Cisco 5915 Embedded Services Router

Security Target

Revision 1.0

10 January 2013

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 5915 Embedded Services Router running IOS 15.2(3)GC. 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.

REVISION HISTORY

Rev	Date	Description
0.01	15 November 2011	Initial Draft
0.02	29 November 2011	Updates for ASE ETR
0.03	5 January 2012	Updates post iVOR
0.04	18 January 2012	Updates post iVOR, part 2
0.05	9 April 2012	Updated IOS version to 15.2(3)GC
0.06	17 May 2012	Updated for ADV ETR
0.0.7	25 July 2012	Updated section 1.7.5 per Validator instructions
0.0.8	25 July 2012	Added details to FAU_GEN.1 in the TSS
0.09	10 September 2012	Updated per FVOR comments
0.10	13 September 2012	Updated per FVOR comments
1.0	10 January 2013	OS updated to IOS v15.2(3)

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 5915 Embedded Services Router Security Target
ST Version	1.0
Publication Date	10 January 2013
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco 5915 Embedded Services Router
TOE Hardware Models	conduction-cooled or air-cooled Cisco 5915 Embedded Services Routers
TOE Software Version	IOS 15.2(3)GC
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
BGP	Border Gateway Protocol. An exterior gateway protocol. It performs routing between multiple autonomous systems and exchanges routing and reachability information with other BGP systems.
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
cPCI	Compact Peripheral Component Interconnect
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol

Acronyms / Abbreviations	Definition
EAL	Evaluation Assurance Level
HTTPS	Hyper-Text Transport Protocol Secure
EEPROM	Electrically erasable programmable read-only memory, specifically the memory in the switch where the Cisco IOS is stored.
EIGRP	Enhanced Interior Gateway Routing Protocol
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
HTTPS	Hyper-Text Transport Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IOS	The proprietary operating system developed by Cisco Systems.
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP Security
ISR	Integrated Service Router
IT	Information Technology
J2	A pin connection type for the backplanes of PCI cards. Not an acronym.
JTAG	Joint Test Action Group
MAC	Media Access Control
NTP	Network Time Protocol
NVRAM	Non-volatile random access memory, specifically the memory in the switch where the configuration parameters are stored.
OS	Operating System
PCI	Peripheral Component Interconnect
OSPF	Open Shortest Path First. An interior gateway protocol (routes within a single autonomous system). A link-state routing protocol which calculates the shortest path to each node.
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
PIM	Protocol Independent Multicast
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PVLAN	Private VLAN
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol. An interior gateway protocol (routes within a single autonomous system). A distance-vector protocol that uses hop count as its metric.
RJ-45	Registered Jack 45
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SM	Service Module
SHS	Secure Hash Standard
SSH	Secure Shell
SSHv2	Secure Shell (version 2)
ST	Security Target
TACACS	Terminal Access Controller Access Control System
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control

Acronyms / Abbreviations	Definition
TSF	TOE Security Function
UDP	User Datagram Protocol
VACL	Virtual Access Control List
VLAN	Virtual Local Area Network
VSS	Virtual Switching System
TSP	TOE Security Policy
WAN	Wide Area Network
WIC	WAN Interface Card

1.3 TOE Overview

The Cisco 5915 Embedded Services Router (ESR) running IOS 15.2(3)GC (herein after referred to as 5915 ESR, the router, or the TOE). The TOE is a high-performance, ruggedized router designed for use in harsh environments-offering reliable operation in extreme temperatures and under shock and vibration conditions typical for mobile applications in rugged terrain.

1.3.1 TOE Product Type

The Cisco 5915 ESR is a router platform used to construct IP networks by interconnecting multiple smaller networks or network segments. The TOE provides connectivity and security services onto a single, secure device. The flexible, compact form factor of these routers, complemented by Cisco IOS® Software, provides highly secure data, voice, and video communications to stationary and mobile network nodes across wired links.

In support of the routing capabilities, the 5915 ESR provides IPSec connection capabilities for VPN enabled clients connecting through the 5915 ESR. The 5915 ESR is also compatible with VPN clients that use GDOI.
The 5915 ESR is a PCI-104 router module solution for protecting the network. The firewall capabilities provided by the TOE are provided via a stateful packet filtering firewall. A stateful packet filtering firewall 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 for firewalls. This header information includes source and destination host (IP) addresses, source and destination port numbers, and the transport service application protocol (TSAP) held within the data field of the IP packet. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated.

In addition to IP header information, the TOE mediates information flows on the basis of other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface. For connection-oriented transport services, the firewall

either permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection.

The TOE also includes on the 5915 Embedded Services Router modules a network-based Intrusion Prevention System that monitors traffic in real-time. It can analyze both the header and content of each packet. The TOE uses a rule-based expert system to interrogate the packet information to determine the type of attack, be it simple or complex.

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
Chassis	Yes	The router supports Input/Ouput connectors through standard RJ-45 connectors, or any other cPCI compatible network connector. The chassis can be any off-the-shelf module that is capable of holding a PCI-104 form factor.
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.
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.
VPN Peer	No	This includes any peer with which the TOE participates in VPN communications. VPN peers may be any device or software client that supports IPSec v3 communications. Both VPN clients and VPN gateways are considered VPN peers by the TOE.
NTP Server	No	The TOE supports communications with an NTP server. A solution must be used that supports MD5 hashing of communications with up to a 32 character key.
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.

1.4 TOE DESCRIPTION

This section provides an overview of the 5915 ESR Target of Evaluation (TOE). The TOE is comprised of a single PCI-104 router module running IOS 15.2(3)GC.

