized administrators to specify the flow control policies rules used to enforce the SFP through the administrative interface.
FMT_MTD.1	The TOE provides the ability for administrators to modify TOE data, such as audit settings, configuration data, security attributes, information flow rules, routing tables, and session thresholds. Each of the predefined and administratively configured roles has create modify access to this TOE data.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The administrative user can connect to the TOE using the CLI to perform these functions via SSHv2, a terminal server, or at the local console. Rrefer to the Guidance documentation for configuration syntax, commands, and information related to each of these functions. The management functionality provided by the TOE include the following administrative functions: • Ability to manage the cryptographic functionality - allows the authorized administrator the ability to identify and configure the algorithms used to provide protection of the data • Ability to manage the audit logs and functions - allows the authorized administrator to configure the audit logs, view the audit logs, and to clear the audit logs • Ability to manage information flow control attributes - allows the authorized administrator to configure the ACLs, to control the Ethernet and IP network traffic • Ability to manage routing tables - allows the authorized administrator the ability to create, modify, and delete the routing tables to control the routed network traffic • Ability to manage security attributes belonging to individual users - allows the authorized administrator to create, modify, and delete other administrative users • Ability to manage the default values of the security attributes - allows the authorized administrator to specify the attributes that are used control access and/or manage users • Ability to manage the warning banner message and content – allows the authorized administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users • Ability to manage the time limits of session inactivity – allows the authorized administrator the ability to set and modify the inactivity time threshold • Ability to manage the date and time maintained by the TSF – allows the authorized administrator the ability to set and modify the system clock, as well as to configure the NTP setting of the TOE. • Ability to run cryptographic self-tests – allows the authorized

TOE SFRs	How the SFR is Met
	administrator to cause the system to shutdown. • Ability to manage VLAN configuration – this allows for the configuration of VLAN parameters such as VLAN ID, name, and type.
FMT_SMR.1	The TOE maintains two default levels of administration, and allows for customization of other levels. The default levels are defined in this ST as the roles of privileged administrator, and semi-privileged administrator where semi-privileged administrator includes roles that may be customized. The TOE maintains all Cisco IOS administrator roles (privileged and semi-privileged administrators). The TOE can and shall be configured to authenticate all 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. Privilege levels are number 0-15 that specifies the various levels for the user. The privilege levels are not necessarily hierarchical. Privilege level 15 has access to all commands on the TOE. Privilege levels 0 and 1 are defined by default, while levels 2-14 are undefined by default. Levels 0-14 can be set to include any of the commands available to the level 15 administrator, and are considered the semi-privileged administrator for purposes of this evaluation. The privilege level determines the functions the user can perform; hence the authorized administrator with the appropriate privileges. The TOE also supports neighbor router role that is authorized to update routing tables per the information flow rules. Refer to the Guidance documentation and IOS Command Reference Guide for available commands and associated roles and privilege levels.
FPT_RPL.1	By virtue of the cryptographic and path mechanisms implemented by the TOE, replayed network packets directed (terminated) at the TOE will be detected and discarded. Note: The intended scope of this requirement is trusted communications with the TOE (e.g., administrator to TOE, IT entity (e.g., authentication server) to TOE,). As such, replay does not apply to receipt of multiple network packets due to network congestion or lost packet acknowledgments.
FPT_STM.1	The TOE provides a source of date and time information used in audit timestamps and in calculating session inactivity. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive clock updates from an NTP server. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions.
FPT_TST_EXT.1	As a FIPS 140-2 validated product, the TOE runs a suite of self tests during initial start-up to verify its correct operation. Refer to the FIPS Security Policy for available options and management of the cryptographic self test. For testing of the TSF, the TOE automatically runs checks and tests at startup and during resets to ensure the TOE is operating correctly. Refer to the Guidance documentation for installation configuration settings and information and troubling shooting if issues are identified.
FTA_SSL.3	An administrator can configure maximum inactivity times for both local and remote administrative sessions. When a session is inactive (i.e., not session input) for the configured period of time the TOE will terminate the session,

TOE SFRs	How the SFR is Met
	flush the screen, and no further activity is allowed, requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session. The allowable range is from 1 to 65535 seconds.
FTA_TAB.1	The TOE displays a customizable login banner on the local and remote CLI management interface prior to allowing any administrative access to the TOE.

