Motorola Network Devices
S2500, S6000, GGM 8000
Security Target
EAL 2 augmented ALC_FLR.2

Release Date: June 13, 2012
Document ID: 09-1757-R-0057
Version: 1.0

Prepared By: M. McAlister
K. Yoshino
InfoGard Laboratories
J. Hintermeister et al.
Motorola Solutions®, Inc.

Prepared For: Motorola Solutions®, Inc.
6480 Via Del Oro
San Jose, CA 95119

Table of Contents

List of Tables

List of Figures

1 Introduction

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

1.1 Identification

TOE Identification:	Motorola Network Devices S2500, S6000, GGM 8000 with EOS version 16.0
ST Identification:	Motorola Network Devices S2500, S6000, GGM 8000 Security Target EAL 2 augmented ALC_FLR.2
ST Version:	1.0
ST Publish Date:	June 13, 2012
ST Author:	Mike McAlister (InfoGard) Jan Hintermeister et al. (Motorola Solutions, Inc.) Kenji Yoshino (InfoGard)

The Common Criteria configuration of the GGM 8000 and S2500 can be ordered as part of an integrated networking solution or as standalone units. The Common Criteria configuration of the S6000 can only be ordered as an individual unit. For each hardware platform, the following must be ordered:

GGM 8000

Description	Tanapa Number
GGM 8000 Base Unit	CLN1841A Rev D
Encryption Module	CLN8492D Rev D
FIPS 140-2 Kit	CLN1854A Rev B
AC Power Option[1]	CLN1850A Rev D
DC Power Option[2]	CLN1849A Rev C
Choice of Pluggable Modules for the GGM 8000 from Table 2	
Optional Analog CCGW support	

With EOS Software SW/GGM8000-XS-16.0.1.44 and Firmware FW/GGM8000, 16.0.1.44.

S2500

Description	Tanapa Number

[1] Either the AC or DC Power Option must be selected.

[2] Either the AC or DC Power Option must be selected.

S2500 Base Unit	CLN1713F Rev D
Encryption Module	CLN8262E Rev A
Choice of Pluggable Modules for the S2500 from Table 2	
Optional Analog CCGW support	

With EOS Software SW/S2500-XS-16.0.1.44 and Firmware FW/S2500-BOOT1,8.0.0.02 or FW/S2500-BOOT2,8.0.0.02.

S6000

Description	**Tanapa Number**
S6000 Base Unit	CLN1780H Rev B
Encryption Module	CLN8261D Rev M
Choice of Pluggable Modules for the S6000 from Table 2	

With EOS Software SW/S6000-PS-16.0.1.44 and Firmware FW/S6000,16.0.1.44.

1.2 Overview

The Motorola Network Device models S2500, S6000, and GGM 8000 provide a flexible routing solution for integrated data, voice and virtual private network (VPN) applications.

These solutions feature the Motorola Enterprise OS software suite with a choice of three hardware platforms: S2500/S6000/GGM 8000 series. Each series provides different throughput and scalability capabilities. The common OS software provides Enterprise networking features including: traffic shaping and Quality of Service (QoS), WAN/LAN connectivity, Voice & Multi-Service and Network Management support. A comprehensive set of security features provide network and data protected through:

- Firewall Features: Pre-defined attack types, custom traffic filters.
- Encryption support: The TOE is FIPS 140-2 validated to Level 1 (S2500, S6000) or Level 2 (GGM 8000).
- Secure Tunneling/VPN support: IPsec, FRF.17, and IKE.
- Protocol Authentication: Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Protocol Independent Multicast (PIM) protocols.

The Network Device features a comprehensive Administrative-user interface that allows for the setup, configuration, monitoring and management of the device using a Command Line Interface (CLI) over a local console interface or secured over an SSHv2 secured connection. The TOE also supports encrypted SNMPv3 for a limited set of management functions.

Cryptographic operations provided by the TOE are FIPS 140-2 validated.

The TOE model S2500 and GGM 8000 platforms are suitable for use as edge routers for analog and digital voice systems as well as remote radio frequency (RF) site routers in digital voice systems. Both the S2500 and GGM 8000 may include up to 2 V.24 modules that allow the processing of digital voice, Voice over IP (VoIP). When combined with the analog conventional pluggable module (E&M), the S2500 and GGM 8000 are also suitable as a Conventional Channel Gateway (CCGW) in a Motorola ASTRO® 25 trunked radio communication network. In this role, the TOE exchanges call control traffic via communication with peer devices with ASTRO® 25 controllers.

The E&M pluggable module cannot be used with the S6000 platform.

The S6000 series is suitable as a Wide Area Network (WAN) interface for radio communications network transport systems or as a Core/Edge Network Device.

The S6000 series can also be used to maintain connectivity among small, midsize, and large Local Area networks via a wide variety of WAN services and accommodates extensive virtual port tunneling capabilities with data compression and high speed processing.

When used in the network core, the S6000 supplies high speed, scalable performance for WAN concentration, virtual private network (VPN) tunnel termination, and efficient bandwidth utilization. The S6000 concentrates T1/E1 or T3/E3 internet traffic at the network core, enabling multiple secure tunnels to be maintained through the public network to many remote locations simultaneously.

1.3 Organization

- **Security Target Introduction (Section 1) –** Provides identification of the TOE and ST, an overview of the TOE, an overview of the content of the ST and relevant terminology. The introduction also provides a description of the TOE security functions, hardware and software that make up the TOE and the physical and logical boundaries of the TOE.
- **Conformance Claims (Section 2) –** Provides applicable Common Criteria (CC) conformance claims, Protection Profile (PP) conformance claims and Assurance Package conformance claims.
- **Security Problem Definition (Section 3) –** Describes the threats, organizational security policies, and assumptions pertaining to the TOE and the TOE environment.
- **Security Objectives (Section 4) –** Identifies the security objectives for the TOE and its supporting environment as well as a rationale that objectives are sufficient to counter the threats identified for the TOE.
- **Extended Components Definition (Section 5) –** Presents components needed for the ST but not present in Part II or Part III of the Common Criteria Standard.
- **Security Requirements (Section 6) –** Presents the Security Functional Requirements (SFRs) met by the TOE and the security functional requirements rationale. In addition this section presents Security Assurance Requirements (SARs) met by the TOE as well as the assurance requirements rationale. Provides pointers to all other rationale sections, to include the rationale for the selection of IT security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- **Summary Specification (Section 7) –** Describes the security functions provided by the TOE that satisfy the security functional requirements, provides the rationale for the security functions.

1.4 Document Terminology

Please refer to CC v3.1 Part 1 Section 4 for definitions of commonly used CC terms.

1.4.1 ST Specific Terminology

Administrative-users	Refers to a TOE account holder for the purpose of performing Administrative duties including the following roles: (CLI roles) Root, Network Manager, User; (SNMPv3 roles) MotoAdmin, MotoMaster.
Base Unit	The gateway or router without any interface modules installed.
Conventional Channel Gateway	Refers to a TOE feature applicable to the S2500 and GGM 8000 platform where the TOE provides an analog or digital voice interface and control functions for a conventional voice network
Critical Security Parameter	Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.
Key Encryption Key (KEK)	The master key that encrypts persistent critical security parameters (CSPs) such as keys, secrets, and passwords.
IKE Pre-Shared Keys	Used to authenticate peer to peer during IKE session
FRF.17	(Frame Relay Forum) Frame Relay Privacy Implementation Agreement
Network Management Console	Refers to the IT Entity used by an authorized administrative-user to communicate via CLI or SNMPv3 with the TOE for TSF management.
User Security Model	Provides authentication and privacy (encryption) functions and operates at the message level. (SNMPv3)
View based access control model	Determines whether a given principal is allowed to access a particular MIB object to perform specific functions and operates at the protocol data unit (PDU) level.

1.4.2 Acronyms

CEN	Customer Enterprise Network
CCGW	Conventional Channel Gateway
CSP	Critical Security Parameter
CWR	Cooperative WAN Routing
EOS	Enterprise Operating System
FQDN	Fully Qualified Domain Name

GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
IMSI	International Mobile Subscriber Identity
L2TP	Layer 2 Tunneling Protocol
L2VPN	Layer 2 Virtual Private Network
LAN	Local Area Network
MIP	(IGMP) Multicast Internet Protocol
MNR	Motorola Network Router
PIM	Protocol Independent Multicast
PPTP	Point-to-Point Tunneling Protocol
SNMP	Simple Network Management Protocol
Tanapa	A type of part number. Used for high level identification.
USM	User Security Model
VACM	View-Based Access Control Model
WAN	Wide Area Network

1.5 Common Criteria Product type

The TOE is classified as **Miscellaneous** for Common Criteria purposes. The TOE is made up of *hardware and software* components.