1.5 TOE Evaluated Configuration

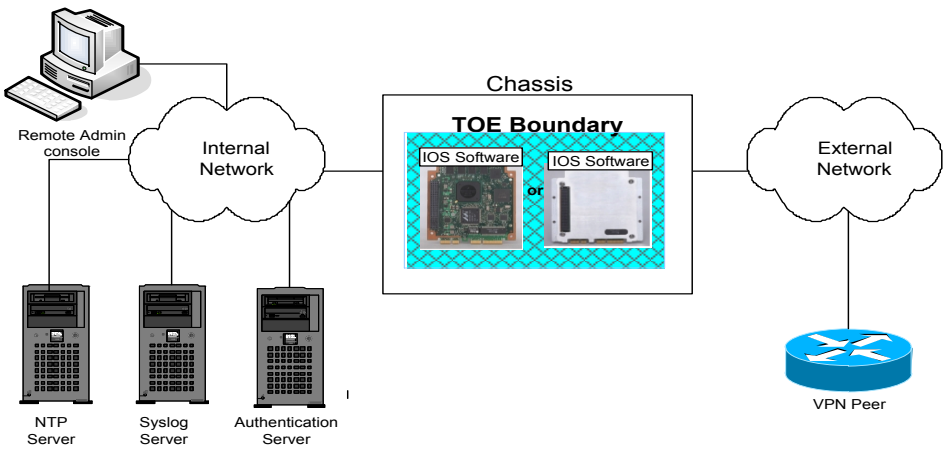
Table 4: Evaluated Configurations

TOE	• One or more Cisco 5915 Embedded Security Routers (conduction-cooled or air-cooled models) • Each router running IOS 15.2(3)GC (FIPS validated)

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



1.6 Physical Scope of the TOE

The TOE is a hardware solution obtained from HCL under OEM contract running the IOS 15.2(3)GC software solution. The image name for the 5915 ESR TOE is c5915-adventerprisek9-mz.SPA.152-1.GC1.bin.

The key components on the board are:

- Freescale MPC8358E processor
- Marvell 88E6046 six port Ethernet switch (only 3 ports are used)

- Broadcom BCM5221 Ethernet PHY
- Numonyx PC28F00BM29EWH NOR flash chip

Both an air-cooled and a conduction-cooled board exist. They differ only in cooling mechanism. The very same circuit board/components are used, but the conduction cooled version includes thermal plates.

The board provides the following external interfaces:

- RS-232 Console port accessible via card edge fingers
- (2) Routed FE ports, (3) Switched FE ports
- JTAG: A JTAG chain is present on the board (connects to the uP and a CPLD). The JTAG interface connects to the card edge fingers. It is to be disabled in the evaluated configuration and not re-enabled.

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
8. Intrusion Prevention Services

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.

These audit messages include a timestamp that can be provided by the TOE or an optional NTP server in the operational environment.

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 SL1 validated, certificate number 1935. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; digital signature using RSA; 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. For GDOI, the TOE can perform the role of the GDOI key server and the group controller.

1.7.3 Traffic Filtering (ACLs)

This product supports IP ACLS, VPN policies and VLANs.

IP 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.

5915 ESR delivers VPN connections to remote entities. 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.

5915 ESR 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 the network traffic is received /destined. This policy is applied after the Firewall policy.

1.7.4 Identification and 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 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 Secure Management

The TOE allows authorized administrators to add new administrators, start-up and shutdown the device, create, modify, or delete configuration details such as interface parameters and ACLs, and to modify and set the time and date. All TOE administration occurs either through a secure SSH session via a SSH client, or via a local console connection.

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.

1.7.8 Intrusion Prevention Services

The 5915 ESR IOS software Intrusion Prevention System (IPS) operates as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When Cisco IOS IPS detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages stored in the local buffer and then offloaded to an external syslog server. The privileged administrator can configure Cisco IOS IPS to choose the appropriate response to various threats. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

- Send an audit record to a syslog server or a management interface
- Drop the packet
- Reset the connection
- Deny traffic from the source IP address of the attacker for a specified amount of time
- Deny traffic on the connection for which the signature was seen for a specified amount of time

For inbound packets the IDS processing is done after IP ACLs and then VPN policies have been applied.

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.

In addition, 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 5915 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 included in the TOE:

- Preparative Procedures and Operational Guidance for the Common Criteria EAL2 Evaluated Cisco 5915 Embedded Service Routers with IOS 15.2(3)GC
- Cisco IOS Security Command Reference
- Cisco IOS Security Configuration Guide

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 3, dated: July 2009.
The TOE and ST are EAL2 Augmented with ALC_FLR.2 and ALC_DVS.1 Part 3 conformant.
The TOE and ST are CC Part 2 extended.

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 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.
T.UNAUTHORIZED_PEER	An unauthorized IT entity may attempt to establish a security association with the TOE.
T.VPNMEDIAT	An unauthorized person may send or receive unauthorized IPSec traffic through the TOE which results in the exploitation of resources on the internal network.
T.VLAN	An attacker may force a packet destined for one VLAN to cross into another VLAN for which it is not authorized compromising the confidentiality and integrity of information.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an

Threat	Threat Definition
	IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.
T.INTEGRITY	An attacker may compromise the integrity of IPSec traffic sent to/from the TOE.

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.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.

TOE Objective	TOE Security Objective Definition
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.PEER_AUTHENTICATION	The TOE will authenticate each peer TOE that attempts to establish a security association with the TOE.
O.INTEGRITY	The TOE must be able to protect the integrity of data transmitted to a peer via encryption and provide IPSec authentication for such data. Upon receipt of data from a peer, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.
O.VPNMEDIAT	The TOE must mediate the flow of all IPSec traffic through the TOE and must ensure that residual information from a previous IPSec traffic flow is not transmitted in any way.
O.VLAN	The TOE must provide a means for the logical separation of Virtual LANs to ensure that packets flows are restricted to their authorized Virtual LANs ensuring VLAN separation is achieved.
O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	The Analyzer must accept data from IDS Sensors and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.

