Cisco 5940 Series Embedded Services Router

Security Target

Revision 1.2

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 5940 Series Embedded Services Router. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

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

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

1.1 ST and TOE Reference

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

Table 1: ST and TOE Identification

ST Title	Cisco 5940 Series Embedded Services Router Security Target
ST Version	1.2
Publication Date	January 2013
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco 5940 Series Embedded Services Router
TOE Hardware Models	conduction cooled processor module; air cooled processor module
TOE Software Version	IOS 15.2(3)GC
ST Evaluation Status	In Evaluation
Keywords	Switch, Data Protection, Authentication, Firewall, IDS

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
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
cPCI	Compact Peripheral Component Interconnect
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
HTTPS	Hyper-Text Transport Protocol Secure
IPS	Intrusion Prevention System
ISR	Integrated Service Router
IT	Information Technology

Acronyms / Abbreviations	Definition
J2	A pin connection type for the backplanes of PCI cards. Not an acronym.
JTAG	Joint Test Action Group
OS	Operating System
PCI	Peripheral Component Interconnect
PP	Protection Profile
pp_fw_tf_br_v1.1	U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments
RJ-45	Registered Jack 45
SHS	Secure Hash Standard
SSH	Secure Shell
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
WAN	Wide Area Network
WIC	WAN Interface Card

1.3 TOE Overview

The Cisco 5940 Series Embedded Services Router TOE is a purpose-built, routing platform that includes firewall, Intrusion Prevention, and VPN functionality. The firewall functionality included within the TOE provides the functionality specified in the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments. The TOE includes one router module that can operate in any CompactPCI (cPCI) 3 unit (3U) chassis.

1.3.1 TOE Product Type

The Cisco 5940 Series Embedded Services Router is a router platform that 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 Cisco 5940 Series Embedded Services Router provides IPSec connection capabilities for VPN enabled clients connecting through the Cisco 5940 Series Embedded Services Router. The Cisco 5940 Series Embedded Services Router is also compatible with the GET VPN (using GDOI).

The Cisco 5940 Series Embedded Services Router also supports firewall capabilities consistent with the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments. The Cisco 5940 Series Embedded Services Router is a 3U (cPCI) 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 5940 Series 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
Router Chassis	Yes	The host chassis for the router provides the power to the module as well as directly connected Ethernet interfaces via a standard cPCI backplane. The chassis selected can be any off –the-shelf chassis that supports 3U cPCI cards.
Rear Transition Module (RTM)	Yes	The RTM supports Input/Ouput connectors through standard RJ-45 connectors, or any other cPCI compatible network connector. The RTM can be any off-the-shelf module that is a cPCI form factor. It is installed in the chassis directly opposite the card with which it is to be used.
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 SSH v2 may be used.
AAA Server	Yes	This includes any IT environment AAA server that provides single-use authentication mechanisms. This can be any AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this AAA server to provide single-use authentication to administrators.
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

Component	Required	Usage/Purpose Description for TOE performance
		must be used that supports MD5 hashing of communications with up to a 32 character key.
Syslog Server	Yes	A syslog server with the capability to support TCP syslog communications over an IPSec tunnel is required for use with the TOE.
Certificate Authority (CA)	No	This includes any IT Environment Certificate Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment for IKE authentication.

1.4 TOE DESCRIPTION

This section provides an overview of the Cisco 5940 Series Embedded Services Router Target of Evaluation (TOE). The TOE is comprised of a single cPCI router module running IOS 15.2(3)GC.

1.5 Physical Scope of the TOE

The TOE is a hardware solution obtained from General Dynamics under OEM contract running the IOS 15.2(3)GC software solution. The image name for the 5940 Series Embedded Services Router TOE is c59xx-adventerprisek9-mz.SPA. The key components on the board are:

- Freescale MPC8548E processor
- Marvell 88E1145 quad Ethernet transceiver
- Spansion S29GL01GP flash or Numonyx flash chip

Both an air-cooled and a conduction-cooled board exist. Aside from the differences outlined below, they differ only in cooling mechanism.

The board provides the following external interfaces:

- Serial port.
  - Via a connection on the J2 connector on the cPCI backplane on the conduction-cooled model and via direct access RJ-45 port or the J2 connector on the cPCI backplane on the card on the air-cooled model.
- Four Gigabit Ethernet ports, via connections on the J2 connector on the cPCI backplane.
- PCI interface connection to the backplane. This PCI interface is used to connect to the RTM
- PCI bus connection to the backplane. This PCI controller is disabled within the IOS running on the TOE.
- JTAG header. The JTAG will be connected to the J2 connector on the cPCI backplane. It is to be disabled in the evaluated configuration and not re-enabled.

1.6 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. Identification and Authentication
2. Secure Management
3. VPN and/or Firewall Information Flow Control
4. Intrusion Prevention Services
5. Cryptography
6. Secure Auditing

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

1.6.1 Identification and Authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the administrators of the TOE. 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. The TOE provides authentication services for all administrators wishing to connect to the TOEs secure CLI administrative interface. The TOE requires all administrators to authenticate prior to being granted access to any of the management functionality.

The TOE facilitates single-use authentication for all administrators and external IT entities attempting to connect to the TOE by invoking an external RADIUS AAA (IT environment) to provide single-use authentication. The TOE provides single use authentication to external IT entities through the use of IKE/IPSec mutual authentication.

1.6.2 Secure Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSH session, via terminal server (such as a Cisco 2811), or via a local console connection. The TOE provides the ability to securely manage all TOE administrators; all identification and authentication; all audit functionality of the TOE; all TOE cryptographic functionality; the timestamps maintained by the TOE (including settings for an NTP server, if used as the timestamp source); TOE configuration backup and recovery, and the information flow control policies enforced by the TOE. The TOE supports two separate administrative roles that make up the authorized administrator: non-privileged Administrator and privileged Administrator.

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 which the TOE exchanges information, including VPN clients and VPN gateways.

Once a configured threshold of consecutive authentication failures is reached, the TOE locks-out the administrator (either privileged or non-privileged) or external IT entity attempting to log into the TOE until another administrator unlocks their account. No

administrator can unlock their own account, therefore there should always be at least two privileged administrators configured on the device.

1.6.3 Information Flow Control

1.6.3.1 Firewall Information Flow Control

The Cisco 5940 Series Embedded Services Router mediate information flows through the TOE for unauthenticated information flows. The Information Control functionality of the TOE allows privileged administrators to set up rules between interfaces of the TOE. These rules control whether a packet is transferred from one interface to another and/or transferred encrypted based upon:

1. Presumed address of source subject
2. Presumed address of destination subject
3. Service used
4. Transport layer protocol
5. Network interface on which the connection request occurs and is to depart

Packets will be dropped unless a specific rule or policy in an access control list (ACL) has been set up to allow the packet to pass. The order of Access Control Entries (ACEs) in an ACL is important. When the TOE decides whether to forward or drop a packet, the TOE tests the packet against the ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked such that if the ACE at the beginning of the ACL explicitly permits all traffic, no further ACEs are checked. Interface ACLs are applied first before IPsec negotiations occur in the evaluated configuration.

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeroes. Residual data is never transmitted from the TOE.

1.6.3.2 VPN Information Flow Control

Cisco 5940 Series Embedded Services Router 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.

1.6.3.3 VLAN Information Flow Control

Cisco 5940 Series Embedded Services Router 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.

1.6.4 Intrusion Prevention Services

The Cisco 5940 Series Embedded Services Router 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 firewall policies and then VPN policies have been applied.

1.6.5 Cryptography

The TOE provides cryptography in support of other Cisco 5940 Series Embedded Services Router security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 1. Further details regarding the FIPS validation can be found in Certificate #1639. The TOE provides cryptography in support of VPN connections and remote administrative management via SSH. The cryptographic services provided by the TOE include