1.6 Architecture Overview

The TOE consists of the Enterprise Operating System Version 16.0 and the S2500, S6000, or GGM 8000 hardware.

1.6.1 TOE Hardware

The following table describes the features of each hardware base unit:

Implementation Characteristics	S2500	GGM 8000	S6000
CPU Internal Operating Frequency	100MHz	1GHz	1GHz
Level-1 Instruction Cache Size / Structure	16KB, 4-Way Set Associative	32KB, 8-Way Set Associative	32KB, 8-Sets (Built-In)
Level-1 Data Cache Size / Structure	8KB, 4-Way Set Associative	32KB, 8-Way Set Associative	32KB, 8-Sets (Built-In)
Level-2 Cache Size	None	512KB	512KB (Built-In)

Implementation Characteristics	S2500	GGM 8000	S6000
Cache Coherency on Shared Memory Accesses	No	Yes	Yes
Shared Memory Type	SDRAM	DDR2	SDRAM
Shared Memory Size	32 MB	512 MB	256 MB (DIMM)
Shared Memory Bus Width	32 Bits	64 Bits	64 Bits
Shared Memory Peak Transfer Rate	200 MBS	3,200 MBS	1,064 MBS (133 MTS)
Embedded SW (Flash PROM Memory)	1 MB	32 MB	1 MB
Flash File System (Flash PROM Memory)	16 MB	64 MB	16 MB
Built-In LAN Ports	1 - 10/100	4 – 10/100/1000	3 - 10/100
Built-In WAN Ports	None	2 – T1/E1	None
Pluggable Module Options[3]	Slots for two I/O Modules	Slots for two I/O Modules	Slots for two I/O Modules
Analog CCGW option (4 Port E&M Analog module and DSP module)	Yes	Yes	No

Table 1: Feature comparisons: S2500, S6000 and GGM 8000

The hardware platforms allow various configurations using pluggable interface modules to allow the end user to customize the available ports. The following tables illustrate the module combinations that may be used with each platform.

Pluggable Module Combinations by Hardware Platform

Shaded = N/A

Numbers indicate possible configuration options (number of modules supported per chassis)

A single hardware platform device of one of the 3 shown is required for the CC Evaluated configuration.

Module Type/Hardware Platform	S2500 Hardware	GGM 8000 Hardware	S6000 Hardware
T1/E1 (WAN/Telco), 1 port per module	0, 1, 2	▨	▨

[3] Table 2 specifies the maximum number of each module type that each base unit supports.

T1/E1 (WAN/Telco), 2 ports per module		0, 1, 2	
T1/E1 (UltraWAN), 4 ports per module			0, 1, 2
T1/E1, 12 ports per module			0, 1, 2
FlexWAN Serial, 1 port per module	0, 1, 2	0, 1, 2	
FlexWAN Serial, 4 ports per module			0, 1, 2
Ethernet 10BASET, 1 port per module	0, 1, 2		
V.24, 2 ports per module	0, 1	0, 1, 2	
T3/E3, 2 ports (one T3/E3) per module			0, 1, 2

Table 2: Pluggable Module Combinations by Hardware Platform

1.6.2 TOE Software

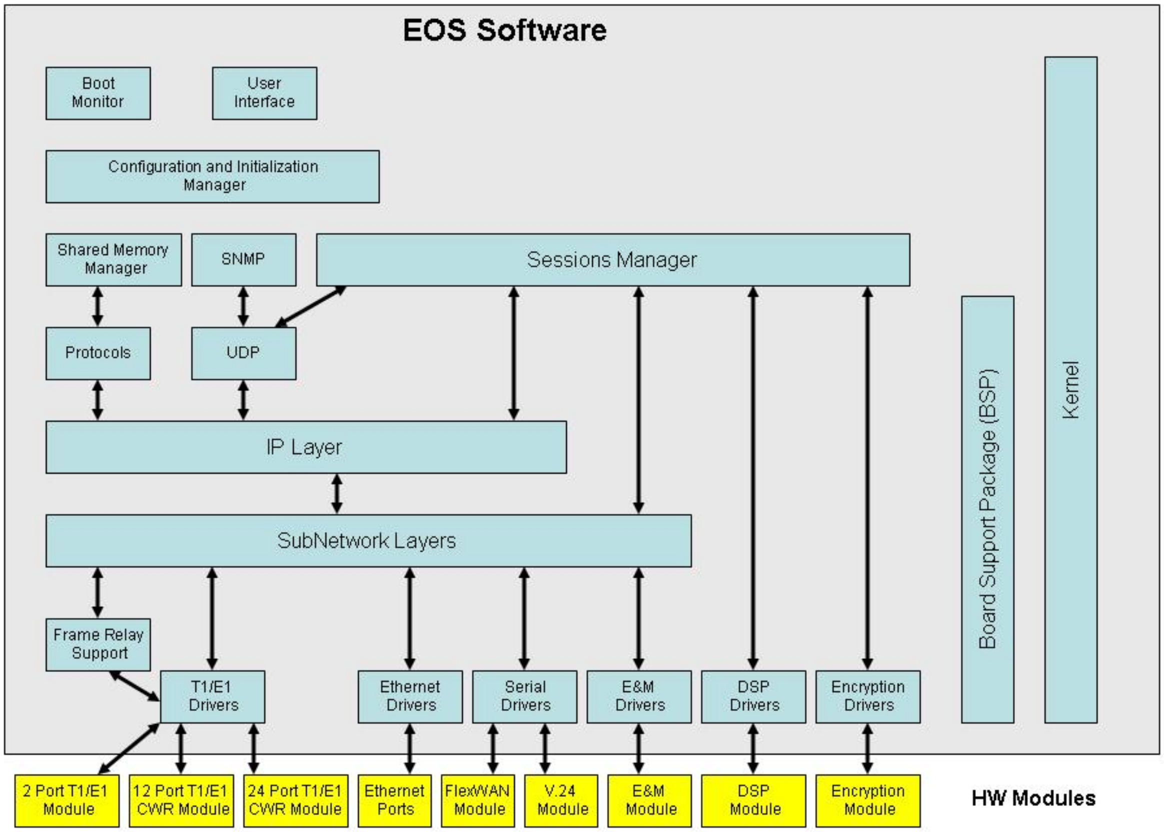

Figure 1: Architecture Overview – Enterprise OS

EOS implements the TOE security functionality. The hardware provides the user with interface and performance options.

1.6.3 Operational Environment Components

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
RADIUS	Authentication Server (optional)[4]
Syslog Host	Syslog host for offloading of audit records
NTP Server	NTP Server
SSHv2 client	SSHv2 client to support Administrative tunnels to the TOE
SNMPv3 Host	Supports SNMPv3 to the net-snmp client on the TOE
Serial Console	Console to perform local administration of the TOE.

Table 3: Operational Environment Components

1.6.4 Guidance Documents

The following guidance documents are provided with the TOE upon delivery in accordance with EAL 2 requirements:

- Motorola Enterprise OS Software Version 16.0 User Guide, Published January 6, 2011
- Motorola Enterprise OS Software Version 16.0 Reference Guide, Published January 27, 2011
- Motorola Network Router S2500 Hardware User Guide, Published March 23, 2011
- Motorola GGM 8000 Hardware User Guide, Published March 23, 2011
- Motorola Network Router S6000 Hardware User Guide, Published March 23, 2011
- Motorola Network Device S2500, S6000, and GGM 8000 with EOS Version 16.0 Common Criteria Supplement, Published April 19, 2012

1.7 Logical Boundaries

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the Motorola Network Device TOE:

- Security Audit
- Identification and Authentication
- User Data Protection: Flow Control
- Cryptographic Operations
- Security Management
- Protection of the TSF

[4] If your organization requires authentication failure counters and account lockouts for remote accounts, ensure your RADIUS Server supports these features.

1.7.1 Security Audit

The Network Device provides a comprehensive audit capability that generates audit records for administrative-user authentication, configuration and device management (local console, SSH and SNMP sessions), and detailed information about traffic management actions taken by the TOE.

The TOE includes separate log categories for System Messaging, User and Configuration Management logs, VPN related logs for IPsec/FRF.17 traffic and Firewall logs that detail packet filtering and actions taken to either permit or deny traffic based on configured attributes.