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

Environment Security Objective	IT Environment Security Objective Definition
	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
	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 cryptographic hashing)
	FCS_COP.1(5): Cryptographic operation (for keyed-hash message authentication)
	FCS_GDOI_EXT.1: Group Domain of Interpretation
	FCS_IPSEC_EXT.1: IPSEC
	FCS_SSH_EXT.1: SSH
FDP: User data protection	FDP_IFC.1(1): Subset Information Flow Control – IP ACL
	FDP_IFF.1(1): Simple Security Attributes – IP ACL
	FDP_IFC.1(2): Subset Information Flow Control – VPN
	FDP_IFF.1(2): Simple Security Attributes – VPN
	FDP_IFC.1(3): Subset Information Flow Control – VLAN
	FDP_IFF.1(3): Simple Security Attributes – VLAN
	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

Functional Component	
FMT: Security management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MSA.3(1): Static Attribute Initialization –VPN
	FMT_MSA.3(2): Static Attribute Initialization – IP ACL and VLAN
	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
FTP: Trusted Path/ Channel	FTP_ITC.1: Inter-TSF Trusted Channel
	FTP_TRP.1: Trusted Path
IDS: IDS Component Requirements	IDS_SDC_EXT.1: System Data Collection
	IDS_ANL_EXT.1: Analyzer analysis
	IDS_RCT_EXT.1: Analyzer react
	IDS_RDR_EXT.1: Restricted data review
	IDS_STG_EXT.1: Guarantee of system data availability
	IDS_STG_EXT.2: Prevention of system data loss

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: Security Functional Requirements

SFR	Auditable Event	Additional Contents
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_IFF.1(1)	All decisions on requests for information flow.	None.
FDP_IFF.1(2)	Errors during IPSec processing	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).
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 (1) FMT_MSA.3 (2)	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 cryptographic hashing)

FCS_COP.1.1(4) 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"**]

5.2.2.8 FCS_COP.1(5): Cryptographic operation (for keyed-hash message authentication)

FCS_COP.1.1(5) 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."]

5.2.2.9 FCS_GDOI_EXT.1 Group Domain of Interpretation

FCS_GDOI_EXT.1.1 The TSF shall provide negotiation of security services for IPsec in accordance with RFC 3457 as an extension of phase 2 of the protocol defined in RFC 2409, negotiation of security services for IPsec.

FCS_GDOI_EXT.1.2 The TSF shall provide the "GROUPKEY-PULL" registration protocol as defined in RFC 3457 that protects the key agreement packets providing confidentiality and integrity for the communications between a new group member and the group controller.

FCS_GDOI_EXT.1.3 The TSF shall provide the "GROUPKEY-PUSH" rekey protocol as defined in RFC 3457 that protects the key agreement packets as they pass from the controller to the members, for confidentiality using the AES encryption algorithm specified in FCS_COP.1.1(2).

5.2.2.10 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 14 (2048-bit MODP).

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.

5.2.2.11 FCS_SSH_EXT.1 SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 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(1) Subset information flow control – IP ACL

FDP_IFC.1.1(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 or fiber interface)

b) information: IP packets

c) operation: forward or drop the packets].

5.2.3.2 FDP_IFF.1(1) Simple security attributes – IP ACL

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

a) subject security attributes:
- **presumed address;**
- **[configured zone];**

b) information security attributes:
- **presumed IP address of source subject;**
- **presumed IP address of destination subject;**
- **transport layer protocol;**
- **TOE interface on which traffic arrives and departs;**
- **service;**
- **[No other attributes]**].

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

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

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
- **all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information**

flow security attributes, created by the authorized administrator;

- **the presumed address of the source subject, in the information, translates to an external network address;**
- **and the presumed 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].

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

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules: [**none**].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules:

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

5.2.3.3 FDP_IFC.1(2) Subset information flow control – VPN

FDP_IFC.1.1(2) The TSF shall enforce the [**VPN SFP**] on [

- **source subject: TOE interface on which information is received;**
- **destination subject: TOE interface to which information is destined.**

- **information: network packets; and**
- **operations:**
  - **pass packets without modifying;**
  - **send IPSec encrypted and authenticated packets to a peer TOE using ESP in tunnel mode as defined in RFC 2406;**
  - **decrypt, verify authentication and pass received packets from a peer TOE in tunnel mode using ESP**].

5.2.3.4 FDP_IFF.1(2) Simple security attributes – VPN

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

a) Source subject security attributes:
- **set of source subject identifiers (IP address).**

b) Destination subject security attributes:
- **Set of destination subject identifiers (IP address).**

c) Information security attributes:
- **presumed identity of source subject;**
- **identity of destination subject**
- **receiving/transmitting interface**
- **transport protocol**].

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

a) the information security attributes match the attributes in an information flow policy rule according to the following algorithm: The TOE examines a packet's source IP address (presumed identity), destination IP address (destination identity), interface, and transport protocol and compares them to the configured VPN policy to determine the action to apply to the network packets, as follows:
- **If the packet is a plaintext packet that matches a policy rule that allows packets to be passed without modification, the packet is passed without modification.**
- **If the packet is a plaintext packet that matches a policy rule that requires the TOE to send IPSEC encrypted and authenticated packets to a peer, the TOE encrypts and applies a authentication**

mechanism to the packet using ESP in tunnel mode as defined in RFC 2406 and sends it to its peer.

- **If the packet matches a policy that requires the TOE to decrypt, verify authentication and pass received packets from a peer TOE in tunnel mode using ESP, the TOE decrypts, verifies authentication and passes received packets from a peer TOE in tunnel mode using ESP**].

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

FDP_IFF.1.4(2) The TSF shall explicitly authorize an information flow based on the following rules: [**none**].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: [

- **The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject;**
- **The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a broadcast identity;**
- **The TOE shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier**].

5.2.3.5 FDP_IFC.1(3) Subset information flow control – VLAN

FDP_IFC.1.1(3) The TSF shall enforce the [**VLAN SFP**] on: [

- **subjects: physical network interfaces;**
- **information: network packets;**
- **operations: permit or deny layer two communication].**

5.2.3.6 FDP_IFF.1(3) Simple security attributes – VLAN

FDP_IFF.1.1(3) The TSF shall enforce the [**VLAN SFP**] based on the following types of subject and information security attributes: [

a) subject security attributes:

- **receiving/transmitting VLAN interface;**

b) information security attributes:

- **VLAN ID in Packet Header**].

FDP_IFF.1.2(3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- **if the receiving VLAN interface is configured to be in the same VLAN as the transmitting VLAN interface**].

FDP_IFF.1.3(3) The TSF shall enforce the [**none**].

FDP_IFF.1.4(3) The TSF shall explicitly authorize an information flow based on the following rules: [**none**].

FDP_IFF.1.5(3) The TSF shall explicitly deny an information flow based on the following rules: [**none**].

5.2.3.7 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 TOE administrators:

a) user identity;

b) privilege levels; and

c) password.

For VPN peers:

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

e) IKE Security Attributes].