Table 4: TOE Provided Cryptography

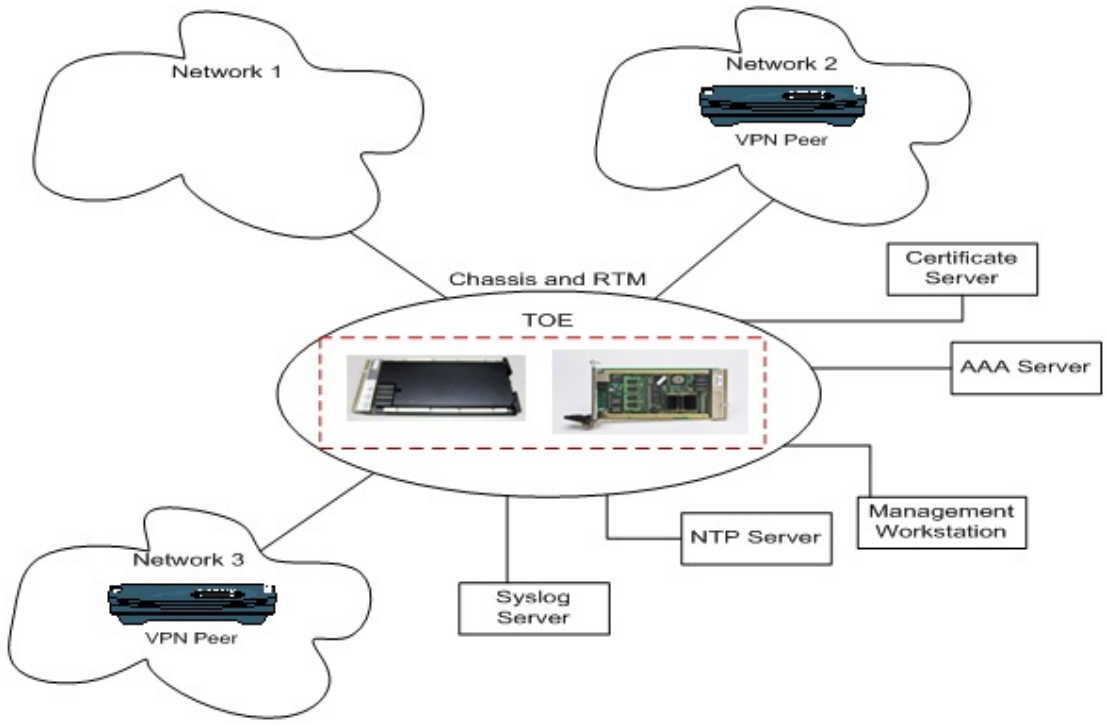
Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPSec session.
ANSI X9.31 PRNG	Used in IPSec session establishment.
AES	Used to encrypt IPSec session traffic. Used to encrypt SSH session traffic.
Group Domain of Interpretation	Used in IPSec session establishment.
RSA	IKE RSA authentication
DSA	SSH host authentication, SSH client authentication
SHA256	IKE

1.6.6 Secure Auditing

The Cisco 5940 Series Embedded Services Router provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, information flow control enforcement, intrusion prevention, identification and authentication, and administrative actions. The Cisco 5940 Series Embedded Services Router generates an audit record for each auditable event. These events include a timestamp that can be provided by the TOE or an optional NTP server in the operational environment. The Cisco 5940 Series Embedded Services Router provides the privileged administrator with a sorting and searching capability to improve audit analysis. The privileged administrator configures auditable events, backs-up and manages audit data storage. The TOE provides the privileged administrator with a local circular audit trail, also referred to as the Event Store,and allows for configuration of offload of audit data via TCP syslog to a syslog server in the operational environment so that audit events are not lost when the Event Store reaches capacity and begins to overwrite old events.

1.7 TOE Evaluated Configuration

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a dashed red line.



The previous figure includes the following:

- The 5940 TOE Model (both the conduction-cooled and air-cooled models are pictured.)

- IT Environment: Chassis and RTM
- IT Environment: (2) VPN Peers
- IT Environment: Management Workstation
- IT Environment: AAA Server
- IT Environment: NTP Server
- IT Environment: Syslog Server

1.7.1 Excluded Functionality

The following functional 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.
Telnet for management purposes.	Telnet passes authentication credentials in clear text. SSHv2 is to be used instead.

The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments.

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 Part 3 conformant.
The TOE and ST are CC Part 2 extended.

2.2 Protection Profile Conformance

This ST claims compliance to the following Common Criteria validated Protection Profiles:

Table 6: Protection Profiles

Protection Profile	Version	Date
U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments (pp_fw_tf_br_v1.1)	1.1	July 25, 2007

2.2.1 Protection Profile Refinements

The following table identifies the refinements made to the Protection Profile and provides rationale for the refinement:

Table 7: Protection Profile Refinements

Refinement	Rationale
FAU_GEN.1	Refined to refer to the correct table number and to add an additional event to the audit table.
FAU_SAR.1	Refined to clarify that privileged administrators are affected.
FMT_SMR.1	Refined to also address External IT entities and to clarify that both privileged and non-privileged administrators are included.
FIA_ATD.1	Refined to also address External IT entities
FMT_MSA.3(1)	Refined to specify the privileged administrator.
FMT_MOF.1	Refined to specify the privileged administrator and what a non-privileged administrator is able to access.

The names of all of the Objectives on the Environment were changed from O.XXXXX to OE.XXXXX in this ST.

2.2.2 Protection Profile Additions

The following threats were added to the TOE:

- T.UNAUTHORIZED_PEER
- T.EAVESDROP
- T.VPNMEDIAT
- T.VLAN
- T.NOHALT
- T.FALACT
- T.FALREC

- T.FALASC
- T.MISUSE
- T.INADVE
- T.MISACT
- T.INTEGRITY

The following objectives were added to the TOE:

- O.CRYPTOGRAPHIC_ FUNCTIONS
- O.PEER_AUTHENTICATION
- O.INTEGRITY
- O.VPNMEDIAT
- O.VLAN
- O.IDSENS
- O.IDANLZ
- O.RESPON

The following requirements were added to the set of SFRs on the TOE:

- FCS_CKM.4
- FCS_COP_(EXT).1
- FCS_GDOI_(EXT).1
- FCS_IKE_(EXT).1
- FDP_IFC.1(2)
- FDP_IFF.1(2)
- FDP_IFC.1(3)
- FDP_IFF.1(3)
- FMT_MSA.3(2)
- FMT_MSA.3(3)
- FMT_SMF.1
- FTP_ITC.1
- FTP_TRP.1
- IDS_SDC_(EXT).1
- IDS_ANL_(EXT).1
- IDS_RCT_(EXT).1
- IDS_RDR_(EXT).1
- IDS_STG_(EXT).1
- IDS_STG_(EXT).2

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

The TOE provides all of the Traffic Filter Firewall functionality at a level of security commensurate with that identified in the U.S. Government Protection Profile:

- U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments (pp_fw_tf_br_v1.1)

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments for which conformance is claimed verbatim. Several additional Threats are also included. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target. None of the additional Threats contradicts the functionality specified in the Protection Profile. The additional Threats augment the firewall functionality specified in the Protection Profiles and discuss additional TOE functionality that is not addressed in the Protection Profile. The following table identifies each additional Threat included in the ST and provides rationale for its inclusion in the Security Target with regards to the claims Protection Profiles.

Table 8: Protection Profile Threat Additions

Threat/OSP	Rationale
T.UNAUTHORIZED_PEER	This threat is associated with VPN functionality. The PP addresses firewall functionality and not VPN functionality. This VPN functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
T.EAVESDROP	This threat is associated with VPN functionality. The PP addresses firewall functionality and not VPN functionality. This VPN functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
T.VPNMEDIAT	This threat is associated with VPN functionality. The PP addresses firewall functionality and not VPN functionality. This VPN functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
T.VLAN	This threat is associated with VLAN functionality. The PP addresses firewall functionality and not VLAN functionality. This VLAN functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
T.NOHALT	This threat is associated with IDS functionality. The PP addresses firewall functionality and not IDS functionality. This IDS functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
T.FALACT	This threat is associated with IDS functionality. The PP addresses firewall functionality and not IDS functionality. This IDS functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
T.FALREC	This threat is associated with IDS functionality. The PP addresses firewall functionality and not IDS functionality. This IDS functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
T.FALASC	This threat is associated with IDS functionality. The PP addresses firewall functionality and not IDS functionality. This IDS functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
T.MISUSE	This threat is associated with IDS functionality. The PP addresses firewall functionality and not IDS functionality. This IDS functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.

Threat/OSP	Rationale
T.INADVE	This threat is associated with IDS functionality. The PP addresses firewall functionality and not IDS functionality. This IDS functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
T.MISACT	This threat is associated with IDS functionality. The PP addresses firewall functionality and not IDS functionality. This IDS functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
T.INTEGRITY	This threat is associated with VPN functionality. The PP addresses firewall functionality and not VPN functionality. This VPN functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.

2.3.3 Statement of Security Objectives Consistency

The Security Objectives included in the Security Target represent the Security Objectives specified in the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments for which conformance is claimed verbatim. Several additional Security Objectives are also included. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target. None of the additional Security Objectives contradicts the functionality specified in the Protection Profile. The additional Security Objectives augment the firewall functionality specified in the Protection Profiles and discuss additional TOE functionality that is not addressed in the Protection Profile. The following table identifies each additional Security Objective included in the ST and provides rationale for its inclusion in the Security Target with regards to the claims Protection Profiles.