SNMP traps may also be configured to alert Administrative-users with notification messages for anomalous events or potential security issues as configured by an authorized administrative-user. A series of traps are provided by default, and administrative-users may also customize trap notifications.

Logs are buffered on the TOE and output to a Syslog server in the Operational Environment. The Network Manager and Root roles may access audit logs for review and may delete audit logs within the device buffer. The User role does not have access to audit logs.

1.7.2 Identification and Authentication

The TOE requires all users to be positively identified and authenticated prior to accessing TSF resources. Administrative-users access the TOE via a local console or SSHv2 (CLI) and SNMPv3. Authentication may be performed by the TOE or a RADIUS server in the Operational Environment.

The TOE maintains three roles by default for CLI access:

- Root (full read/write access)
- Network Manager (full read/write access, except enable/disable of Audit)
- User (read/show current configuration, status)

The TOE maintains two privilege levels for SNMPv3 access:

- MotoAdmin (full read/write access)
- MotoMaster (full read/write access, except for passphrases)

1.7.3 User Data Protection: Flow Control

The TOE mediates traffic passed through the device, implements packet filtering and enforces configured routing policies as configured by the Network Manager or Root administrative-user.

Flow control rules are enforced through packet filter parameters that explicitly permit or deny traffic flows based on protocol, IP address and connection characteristics that may be indicative of a malicious traffic flow or denial of service attempt. The TOE performs stateful packet inspection based on configured IP addresses and TCP port combinations. This feature allows identification of threats such as Denial of Service (DoS), TCP/IP packet fragmentation attacks, and malicious data injection.

The TOE also supports Internet Key Exchange (IKE) authentication (negotiation) using pre-shared keys as part of FRF.17 and IPsec protocol sessions. IKE negotiation may be initiated in a Data Packet trigger mode or Pre-connect mode.

In support of the Protocol Authentication feature, Protocol Independent Multicast (PIM) authentication support is provided through a manual configuration of cryptographic keys on configured peers. Authentication for BGP and OSPF traffic is provided by the TOE using a shared secret key configured by an authorized administrative-user on peer devices.

1.7.4 Cryptographic Operations

The TOE is FIPS 140-2 validated and uses this cryptographic functionality to encrypt message traffic for administrative-user sessions, VPN sessions, IPsec tunnels, and FRF.17 sessions. The TOE also performs key generation.

1.7.5 Security Management

The Network Device is managed using a CLI and SNMPv3. Administrative-users can perform user management, configuration of routing rules and packet filtering (firewall) options, establish message notifications through SNMP traps and configuration of authentication credentials (key management) to peer devices.

SNMPv3 sessions may also be established with the TOE to provide basic USM user maintenance functions: create, delete, change passphrase, and change security level.

1.7.6 Protection of TSF

The TOE requires authentication prior to establishing a security association with any device or administrative-user. The TOE is physically secured by the Operational Environment.

TSF data passed during administrative sessions is encrypted to prevent disclosure and is message integrity checked to assure modifications during transit are detected. Trusted channels are established for administrative-user sessions.

TOE services are protected from Denial of Service attacks through quotas placed on TCP connect attempts and for connection-oriented sessions.

Through the enforcement of flow control policies and packet inspection features, potentially malicious data that could affect the TOE or Operational Environment resources may be mitigated based on configuration actions and an audit trail produced allowing detection by administrative-users.

1.8 Features Excluded from the Common Criteria Evaluation

This section identifies features that were not evaluated. These features were not evaluated, because they were either deemed non-security relevant or are disabled in the Common Criteria Evaluated configuration.

1.8.1 Non-Security Relevant Features

The following features of the TOE relate to network and routing functionality that does not relate to security functions provided by the TOE and are therefore excluded from the Common Criteria Evaluation:

Conventional Channel Gateway (CCGW) deployment aspect

Cooperative WAN Routing (CWR)

IP Packet Delay Variation (IPDV)

SCH Service – Event Schedule features (i.e.: automated backup)

Bridge service – provides transparent bridging over a variety of LAN and WAN topologies

Rempolling – Remote Polling Protocol monitors reachability and performance of network devices by polling

Quality of Service (IPQoS) features

Load Balancing features

Performance Management Tools

Auto startup feature – automatic establishment of PPP and Frame Relay paths upon platform boot

Distance Vector Multicast Routing Protocol (DVMRP)

Port Bandwidth Management feature

Data Compression feature

Data Prioritization feature

UDP Broadcast Helper feature

Diagnostic services

Integrated Intermediate System to Intermediate System (IISIS) Service – used for IP routing

IPName Service – determines how names are resolved for Telnet, Ping, and TraceRoute

IPv6 based rules

Router Discovery Protocol (RDP)

Routing Information Protocol/Internet Protocol (RIPIP) Service

Routing Information Protocol Next Generation (RIPNG) Service

Resource Reservation Protocol (RSVP)

Spanning Tree Protocol (STP)

IP-over-IP Tunnel Route Short Cut (TRSC)

Remote Monitoring (RMON) agent

1.8.2 Security Relevant features excluded for the CC evaluated configuration

The following security relevant features are disabled in the CC evaluated configuration:

Telnet access to CLI – only local console and SSHv2 secured sessions are allowed for Common Criteria

SNMPv1 and SNMPv2 – only SNMPv3 is allowed for Common Criteria

Point to Point Tunneling Protocol (PPTP)

Layer 2 Tunneling Protocol (L2TP)

Gateway GPRS Support Node (GGSN)

2048 bit RSA and DSA key generation and usage

2 Conformance Claims

The TOE is Conformant with Common Criteria (CC) Version 3.1r3 Part 2 Extended

The TOE is Common Criteria (CC) Version 3.1r3 Part 3 Conformant at EAL 2 augmented ALC_FLR.2

The TOE is compliant with International Interpretations with effective dates on or before 22 September 2009.

The TOE does not comply with a Protection Profile.

3 Security Problem Definition

The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed. This section contains assumptions regarding the security environment and the intended usage of the TOE and threats on the TOE and the Operational Environment.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

A.USE	The administrative-user ensures there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
A.PHYSICAL	It is assumed that the Operational Environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
A.AVAILABILITY	Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.
A.NTP_SERVER	It is assumed that the Operational Environment provides an NTP server resource for time synchronization purposes for use by the TOE.
A.EAUTH	It is assumed that the Operational Environment provides a RADIUS server resource for remote authentication purposes for use by the TOE if necessary.
A.NOEVIL	The authorized administrative-users are competent; are not careless, willfully negligent, or hostile; and abide by the instructions provided by the TOE documentation.

3.2 TOE Threats

The threats discussed below are addressed by the TOE. The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

T.AUDIT_COMP	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user’s action.
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.TSF_COMP	A malicious user or process may cause TSF data or executable code

	to be inappropriately accessed (viewed, modified, or deleted).
T.MASQUERADE	A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources.
T.RESOURCE	A malicious process or user may block others from system resources (e.g., connection state tables, TCP connections) via a resource exhaustion denial of service attack.
T.UNATTENDED	A user may gain unauthorized access to an unattended session.
T.UNAUTH	A user may gain access to user data for which they are not authorized according to the TOE security policy.
T.UNIDENT	The administrative-user may fail to notice potential security violations, thus limiting the administrative-user’s ability to identify and take action against a possible security breach.
T.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 between physically separated parts of the TOE or a trusted IT Entity.

3.3 Organizational Security Policies

There are no Organizational Security Policies applicable for the TOE.

4 SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the TOE's operating Environment. The security objectives are divided between TOE Security Objectives and Security Objectives for the Operating Environment.

The following are the IT security objectives for the TOE:

O.AUDIT_GEN	The TOE will provide the capability to detect and create records of security-relevant events with accurate dates and times associated with users.
O.AUDIT_PROT	The TOE will provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE will provide the capability to view audit information.
O.CRYPTO	The TOE shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrative-users in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.
O.PEER	The TOE will authenticate each peer TOE that attempts to establish a security association with the TOE.
O.PROTECT_IN_TRANSIT	The TSF shall protect TSF data when it is in transit between the TSF and another trusted IT entity.
O.RESOURCE	The TOE shall provide mechanisms that mitigate attempts to exhaust transport layer or connection-oriented resources provided by the TOE
O.ROBUST_TOE	The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrative-user to set the time used for these time

	stamps. The TOE shall support the use of an NTP server in the Operational Environment for time synchronization.
O.TRUSTED_PATH	The TOE will provide a means to ensure that users are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data.
O.UNATTEND_PROTECT	The TOE will provide a means to ensure a user is unlikely to gain unauthorized access to an unattended session.