6.2 TOE Bypass and interference/logical tampering Protection Measures

The TOE consists of a hardware platform in which all operations in the TOE scope are protected from interference and tampering by untrusted subjects. All administration and configuration operations are performed within the physical boundary of the TOE. Also, all TSP enforcement functions must be invoked and succeed prior to functions within the TSC proceeding.

The TOE has been designed so that all locally maintained TSF data can only be manipulated via the secured management interface, the CLI interface. There are no undocumented interfaces for managing the product.

All sub-components included in the TOE rely on the main chassis for power, memory management, and access control. In order to access any portion of the TOE, the Identification and Authentication mechanisms of the TOE must be invoked and succeed.

No processes outside of the TOE are allowed direct access to any TOE memory. The TOE only accepts traffic through legitimate TOE interfaces. Specifically, processes outside the TOE are not able to execute code on the TOE. None of these interfaces provide any access to internal TOE resources.

The TOE enforces information flow control policies and applies network traffic security on its interfaces before traffic passes into or out of the TOE. The TOE controls every ingress and egress traffic flow. Policies are applied to each traffic flow. Traffic flows characterized as unauthorized are discarded and not permitted to circumvent the TOE. There are no unmediated traffic flows into or out of the TOE. The information flow policies identified in the SFRs are applied to all traffic received and sent by the TOE. Each communication including data plane communication, control plane communications, and administrative communications are mediated by the TOE. The data plane allows the ability to forward network traffic; the control plane allows the ability to route traffic correctly; and the management plane allows the ability to manage network elements. There is no opportunity for unaccounted traffic flows to flow into or out of the TOE.

This design, combined with the fact that only an administrative user with the appropriate role may access the TOE security functions, provides a distinct protected domain for the TOE that is logically protected from interference and is not bypassable.

7 RATIONALE

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined within this Security Target.

7.1 Rationale for TOE Security Objectives

Table 17: Threats/Policies & IT Security Objectives Mappings

	T.AUDIT_REVIEW	T.MEDIATE	T.NOAUDIT	T.NOAUTH	T.NOMGT	T.UNAUTH_MGT_ACCESS	T.TIME	T.USER_DATA_REUSE	P.ACCESS_BANNER
O.ACCESS_CONTROL				X	X	X			
O.AUDIT_GEN	X						X		
O.AUDIT_VIEW	X		X						
O.CFG_MANAGE					X				
O.IDAUTH						X			
O.MEDIATE		X							
O.SELFPRO				X	X	X			
O.STARTUP_TEST						X			
O.TIME							X		
O.DISPLAY_BANNER									X
O.RESIDUAL_INFORMATION_CLEARING								X	

Table 18: TOE Threat/Policy/Objective Rationale

Threat / Policy	Rationale for Coverage
T.AUDIT_REVIEW	Actions performed by users may not be known to the administrators due to actions not being recorded locally or remotely in a manner suitable for allow interpretation of the messages. 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, and/or to configure the TOE to transmit audit records to a remote syslog server.
T.MEDIATE	An unauthorized entity may send impermissible information through the TOE which results in the exploitation of the recipient of the network

Threat / Policy	Rationale for Coverage
	traffic. 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 only the authorized administrator the capability to review and clear the 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. The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. The O.ACCESS_CONTROL objective ensures that only authorized administrator have access to the TOE management functions.
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. The O.ACCESS_CONTROL objective ensures that only authorized administrator have access to the TOE management functions. The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions. The combination of these objectives mediates the ability for the administrators to 'easily' gain access to and manage the TOE.
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 requires the TOE to perform initial tests upon system startup to ensure the integrity of the TOE security configuration and operations. The O.SELFPRO objective requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.
T.TIME	Evidence of a compromise or malfunction of the TOE may go unnoticed or not be properly traceable if recorded events are not properly sequenced through application of correct timestamps. The O.TIME objective mitigates this threat by providing the accurate time to the TOE for use in the audit records (O.AUDIT_GEN).
T.USER_DATA_REUSE	User data that is temporarily retained by the TOE in the course of processing network traffic could be inadvertently re-used in sending network traffic to a destination other than intended by the sender of the original network traffic. This threat is countered by the security objective O.RESIDUAL_INFORMATION_CLEARING so that data traversing the TOE could not inadvertently be sent to a user other than that intended by the sender of the original network traffic. This objective requires that residual data be