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+**] 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 **[*disable, enable, or modify the behavior of*]** the functions:

- **a) [information flow security policy rules that permit or deny information flows;**
- **b) user attribute values defined in FIA_ATD.1;**
- **c) authentication mechanisms in FIA_UAU.5;**
- **d) external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);**
- **e) session inactivity time period;**
- **f) TSF self-test;**
- **g) the time and date;**
- **h) the audit trail;**
- **i) remote administration from internal and external networks;**
- **j) addresses from which remote administration can be performed;**
- **k) the security attributes referenced in the VPN information flow polices;**
- **l) the security attributes referenced in the VLAN information flow polices**
- **m) the IPS settings on the box**
- **n) the IPSec, GDOI, and SSH settings on the box**]

to [**privileged administrator, and semi-privileged administrator with appropriate privileges**].

5.2.5.2 FMT_MSA.3(1) Static Attribute Initialization –VPN

FMT_MSA.3.1(1) The TSF shall enforce the [**VPN SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) 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.

5.2.5.3 FMT_MSA.3(2) Static Attribute Initialization - IP ACL and VLAN

FMT_MSA.3.1(2) The TSF shall enforce the [**ACL SFP and VLAN SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(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 [***manage***] the [**TSF 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.1.1 The TSF shall be capable of performing the following management functions: [

- **TOE Audit Review and Configuration;**
- **IP ACL Configuration;**
- **TOE Authentication Functionality Configuration;**
- **IPSec Configuration;**
- **VLAN Configuration;**
- **IDS Configuration;**
- **Timestamp Configuration;**
- **Banner Configuration;**
- **Session Timeout Configuration;**
- **Routing Table Configuration;**
- **Cryptographic Algorithm Configuration;**
- **Cryptographic self-test Execution**].

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 vpn peer**].

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.

5.2.8 Trusted Path/Channel (FTP)

5.2.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall **use IPSEC as specified in FCS_IPSEC_EXT.1 or GDOI as specified in FCS_GDOI_EXT.1 to** provide a **trusted** communication channel between itself and **authorized IT entities** ~~**another trusted IT product**~~ that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~**modification or**~~ disclosure.

FTP_ITC.1.2 The TSF shall permit [***the TSF***]**, or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**vpn connections**].

5.2.8.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***remote***] **administrators** ~~**users**~~ **using SSH as specified in FCS_SSH_EXT.1** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***disclosure***].

FTP_TRP.1.2 The TSF shall permit [***remote*** ~~***users***~~] **administrators** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**all remote administrative actions**].

5.2.9 IDS Component Requirements (IDS)

5.2.9.1 IDS_SDC_EXT.1 System data collection

IDS_SDC_EXT.1.1 The TSF shall be able to collect the following information from the targeted IT System resources: Network Traffic.

IDS_SDC_EXT.1.2 The TSF shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information specified in the Details column of Table 13: System Events.

Table 13: System Events

Component	Event	Details
IDS_SDC_EXT.1	Network traffic	Protocol, source address, destination address

5.2.9.2 IDS_ANL_EXT.1 Analyzer analysis

IDS_ANL_EXT.1.1 The TSF shall perform the following analysis function on all IDS data received:
a) Signature; and
b) Event correlation.

IDS_ANL_EXT.1.2 The TSF shall record within each analytical result at least the following information:
a) Date and time of the result, type of result, and identification of data source; and
b) Risk rating.

5.2.9.3 IDS_RCT_EXT.1 Analyzer react

IDS_RCT_EXT.1.1 The TSF shall send an audit record to the Event Store and take the following actions: Drop the packet, and/or reset the connection, and/or modify the firewall access list to deny future traffic from that source IP or connection when an intrusion is detected.

5.2.9.4 IDS_RDR_EXT.1 Restricted data review

IDS_RDR_EXT.1.1 The TSF shall provide authorized administrators with the capability to read Event data from the System data.

IDS_RDR_EXT.1.2 The TSF shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR_EXT.1.3 The TSF shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

5.2.9.5 IDS_STG_EXT.1 Guarantee of system data availability

IDS_STG_EXT.1.1 The TSF shall protect the stored System data from unauthorized deletion.

IDS_STG_EXT.1.2 The TSF shall protect the stored System data from modification.

IDS_STG_EXT.1.3 The TSF shall ensure that [the most recent, limited by available storage space] System data will be maintained when the following conditions occur: System data storage exhaustion.

5.2.9.6 IDS_STG_EXT.2 Prevention of system data loss

IDS_STG_EXT.2.1 The TSF shall overwrite the oldest stored System data if the storage capacity has been reached.

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 14).

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.

FCS_GDOI_EXT.1: The FCS class of SFRs identifies cryptographic functionality provided by the TOE. FCS_GDOI_(EXP).1 describes the cryptographic functionality associated with the Group Domain of Interpretation extension of IPSec (defined in RFC 3457) provided by the TOE. This is cryptographic functionality and consistent with the FCS class of SFRs. This is a newly created SFR family, GDOI. This family was created to describe the Group Domain of Interpretation functionality provided by the TOE. There is not a family defined in the Common Criteria Part 2 to address Group Domain of Interpretation. This is why the new family was created. This is the only component in the family. This is why the component is identified as "1."

All "IDS" SFRs: This set of SFRs was modeled from the IDS System PP, Version 1.7 – where it was created to specify IPS functionality. Compliance to the IDS System PP is not being claimed and the

SFR has been adapted in this ST to support the TOE's implementation of the protocol.

5.4 TOE SFR Dependencies Rationale

Table 14: 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_GDOI_EXT.1	No dependencies	N/A
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)

SFR	Dependency	Rationale
FDP_IFC.1(1)	FDP_IFF.1	Met by FDP_IFF.1(1)
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(1) and FMT_MSA.3(2)
FDP_IFC.1(2)	FDP_IFF.1	Met by FDP_IFF.1(2)
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(2) and FMT_MSA.3(1)
FDP_IFC.1(3)	FDP_IFF.1	Met by FDP_IFF.1(3)
FDP_IFF.1(3)	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1(3) and FMT_MSA.3(2)
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.3(1)	FMT_MSA.1 FMT_SMR.1	Met by FMT_SMR.1 See rationale below regarding FMT_MSA.1
FMT_MSA.3(2)	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
FTP_ITC.1	No Dependencies	N/A
FTP_TRP.1	No Dependencies	N/A
IDS_SDC_EXT.1	FPT_STM.1	FPT_STM.1
IDS_ANL_EXT.1	FPT_STM.1	FPT_STM.1
IDS_RCT_EXT.1	FPT_STM.1	FPT_STM.1
IDS_RDR_EXT.1	FPT_STM.1	FPT_STM.1

SFR	Dependency	Rationale
IDS_STG_EXT.1	FPT_STM.1	FPT_STM.1
IDS_STG_EXT.2	FPT_STM.1	FPT_STM.1

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) (cryptographic hashing), and FCS_COP.1(5) (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 15: 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 Reporting 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 16: 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)).
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. Cisco uniquely identifies configuration items and each release of the TOE has a unique reference. The Configuration Management documentation contains a configuration item list.