Table 9: Protection Profile Security Objective Additions

Security Objective	Rationale
O.CRYPTOGRAPHIC_ FUNCTIONS	This Security Objective augments the cryptographic functionality discussed in the PP for which conformance is claimed. This policy does not introduce any functionality that is inconsistent with the cryptography specified in the PP for which conformance is claimed.
O.PEER_AUTHENTICATION	This Security Objective is associated with VPN functionality. The PP addresses firewall functionality and not VPN functionality. This VPN functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
O.INTEGRITY	This Security Objective is associated with VPN functionality. The PP addresses firewall functionality and not VPN functionality. This VPN functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
O.VPNMEDIAT	This Security Objective is associated with VPN functionality. The PP addresses firewall functionality and not VPN functionality. This VPN functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
O.VLAN	This Security Objective is associated with VLAN functionality. The PP addresses firewall functionality and not VLAN functionality. This VLAN functionality provided to counter this threat does not contradict

Security Objective	Rationale
	any of the functionality required by the PP for which conformance is claimed.
O.IDSENS	This Security Objective is associated with IPS functionality. The PP addresses firewall functionality and not IPS functionality. This IPS functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
O.IDANLZ	This Security Objective is associated with IPS functionality. The PP addresses firewall functionality and not IPS functionality. This IPS functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.
O.RESPON	This Security Objective is associated with IPS functionality. The PP addresses firewall functionality and not IPS functionality. This IPS functionality provided to counter this threat does not contradict any of the functionality required by the PP for which conformance is claimed.

2.3.4 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments for which conformance is claimed verbatim. Several additional Security Functional Requirements are also included. All concepts covered the Protection Profile's Statement of Security Requirements are included in the Security Target. Additionally, the Security Assurance Requirements included in the Security Target are identical to the Security Assurance Requirements included in each of the Protection Profiles. None of the additional Security Functional Requirements contradicts the functionality specified in the Protection Profile. The additional Security Functional Requirements augment the firewall functionality specified in the Protection Profiles and discuss additional TOE functionality that is not addressed in the Protection Profile. The following table identifies each additional Security Functional Requirement included in the ST and provides rationale for its inclusion in the Security Target with regards to the claims Protection Profiles.

Table 10: Protection Profile Security Functional Requirement Additions and Refinements

SFR	Rationale
FAU_GEN.1	This SFR was refined to add an additional event type to be audited and to refer to the correct table within the requirement wording. This does not contradict any claims in the PP or weaken the claimed security functionality.
FAU_SAR.1	This SFR was refined to clarify that this instance of "authorized administrators" applies to privileged administrators. This does not contradict any claims in the PP or weaken the claimed security functionality.
FMT_SMR.1	This SFR was refined to add a role used elsewhere in the PP SFRS: external IT entities. This does not contradict any claims in the PP or weaken the claimed security functionality.
FIA_ATD.1	This SFR was refined to add the authentication attributes for external IT entities. This does not contradict any claims in the PP or weaken the claimed security functionality.
FMT_MSA.3(1)	This SFR was refined to clarify that this instance of "authorized administrators" applies to only privileged administrators. This does not

SFR	Rationale
	contradict any claims in the PP or weaken the claimed security functionality.
FMT_MOF.1	This SFR was refined to clarify that this instance of "authorized administrators" applies to privileged administrators. This does not contradict any claims in the PP or weaken the claimed security functionality.
FCS_CKM.4	This SFR discusses the cryptographic key destruction. This functionality is not discussed in the Protection Profile for which conformance is claimed. Cryptographic key destruction does not contradict any of the cryptographic functionality included in the PP.
FCS_COP_(EXT).1	This SFR discusses random number generation. This functionality is not discussed in the Protection Profile for which conformance is claimed. Random number generation does not contradict any of the cryptographic functionality included in the PP.
FCS_GDOI_(EXT).1	This SFR discusses Group Domain of Interpretation. This functionality is not discussed in the Protection Profile for which conformance is claimed. Group Domain of Interpretation does not contradict any of the cryptographic functionality included in the PP.
FCS_IKE_(EXT).1	This SFR discusses IKE Key establishment. This functionality is not discussed in the Protection Profile for which conformance is claimed. IKE Key Establishment does not contradict any of the cryptographic functionality included in the PP.
FDP_IFC.1(2)	This SFR discusses VPN functionality. This functionality is not discussed in the Protection Profile for which conformance is claimed. VPN functionality does not contradict any of the information flow control included in the PP.
FDP_IFF.1(2)	This SFR discusses VPN functionality. This functionality is not discussed in the Protection Profile for which conformance is claimed. VPN functionality does not contradict any of the information flow control included in the PP.
FDP_IFC.1(3)	This SFR discusses VLAN functionality. This functionality is not discussed in the Protection Profile for which conformance is claimed. VLAN functionality does not contradict any of the information flow control included in the PP.
FDP_IFF.1(3)	This SFR discusses VLAN functionality. This functionality is not discussed in the Protection Profile for which conformance is claimed. VLAN functionality does not contradict any of the information flow control included in the PP.
FMT_MSA.3(2)	This SFR discusses the required security attribute management associated with VPN controls. The PP for which conformance is claimed does not address VPN information flow. Therefore it does not address the management of the security attributes associated with VPNs. This management functionality does not contradict any of the functionality described in the PP for which conformance is claimed.
FMT_SMF.1	This SFR discusses the overall security functions associated with secure management of the TOE. While the PP does not include this SFR, the CCTL requested its inclusion for consistency with other Security Target.
FTP_ITC.1	This SFR discusses protected communications between a remote syslog and the TOE. This SFR complements the cryptographic requirements already included in the SFR for management communications with the TOE. This SFR does not introduce any functionality that is conflicting with the functionality required by the PP for which conformance is claimed.
FTP_TRP.1	This SFR discusses trusted paths between a remote workstation and the TOE. This SFR complements the cryptographic requirements already included in the SFR for management communications with the TOE. This SFR does not introduce any functionality that is conflicting with the functionality required by the PP for which conformance is claimed.
IDS_SDC_(EXT).1	This SFR discusses IDS functionality on the TOE. This SFR does not introduce any functionality that is conflicting with the functionality required by the PP for which conformance is claimed.

SFR	Rationale
IDS_ANL_(EXT).1	This SFR discusses IDS functionality on the TOE. This SFR does not introduce any functionality that is conflicting with the functionality required by the PP for which conformance is claimed.
IDS_RCT_(EXT).1	This SFR discusses IDS functionality on the TOE. This SFR does not introduce any functionality that is conflicting with the functionality required by the PP for which conformance is claimed.
IDS_RDR_(EXT).1	This SFR discusses IDS functionality on the TOE. This SFR does not introduce any functionality that is conflicting with the functionality required by the PP for which conformance is claimed.
IDS_STG_(EXT).1	This SFR discusses IDS functionality on the TOE. This SFR does not introduce any functionality that is conflicting with the functionality required by the PP for which conformance is claimed.
IDS_STG_(EXT).2	This SFR discusses IDS functionality on the TOE. This SFR does not introduce any functionality that is conflicting with the functionality required by the PP for which conformance is claimed.

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 11: TOE Assumptions

Assumption	Assumption Definition
Reproduced from the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments	
A.PHYSEC	The TOE is physically secure.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.

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 unsophisticated.

Table 12: Threats

Threat	Threat Definition
Threats addressed by the TOE	

Threat	Threat Definition
Reproduced from the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments	
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.
In addition to what is included in the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments	
T.UNAUTHORIZED_PEER	An unauthorized IT entity may attempt to establish a security association with the TOE.
T.EAVESDROP	A malicious user or process may observe or modify user or TSF data transmitted to and from 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 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.
Threats addressed by the environment	

Threat	Threat Definition
Reproduced from the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments	
T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

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. This ST contains no claims for organizational security policies.

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 13: Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
Reproduced from the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments	
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.
O.MEDIAT	The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
In addition to what is included in the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments	
O.CRYPTOGRAPHIC_ FUNCTIONS	The TOE shall provide cryptographic functions to provide confidentiality for TSF data that is transmitted to and from the TOE.

TOE Objective	TOE Security Objective Definition
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 Protection Profile 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 14: Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
Reproduced from the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments	
A.PHYSEC	The TOE is physically secure.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.

Environment Security Objective	IT Environment Security Objective Definition
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
In addition to what is included in the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments	
OE.NTP	The IT environment may be configured with an NTP server that is able to provide reliable time to the TOE. The communications must be protected using MD5 hashing with up to a 32 character key.
OE.SYSLOG	The IT environment must supply a syslog server capable of receiving TCP syslog information over an IPSec tunnel.

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*.

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: Indicated by showing the value in square brackets, [assignment_value];
- Refinement made by PP author: Indicated with **bold** text and strikethroughs, if necessary;
- Refinement made by ST author: Indicated with ***bold italicized*** text and strikethroughs, if necessary;
- Selection: Indicated with *italicized* text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

Explicitly stated SFRs are identified by having a label '(EXT)' after the requirement name for TOE SFRs.