Threat / Policy	Rationale for Coverage
	cleared so that it is not inadvertently sent back out of the TOE.
P.ACCESS_BANNER	This Organization Security Policy is addressed by the organizational security policy O.DISPLAY_BANNER to ensure an advisory notice and consent warning message regarding unauthorized use of the TOE is displayed before the session is established.

7.2 Rationale for the Security Objectives for the Environment

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, the tables below illustrate the mapping between the security requirements and the security objectives and the relationship between the threats, policies and IT security objectives. The functional and assurance requirements presented in this Security Target are mutually supportive and their combination meets the stated security objectives.

Table 19: Threats & IT Security Objectives Mappings for the Environment

	A.NOEVIL	A.TRAIN_AUDIT	A.TRAIN_GUIDAN	A.LOCATE	A.CONFIDENTIALITY	A.INTEROPERABILITY	A.LOWEXP	T.AUDIT_REVIEW
OE.AUDIT_REVIEW		X						X
OE.CONFIDENTIALITY					X			
OE.INTEROPERABILITY						X		
OE.LOCATE				X				
OE.LOWEXP							X	
OE.NOEVIL	X							
OE.TRAIN_GUIDAN			X					

Table 20: Assumptions/Threats/Objectives Rationale

Assumptions	Rationale for Coverage of Environmental Objectives
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.

Assumptions	Rationale for Coverage of Environmental Objectives
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 and soft-copy representations 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. Audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic. 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, and audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic.
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.

7.3 Rationale for requirements/TOE Objectives

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, the tables below illustrate the

mapping between the security requirements and the security objectives and the relationship between the threats, and IT security objectives.

Table 21: Security Objective to Security Requirements Mappings

	O.ACCESS_CONTROL	O.AUDIT_GEN	O.AUDIT_VIEW	O.CFG_MANAGE	O.IDAUTH	O.MEDIATE	O.SELFPRO	O.STARTUP_TEST	O.TIME	O.DISPALY_BANNER	O.RESIDUAL_INFORMATION_CLEARING
FAU_GEN.1		X									
FAU_GEN.2		X									
FAU_SAR.1			X								
FAU_STG.1	X										
FCS_CKM.1(1)							X				
FCS_CKM.1(2)							X				
FCS_CKM.4							X				
FCS_COP.1(1)							X				
FCS_COP.1(2)							X				
FCS_COP.1(3)							X				
FCS_COP.1(4)							X				
FCS_COP.1(5)							X				
FCS_COP.1(6)							X				
FCS_IPSEC_EXT.1							X				
FCS_SSH_EXT.1							X				
FDP_IFC.1						X					
FDP_IFF.1						X					
FDP_RIP.2											X
FIA_ATD.1					X						
FIA_UAU.2					X						
FIA_UAU.5					X						

FIA_UAU.7					X						
FIA_UID.2					X						
FMT_MOF.1	X										
FMT_MSA.2							X				
FMT_MSA.3	X					X					
FMT_MTD.1	X										
FMT_SMF.1				X							
FMT_SMR.1	X			X							
FPT_RPL.1							X				
FPT_STM.1		X							X		
FPT_TST_EXT.1								X			
FTA_SSL.3	X			X	X		X				
FTA_TAB.1										X	