4.1 Security Objectives for the Environment

The following security objectives apply to the Operational Environment and are satisfied by technical means by Operational Environment hardware/software:

OE.NTP_SERVER
The operational environment will provide an NTP server to provide an accurate time synchronization resource to the TOE.

OE.EAUTH
A RADIUS server must be available for external authentication services if necessary.

The following security objectives apply to the Operational Environment and are satisfied by non-technical procedural measures:

OE.AVAILABILITY
Network resources will be available to allow clients to satisfy mission requirements and to transmit information.

OE.USE
The Administrative-user ensures there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

OE.PHYSICAL
Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the Operational Environment.

OE.NOEVIL
The authorized administrative-users are competent; are not careless, willfully negligent, or hostile; and abide by the instructions provided by the TOE guidance.

4.2 Mapping of Security Objectives to the Security Problem

The following table represents a mapping of the threats to the security objectives defined in this ST.

	A.AVAILABILITY	A.PHYSICAL	A.USE	A.NTP_SERVER	A.EAUTH	A.NOEVIL	T.AUDACC	T.AUDIT_COMP	T. TSF_COMP	T.MASQUERADE	T.RESOURCE	T.UNATTENDED	T.UNAUTH	T.UNIDENT	T. PEER	T.EAVESDROP
OE.AVAILABILITY	X															
OE.PHYSICAL		X														
OE.USE			X													
OE.NTP_SERVER				X												
OE.EAUTH					X											
OE.NOEVIL						X										
O.AUDIT_GEN							X									
O.AUDIT_PROT							X	X								
O.AUDIT_REVIEW							X							X		
O.CRYPTO																X
O.MANAGE									X							
O.MEDIATE													X			
O.PEER															X	
O.PROTECT_IN_TRANSIT																X
O.RESOURCE											X					
O.ROBUST_TOE										X						
O.TIME_STAMPS							X									
O.TRUSTED_PATH									X							
O.UNATTEND_PROTECT												X				

Table 4: Mappings between Security Objectives and the Security Problem

4.3 Rationale for Security Objectives

This section provides a justification for each threat or assumption and the security objectives for the environment which cover that assumption.

A.AVAILABILITY Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.	OE.AVAILABILITY Network resources will be available to allow clients to satisfy mission requirements and to transmit information.	Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.
A.USE	OE.USE	The TOE must not include any general-purpose commuting or storage

The administrative-user ensures there are no general-purpose computing or storage repository capabilities available on the TOE.	The Administrative-user ensures there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.	capabilities. This will protect the TSF data from malicious processes.
A.PHYSICAL It is assumed that the Operational environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.	The TOE, the TSF data, and protected user data is assumed to be protected from physical attack. Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.
A.NTP_SERVER It is assumed that the Operational Environment provides an NTP Server resource for time synchronization purposes for use by the TOE.	OE.NTP_SERVER The operational environment will provide an NTP server to provide an accurate time synchronization resource to the TOE.	The NTP Server enables synchronization of time with all IT Entities on the network.
A.EAUTH It is assumed that the Operational Environment provides a RADIUS Server resource for remote authentication purposes for use by the TOE if necessary.	OE.EAUTH A RADIUS server must be available for external authentication services if necessary.	The RADIUS server provides authentication services to the TOE.
A.NOEVIL The authorized administrative-users are competent; are not careless, willfully negligent, or hostile; and abide by the instructions provided by the TOE guidance.	OE.NOEVIL The authorized administrative-users are competent; are not careless, willfully negligent, or hostile; and abide by the instructions provided by the TOE guidance.	Authorized administrative-users are competent; are not careless, willfully negligent, or hostile; and abide by the instructions provided by the TOE guidance.
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.	O.AUDIT_GEN The TOE will provide the capability to detect and create records of security-relevant events with accurate dates and times associated with users.	O.AUDIT_GEN mitigates this threat by detecting events and creating audit records with time stamps associated with users to assure persons are accountable.
	O.TIME_STAMPS The TOE shall provide reliable time stamps and the capability for the Root or Network Manager to set the time used for these time stamps.	O.TIME_STAMPS contributes to mitigating this threat by assuring the TOE provides a Time Stamp resource.
	O.AUDIT_PROT	O.AUDIT_PROT contributes to

	The TOE will provide the capability to protect audit information.	mitigating this threat by controlling access to the audit trail. Authorized (authenticated) users are the only ones allowed to read the audit trail. No one is allowed to modify audit records
	O.AUDIT_REVIEW The TOE will provide the capability to view audit information.	O.AUDIT_REVIEW helps to mitigate this threat by providing mechanisms for monitoring the use of the system. Access to audit records is restricted to Audit record review and the deletion of the audit trail for maintenance purposes.
T.AUDIT_COMP A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	O.AUDIT_PROT The TOE will provide the capability to protect audit information.	O.AUDIT_PROT contributes to mitigating this threat by controlling access to the audit trail. Authorized (authenticated) users are the only ones allowed to read the audit trail. No one is allowed to modify audit records
T. TSF_COMP A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).	O.MANAGE The TOE will provide all the functions and facilities necessary to support the administrative-users in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	O.MANAGE provides the capability to restrict access to TSF to those that are authorized to use the functions. Satisfaction of this objective (and its associated requirements) prevents unauthorized access to TSF functions and data through the administrative mechanisms.
	O.TRUSTED_PATH The TOE will provide a means to ensure that users are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data.	O.TRUSTED_PATH plays a role in addressing this threat by ensuring that there is a trusted communication path between the TSF and administrative-users or trusted IT entities. This ensures the transmitted TSF data cannot be compromised or disclosed during the duration of the trusted path.
T.MASQUERADE A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources.	O.ROBUST_TOE The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	O.ROBUST_TOE mitigates this threat by controlling the logical access to the TOE and its resources. By mandating the type and strength of the authentication mechanisms, this objective helps mitigate the possibility of a user attempting to log in and masquerade as an authorized user. In addition, this objective provides the administrative-user the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.
T.RESOURCE	O.RESOURCE	O.RESOURCE mitigates this threat by

A malicious process or user may block others from system resources (e.g., connection state tables, TCP connections) via a resource exhaustion denial of service attack.	The TOE shall provide mechanisms that mitigate attempts to exhaust connection-oriented resources provided by the TOE (e.g., entries in a connection state table; TCP connections to the TOE).	requiring the TOE to provide controls relating available network connections. The administrative-user is allowed to specify a percentage of audit usage prior to needed action. This objective also addresses the denial-of-service attack of a user attempting to exhaust the connection-oriented resources by generating a large number of half-open connections (e.g., SYN attack).
T.EAVESDROP A malicious user or process may observe or modify user or TSF data transmitted between physically separated parts of the TOE or a trusted IT Entity.	O.CRYPTO The TOE shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE.	O.CRYPTO mitigates this threat by providing for the use of cryptographic functions to detect when information has been modified.
	O.PROTECT_IN_TRANSIT The TSF shall protect TSF data when it is in transit between the TSF and another trusted IT entity.	O.PROTECT_IN_TRANSIT satisfies this threat by ensuring protection of the communication between the TOE and trusted IT entities while transmitting data.)
T.UNATTENDED A user may gain unauthorized access to an unattended session.	O.UNATTEND_PROTECT The TOE will provide a means to ensure a user is unlikely to gain unauthorized access to an unattended session.	O.UNATTEND_PROTECT satisfies this threat by providing mechanisms to close remote administrator sessions after a defined time period of inactivity.
T.UNAUTH A user may gain access to user data for which they are not authorized according to the TOE security policy.	O.MEDIATE The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.	O.MEDIATE works to mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. One of the rules ensures that the network identifiers in a packet are in the set of network identifiers associated with a TOE’s network interface. The authenticated TOE policy ensures that user data being sent between PEER TOE's is encrypted if there is a rule that states data is to be encrypted between those two hosts.
T.UNIDENT The administrative-user may fail to notice potential security violations, thus limiting the administrative-user’s ability to identify and take action against a possible security breach.	O.AUDIT_REVIEW The TOE will provide the capability to view audit information.	O.AUDIT_REVIEW helps to mitigate this threat by providing mechanisms for monitoring the use of the system. The way audit review is performed is through analysis of the audit trail produced by the audit mechanism. Access to audit records is restricted to Audit record review and the deletion of the audit trail for

		maintenance purposes.
T. PEER An unauthorized IT entity may attempt to establish a security association with the TOE.	O.PEER The TOE will authenticate each peer TOE that attempts to establish a security association with the TOE.	O.PEER mitigates this threat by requiring that the TOE implement the Internet Key Exchange protocol, as specified in RFC 2409, to establish a secure, authenticated channel between the TOE and another remote router before establishing a security association with that router.