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 15: Security Functional Requirements

Functional Component	
SFR Component ID	**Component Name**
Security Functional Requirements Drawn from pp_fw_tf_br_v1.1	
FMT_SMR.1	Security roles
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action

Functional Component	
FIA_UAU.1	Timing of authentication
FIA_AFL.1	Authentication failure handling
FIA_UAU.4	Single-use authentication mechanisms
FDP_IFC.1 (1)	Subset information flow control
FDP_IFF.1 (1)	Simple security attributes
FMT_MSA.3 (1)	Static attribute initialization
FDP_RIP.1	Subset residual information protection
FCS_COP.1	Cryptographic operation
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FMT_MOF.1	Management of security functions behavior
FPT_STM.1	Reliable time stamps
SFRs in addition to the SFRs found in pp_fw_tf_br_v1.1	
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP_(EXT).1	Explicit: Random Number Generation
FCS_GDOI_(EXT).1	Group Domain of Interpretation
FCS_IKE_(EXT).1	Internet Key Exchange
FDP_IFC.1 (2)	Subset information flow control
FDP_IFF.1 (2)	Simple security attributes
FDP_IFC.1 (3)	Subset information flow control
FDP_IFF.1 (3)	Simple security attributes
FMT_MSA.3 (2)	Static attribute initialization
FMT_MSA.3 (3)	Static attribute initialization
FMT_SMF.1	Specification of Management Functions
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path
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

5.3 SFRs Drawn from pp_fw_tf_br_v1.1

5.3.1 Security audit (FAU)

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 - *Refinement:* 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 **relevant** auditable events for the *minimal or basic* level of audit **specified in Table 5.2;** and
c) [the event in ***the following t***~~T~~able ~~5.2~~ listed at the "extended" level].

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

a) Date and time of the event, type of event, subject**s** identit**ies**, 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 column four of ***the following t***~~T~~able ~~5.2~~].

Table 16: Security Functional Requirements

SFR	Level	Auditable Event	Additional Contents
FMT_SMR.1	minimal	Modifications to the group of users that are part of **the authorized administrator** role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
FIA_UID.2	basic	All use of the user identification mechanism	The user identities provided to the TOE
FIA_UAU.1	basic	Any use of the authentication mechanism.	The user identities provided to the TOE
FIA_AFL.1	minimal	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the authorized administrator of the user's capability to authenticate.**	The identity of the offending user and the authorized administrator
FDP_IFF.1(1)	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FDP_IFF.1(2)	***minimal***	***Errors during IPSec processing, errors during TLS processing***	***The presumed addresses of the source and destination subject.***
FCS_COP.1	minimal	Success and failure, and the type of cryptographic operation	The identity of the external IT entity attempting to perform the cryptographic operation
FPT_STM.1	minimal	Changes to the time.	The identity of the authorized administrator performing the operation.
FMT_MOF.1	extended	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation.

FAU_SAR.1 Audit review

FAU_SAR.1.1 - ***Refinement:*** The TSF shall provide [an authorized administrator ***(privileged)***] with the capability to read [all audit trail data] from the audit records.

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

FAU_SAR.3 Selectable audit review

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

a) [presumed subject address;
b) ranges of dates;
c) ranges of times;
d) ranges of addresses].

FAU_STG.1 Protected audit trail storage

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

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

FAU_STG.4 Prevention of audit data loss

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

5.3.2 Cryptographic Support (FCS)

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 - The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with a specified cryptographic algorithm:

- [AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67)] and cryptographic key sizes [that are at least 128 binary digits in length] that meet the following: [FIPS PUB 140-2 (Level 1)].

5.3.3 User data protection (FDP)

FDP_IFC.1(1) Subset information flow control

FDP_IFC.1.1(1) - The TSF shall enforce the [UNAUTHENTICATED SFP] on:

a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;
b) information: traffic sent through the TOE from one subject to another;
c) operation: pass information].

FDP_IFF.1(1) Simple security attributes

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

a) [subject security attributes:
    - presumed address;

- [configured zone];

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

FDP_IFF.1.2(1) - The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** 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.]

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

FDP_IFF.1.4(1) - The TSF shall provide the following [none].

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

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

a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed 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.]

FDP_RIP.1 Subset residual information protection

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

5.3.4 Identification and authentication (FIA)

FIA_ATD.1 User attribute definition

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

a) **[*For TOE administrators***
    a. identity;
    b. association of a human user with the authorized administrator role;
    c. User Password
b) ***For External IT entities***
    a. subject identity (IP address/Host Name);
    b. IKE Security Attributes].

.

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.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 - The TSF shall allow [identification as stated in FIA_UID.2] on behalf of the authorized administrator or authorized external IT entity accessing the TOE to be performed before the authorized administrator or authorized external IT entity is authenticated.

FIA_UAU.1.2 - The TSF shall require each authorized administrator or authorized external IT entity to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that authorized administrator or authorized IT entity.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 - The TSF shall detect when [a settable, non-zero number between 1 and 25] **of** unsuccessful authentication attempts occur related to [external IT entities attempting to authenticate from an internal or external network.]

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

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 - The TSF shall prevent reuse of authentication data related to [authentication attempts from either an internal or external network by:

a) authorized administrators;
b) authorized external IT entities].

5.3.5 Security management (FMT)

FMT_SMR.1 Security roles

FMT_SMR.1.1 - ***Refinement:*** The TSF shall maintain the role [authorized ***(privileged/non-privileged)*** administrator***, External IT entities***].

FMT_SMR.1.2 - The TSF shall be able to associate **human** users with **the authorized administrator** role.

FMT_MSA.3(1) Static attribute initialization

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

FMT_MSA.3.2(1) - ***Refinement:*** The TSF shall allow the [~~authorized~~ ***privileged*** administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 - ***Refinement:*** The TSF shall restrict the ability to **perform** the functions:

a) [start-up and shutdown;

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;
c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;
d) enable and disable single-use authentication mechanisms in FIA_UAU.4 (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);
e) modify and set the threshold for the number of permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);
f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);
g) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);
h) modify and set the time and date;
i) archive, create, delete, empty, and review the audit trail;
j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;
k) recover to the state following the last backup;
l) additionally, if the TSF supports remote administration from either an internal or external network:
    - enable and disable remote administration from internal and external networks;
    - restrict addresses from which remote administration can be performed;
m) [manipulate the security attributes referenced in the VPN information flow polices;
n) manipulate the security attributes referenced in the VLAN information flow polices
o) enable, disable, and modify the IPS settings on the box**]**].

to [a~~n authorized~~ ***privileged*** administrator].

5.3.6 Protection of the TSF (FPT)

FPT_STM.1 Reliable time stamps

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

5.4 SFRs in addition to the SFRs found in pp_fw_tf_br_v1.1

5.4.1 Cryptographic Support (FCS)

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 - The TSF shall destroy cryptographic keys in accordance with specified cryptographic key destruction method [zeroization] that meets the following: [Key

zeroization requirements of FIPS PUB 140-2, "Security Requirements for Cryptographic Modules"].

FCS_COP_(EXT).1 Explicit: Random Number Generation

FCS_COP_(EXT).1.1 - The TSF shall perform all Random Number Generation used by the cryptographic functionality of the TSF using a FIPS-approved Random Number Generator implemented in a FIPS-approved crypto module running in a FIPS-approved mode.

Extended Requirements Rationale – FCS_COP_(EXT).1:

A. Class – The FCS class of SFRs identifies cryptographic functionality provided by the TOE. FCS_COP_(EXP).1 describes the Random Number Generator (RNG) implemented by the TOE. This is cryptographic functionality and consistent with the FCS class of SFRs.
B. Family – The COP family exists within the CC. This family describes cryptographic operations implemented within the TOE. Since this SFR describes random number generation (which is a cryptographic operation), this SFR was included in the COP family.
C. Component – This is the only component included as an extension of the family. This is why the component is identified as "1."

Management – FCS_COP_(EXT).1:

There are no management activities foreseen.

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(1).

Extended Requirements Rationale – FCS_GDOI_(EXT).1:

A. Class – 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.

B. Family – 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.

C. Component – This is the only component in the family. This is why the component is identified as "1."

Management – FCS_GDOI_(EXT).1:

There are no management activities foreseen.

FCS_IKE_(EXT).1 Internet Key Exchange

FCS_IKE_(EXT).1.1 – The TSF shall provide cryptographic key establishment techniques in accordance with RFC 2409 as follows(s):

- Phase 1, the establishment of a secure authenticated channel between the TOE and another remote VPN endpoint, shall be performed using one of the following, as configured by the privileged administrator:
  - Main Mode
  - Aggressive Mode
  - New Group mode shall include the private group 14, 2048-bit MOD P
- Phase 2, negotiation of security services for IPSec, shall be done using Quick Mode, using SHA-1 as the pseudo-random function. Quick Mode shall generate key material that provides perfect forward secrecy. The use of SHA-256 and SHA-384 as the PRF in IKEv1 KDF is also allowed.

FCS_IKE_(EXT).1.2 – The TSF shall require the x of g^xy be randomly generated using a FIPS-approved random number generator when computation is being performed.

FCS_IKE_(EXT).1.3 - When performing authentication using pre-shared keys, the key shall be generated using the FIPS approved random number generator specified in FCS_COP_(EXT).1.