Table 22: Objectives to Requirements Rationale

Objective	Rationale
O.ACCESS_CONTROL	The 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 performed on the TOE by the authorized administrators [FMT_MOF.1]. Only authorized administrators of the TOE may modify TOE data [FMT_MTD.1] or delete audit data stored locally on the TOE [FAU_STG.1]. The TOE must be able to recognize the administrative role that exists for the TOE [FMT_SMR.1]. The TOE must allow the authorized 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. The SFR FTA_SSL.3 also meets this objective by terminating a session due to meeting/exceeding the inactivity time limit.
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 and FAU_GEN.2]. Timestamps associated with the audit record must be reliable [FPT_STM.1].
O.AUDIT_VIEW	The TOE will provide the authorized administrators the capability to review Audit data. Security relevant events must be available for review by authorized administrators [FAU_SAR.1].
O.CFG_MANAGE	The TOE will provide management tools/applications to allow authorized administrators to manage its security functions. The TOE is capable of performing numerous management functions including the ability to manage the cryptographic functionality, to manage the audit logs and functions, to manage information flow control attributes, to manage security attributes that allows authorized administrators to manage the specified security

Objective	Rationale
	attributes, to manage the default values of the security attributes, to initiate TOE self test, to manage the warning banner message and content, and to manage the time limits of session inactivity [FMT_SMF.1]. The TOE must be able to recognize the administrative roles that exist for the TOE [FMT_SMR.1]. FTA_SSL.3 also meets this objective by terminating a session due to meeting/exceeding the inactivity time limit. The TOE requires that all users, routers, 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 store user 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_UAU.5]. Before access is granted, all users must be successfully identified and authenticated [FIA_UID.2 and FIA_UAU.2]. The password is obscured when entered [FIA_UAU.7]. If the period of inactivity has been exceeded, the user is required to re-authenticate to re-establish the session [FTA_SSL.3].
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 subject attributes and information attributes necessary to enforce the IP information flow control SFP [FDP_IFC.1, and FDP_IFF.1]. The policy is defined by rules defining the conditions for which information is permitted or denied to flow [FDP_IFF.1]. The TOE provided the capability for administrators to define default deny rules, though the default policy for the information flow control security rules is permissive where no explicit rules exist until created and applied by an authorized administrator [FMT_MSA.3].
O.SELFPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. The router component of the TOE provides an encrypted mechanism for remote management of the TOE and for protection of authentication data transferred between the router and endpoints are secure by implementing the encryption protocols as defined in the SFRs and as specified by the RFCs, [FCS_COP.1(1), (2), (3), (4), (5), (6)), FCS_CKM.1(1), (2), FCS_CKM.4, FCS_IPSEC_EXT.1, FCS_SSH_EXT.1, FMT_MSA.2]. The SFR FTA_SSL.3 also meets this objective by terminating a session due to meeting/exceeding the inactivity time limit thus ensuring the session does not remain active and subject to attack. FPT_RPL.1 supports this objective by leveraging the ability of SSHv2 to terminate sessions when information replay is detected.
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_TST_EXP.1].
O.TIME	The TSF will provide a reliable time stamp for its own use. The TOE is required to provide reliable timestamps for use with the audit record. [FPT_STM.1]. The TOE can optionally be configured to allow clock updates from a designated NTP server.
O.DISPLAY_BANNER	The TSF shall display a banner, before the user establishes a session. The SFR, FTA_TAB.1 meets this objective by displaying an advisory notice and consent warning message regarding unauthorized use of the TOE.

Objective	Rationale
O.RESIDUAL_INFORMATION _CLEARING	The TOE must ensure that previous data are zeroized/overwritten so that the area used by a packet and then reused, data from the previous transmission does not make its way into a new packet transmission. The SFR, FDP_RIP.2 meets this objective by ensuring no left over user data from the previous transmission is included in the network traffic.

ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 23: References

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated July 2009, version 3.1, Revision 3, CCMB-2007-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-004
[NDPP]	Security Requirements for Network Devices, 10 December 2010, Version 1.0.