Component	How requirement will be met
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 17: How TOE SFRs Measures

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 (both firewall and VPN), 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. The startup and shutdown of the TOE generates an audit record to indicate the TOE is up and operational or is shutting down and all processes are stopping. To ensure audit records are generated for the required auditable events, the TOE must be configured in its evaluated configuration as specified in the AGD documents. This is to ensure that auditing is enabled so that the audit records are being generated for the required auditable events. If the command 'no logging on' is entered the TOE is deemed no longer in the evaluated configuration 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

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>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 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</td></tr>
</table>

TOE SFRs	How the SFR is Met
	documentation for configuration syntax and information.
FAU_SAR.1	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, 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 # 1935). 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 # 1935) The TOE also implements AES encryption in support of IKE/IPSec, IPSec protection of the syslog communication, and remote administration (SSH). The cryptography provided by the TOE has been FIPS 140-2 validated to overall level 2. Please see FIPS certificate # 1935 for validation details. This FIPS validation also covers a three key TDES algorithm for SSH protection. In support of SSH. The TOE supports the following FIPS approved/allowed algorithms: • Encryption - Triple-DES - AES • MACs - HMAC-SHA-1 • Key Exchange - Diffie-Hellman
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 # 1935).
FCS_COP.1(4)	The TOE provides cryptographic hashing services using SHA-1that meets FIPS Pub 180-3 "Secure Hash Standard".
FCS_COP.1(5)	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_GDOI_EXT.1	In support of IPSec the TOE provides a key transport method of a key server transferring cryptographic keys and policy to authenticated and authorized group members over Internet Protocol. The TOE supports GDOI, RFC 3547. The TSF supports "GROUPKEY PUSH" and "GROUPKEY PULL" for keying and rekeying. This service was evaluated as part of the TOE's FIPS 140-2 validation. Further details regarding the FIPS validation can be found in Certificate #1935.

TOE SFRs	How the SFR is Met
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.
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(1) FDP_IFF.1(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. The privileged administrator configures unauthenticated information flow policies for network traffic flowing through the TOE. The TOE supports the ability to set up rules between interfaces of the router for unauthenticated traffic. These rules control whether a packet is transferred from one interface to another based on: 1. presumed address of source 2. presumed address of destination 3. transport layer protocol 4. service used 5. network interface on which the connection request occurs Packets will be dropped unless a specific rule has been set up to allow the packet to pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied. These rules are entered in the form of access lists at the CLI (via 'access list' and

TOE SFRs	How the SFR is Met
	'access group' commands).
FDP_IFC.1(2)	The TOE facilitates VPN connections with other IPSec capable IT entities. The TOE first determines if the communication is allowed. After it is determined that the VPN connection is allowed, the TOE participates in the IPSec communication based on the established IPSec parameters. When network packets are received on a TOE interface, the TOE verifies whether the packet is allowed or not and performs one of the following actions: pass packets to the destination without modifying; send IPSEC encrypted and authenticated packets to a peer TOE using ESP in tunnel mode as defined in RFC 2406; decrypt and verify authentication and pass received packets from a peer TOE in tunnel mode using ESP.
FDP_IFC.1(3)	The TOE facilitates VLAN connections with other connected devices. The TOE verifies if packets received on a particular VLAN is allowed. After the TOE determines if the communication is permitted, the TOE either allows of denies the communication appropriately based on the configured VLANs.
FDP_IFF.1(2)	The TOE facilitates IPSec VPN communication with IPSec enabled IT devices. The TOE compares plaintext traffic received from IPSec VPN or destined to IPSec VPN to the configured information flow policies. If the information flow meets a configured information flow policy that allows the traffic, then traffic originated from a VPN tunnel or destined to a VPN tunnel is permitted. If the information flow meets a configured policy that denies traffic, such traffic is not permitted. The TOE allows network traffic based on the following determination: • The information security attributes match the attributes in an information flow policy rule (contained in the information flow policy ruleset defined by the privileged administrator) according to the following algorithm. The TOE examines a packet's source IP address, destination IP address, transport protocol, and layer 4 source and destination ports and compares them to the configured VPN policy to determine the action to apply to the network packets. If the packet is a plaintext packet that matches a policy rule that allows packets to be passed without modification, the packet is passed without modification. If the packet is a plaintext packet that matches a policy rule that requires the TOE to send IPSEC encrypted and authenticated packets to a peer, the TOE encrypts and applies a authentication mechanism to the packet using ESP in tunnel mode as defined in RFC 2406 and sends it to its peer. If the packet matches a policy that requires the TOE to decrypt, verify authentication and pass received packets from a peer TOE in tunnel mode using ESP, the TOE decrypts, verifies authentication and passes received packets from a peer TOE in tunnel mode using ESP and The TOE denies network traffic for the following scenarios: • The TOE rejects requests for access or services when the traffic is received from an IP or MAC address that is not included in the set of allowed addresses; • The TOE shall reject requests for access or services when the traffic is received from an IP or MAC address that is a broadcast identity; • The TOE shall reject requests for access or services when the traffic is received from an IP or MAC address that is defined as a loopback address
FDP_IFF.1(3)	The TOE facilitates VLAN connections with other connected devices. When network traffic is received by the TOE, the TOE verifies the VLAN ID included in the traffic header. If the VLAN ID in the traffic header matches the receiving

TOE SFRs	How the SFR is Met
	VLAN ID, then the traffic is permitted. If the in the VLAN ID in packet header is not configured on the receiving interface, the traffic is not permitted. Packets are only forwarded if the VLANs match the configured VLANs.
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 zeroized 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 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 can 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. All TOE passwords are stored encrypted on the TOE. When RADIUS and/or 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