5 Extended Components Definition

5.1 Extended: Baseline Cryptographic Module (FCS_BCM_EXT)

The cryptographic requirements are structured to accommodate use of the FIPS 140-2 standard and NIST's Cryptographic Module Validation Program (CMVP) in meeting the requirements. Note that FIPS-approved cryptographic functions are required to be implemented in a FIPS-validated module running in FIPS-approved mode. FCS_BCM reflects this requirement, and it specifies the required FIPS validation levels for the security functions. Note also that some of the requirements of this Protection Profile go beyond what is required for FIPS 140-2 validation.

Application Note: A FIPS-approved cryptographic function is a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either: 1) specified in a Federal Information Processing Standard (FIPS), or 2) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.

Application Note: This Security Target shall use the term "FIPS 140-2" for simplicity.

5.1.1 Extended: Baseline Cryptographic Module (FCS_BCM_EXT.1)

Hierarchical to: No other components.

Dependencies: None.

Audit: There are no auditable actions foreseen.

Management: There are no management functions foreseen.

FCS_BCM_EXT.1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a cryptographic module that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

FCS_BCM_EXT.1.2 All cryptographic modules implemented in the TOE shall have a minimum overall rating of FIPS 140-2, Level 1.

5.2 Internet key exchange (FCS_IKE_EXT.1)

Hierarchical to: No other components.

Dependencies: FCS_COP.1, FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2. FCS_CKM.4

Audit: Minimal: Failure of IKE operations.

Management: Configuration of authentication methods.

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 router endpoint, shall be performed using

[selection: “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.

FCS_IKE_EXT.1.2 The TSF shall require the nonce, and the x of g^xy be randomly generated using FIPS-approved random number generator when computation is being performed. The recommended nonce sizes are to be between 8 and 256 bytes; the size of x is equal to the group size.

FCS_IKE_EXT.1.3 The TSF shall compute the value of SKEYID (as defined in RFC 2409), using a NIST-approved hashing function as the pseudo-random function. The TSF shall be capable of authentication using the methods for: [selection:

“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(sha(Ni_b | Nr_b), CKY-I | CKY-R)”,

[assignment: other authentication method]]

Application Note: If public key encryption is the method of choice, the sha algorithm listed in the requirement will be used. If another option is selected, a different authentication method or a different hash algorithm for generating SKEYID may be specified.

Application Note: Refer to RFC 2409 for an explanation of the notation and definitions of the terms.

FCS_IKE_EXT.1.4 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)
- [selection: [assignment: other methods for computing the authenticated keying material], “no other methods”]]

Application Note: If the assignment is selected, a different method for computing the authenticated keying material may be used, or a different hash algorithm may be specified.

FCS_IKE_EXT.1.5 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)

Application Note: Refer to RFC 2409 for an explanation of the notation and definitions of the terms.

FCS_IKE_EXT.1.6 The TSF shall be capable of authenticating IKE Phase 1 using the following methods as defined in RFC 2409: [selection:

- "Authentication with digital signatures: The TSF shall use [selection: RSA, DSA, [selection: [assignment: other digital signature algorithms], "no other digital signature algorithms"]]",
- "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 the phase one. If changes are detected, the session shall be terminated and an alarm shall be generated.",
- "[selection:[assignment: X.509 certificates Version 3 [selection: other version of X.509 certificates, "no other versions"]] 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 using [selection: CRL, OCSP, SVCP].",
- "Authentication with a pre-shared key: The TSF shall allow authentication using a pre-shared key."]

FCS_IKE_EXT.1.7 The TSF shall compute the hash values for Quick Mode in the following way:

- HASH(1) = sha(SKEYID_a, M-ID | (assignment: any ISAKMP payload after HASH(1) header contained in the message)
- HASH(2) = sha(SKEYID_a, M-ID | Ni_b | (assignment: any ISAKMP payload after HASH(2) header contained in the message)
- HASH(3) = sha(SKEYID_a, 0 | M-ID | Ni_b | Nr_b)

Application Note: The following steps will be performed when using the HASH computation:

- *initiator computes HASH(1) and sends to responder*
- *responder validates computation of HASH(1) and computes HASH(2) and sends HASH(2) to initiator*
- *initiator validates computation of HASH(2) and computes HASH(3) and sends HASH(3) to responder*

IKE is only optional when Security Association (SA) elects not to use perfect forward secrecy.

Verifying that a TFS implementation actually checks HASH(1) , HASH(2), and HASH(3) values sent against a computed value is important in detecting changes that could have been made to propose transform negotiated in Quick Mode (not as likely as Phase One because Quick Mode is encrypted).

The ordering of the ISAKMP payloads may differ because Quick Mode only specifies the location of the HASH and SA payload.

FCS_IKE_EXT.1.8 The TSF shall compute new keying material during Quick Mode as follows:

[selection: 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)”]

FCS_IKE_EXT.1.9 The TSF shall at a minimum, support the following ID types: [selection: ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, ID_KEY_ID].

6 Security Requirements

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

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

Assignment: **indicated with bold text**

Selection: indicated with underlined text

Refinement: ***additions indicated with bold text and italics***

deletions indicated with strike-through ~~bold text and italics~~

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

The extended requirements claimed in this ST are denoted by the _EXT suffix in the unique short name of the requirement. Requirements without the suffix are taken from Part 2 of the CC.

Security Functional Requirements	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SEL.1	Audit event selection
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_BCM_EXT.1	Baseline Cryptographic Module
FCS_CKM.1a	Cryptographic key generation (for symmetric keys)
FCS_CKM.1b	Cryptographic key generation (for asymmetric keys)
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1a	Cryptographic operation (for data encryption/decryption)
FCS_COP.1b	Cryptographic operation (for cryptographic signature)
FCS_COP.1c	Cryptographic operation (for cryptographic hashing)
FCS_COP.1d	Cryptographic operation (for cryptographic key agreement)
FCS_IKE_EXT.1	Internet key exchange
FDP_IFC.1a	Subset information flow control (unauthenticated policy)
FDP_IFC.1b	Subset information flow control (authenticated policy)
FDP_IFF.1a	Simple security attributes (unauthenticated policy)

FDP_IFF.1b	Simple security attributes (authenticated policy)
FIA_AFL.1	Authentication failure handling
FIA_ATD.1a	User attribute definition (Human users)
FIA_ATD.1b	User attribute definition (IT Entities)
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MOF.1a	Management of security functions behavior
FMT_MOF.1b	Management of security functions behavior
FMT_MSA.1a	Management of security attributes (unauthenticated)
FMT_MSA.1b	Management of security attributes (unauthenticated) - Query
FMT_MSA.1c	Management of security attributes (authenticated)
FMT_MSA.1d	Management of security attributes (authenticated) - Query
FMT_MSA.3a	Static attribute initialization (unauthenticated services)
FMT_MSA.3b	Static attribute initialization (authenticated services)
FMT_MTD.1a	Management of TSF data – modify (TSF data)
FMT_MTD.1b	Management of TSF data – query (audit records/user management)
FMT_MTD.1c	Management of TSF data – query (CLI TSF data)
FMT_MTD.1d	Management of TSF data – modify (SNMPv3TSF data)
FMT_MTD.1e	Management of TSF data – modify (CLI user management data)
FMT_MTD.1f	Management of TSF data – delete (Audit Records)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_STM.1	Reliable time stamps
FRU_RSA.1	Maximum quotas
FTA_SSL.3	TSF-initiated termination
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

Table 5: Functional Requirements

6.1 Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit data generation

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

a) Start-up and shutdown of the audit functions[5];
b) All auditable events for the minimal[6] level of audit; and
c) **Events as listed in Table 6: Audited Events**

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

a) Date and time of the event, type of event, subject identity, and the outcome ~~(success or failure)~~ ***(specified in the Auditable Events column of Table 6: Audited Events)*** 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, **the additional information specified in the Additional Audit Record Contents column of Table 6: Audited Events**

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	none
FCS_CKM.1a	Success and Failure of the activity.	none
FCS_CKM.1b	Success and Failure of the activity.	none
FCS_CKM.4	Success and Failure of the activity.	none
FCS_COP.1a,b,c,d	Success and Failure of cryptographic operation.	Type of cryptographic operation.
FCS_IKE_EXT.1	***Success and*** Failure of IKE operation.	If failure occurs, reason for the failure.
FDP_IFF.1a	Decisions to permit ***or deny*** requested information flows.	Presumed identity of source subject. Identity of destination subject. Transport layer protocol, if applicable. Source subject service identifier,

[5] The audit function starts up with the TOE and cannot be disabled.