FCS_IKE_(EXT).1.4 - The TSF shall compute the value of SKEYID (as defined in RFC 2409), using SHA-1 as the pseudo-random function. The TSF shall be capable of authentication using the methods for

- Signatures: SKEYID = sha(Ni_b | Nr_b, g^xy)
- Pre-shared keys: SKEYID = sha(pre-shared-key, Ni_b | Nr_b)

- Authentication using Public key encryption, computing SKEYID as follows: SKEYID = sha(Ni_b | Nr_b), CKY-I | Nr_b

FCS_IKE_(EXT).1.5 - The TSF shall compute authenticated keying material as follows:

- SKEYID_d = sha(SKEYID, g^xy | CKY-I | CKY-R | 0)
- SKEYID_a = sha(SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)
- SKEYID_e = sha(SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)

FCS_IKE_(EXT).1.6 - To authenticate the Phase 1 exchange, the TSF shall generate HASH_I if it is the initiator, or HASH_R if it is the responder as follows:

- HASH_I = sha(SKEYID, g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDii_b)
- HASH_R = sha(SKEYID, g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDir_b)

FCS_IKE_(EXT).1.7 - The TSF shall be capable of authenticating IKE Phase 1 using the following methods as defined in RFC 2409, as configured by the privileged administrator:

a) Authentication with digital signatures: The TSF shall use RSA;
b) when an RSA signature is applied to HASH I or HASH R it must be first PKCS#1 encoded. The TSF shall check the HASH_I and HASH_R values sent against a computed value to detect any changes made to the proposed transform negotiated in phase one. If changes are detected the session shall be terminated and an alarm shall be generated.
c) X.509 certificates Version 3. X.509 V3 implementations, if implemented, shall be capable of checking for validity of the certificate path, and at option of SA, check for certificate revocation.
d) Authentication with a pre-shared key: The TSF shall allow authentication using a pre-shared key.

FCS_IKE_(EXT).1.8 - The TSF shall compute the hash values for Quick Mode in the following way

HASH(1) = sha(SKEYID_a, M-ID | SA | Ni [| KE] [| IDci | IDcr)]
HASH(2) = sha(SKEYID_a, M-ID | Ni_b |SA| Nr [| KE] [| IDci | IDcr)]
HASH(3) = sha(SKEYID_a, 0 | M-ID | Ni_b | Nr_b)

FCS_IKE_(EXT).1.9 - The TSF shall compute new keying material during Quick Mode as follows:

when using perfect forward secrecy
KEYMAT = sha(SKEYID_d, g(qm)^xy | protocol | SPI | Ni_b | Nr_b),
When perfect forward secrecy is not used
KEYMAT = sha(SKEYID_d | protocol | SPI | Ni_b | Nr_b)

Extended Requirements Rationale – FCS_IKE_(EXT).1:

This SFR format was taken directly from PD-0105 where IKE is defined as an acceptable instance of single-use authentication.

Management – FCS_IKE_(EXT).1:

There are no management activities foreseen.

5.4.2 User data protection (FDP)

FDP_IFC.1(2) Subset information flow control

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].

FDP_IFC.1(3) Subset information flow control

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.]

FDP_IFF.1(2) Simple security attributes

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) - ***Refinement:*** 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:
- [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].

FDP_IFF.1(3)Simple security attributes

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) - ***Refinement:*** 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].

5.4.3 Security management (FMT)

FMT_MSA.3(2) Static attribute initialization

FMT_MSA.3.1(2) - ***Refinement:*** The TSF shall enforce the [VPN SFP] to provide *restrictive* default values for ***information flow*** security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) - The TSF shall allow the [privileged Administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(3) Static attribute initialization

FMT_MSA.3.1(3) - ***Refinement:*** The TSF shall enforce the [VLAN SFP] to provide *restrictive* default values for ***information flow*** security attributes that are used to enforce the SFP.

FMT_MSA.3.2(3) - The TSF shall allow the [privileged administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_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;
- Firewall Configuration;
- TOE Authentication Functionality Configuration;
- IPSec Configuration;
- VLAN Configuration;
- IDS Configuration].

5.4.4 Trusted Path/Channel (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 - The TSF shall provide a communication channel between itself and 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 another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 - The TSF shall initiate communication via the trusted channel for [TCP syslog transfer to an external syslog server].

FTP_TRP.1 Trusted path

FTP_TRP.1.1 - ***Refinement:*** The TSF shall provide ***an encrypted*** communication path between itself and *remote* ***administrators*** ~~**users**~~ 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* to initiate communication via the trusted path.

FTP_TRP.1.3 – The TSF shall require the use of the trusted path for *user authentication*, [all remote administration actions].

5.4.5 IDS Component Requirements (IDS)

IDS_SDC_(EXT).1 System data collection

IDS_SDC_(EXT).1.1 - The System shall be able to collect the following information from the targeted IT System resources: Network Traffic.

IDS_SDC_(EXT).1.2 - The System 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 17: System Events.

Table 17: System Events

Component	Event	Details
IDS_SDC_(EXT).1	Network traffic	Protocol, source address, destination address

IDS_ANL_(EXT).1 Analyzer analysis

IDS_ANL_(EXT).1.1 - The System shall perform the following analysis function on all IDS data received:

a) Signature; and
b) Event correlation.

IDS_ANL_(EXT).1.2 - The System 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.

IDS_RCT_(EXT).1 Analyzer react

IDS_RCT_(EXT).1.1 - The System 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.

IDS_RDR_(EXT).1 Restricted data review

IDS_RDR_(EXT).1.1 - The System shall provide authorized administrators with the capability to read Event data from the System data.

IDS_RDR_(EXT).1.2 - The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR_(EXT).1.3 - The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

IDS_STG_(EXT).1 Guarantee of system data availability

IDS_STG_(EXT).1.1 - The System shall protect the stored System data from unauthorized deletion.

IDS_STG_(EXT).1.2 - The System shall protect the stored System data from modification.

IDS_STG_(EXT).1.3 - The System 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.

IDS_STG_(EXT).2 Prevention of system data loss

IDS_STG_(EXT).2.1 - The System shall overwrite the oldest stored System data if the storage capacity has been reached.

Extended Requirements Rationale – All IDS SFRs:

These SFR formats were taken from the IDS System PP, Version 1.7.

Management – All IDS SFRs:

There are no management activities foreseen.

5.5 TOE SFR Dependencies Rationale for SFRs Found in pp_fw_tf_br_v1.1

Functional component FMT_MSA.3(1) 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 Protection Profile.

Functional component FCS_COP.1 depends on the following functional components: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction and FMT_MSA.2 Secure Security Attributes. Cryptographic modules must be FIPS PUB 140-2 compliant. If the cryptographic module is indeed compliant with this FIPS PUB, then the dependencies of key generation, key destruction and secure key values will have been satisfied in becoming FIPS PUB 140-2 compliant. For more information, refer to section 4.7 of FIPS PUB 140-2.

5.6 TOE SFR Dependencies for SFRs in addition to the SFRs found in pp_fw_tf_br_v1.1

The following table provides dependency rational for SFRs included in the ST that were not originally found in pp_fw_tf_br_v1.1.

Table 18: Dependency Rationale

SFR	Dependency	Rationale
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Since keys are established by Internet Key Establishment. This dependency is met by FCS_IKE_(EXT).1
FCS_COP_(EXT).1	No Dependencies	Not applicable
FCS_GDOI_(EXT).1	FCS_COP.1	Met by FCS_COP.1
FCS_IKE_(EXT).1	FCS_COP_(EXT).1	Met by FCS_COP_(EXT).1
FDP_IFC.1(2)	FDP_IFF.1	Met by FDP_IFF.1(2)
FDP_IFF.1(2)	FDP_IFC.1	Met by FDP_IFC.1(2)
	FMT_MSA.3	Met by FMT_MSA.3(2)
FDP_IFC.1(3)	FDP_IFF.1	Met by FDP_IFF.1(3)
FDP_IFF.1(3)	FDP_IFC.1	Met by FDP_IFC.1(3)
	FMT_MSA.3	Met by FMT_MSA.3(3)
FMT_MSA.3(2)	FMT_MSA.1	In an effort to place all the management

SFR	Dependency	Rationale
		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.
	FMT_SMR.1	Met by FMT_SMR.1
FMT_MSA.3(3)	FMT_MSA.1	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.
	FMT_SMR.1	Met by FMT_SMR.1
FMT_SMF.1	No Dependencies	Not applicable
FTP_ITC.1	No Dependencies	Not applicable
FTP_TRP.1	No Dependencies	Not applicable
IDS_SDC_(EXT).1	No Dependencies	Not applicable
IDS_ANL_(EXT).1	No Dependencies	Not applicable
IDS_RCT_(EXT).1	No Dependencies	Not applicable
IDS_RDR_(EXT).1	No Dependencies	Not applicable
IDS_STG_(EXT).1	No Dependencies	Not applicable
IDS_STG_(EXT).2	No Dependencies	Not applicable

5.7 Security Assurance Requirements

5.7.1 SAR Requirements

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

Table 19: 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

5.7.2 Security Assurance Requirements Rationale

This Security Target claims conformance to EAL2 Augmented with ALC_FLR.2. This target was chosen to ensure that the TOE has a low to 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 having flaw remediation procedures and correcting security flaws as they are reported.