TOE SFRs	How the SFR is Met
	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.
FIA_UAU.7	When a user enters their password at the local console or via SSH, the TOE does not echo any of the characters of the password or any representation of the characters.
FMT_MOF.1	The TOE provides the authorized administrator the ability to perform the actions required to control the TOE, including: a. network traffic (information flow) rule management (create, delete, modify, and view), b. user and VPN peer attribute value modification, c. configuration of an external authentication service, d. VPN peer configuration (create, delete, modify), e. session inactivity time period (set, modify threshold limits), f. TSF self test (TOE and cryptographic module), g. time determination (set, change date/timestamp), h. audit trail (create, delete, empty, review) management, i. remote administration capabilities, j. Specification of remote administration endpoints, k. VPN and VLAN SFP management (create, modify, delete), l. IDS/IPS setting configuration, m. IPSec, SSH and GDOI configuration (create, modify and delete). 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).
FMT_MSA.3(1)	The default TOE SFP is restrictive for the VPN SFP implemented within the TOE. VPN information flows must be administratively configured to be allowed. The TOE only permits the authorized administrators to specify the flow control policies rules used to enforce the SFP through the administrative interface.
FMT_MSA.3(2)	The default TOE SFP is restrictive for the ACLs SFP and VLAN SFPs implemented within the TOE. Once the setting for 'ip routing' has been enabled on the box, and before ACLs have been explicitly created and applied to interfaces, IP traffic is allowed to flow between configured VLANs on the product. Once the IP ACLs have been created and applied to interfaces, they take precedence over any VLAN traffic flows on those interfaces. The TOE only allows the privileged administrator to specify alternate values for the attributes used to enforce the SFPs.
FMT_MTD.1	The TOE provides the ability for administrators to manage TOE data, such as audit data, configuration data, security attributes, information flow rules, routing tables, and session thresholds. Each of the predefined and administratively configured roles has create (set), query, modify, or delete access to the TOE data. 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; 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

TOE SFRs	How the SFR is Met
	refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges can also modify TOE data based if granted the privilege.
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 using a SSH client 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: ***1.*** 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 and manage the cryptographic self-tests ***2.*** 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 ***3.*** Ability to manage information flow control attributes - allows the authorized administrator to configure the ACLs, to control the Ethernet and IP network traffic ***4.*** 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 ***5.*** Ability to manage security attributes belonging to individual users - allows the authorized administrator to create, modify, and delete other administrative users ***6.*** 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 ***7.*** 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 8. Ability to manage the time limits of session inactivity – allows the authorized administrator the ability to set and modify the inactivity time threshold 9. Ability to manage the configuration of the TOE authentication functions – allows the authorized administrator the ability to set, modify or delete the use of a AAA server. 10. Ability to manage the configuration of the TOE IPSec functionality – allows the authorized administrator the ability to add, and remove VPN peers. 11. Ability to manage the configuration of the TOE VLAN SFP – allows the authorized administrator to specify the attributes that are used to define VLANs.

TOE SFRs	How the SFR is Met
	12. Ability to manage the configuration of the TOE IDS functionality. 13. Ability to manage the configuration of the TOE clock and NTP configuration – allows the authorized administrator the ability to set and modify the internal clock as well as to configure NTP.
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 vpn peers connecting to the TOE via VPN tunnels.. 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 for the router, used in audit timestamps. This function can only be accessed from within the configuration exec mode via the privileged mode of operation of the TOE. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive time from an NTP server. Only NTP servers that support MD5 hashing of communications should be used for integrity purposes.
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, flush the screen, and no further

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>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.</td></tr>
<tr><td>FTA_TAB.1</td><td>The TOE displays a customizable login banner on the local and remote CLI management interface prior to allowing any administrative access to the TOE.</td></tr>
<tr><td>FTP_ITC.1</td><td>The TOE protects communications with vpn peers by transmitting them via an IPSec tunnel. See the discussion under FCS_GDOI_EXT.1 and FCS_IPSEC_EXT.1 above.</td></tr>
<tr><td>FTP_TRP.1</td><td>All remote administrative communications take place over a secure encrypted SSH session. The SSH session is encrypted using AES encryption. The remote privileged administrator or semi-privileged administrators are able to initiate SSH communications with the TOE.</td></tr>
<tr><td>IDS_SDC_EXT.1
IDS_ANL_EXT.1 and
IDS_RCT_EXT.1</td><td>The TOE collects and analyzes data that traverses it. This includes system data collection and the operations of analysis performed on network traffic. In addition the IDS functionality responds to an attack as configured by the privileged administrator.
The TOE is a software based Intrusion Prevention System collects and analyzes single packets, and retains state on user sessions to detect multiple packet attacks and packet content string matches. It captures network packets from the router, then reassembles and compares this data against a rule set that indicates typical intrusion activity. The information collected and recorded with each event includes date and time of the event, type of event and risk rating, IP and port address of the event (both source and destination), protocol type, and data associated with the event. The risk rating is used to indicate the relative risk of the traffic or offending host continuing to access the IT network. This rating can be used to illuminate the events that require immediate privileged administrator attention. The risk rating is an integer value in the range from 0 to 100. The higher the value, the greater the security risk of the trigger event for the associated alert.