ANNEX B: COMPATIBLE CISCO 7600 SERIES LINE CARDS

The following line cards are compatible with the Cisco 7600 Series and can be used with this evaluation:

Part Number	Description
WS-X6704-10GE	Cat6500 4-port 10 Gigabit Ethernet Module
WS-X6148A-GE-45AF	Cat6500 48-Port PoE 802.3af & ePoE 10/100/1000 w/Jumbo Frame
WS-X6708-10G-3CXL	C6K 8 port 10 Gigabit Ethernet module with DFC3CXL
WS-X6708-10G-3C	C6K 8 port 10 Gigabit Ethernet module with DFC3C
76-ES+T-4TG	ES+ Low Queue 4 port 10GE - 3CXL
76-ES+XT-4TG3C	7600 ES+XT, LAN/WAN PHY, OTN/G.709, 4x10GE, XFP, DFC3C
76-ES+XT-4TG3CXL	7600 ES+XT, LAN/WAN PHY, OTN/G.709, 4x10GE, XFP, DFC3CXL
76-ES+T-2TG	ES+ Low Queue 2 port 10GE - 3CXL
76-ES+XT-2TG3C	7600 ES+XT, LAN/WAN PHY, OTN/G.709, 2x10GE, XFP, DFC3C
76-ES+XT-2TG3CXL	7600 ES+XT, LAN/WAN PHY, OTN/G.709, 2x10GE, XFP, DFC3CXL
76-ES+T-40G	ES+ Low Queue 40 port GE - 3CXL
76-ES+T-20G	ES+ Low Queue 20 port GE - 3CXL
76-ES+XC-40G3CXL	7600 ES+XC Combo 20x1GE/ 2x10GE,

	DFC3CXL
76-ES+XC-40G3C	7600 ES+XC Combo 20x1GE/ 2x10GE, DFC3C
76-ES+XC-20G3CXL	7600 ES+XC Combo 10x1GE/ 1x10GE, DFC3CXL
76-ES+XC-20G3C	7600 ES+XC Combo 10x1GE/ 1x10GE, DFC3C
WS-X6748-GE-TX	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45
WS-X6748-SFP	Catalyst 6500 48-port GigE Mod: fabric-enabled
WS-X6724-SFP	Catalyst 6500 24-port GigE Mod: fabric-enabled
7600-SIP-200	Cisco 7600 Series SPA Interface Processor-200
7600-SIP-400	Cisco 7600 Series SPA Interface Processor-400
SPA-4XOC3-POS (SIP-400)	4-port OC3/STM1 POS Shared Port Adapters
SPA-2XOC3-POS –V2	2-port OC3/STM1 POS Shared Port Adapters
SPA-1XCHSTM1/OC3	1-port Channelized STM-1/OC-3c to DS0 Shared Port Adapter
SPA-1XOC12-POS (SIP-400)	1-port OC12/STM4 POS Shared Port Adapters
SPA-1XCHOC12/DS0	1-port Channelized OC12 to DS0 SPA
SPA-1XOC48POS/RPR	1-port OC48/STM16 POS/RPR Shared Port Adapters
SPA-4XT-SERIAL (SIP-200)	Cisco 4 port serial SPA
SPA-4XT3/E3 (SIP-200)	4-port Clear Channel T3/E3 Shared Port Adapter
SPA-2XT3/E3	2-port Clear Channel T3/E3 Shared Port Adapter
SPA-4XCT3/DS0	4-port Channelized T3 to DS0 Shared Port Adapter
SPA-8XCHT1/E1 (SIP-200)	8-port Channelized T1/E1 to DS0 Shared Port Adapter
SPA-8X1FE-TX-V2 (SIP-200)	Cisco 8-Port Fast Ethernet (TX) Shared Port Adapter
SPA-4X1FE-TX-V2	Cisco 4-Port Fast Ethernet (TX) Shared Port Adapter
SPA-3XOC3-ATM-V2 (SIP-400)	3 port OC-3c/STM-1 ATM Shared Port Adapter
SPA-1XOC3-ATM –V2	1 port OC-3c/STM-1 ATM Shared Port Adapter
SPA-1XOC12-ATM-V2 (SIP-400)	1 port OC12 STM Shared Port Adapter