5.8 Assurance Measures

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 20: Assurance Measures

Component	How requirement will be met
ADV_ARC.1	The architecture of the TOE that is used to protect the TSF documented by Cisco in their development evidence.
ADV_FSP.2	The externally visible interfaces of the TOE used by the users of the TOE along with the description of the security functions and a correspondence between the interfaces and the security functions from the ST are documented by Cisco in their development evidence. The development evidence also contains a tracing to the SFRs described in this ST.
ADV_TDS.1	The design of the TOE will be described in the development evidence. This evidence will also contain a tracing to the TSFI defined in the FSP.
AGD_OPE.1	The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.
AGD_PRE.1	Cisco documents 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	Cisco performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE and the implementation representation of the TOE.
ALC_CMS.2	Cisco uniquely identifies configuration items and each release of the TOE has a unique reference. The Configuration Management documentation contains a configuration item list.
ALC_DEL.1	Cisco documents the delivery procedure 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	Cisco implements security controls over the development environment. Cisco meets these requirements by documenting the security controls.
ALC_FLR.2	Cisco documents 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	Cisco demonstrates the interfaces tested during functional testing using a coverage analysis.
ATE_FUN.1	Cisco functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of the test conducted against the functions specified in the ST.
ATE_IND.2	Cisco will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_VAN.2	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

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

Table 21: How TOE SFRs Measures

TOE SFRs	How the SFR is Met
Security Functional Requirements Drawn from pp_fw_tf_br_v1.1	
FMT_SMR.1	The TOE supports two levels of administrative user, non-privileged administrator and privileged administrator. Users assume the non-privileged level of administrator when they log into the TOE via the CLI interface. The administrative user then becomes a privileged administrator by entering the "enable" command and the "enable password." Once an administrative user becomes a privileged administrator, they have access to all privileged commands available through the administrative CLI. In order to gain access to the TOE administrative services, human users must provide a username and password. After the credentials are entered, the TOE associates the user with the assumed role. The TOE also supports external IT entities connecting to the TOE via VPN tunnels to pass network control information, such as, routing tables.
FIA_ATD.1	For each administrative user (privileged or non-privileged) configured on the TOE, the TOE maintains the username and password of the user. When the user logs into the TOE, the user is associated with the non-privileged role. When the non-privileged administrator enters the "enable" command and "enable password" the TOE then associates that user with the privileged administrator role. For each external IT entity, the TOE maintains the identity of the external IT entity and the IKE security attributes associated with the external IT entity.
FIA_UID.2	The TOE provides no access to the administrative capabilities of the TOE prior to the administrative user presenting the authentication credentials.
FIA_UAU.1	The TOE provides no access to the administrative capabilities of the TOE prior to the administrative user presenting the authentication credentials. The TOE also requires that peers establish an IKE/IPSec connection in order to forward routing tables used by the TOE.
FIA_AFL.1	The TOE provides the privileged administrator the ability to specify the maximum number of unsuccessful authentication attempts (between 1 and 25) before privileged administrator or non-privileged administrator is locked out through the administrative CLI using a privileged CLI command. When a privileged administrator or non-privileged administrator attempting to log into the administrative CLI reaches the administratively set maximum number of failed authentication attempts, the user will not be granted access to the administrative functionality of the TOE until a privileged administrator resets the user's number of failed login attempts through the administrative CLI. For IKE peers, the TOE denies access to the TOE based on failed Phase 1 authentication attempts when negotiating the Internet Key Exchange Protocol.
FIA_UAU.4	The TOE correctly invokes an external authentication server to provide a single-use authentication mechanism. The TOE then takes the correct actions (to either allow or not allow administrator (privileged or non-privileged) access) based on authentication decisions provided by the external authentication server. In keeping with industry practice, the choice of authentication server is not mandated by this ST document. However, the selected server must support RADIUS communications including the security measures specified the RADIUS standard (RFC 2865) in order to protect against replay of authentication information.

TOE SFRs	How the SFR is Met
	For peers connecting to the TOE through IKE/IPSec, the TOE uses the reuse prevention mechanisms included in IKE to provide single-use authentication.
FDP_IFC.1(1)	The TOE enforces information flow policies on traffic through the TOE from unauthenticated IT entities. These policies are enforced on network packets that are received by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface from an unauthenticated source, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, pass/not pass information.
FDP_IFF.1(1)	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 'access group' commands).
FMT_MSA.3(1)	The default TOE SFP is restrictive within the TOE. Information flows must be administratively configured to be allowed. The TOE only permits privileged administrators to specify the information flow policies rules used to enforce the SFP through the administrative CLI.
FDP_RIP.1	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 both data plane traffic and administrative session traffic.
FCS_COP.1	The TOE 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 # 1639 for validation details. This FIPS validation also covers a three key TDES algorithm for SSH protection. Further, in support of TLS. The TOE supports the following FIPS-allowed cipher suites: • DHE-RSA-WITH-3DES-EDE-CBC-SHA • DHE-RSA-WITH-AES-128-CBC-SHA • DHE-RSA-WITH-AES-256-CBC-SHA • RSA-WITH-3DES-EDE-CBC-SHA • RSA-WITH-AES-128-CBC-SHA • RSA-WITH-AES-256-CBC-SHA In support of SSH. The TOE supports the following FIPS approved/allowed algorithms: • Encryption - Triple-DES - AES • MACs - HMAC-SHA-1

TOE SFRs	How the SFR is Met
	• Key Exchange - Diffie-Hellman
FAU_GEN.1	The TOE generates an audit record that is stored internally within the TOE whenever an auditable event occurs. The types of events that cause audit records to be generated include, cryptography related events, 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 syslog internal to the TOE in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited. Both local storage of the generated audit records, and simultaneous offload of those events to the external syslog server are supported.
FAU_SAR.1	The TOE provides the ability for the administrators (privileged) of the TOE to view all audit events stored within the TOE. The TOE provides CLI commands that allow the display of the audit event to the console screen.
FAU_SAR.3	Through the TOE CLI administrative interface, the TOE provides the ability for privileged administrators to search and sort the internally stored audit records. The TOE provides a dedicated CLI to all privileged administrators to facilitate search and sorting of audit records within the TOE. The criteria for which audit records can be searched and sorted include, source IP address/range of address and date/time.
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.
FAU_STG.4	The TOE monitors the amount of free storage space available for audit records stored internal to the TOE. As the router's internal buffer fills up, it will begin to overwrite the oldest events first. In order to minimize the number of events that will be lost, events can be exported from the server to an external syslog server using TCP syslog connections. In the event that the external server cannot be reached by the router new traffic sessions through the router will be stopped, and an alert event will be logged to alert the privileged administrators. New VPN sessions will also be denied. The router will continue to attempt to connect to the external server, and once a connection is re-established new connections will resume. Existing connections will have already been logged and are therefore unaffected during the pause in new flows. The number of events that will be lost is equal to the number of events that it takes the privileged administrator to note the issue, copy events off the system, and clear the logs.
FMT_MOF.1	The TOE supports two levels of administrative user, non-privileged administrator and privileged administrator. Users assume the non-privileged level of administrator when they log into the TOE via the CLI interface. The administrative user then becomes a privileged administrator by entering the "enable" command and the "enable password." Once an administrative user becomes a privileged administrator, the administrator has access to all privileged commands available through the administrative CLI. The TOE provides the privileged administrator the ability to perform all commands required to control the TOE, including: • The ability to start and shutdown. • The creation, deletion, modification, and viewing information policy rules (including traffic flow/firewall, VPN, and VLAN). • The ability to create, delete, modify, and view user attributes through the TOE CLI. • The TOE uses an external radius server to provide Single-use authentication mechanisms. The TOE requires that IKE/IPSec sessions are used for peer routers or other