The Network Traffic Analysis function applies a signature analysis method, different threat identification methods, and event correlation to analyze network traffic. For signature analysis method, it matches specific signatures or patterns that may characterize attack attempts to a database of known attacks. Different attacks involve different patterns of traffic, allowing definitions of traffic signatures for these attacks. This signature database can be updated and user customized only by privileged administrators to provide up-to-date coverage of known attacks. The updated signatures are available directly from Cisco. The table below summarizes examples of specific attacks the TOE attempts to defend against. Custom signatures may also be created by the privileged administrator. In order to manage the signatures in use, the administrator uses the “ip ips config location” command to specify the IPS configuration and the “ip ips signature-definition” command to define and tune the active signatures.
<table>
<tr><th>Category of Attack</th><th>Details</th><th>Example Attacks</th></tr>
<tr><td>Named attacks</td><td>Single attacks that have specific names or common identities</td><td>- Smurf
- PHF
- Land</td></tr>
<tr><td>General Category attacks</td><td>Attacks that keep appearing in new variations with the same basic</td><td>- Impossible IP Packet
- IP fragmentation</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>methodology</td><td></td></tr>
<tr><td>Extraordinary attacks</td><td>Extremely complicated or multi-faceted attacks</td><td>- TCP hijacking
- E-mail spam</td></tr>
</table>

Threat Identification Methods include stateful pattern recognition to identify vulnerability-based attacks through the use of multipacket inspection across all protocols; protocol analysis to provide protocol decoding and validation for network traffic; traffic and protocol anomaly detection that identify attacks based on observed deviations from normal traffic or protocol behavior; Layer 2 detection; anti-IPS evasion techniques to provide traffic normalization, IP defragmentation, TCP stream reassembly, and de-obfuscation. The Threat Identification Methods used by the Network Traffic Analysis function is dependent on whether the interface examined is configured for IPS or IDS services.

The Network Traffic Analysis function provides the Meta Event Generator to correctly classify malicious activity detected by the TOE by event correlation. Event correlation addresses those types of attacks that set off multiple low severity audit events which together results into a single event at a higher severity level. Classification of malicious activity is accomplished through:
• correlation of events pertaining to worms that exploit multiple vulnerabilities,
• correlation of a sequence of actions that lead up to worm infestation,
• correlation of multiple events at low severity level to result in a single event of higher severity, and
• enhancement of audit events fidelity through simultaneous triggers based on hybrid detection algorithms.

Each analytical result is written to the same event store as the other audit records. These events can then be viewed by the privileged administrator through the CLI Interface.

When the TOE generates an audit record, it is automatically sent to the event store in the form of an audit record. By default the TOE only generates an audit record when an intrusion is detected, however in inline mode (IPS), it can also be configured to send a command to the firewall functionality to block specific offending network traffic.</td></tr>
<tr><td>IDS_RDR_EXT.1
IDS_STG_EXT.1 and
IDS_STG_EXT.2</td><td>All IDS signatures trigger an Alert event, which provides notification of some suspicious activity that may indicate an intrusion attack is in progress or has been attempted. Alert events are generated by the analysis-engine whenever an IPS signature is triggered by network activity. The TOE IPS module provides continuously running audit functions which are used to record audit events. These audit events are then written to the fixed-size circular event store that is only writable by the TOE (that is, all generated audit and IPS events are written to one event store). Each event is stored in Extensible Markup Language (XML) format and can be viewed via the module’s CLI Interface. Valid authentication credentials are required in order to authenticate to the TOE. Only after authenticating is the privileged administrator allowed to view audit records; and this is the only way by which users can view audit records. Only a privileged administrator can clear audit records via the clear events command through the CLI Interface.
When the event store becomes full the number of records saved will be the most</td></tr>
</table>

TOE SFRs	How the SFR is Met
	recent system events stored in the event store limited by the storage space allocated to the event store. The actual bit size of the amount maintained is both proportional to the size of the event store and the actual bit size of the system events inserted in the event store subsequent to exhaustion. When the event store's capacity is reached, the TOE overwrites the oldest stored audit records

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, a 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, however, memory management and access control are all provided by the router module itself. In order to access any portion of the TOE, the Identification & 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. None of these interfaces provide any access to internal TOE resources.

The TOE provides a secure domain for each VLAN to operate within. Each VLAN has its own forwarding plane resources that other VLANs within the same TOE are not able to affect.

Finally, 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 traffic to or through the TOE is mediated by the TOE. 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 (either privileged administrator or semi-privileged administrator) 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 18: Threat/Policies/Objectives Mappings

	T.AUDIT_REVIEW	T.MEDIATE	T.NOAUDIT	T.NOAUTH	T.NOMGT	T.UNAUTH_MGT_ACCESS	T.TIME	T.USER_DATA_REUSE	T.UNAUTHORIZED_PEER	T.VPNMEDIAT	T.VLAN	T.NOHALT	T.FALACT	T.FALREC	T.FALASC	T.MISUSE	T.INADVE	T,MISACT	T.INTEGRITY	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												
O.PEER_AUTHENTICATION									X											
O.INTEGRITY										X									X	
O.VPNMEDIAT										X										
O.VLAN											X									
O.IDSENS												X				X	X	X		
O.IDANLZ												X		X	X					
O.RESPON													X							

Table 19: Threat/Policies/TOE Objectives Rationale

Threat / Policy	Rationale for Coverage
T.AUDIT_REVIEW	Actions performed by users may not be known to the administrators due to

Threat / Policy	Rationale for Coverage
	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 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.

Threat / Policy	Rationale for Coverage
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 cleared so that it is not inadvertently sent back out of the TOE.
T.UNAUTHORIZED_PEER	An unauthorized IT entity may attempt to establish a security association with the TOE. This threat is countered by the security objective O.PEER_AUTHENTICATION by requiring that the TOE implement IPSEC and IKE RFCs: RFCs 2407, 2408, 2409, 4109, and 4303, to establish a secure, authenticated channel between the TOE and another remote VPN endpoint before establishing a security association with that remote endpoint or another remote router before establishing a security association with that router. This security objective further mitigates this threat by requiring that the TOE implement the GDOI protocol, as specified in RFC 3547, as an extension to RFC2409. This protocol is used to establish security associations between groups of IPSec users.
T.VPNMEDIAT	An unauthorized person may send or receive unauthorized IPSec traffic through the TOE which results in the exploitation of resources on the internal network. This threat is countered by the security objective O.INTEGRITY which ensures that all IPSEC encrypted data received from a peer is properly decrypted and authentication verified. This threat is further countered by the security objective O.VPNMEDIAT which requires the TOE to mediate all IPSec communications and not allow other unauthorized communications.
T.VLAN	An attacker may force a packet destined for one VLAN to cross into another VLAN for which it is not authorized compromising the confidentiality and integrity of information. This threat is countered by the security objective O.VLAN which ensures that the TOE will be correctly configured in accordance with a security policy which will ensure VLAN separation.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. This threat is countered by the security objective O.IDSENS and O.IDANLZ that requires the TOE to collect and analyze system data, which includes attempts to halt the TOE. This threat is further countered by the security objective O.IDANLZ that requires the TOE to collect and analyze system data, including attempts to halt the TOE. It also requires that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