[6] The minimal level of audit is refined in Table 6: Audited Events.

		if applicable. Destination subject service identifier, if applicable. Identity of the interface on which the TOE received the packet. For denied information flows, the reason for denial.
FDP_IFF.1b	Decisions to permit ***or deny*** requested information flows.	Presumed identity of source subject. Identity of destination subject. Transport layer protocol, if applicable. Source subject service identifier, if applicable. Destination subject service identifier, if applicable. Identity of the interface on which the TOE received the packet. For denied information flows, the reason for denial.
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.	Presumed identity of the user, Terminal identification, action taken.
FIA_UAU.2 FIA_UID.2	Unsuccessful use of the identification and authentication mechanisms.	Presumed identity of the user
FMT_MOF.1a	***All modifications in the behavior of the functions in the TSF.***	none
FMT_MOF.1b	***All modifications in the behavior of the functions in the TSF.***	none
FMT_MSA.1a,c	***All modifications of the values of security attributes.***	none
FMT_MSA.3a,b	***Modifications of the default setting of permissive or restrictive rules.***	none
FMT_MTD.1a,d,e	All modifications of the values of TSF data ***by the administrative-user.***	none
FMT_SMF.1	Use of the management functions.	none
FMT_SMR.1	Modification to the group of users that are part of a role.	none
FPT_STM.1	Changes to the time.	none
FRU_RSA.1	Rejection of allocation operation due to resource limits.	none

FTA_SSL.3	Termination of a remote session by the session locking mechanism.	none
FTP_ITC.1	Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channel functions.
FTP_TRP.1	Failure of the trusted path functions.	Identification of the user associated with all trusted path failures, if available.

Table 6: Audited Events

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **the Network Manager and Root** with the capability to read **all audit 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.

6.1.1.4 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

- **service**
- **severity (value)**
- **facility**
- **message identifier**

6.1.1.5 FAU_STG.1 Protected audit trail storage

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

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

6.1.1.6 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records and **no other actions** if the audit trail is full.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_BCM_EXT.1 Baseline Cryptographic Module

FCS_BCM_EXT.1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a cryptographic module that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

FCS_BCM_EXT.1.2 All cryptographic modules implemented in the TOE shall have a minimum overall rating of FIPS 140-2, Level 1.

6.1.2.2 FCS_CKM.1a Cryptographic Key Management – Symmetric Keys

FCS_CKM.1.1a The TSF shall generate ***symmetric*** cryptographic keys in accordance with **an ANSI X9.31 Random Number Generator using AES** and specified key sizes **128, 168, 192, 256 bit** that meet the following: **FIPS 186-2, Appendix 3, Random Number Generation; FIPS 140-2**

6.1.2.3 FCS_CKM.1b Cryptographic Key Management – Asymmetric Keys

FCS_CKM.1.1b The TSF shall generate ***asymmetric*** cryptographic keys in accordance with **RSA, DSA** and specified key sizes **1024 bit** that meet the following: **FIPS 186-2, Appendix 3, Random Number Generation, FIPS 140-2**

6.1.2.4 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy ***plaintext FIPS CSPs*** ***~~cryptographic keys~~*** in accordance with a cryptographic key method **zeroization** that meets the following: **FIPS PUB 140-2**

6.1.2.5 FCS_COP.1a Cryptographic operation (data encrypt/decrypt)

FCS_COP.1.1a The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES, TDES-CBC** and cryptographic key sizes **128, 192, 256 bit (AES), 168 bit (TDES)** that meet the following: **FIPS 197, FIPS 46-3, FIPS 140-2**

6.1.2.6 FCS_COP.1b Cryptographic operation (cryptographic signature)

FCS_COP.1.1b The TSF shall perform **cryptographic signature services** in accordance with a specified cryptographic algorithm **RSA, DSA** and cryptographic key sizes **1024 bit** that meet the following: **FIPS 186-2, PKCS#1 v1.5, FIPS 140-2**

6.1.2.7 FCS_COP.1c Cryptographic operation (hashing)

FCS_COP.1.1c The TSF shall perform **cryptographic hashing services** in accordance with a specified cryptographic algorithm **SHA-1, MD5** and cryptographic ***message digest*** sizes **160 bit (SHA-1), 128 bit (MD5)** that meet the following: **FIPS 180-2, RFC 1321, FIPS 140-2**

6.1.2.8 FCS_COP.1d Cryptographic operation (key agreement)

FCS_COP.1.1d The TSF shall perform **cryptographic key agreement** in accordance with a specified cryptographic algorithm **Diffie-Hellman** and cryptographic key sizes **1024, 1536, 2048 bit** that meet the following: **RFC 2409, RFC 3526.**

6.1.2.9 FCS_IKE_EXT.1 Internet key exchange (explicit)

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 router endpoint, shall be performed using Main Mode.
- Phase 2, negotiation of security services for IPsec, shall be done using Quick Mode, using SHA-1 as the pseudo-random function.

FCS_IKE_EXT.1.2 The TSF shall require the nonce, and the x of g^xy be randomly generated using FIPS-approved random number generator when computation is being performed. The recommended nonce sizes are to be between 8 and 256 bytes; the size of x is equal to the group size.

FCS_IKE_EXT 1.3 The TSF shall compute the value of SKEYID (as defined in RFC 2409), using a NIST-approved hashing function as the pseudo-random function. The TSF shall be capable of authentication using the methods for:

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

FCS_IKE_EXT.1.4 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)
- no other methods

FCS_IKE_EXT 1.5 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 1.6 The TSF shall be capable of authenticating IKE Phase 1 using the following methods as defined in RFC 2409:

- Authentication with a pre-shared key: The TSF shall allow authentication using a pre-shared key.

FCS_IKE_EXT.1.7 The TSF shall compute the hash values for Quick Mode in the following way:

- HASH(1) = sha(SKEYID_a, M-ID | (assignment: any ISAKMP payload after HASH(1) header contained in the message)

- HASH(2) = sha(SKEYID_a, M-ID | Ni_b | (assignment: any ISAKMP payload after HASH(2) header contained in the message)
- HASH(3) = sha(SKEYID_a, 0 | M-ID | Ni_b | Nr_b)

FCS_IKE_EXT.1.8 The TSF shall compute new keying material during Quick Mode as follows:

- KEYMAT = sha(SKEYID_d | protocol | SPI | Ni_b | Nr_b)]

FCS_IKE_EXT.1.9 The TSF shall at a minimum, support the following ID types: ID_IPV4_ADDR.

6.1.3 User Data Protection (FDP)

6.1.3.1 FDP_IFC.1a Subset information flow control (unauthenticated policy)

FDP_IFC.1.1a The TSF shall enforce the **UNAUTHENTICATED INFORMATION FLOW SFP** on

- **Source subject: TOE interface on which information is received;**
- **Destination subject: TOE interface to which information is destined;**
- **Information: network packets;**
- **Operations: pass information by opening a relay connection through the TSF on behalf of the source subject to the destination subject, and with the TSF ensuring the following conditions:**
  - **the connection from the source subject is from a valid peer network,**
  - **the new relay connection is established to the destination subject on a valid peer network.**

6.1.3.2 FDP_IFC.1.b Subset information flow control (authenticated policy)

FDP_IFC.1.1b The TSF shall enforce the **AUTHENTICATED INFORMATION FLOW SFP** on

- **Source subject representing authenticated peer routers: source network identifier;**
- **Destination subject: TOE interface to which information is destined;**
- **Information: network packets;**
- **Operations: pass by opening a relay connection from the TSF on behalf of the source subject to the destination subject, and with the TSF ensuring the following conditions:**
  - **the connection from the source subject is from a valid peer network,**
  - **the new relay connection is established to the**

destination subject on a valid peer network.