TOE SFRs	How the SFR is Met
	VPN enabled devices connecting to the TOE. • The TOE allows the privileged administrator to set the maximum number of failed login attempts. • The TOE provides the privileged administrator the ability to restore authentication capabilities to privileged administrator or non-privileged administrators that have been locked out. • The TOE allows or denies external IT entities to communicate with the TOE using administratively configured information policies. • The TOE allows the privileged administrator to modify and set the time and date stored locally within the TOE. • The TOE allows the privileged administrator to review and clear the audit records stored within the TOE. The TOE also allows audit data to be sent to an external server to be archived. • The TOE allows configuration data to be backed up to an external server. The configuration data can be recovered to the TOE. • The TOE supports remote administration. • The TOE allows the privileged administrator to configure all of the IPS functionality on the TOE.
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.
SFRs in addition to the SFRs found in pp_fw_tf_br_v1.1	
FCS_CKM.4	The TOE zeroizes all of the cryptographic keys used within the TOE after the key is no longer of use to the TOE. The key and CSP zeroization capabilities of the TOE have been verified as part of the TOE's FIPS 140-2 validation. Further details regarding the FIPS validation can be found in Certificate #1639.
FCS_COP_(EXT).1	In support of the provided cryptography, the TOE implements a pseudo Random Number Generator. This PRNG that is implemented is a FIPS-approved 3-key TDES based ANSI X9.31 compliant PRNG seeded from both a hardware and software entropy source. The TSF prevents tampering of the seeding entropy sources through the FIPS 140-2 physical security mechanisms. 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 #1639.
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 #1639.
FCS_IKE_(EXT).1	The TOE provides the cryptographic services necessary to support IPSec connections with remote IT entities wishing to pass information through an IPSec protected tunnel. The TOE fully supports Internet Key Exchange (IKE), RFC 2409, as follows: • Phase 1, the establishment of a secure authenticated channel between the TOE and another remote VPN endpoint, shall be performed using one of the following, as configured by the privileged administrator, Main Mode, Aggressive Mode • Phase 2, negotiation of security services for IPsec, shall be done using Quick Mode, using SHA-1 as the pseudo-random function. Quick Mode shall generate key material that provides perfect forward secrecy. The use of SHA-256 and SHA-384 as the PRF in IKEv1 KDF is also allowed

TOE SFRs	How the SFR is Met

	• x of g^xy is randomly generated using a FIPS-approved random number generator
	• The minimum size of x is twice the number of bits of the strength level associated with the negotiated DH group
	• The nonce sizes are between 8 and 256 bytes.
	• Nonces are generated in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^(bit strength of the negotiated DH group)
	• The TSF computes the value of SKEYID (as defined in RFC 2409), using SHA-1 as the pseudo-random function
	• The following authentication methods are supported:
	  • SKEYID_d = prf(SKEYID, g^xy | CKY-I | CKY-R | 0)
	  • SKEYID_a = prf(SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)
	  • SKEYID_e = prf(SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)
	• When authenticating a Phase 1 exchange, the TSF generates HASH_I if it is the initiator, or HASH_R if it is the responder as follows
	  • HASH_I = prf(SKEYID, g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDii_b)
	  • HASH_R = prf(SKEYID, g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDir_b)
	• The TSF is capable of authenticating IKE Phase 1 using the following methods
	  • The TSF can use RSA digital signature
	  • When an RSA signature is applied to HASH I or HASH R it is PKCS#1 encoded. The TSF checks the HASH_I and HASH_R values sent against a computed value to detect any changes made to the proposed transform negotiated in phase one. If changes are detected the session is terminated and an alarm generated.
	  • For X.509 V3 certificates, the TOE is capable of checking for validity of the certificate path, and at option of SA, check for certificate revocation.
	  • The TSF supports authentication using a pre-shared key.
	• The TSF computes the hash values for Quick Mode in the following way:
	  • HASH(1) = prf(SKEYID_a, M-ID |[any ISAKMP payload after
	  • HASH(1) header contained in the message)]
	  • HASH(2) = prf(SKEYID_a, M-ID | Ni_b | [any ISAKMP payload after HASH(2) header contained in the message)]
	  • HASH(3) = prf(SKEYID_a, 0 | M-ID | Ni_b | Nr_b)
	• The TSF computes new keying material during Quick Mode as follows:
	  • when using perfect forward secrecy - KEYMAT = prf(SKEYID_d, g(qm)^xy | protocol | SPI | Ni_b | Nr_b),
	  • When perfect forward secrecy is not used - KEYMAT = prf(SKEYID_d | protocol | SPI | Ni_b | Nr_b)
	• The TSF supports the following ID types: ID_IPV4_ADDR, ID_IPV6_ADDR, ID_FQDN, ID_USER_FQDN, [ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, ID_KEY_ID
	A privileged administrator enforces lifetime of asymmetric cryptographic key pairs associated with a digital certificate by specifying certificate validity period when requesting a certificate from an external Certificate Authority during the certificate enrollment procedure. When a certificate and a corresponding private key are imported in a protected cryptographic bundle into TOE certificate validity is verified including the certificate expiration date. The import operation is rejected if the certificate has expired. This functionality was verified as part of the TOE FIPS 140-2 validation.
	Further details regarding the FIPS validation can be found in Certificate #1639.

FDP_IFC.1 (2)	The TOE facilitates VPN connections with other IPSec capable IT entities. The TOE

TOE SFRs	How the SFR is Met
	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 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.
FMT_MSA.3 (2)	The default TOE SFP is restrictive for the VPN SFP implemented within the TOE. Information flows must be administratively configured to be allowed. The TOE only allows the privileged administrator to specify alternate initial values for the attributes used to enforce the SFP.
FMT_MSA.3 (3)	The default TOE SFP is restrictive for the VLAN SFP implemented within the TOE. Information flows must be administratively configured to be allowed. The TOE only

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>allows the privileged administrator to specify alternate values for the attributes used to enforce the SFP.</td></tr>
<tr><td>FMT_SMF.1</td><td>The TOE provides all the capabilities necessary to securely manage the TOE, the services provided by the TOE, and the information flows through the TOE. The management functionality of the TOE is provided through the TOE CLI. The specific management capabilities available from the TOE are identified in the text of FMT_SMF.1.</td></tr>
<tr><td>FTP_ITC.1</td><td>The TOE protects communications with a remote syslog server by transmitting them via an IPSec tunnel.</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 non-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 methodology</td><td>- Impossible IP Packet
- IP fragmentation</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</td></tr>
</table>

TOE SFRs	How the SFR is Met
	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.
IDS_RDR_(EXT).1 IDS_STG_(EXT).1 and IDS_STG_(EXT).2	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 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 data plane communication, control plane communications, and administrative communications are 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 non-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. Additionally, this section describes the rationale for not satisfying all of the dependencies. The table below illustrates the mapping from Security Objectives to Threats and Policies.

7.1 Rationale for TOE Security Objectives

Table 22: Threat/Policies/Objectives Mappings

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T.UNAUTHORIZED_PEER	T.EAVESDROP	T.VPNMEDIAT	T.VLAN	T.NOHALT	T.FALACT	T.FALREC	T.FALASC	T.MISUSE	T.INADVE	T.MISACT	T.INTEGRITY
O.IDAUTH	X																					
O.SINUSE		X	X																			
O.MEDIAT				X	X	X																
O.SECSTA	X								X													
O.ENCRYP	X						X															
O.SELPRO									X	X												
O.AUDREC								X														
O.ACCOUN								X														
O.SECFUN	X		X							X												
O.LIMEXT	X																					
O.CRYPTOGRAPHIC_ FUNCTIONS												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 23: Threat/Policies/TOE Objectives Rationale

Objective	Rationale
O.IDAUTH	This security objective is necessary to counter the threat T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.
O.SINUSE	This security objective is necessary to counter the threats T.REPEAT and T.REPLAY because

Objective	Rationale
	it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.
O.MEDIAT	This security objective is necessary to counter the threats T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
O.SECSTA	This security objective ensures that no information is comprised by the TOE upon start-up or recovery and thus counters the threats T.NOAUTH and T.SELPRO.
O.ENCRYP	This security objective is necessary to counter the threats T.NOAUTH and T.PROCOM by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely.
O.SELPRO	This security objective is necessary to counter the threats T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	This security objective is necessary to counter the threat T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.
O.ACCOUN	This security objective is necessary to counter the threat T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.
O.SECFUN	This security objective is necessary to counter the threats T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.
O.LIMEXT	This security objective is necessary to counter the threat T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.
O.CRYPTOGRAPHIC_ FUNCTIONS	This security objective is necessary to counter the threat T.EAVESDROP by requiring the TOE to provide cryptographic functionalities in support of TOE operations.
O.PEER_AUTHENTICATION	This security objective mitigates the threat T.UNAUTHORIZED_PEER by requiring that the TOE implement the Internet Key Exchange protocol, as specified in RFC2409, 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.
O.INTEGRITY	This security objective mitigates the threat T.INTEGRITY by ensuring that all IPSEC encrypted data received from a peer is properly decrypted and authentication verified.
O.VPNMEDIAT	This security objective mitigates the threat T.VPNMEDIAT by requiring the TOE to mediate all IPSec communications and not allow other unauthorized communications.
O.VLAN	This security objective mitigates the threat T.VLAN by ensuring that the TOE will be correctly configured in accordance with a security policy which will ensure VLAN separation.
O.IDSENS	This security objective is necessary to counter the threats T.NOHALT, T.MISUSE, T.INADVE, and T.MISACT because it requires the TOE to collect system data.
O.IDANLZ	This security objective is necessary to counter the threats T.NOHALT, T.FALREC, and T.FALASC because it 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.
O.RESPON	This security objective is necessary to counter the threat T.FALACT because it ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