Threat / Policy	Rationale for Coverage
	This threat is countered by the security objective O.RESPON that ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source. This threat is countered by the security objective O.IDANLZ that requires the TOE to collect and analyze system data, including attempts to halt the TOE. It also requires that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources. This threat is countered by the security objective O.IDANLZ that requires the TOE to collect and analyze system data, including attempts to halt the TOE. It also requires that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors. This threat is countered by the security objective O.IDSENS that requires the TOE to collect system data.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors. This threat is countered by the security objective O.IDSENS that requires the TOE to collect system data.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors. This threat is countered by the security objective O.IDSENS that requires the TOE to collect system data.
T.INTEGRITY	An attacker may compromise the integrity of IPSec traffic sent to/from the TOE. This threat is countered by the security objective O.INTEGRITY which ensures that all IPSEC encrypted data received from a peer is properly decrypted and authentication verified.
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 20: 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 21: 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.
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

Assumptions	Rationale for Coverage of Environmental Objectives
	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, policies and IT security objectives.

Table 22: Objective to 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	O.PEER_AUTHENTICATION	O.INTEGRITY	O.VPNMEDIAT	O.VLAN	O.IDSENS	O.IDANLZ	O.RESPON
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_GDOI_EXT.1							X					X						
FCS_IPSEC_EXT.1							X					X						
FCS_SSH_EXT.1							X											
FDP_IFC.1(1)						X												
FDP_IFF.1(1)						X												
FDP_IFC.1(2)													X	X				
FDP_IFF.1(2)													X	X				
FDP_IFC.1(3)															X			
FDP_IFF.1(3)															X			
FDP_RIP.2											X							
FIA_ATD.1					X													

	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	O.PEER_AUTHENTICATION	O.INTEGRITY	O.VPNMEDIAT	O.VLAN	O.IDSENS	O.IDANLZ	O.RESPON
FIA_UAU.2					X													
FIA_UAU.5					X													
FIA_UAU.7					X													
FIA_UID.2					X													
FMT_MOF.1	X																	
FMT_MSA.3(1)	X					X								X				
FMT_MSA.3(2)	X					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								
FTP_ITC.1							X											
FTP_TRP.1							X											
IDS_SDC_EXT.1																X		
IDS_ANL_EXT.1																	X	
IDS_RCT_EXT.1																		X
IDS_RDR_EXT.1			X															
IDS_STG_EXT.1	X																	
IDS_STG_EXT.2			X															

Table 23: 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], delete audit data stored locally on the TOE [FAU_STG.1], or delete IDS event data stored locally on the TOE [IDS_STG_EXT.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(1) and FMT_MSA.3(2)]. 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 and IDS event data [IDS_RDR_EXT.1]. Security relevant events must be available for review by authorized administrators [FAU_SAR.1]. IDS audit data will be available until the buffer becomes full, after which the oldest events will be overwritten [IDS_STG_EXT.2].
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 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(1), and FDP_IFF.1(1)]. The policy is defined by rules defining the conditions for which information is permitted or denied to flow [FDP_IFF.1(1)]. The TOE provided the capability for administrators to define default deny rules, and routes must be enabled through the TOE before data can traverse it. Also VPN sessions cannot be established without configuring the appropriate policies [FMT_MSA.3(1)]. The default policy for the information flow control security rules for IP ACLs and VLANs are permissive where no explicit rules exist until created and applied by an authorized administrator [FMT_MSA.3(2)].
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), FCS_CKM.1(1), (2), FCS_CKM.4, FCS_GDOI_EXT.1, FCS_IPSEC_EXT.1, FCS_SSH_EXT.1, FTP_ITC.1, FTP_TRP.1]. The SFR FTA_SSL.3 also meet 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.
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.
O.PEER_AUTHENTICATION	The TOE must authenticate each peer TOE that attempts to establish a security association with the TOE so that the IPSec and GDOI sessions can be established correctly. The TOE must implement the Group Domain of Interpretation protocol defined in RFC 3547. By implementing this protocol, the TOE will establish a secure, authenticated channel with groups of peer TOEs for purposes of establishing a security association, which includes the establishment of a cryptographic key, algorithm and mode to be used for all communication [FCS_GDOI_EXT.1]. The TOE must implement the following IPSEC and IKE RFCs: RFCs 2407, 2408, 2409, 4109, and 4303. By implementing this protocol, the TOE will establish a secure, authenticated channel with each peer TOE for purposes of establishing a security association, which includes the establishment of a cryptographic key, algorithm and mode to be used for all communication [FCS_IPSEC_EXT.1].
O.INTEGRITY	The TOE must be able to protect the integrity of data transmitted to a peer via encryption and provide IPSec authentication for such data. Upon receipt of data from a peer, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted. The TOE ensures that all IPSEC encrypted data received from a TOE is properly decrypted and authentication verified [FDP_IFC.1(2) and FDP_IFF.1(2)].
O.VPNMEDIAT	The TOE must mediate the flow of all IPSec traffic through the TOE and must ensure that residual information from a previous IPSec traffic flow is not transmitted in any

	way. The TOE ensures that all IPSec traffic that should be allowed to flow through the TOE is allowed to flow. This component also ensures that no unauthorized plaintext traffic is allowed to flow through the TOE [FDP_IFC.1(2) and FDP_IFF.1(2)]. There is a restrictive default policy for the VPN information flow control security rules [FMT_MSA.3(1)].
O.VLAN	The TOE must provide a means for the logical separation of Virtual LANs to ensure that packets flows are restricted to their authorized Virtual LANs ensuring VLAN separation is achieved. The TOE ensures that all VLAN traffic sent and received is correctly separated from other VLAN traffic [FDP_IFC.1(3) and FDP_IFF.1(3)]. There is a permissive default policy for the information flow control security rules for IP ACLs and VLAN [FMT_MSA.3(2)].
O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS [IDS_SDC_EXT.1].
O.IDANLZ	The Analyzer must accept data from IDS Sensors and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future) [IDS_ANL_EXT.1].
O.RESPON	The TOE must respond appropriately to analytical conclusions [IDS_RCT_EXT.1].

ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 24: 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-2009-07-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-004