6.1.3.3 FDP_IFF.1 a Simple Security attributes (unauthenticated policy)

FDP_IFF.1.1a The TSF shall enforce the **UNAUTHENTICATED INFORMATION FLOW SFP** based on the following types of subject and information security attributes:

- **Source subject security attributes:**
  - **set of source entity identifiers; and**
- **Destination subject security attributes:**
  - **Set of destination entity identifiers; and**
- **Information security attributes:**
  - **presumed identity of source entity;**
  - **identity of destination entity;**
  - **transport layer protocol;**
  - **source entity service identifier;**
  - **destination entity service identifier (e.g., TCP or User Datagram Protocol (UDP) destination port number)**

FDP_IFF.1.2a The TSF shall permit an information flow between a ***source*** entity and a ***destination entity*** via a controlled operation if the following rules hold:

- **the presumed identity of the source entity is in the set of source entity identifiers;**
- **the identity of the destination entity is in the set of destination entity identifiers;**
- **the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy ruleset defined by the Network Manager or Root) and**
- **the selected information flow policy rule specifies that the information flow is to be permitted.**

FDP_IFF.1.3a The TSF shall enforce the **no additional rules**.

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

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

- **the presumed source identity of the information is not included in the set of source entity identifiers for the source subject;**
- **the presumed source identity of the information is a broadcast identity;**
- **the presumed source identity of the information is a loopback identifier;**
- **The TOE shall reject requests in which the information received by the TOE contains the route (set of host network**

identifiers) by which information shall flow from the source subject to the destination subject.

- **The TOE shall reject connections based on identification of malicious traffic by Filtering configuration settings which may include:**
  - **TCP packet injection**
  - **SYN/ACK flood**
  - **Tiny Fragment attack**

6.1.3.4 FDP_IFF.1b Simple Security attributes (authenticated policy)

FDP_IFF.1.1b The TSF shall enforce the **AUTHENTICATED INFORMATION FLOW SFP** based on the following types of subject and information security attributes:

- **Source subject security attributes:**
  - **source network identifier; and**
  - **port number;**
  - **configured PSK, Secret assignment (as applicable)**
- **Destination subject security attributes:**
  - **Set of destination network identifiers; and**
  - **port number;**
  - **configured PSK, Secret assignment (as applicable)**
- **Information security attributes:**
  - **identity of source subject;**
  - **identity of destination subject;**
  - **transport layer protocol;**
  - **destination subject service identifier (e.g., TCP destination port number);**

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

- **the source subject has successfully authenticated to the TOE;**
- **the identity of the destination subject is in the set of destination identifiers;**
- **the information security attributes match the attributes in a information flow policy rule (contained in the information flow policy ruleset defined by the Network Manager or Root)**

  and

- **the selected information flow policy rule specifies that the information flow is to be permitted.**

FDP_IFF.1.3b The TSF shall enforce **the no additional rules.**

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

FDP_IFF.1.5b The TSF shall explicitly deny an information flow based on the following rules: **none**

6.1.4 ID & Authentication (FIA)

6.1.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within **1 and 6** unsuccessful authentication attempts occur related to **administrative user authentication by the TOE**.

Application Note: FIA_AFL.1 does not apply to administrative users authenticated by RADIUS.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall **lock the account for a Network Manager or Root configurable positive integer within 2 and 1440 minutes.**

6.1.4.2 FIA_ATD.1a User attribute definition (Human Users)

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

- **Username**
- **Authentication Data (Password (CLI); Passphrase (SNMPv3))**
- **Role**

6.1.4.3 FIA_ATD.1b User attribute definition (IT Entities)

FIA_ATD.1.1b The TSF shall maintain the following list of security attributes belonging to individual ~~***users***~~ ***devices***:

- **Source Network Identifier**
- **Pre-Shared keys (IKE) (as applicable)**
- **Shared Secrets (Protocol Authentication) (as applicable)**

6.1.4.4 FIA_UAU.2 User authentication before any action

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

6.1.4.5 FIA_UID.2 User identification before any action

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

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MOF.1a Management of security functions behavior

FMT_MOF.1.1a The TSF shall restrict the ability to enable, disable, modify the behavior of the functions

- **Create/Modify/Delete Audit Selection**
- **Create/Modify/Delete FRF.17, IPsec settings**

- **Create/Modify/Delete Port/Virtual Port setting**
- **Create/Modify/Delete User accounts**
- **Create/Modify/Delete SNMPv3 settings**
- **Generate/Delete Key-Pairs**
- **Create/Modify/Delete Dynamic Cryptography Key Security policies (IKE, PSK)**
- **Enable/Disable Security Policy Checking on Ports**
- **Create/Modify/Delete routing table settings**
- **RADIUS Authentication**
- **Time and NTP server**
- **Syslog server**

to **the Network Manager and Root**.

6.1.5.2 FMT_MOF.1b Management of security functions behavior

FMT_MOF.1.1b The TSF shall restrict the ability to enable, disable the behavior of the functions

- **Audit Log function**

to **Root**.

6.1.5.3 FMT_MSA.1a Management of security attributes - ***unauthenticated***

FMT_MSA.1.1a The TSF shall enforce the **UNAUTHENTICATED INFORMATION FLOW SFP** to restrict the ability modify, delete the security attributes **Source/Destination entity identifiers, Deny (threat based) rules, Service based rules, Filter file (port based) rules** to **the Network Manager and Root**.

6.1.5.4 FMT_MSA.1b Management of security attributes - ***unauthenticated - Query***

FMT_MSA.1.1b The TSF shall enforce the **UNAUTHENTICATED INFORMATION FLOW SFP** to restrict the ability to query the security attributes **Source/Destination entity identifiers, Deny (threat based) rules, Service based rules, Filter file (port based) rules** to **the Network Manager, Root, and User**.

6.1.5.5 FMT_MSA.1c Management of security attributes - ***authenticated***

FMT_MSA.1.1c The TSF shall enforce the **AUTHENTICATED INFORMATION FLOW SFP** to restrict the ability modify, delete the security attributes **Source/Destination entity identifiers Deny (threat based) rules, Service based rules, Filter file (port based) rules** to **the Network Manager and Root**.

6.1.5.6 FMT_MSA.1d Management of security attributes - ***authenticated - Query***

FMT_MSA.1.1d The TSF shall enforce the **AUTHENTICATED INFORMATION FLOW SFP** to restrict the ability to query the security attributes

Source/Destination entity identifiers Deny (threat based) rules, Service based rules, Filter file (port based) rules to **the Network Manager, Root, and User**.

6.1.5.7 FMT_MSA.3a Static attribute initialisation

FMT_MSA.3.1a The TSF shall enforce the **UNAUTHENTICATED INFORMATION FLOW SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2a The TSF shall allow the **Network Manager and Root** to specify alternative initial values to override the default values when an object or information is created.

6.1.5.8 FMT_MSA.3b Static attribute initialisation

FMT_MSA.3.1b The TSF shall enforce the **AUTHENTICATED INFORMATION FLOW SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2b The TSF shall allow the **Network Manager and Root** to specify alternative initial values to override the default values when an object or information is created.

6.1.5.9 FMT_MTD.1a Management of TSF data – ***Modify (CLI TSF data)***

FMT_MTD.1.1a The TSF shall restrict the ability to modify the **all CLI TSF data** to the **Network Manager and Root**.

6.1.5.10 FMT_MTD.1b Management of TSF data – ***Query (audit records/user management)***

FMT_MTD.1.1b The TSF shall restrict the ability to query the **audit records, user management data** to the **Network Manager and Root**.

6.1.5.11 FMT_MTD.1c Management of TSF data – ***Query (CLI TSF data)***

FMT_MTD.1.1c The TSF shall restrict the ability to query the **all TSF data (except audit records and user management data)** to the **Network Manager, Root, and User**.

6.1.5.12 FMT_MTD.1d Management of TSF data – ***Modify (SNMP TSF data)***

FMT_MTD.1.1d The TSF shall restrict the ability to modify the **all SNMP TSF data except for MotoMaster passphrase data** to the **MotoAdmin and MotoMaster**.

6.1.5.13 FMT_MTD.1e Management of TSF data – ***Modify (SNMP TSF data)***

FMT_MTD.1.1e The TSF shall restrict the ability to modify the **SNMP3 passphrases** to the **MotoAdmin**.

6.1.5.14 FMT_MTD.1f Management of TSF data – ***Delete (Audit Records)***

FMT_MTD.1.1e The TSF shall restrict the ability to delete the **Audit Records** to the **Root**.