7.2 Rationale for the Security Objectives for the Environment

Table 24: Threats/Environment Objectives Mappings

	T.TUSAGE
OE.GUIDAN	X
OE.ADMTRA	X
OE.NTP	X
OE.SYSLOG	X

Table 25: Assumptions/Threats/Objectives Rationale

Env. Objective	Rationale
OE.PHYSEC (A.PHYSEC)	The TOE is physically secure.
OE.LOWEXP (A.LOWEXP)	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.GENPUR (A.GENPUR)	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.PUBLIC (A.PUBLIC)	The TOE does not host public data.
OE.NOEVIL (A.NOEVIL)	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.SINGEN (A.SINGEN)	Information can not flow among the internal and external networks unless it passes through the TOE.
OE.DIRECT (A.DIREC)	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
OE.NOREMO (A.NOREMO)	Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.
OE.REMACC (A.REMACC)	Authorized administrators may access the TOE remotely from the internal and external networks
OE.GUIDAN	This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.
OE.ADMTRA	This non-IT security objective is necessary to counter the threat: T.TUSAGE because it ensures that authorized administrators receive the proper training.
OE.NTP	This security objective is used to counter the threat: T.USAGE because it ensures that if an NTP server is used that any modifications by an external party to the time communications with the server are detected.
OE.SYSLOG	This security objective is used to counter the threat: T.USAGE because it ensures that syslog communications between the TOE and the external syslog server cannot be modified.

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. The functional and assurance requirements presented in this Protection Profile are mutually supportive and their combination meets the stated security objectives.

Table 26: Objective to Requirements Mappings

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT	O.CRYPTOGRAPHIC_FUNCTIONS	O.PEER_AUTHENTICATION	O.INTEGRITY	O.VPNMEDIAT	O.VLAN	O.IDSENS	O.IDANLZ	O.RESPON
FMT_SMR.1									X									
FIA_ATD.1	X	X							X									
FIA_UID.2	X							X										
FIA_UAU.1	X	X																
FIA_AFL.1						X												
FIA_UAU.4		X																
FDP_IFC.1(1)			X															
FDP_IFF.1(1)			X															
FMT_MSA.3(1)			X	X					X									
FDP_RIP.1			X															
FCS_COP.1					X						X							
ADV_ARC.1						X												
FPT_STM.1							X											
FAU_GEN.1							X	X										
FAU_SAR.1							X											
FAU_SAR.3							X											
FAU_STG.1						X			X									
FAU_STG.4						X			X									
FMT_MOF.1				X					X	X								
FCS_CKM.4											X							
FCS_COP_(EXT).1											X							
FCS_GDOI_(EXT).1												X						
FCS_IKE_(EXT).1												X						
FDP_IFC.1 (2)													X	X				
FDP_IFC.1 (3)															X			
FDP_IFF.1 (2)													X	X				
FDP_IFF.1 (3)															X			
FMT_MSA.3 (2)				X					X					X				
FMT_MSA.3 (3)				X					X						X			
FMT_SMF.1				X				X	X									

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT	O.CRYPTOGRAPHIC_FUNCTIONS	O.PEER_AUTHENTICATION	O.INTEGRITY	O.VPNMEDIAT	O.VLAN	O.IDSENS	O.IDANLZ	O.RESPON
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								X	X								
IDS_STG_(EXT).1	X					X		X		X								
IDS_STG_(EXT).2								X										

Table 27: Objectives to Requirements Rationale

Req.	Rationale
Security Functional Requirements Drawn from pp_fw_tf_br_v1.1	
FMT_SMR.1	Each of the CC class FMT components in this Protection Profile depend on this component. It requires the PP/ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.
FIA_UID.2	This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.
FIA_UAU.1	This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.
FIA_AFL.1	This component ensures that human users who are not authorized administrators can not

Req.	Rationale
	endlessly attempt to authenticate. After some number of failures that the ST writer decides, that must not be zero, the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.
FIA_UAU.4	This component was chosen to ensure that some one-time authentication mechanism is used in all attempts to authenticate at the TOE from an internal or external network. This component traces back to and aids in meeting the following objective: O.SINUSE.
FDP_IFC.1(1)	This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.
FDP_IFF.1(1)	This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.
FMT_MSA.3(1)	This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT , O.SECSTA, and O.SECFUN.
FDP_RIP.1	This component ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.
FCS_COP.1	This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that AES is used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP. This component specifies the symmetric encryption algorithm implemented by the TOE. This cryptographic algorithm is FIPS 140-2 tested and validated. This component traces back to and aids in meeting the following objective: O.CRYPTOGRAPHIC_ FUNCTIONS
ADV_ARC.1	ADV_ARC.1 must describe how the architecture ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO
FPT_STM.1	FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.
FAU_GEN.1	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
FAU_SAR.1	This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.
FAU_SAR.3	This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.
FAU_STG.1	This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.
FAU_STG.4	This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be

Req.	Rationale
	recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.
FMT_MOF.1	This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA
SFRs in addition to the SFRs found in pp_fw_tf_br_v1.1	
FCS_CKM.4	FCS_CKM.4 provides the functionality for ensuring key and key material is zeroized. This component traces back to and aids in meeting the following objective: O.CRYPTOGRAPHIC_ FUNCTIONS
FCS_COP_(EXT).1	FCS_COP_(EXT).1 requires that any random number generation, are part of a FIPS-validated cryptographic module. This requirement does not mandate that the functionality is generally available, but only that it be implemented in a FIPS-validated module should other cryptographic functions need these services. This component traces back to and aids in meeting the following objective: O.CRYPTOGRAPHIC_ FUNCTIONS
FCS_GDOI_(EXT).1	The O.PEER_AUTHENTICATION objective is satisfied by the requirement FCS_GDOI_(EXT).1, which specifies that 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_IKE_(EXT).1	The O.PEER_AUTHENTICATION objective is satisfied by the requirement FCS_IKE_(EXT).1, which specifies that the TOE must implement the Internet Key Exchange protocol defined in RFC 2409. 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. It is possible to establish multiple security associations between two peers, each with its own cryptography.
FDP_IFC.1 (2)	This component 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. This component traces back to and aids in meeting the following objective: O.VPNMEDIAT This component aids in satisfying O.INTEGRITY by ensuring that all IPSEC encrypted data received from a TOE is properly decrypted and authentication verified.
FDP_IFC.1 (3)	This component satisfies this policy by ensuring that all VLAN traffic sent and received is correctly separated from other VLAN traffic. This component traces back to and aids in meeting the following objective: O.VLAN.
FDP_IFF.1 (2)	This component 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. This component traces back to and aids in meeting the following objective: O.VPNMEDIAT This component aids in satisfying O.INTEGRITY by ensuring that all IPSEC encrypted data received from a TOE is properly decrypted and authentication verified.
FDP_IFF.1 (3)	This component satisfies this policy by ensuring that all VLAN traffic sent and received is correctly separated from other VLAN traffic. This component traces back to and aids in meeting the following objective: O.VLAN.
FMT_MSA.3 (2)	This component ensures that there is a restrictive default policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN, and O.VPNMEDIAT.
FMT_MSA.3 (3)	This component ensures that there is a restrictive default policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN, and O.VLAN.
FMT_SMF.1	This component was chosen and modified to some extent via permitted CC operations

Req.	Rationale
	in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA
FTP_ITC.1	This component ensures that the TSF requires protection of the syslog traffic between the router and the remote syslog server. This traces back to and aids in meeting the following objectives: O.SELPRO.
FTP_TRP.1	This requirement ensures that the TOE provides a protected administrative communication path for administrators to administer the TOE. This is provided by establishing an encrypted administrative session between remote administrators and the TOE. This component traces back to and aids in meeting the following objective: O.ENCRYP.
IDS_SDC_(EXT).1	This component ensures that the System collects events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. This component traces back to and aids in meeting the following objective: O.IDSENS.
IDS_ANL_(EXT).1	This component ensures that the System performs intrusion analysis and generates conclusions. This component traces back to and aids in meeting the following objective: O.IDANLZ.
IDS_RCT_(EXT).1	This component ensures that the System responds accordingly in the event an intrusion is detected. This component traces back to and aids in meeting the following objective: O.RESPON.
IDS_RDR_(EXT).1	This component ensures that the System provides the ability for authorized users to view all System data collected and produced and restrict the review of System data to those granted with explicit read-access. This component traces back to and aids in meeting the following objectives: O.IDAUTH, O.SECFUN, and O.LIMEXT.
IDS_STG_(EXT).1	This component ensures that the System protects the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack. This component traces back to and aids in meeting the following objectives: O.IDAUTH, O.SELPRO, O.ACCOUN, and O.LIMEXT.
IDS_STG_(EXT).2	This component ensures that the System prevents the loss of audit data in the event the audit trail is full. This component traces back to and aids in meeting the following objective: O.ACCOUN.

ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 28: 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