6.1.5.15 FMT_SMF.1 Specification of Management Functions

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

- **Set/Modify Time and NTP settings**
- **Enable/Disable/Modify Syslog server**
- **Enable/Disable Audit Log function**
- **Create/Modify/Delete Audit Selection settings**
- **Query/Delete Audit Records**
- **Create/Modify/Delete FRF.17, IPsec settings**
- **Create/Modify/ Delete Port/Virtual Port setting**
- **Create/Modify/Delete User accounts**
- **Create/Modify/Delete SNMPv3 settings**
- **Generate/Delete Key-Pairs**
- **Create/Modify/Delete Dynamic Cryptography Key Security policies (IKE, PSK)**
- **Enable/Disable Security Policy Checking on Ports**
- **Create/Modify/Delete routing table settings**
- **Create/Modify/Delete RADIUS configuration settings**
- **Configure the authentication failure handling threshold**
- **Configure the lockout timer when the authentication failure handling threshold has been surpassed**
- **Query/Modify/Delete the UNAUTHENTICATED INFORMATION FLOW SFP**
- **Query/Modify/Delete the AUTHENTICATED INFORMATION FLOW SFP**

6.1.5.16 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **(CLI) Root, Network Manager, User; (SNMPv3) MotoAdmin, MotoMaster.**

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

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_STM.1 Reliable time stamps

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

6.1.7 Resource Utilization (FRU)

6.1.7.1 FRU_RSA.1 Maximum quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources:

network connections that subjects can use simultaneously.

6.1.8 TOE Access (FTA)

6.1.8.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive ***CLI*** session after **a Root or Network Manager configured value of inactivity**.

6.1.9 FTP: Trusted Path/Channels

6.1.9.1 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 modifications or disclosure.

FTP_ITC.1.2 The TSF shall permit the TSF, 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 **SSHv2, SMNPv3**.

6.1.9.2 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide ***an encrypted*** communication path between itself and remote ***administrative*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, 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 **all remote administration actions.**

6.2 Rationale for Extended Security Requirements

The only extended requirements were those derived from the reference Protection Profile as needed. These SFRs were required to be extended as suitable SFRs could not be derived from Part II of the Common Criteria Standard as detailed below.

FCS_BCM_EXT.1 – Baseline cryptographic module

This extended requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.

FCS_IKE_EXT.1 – Internet Key Exchange

This extended requirement is necessary since the CC does not include requirements for this specific key exchange protocol. This protocol is specified in RFC 2409, but there are specific configurable settings that must be specified that are documented in the extended requirement.

6.3 Rationale for TOE Security Requirements

	O.AUDIT_GEN	O.AUDIT_PROT	O.AUDIT_REVIEW	O.CRYPTO	O.MANAGE	O.MEDIATE	O.PEER	O.PROTECT_IN_TRANSIT	O.RESOURCE	O.ROBUST_TOE	O.TIME_STAMPS	O.TRUSTED_PATH	O.UNATTEND_PROTECT
FAU_GEN.1	X												
FAU_GEN.2	X												
FAU_SAR.1			X										
FAU_SEL.1	X		X										
FAU_STG.1		X											
FAU_STG.4		X											
FCS_BCM_EXT.1				X									
FCS_CKM.1a,b				X									
FCS_CKM.4				X									
FCS_COP.1a.b,c,d				X									
FCS_IKE_EXT.1							X						
FDP_IFC.1a,b						X							
FDP_IFF.1a,b,c						X							
FIA_AFL.1										X			
FIA_ATD.1a,b										X			
FIA_UAU.2										X			
FIA_UID.2										X			
FMT_MOF.1a,b					X								
FMT_MSA.1a,b,c,d					X								
FMT_MSA.3a,b					X								
FMT_MTD.1a,b,c,d,e,f					X								
FMT_SMF.1					X								

	O.AUDIT_GEN	O.AUDIT_PROT	O.AUDIT_REVIEW	O.CRYPTO	O.MANAGE	O.MEDIATE	O.PEER	O.PROTECT_IN_TRANSIT	O.RESOURCE	O.ROBUST_TOE	O.TIME_STAMPS	O.TRUSTED_PATH	O.UNATTEND_PROTECT
FMT_SMR.1					X								
FPT_STM.1											X		
FRU_RSA.1									X				
FTA_SSL.3													X
FTP_ITC.1								X				X	
FTP_TRP.1								X				X	

Table 7: Summary of Mappings between Security Functions and Security Objectives

6.3.1 TOE Security Functional Requirements Rationale

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, Table 7: Summary of Mappings between Security Functions and Security Objectives illustrates the mapping between the security requirements and the security objectives and Table 4: Mappings between Security Objectives and the Security Problem demonstrates the relationship between the threats, policies and IT security objectives. The functional and assurance requirements presented in this Security Target are mutually supportive and their combination meets the stated security objectives.

Security Objective	Mapping Rationale
O.AUDIT_GEN	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that an administrative-user has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. FAU_GEN.2 ensures that the audit records associate an administrative-user identity with the auditable event. FAU_SEL.1 allows an administrative-user to configure which auditable events will be recorded in the audit trail.
O.AUDIT_PROT	FMT_MOF.1a,b restricts the ability to control the behavior of the audit to the specified roles. FAU_STG.1 restricts the ability to delete audit records to the specified roles and also ensures that no one has the ability to modify audit records. FAU_STG.4 ensures that audit records are always recorded by overwriting the oldest records when the audit buffer is full.

O.AUDIT_REVIEW	FAU_SAR.1 is used to provide specified roles the capability to read the entire audit data contained in the audit trail. This requirement also mandates the audit information be presented in a manner that is suitable for the administrative-user to interpret the audit trail.
O.CRYPTO	FCS_BCM_EXT.1 is an extended requirement that specifies not only that cryptographic functions that are FIPS-approved and must be validated by FIPS, but also what NIST FIPS rating level the cryptographic module must satisfy. FCS_CKM.1a is a requirement that a cryptographic module generate symmetric keys. FCS_CKM.1b is a requirement that a cryptographic module generate asymmetric keys. FCS_COP.1c requires that the TSF provide hashing services using a NIST-approved implementation of the Secure Hash Algorithm. FCS_COP.1d requires that the TSF provide cryptographic key agreement services in accordance with the referenced algorithms/standards. FCS_CKM.4 provides the functionality for ensuring key and key material is zeroized. This applies not only to key that resides in the TOE, but also to intermediate areas (physical memory, page files, memory dumps, etc.) where key may appear. FCS_COP.1a specifies that AES and TDES be used to perform encryption and decryption operations. FCS_COP.1b specifies options for providing the cryptographic signature capability; these requirements reference the appropriate standards for each cryptographic signature option.
O.MANAGE	FMT_MSA.1a,b,c,d provides that the specified roles have the capability to manipulate the security attributes of the objects in their scope of control that determine the access policy. FMT_MOF.1a,b provides that the specified roles can modify security function behavior through the security management interface. FMT_MSA.3a,b requires that by default, the TOE does not allow an information flow, rather than allowing information flows until a rule in the ruleset disallows it. FMT_MTD1a,b,c,d,e,f specifies which roles can either query, or modify TSF data through the applicable security management interfaces. FMT_SMF.1 specifies the security management functions provided by the TOE through the security management interface. FMT_SMR.1 provides that the TOE supports the specified roles and has the ability to associated users with their assigned role.
O.MEDIATE	FDP_IFC.1a,b define the subjects, information (e.g., objects) and the operations that are performed with respect to the two information flow policies. FDP_IFC.1a defines subjects for the unauthenticated access to any services the TOE provides. The destination subject is defined to be the TOE, and the source subject is the TOE interface on which a network packet is received. The information remains the same, a network packet, and the operations are limited to accept or reject the packet. FDP_IFF.1a provides the rules that apply to the unauthenticated use of any services

	provided by the TOE. FDP_IFC.1b, the subjects are the TOE's network interfaces. The objects are defined as the network IP packets on which the TOE performs routing operations. As packets enter the TOE, the network interface where they are received is the source subject. As packets are sent out of the TOE the network interface that they are sent out of is the destination subject. Subjects must be defined as entities that the TOE has control over. The TOE has control over its own network interfaces such that it can make information flow decisions to allow/disallow network packets to flow from in incoming interface to an outgoing interface, and can apply routing operations to packets that are allowed to flow. FDP_IFF.1b specifies the attributes on which authenticated information flow decisions are made. Each TOE interface has a set of source subject identifiers that is the list of senders of information packets that are allowed to send packets to this TOE interface. Each TOE interface also has a list of destination subject identifiers that specifies the receivers that network packets can be sent to on that TOE interface. As packets are received on a particular network interface, the TOE determines if they are allowed to enter on that interface. Then based on rules defined by the Network Manager or Root, the TOE applies authenticated routing operations to the packet. FDP_IFF.1c, the subjects at the mobile subscribers. The objects are the mobile subscriber data. Operations are authentication of the mobile subscriber. The TOE allows objects to flow if the mobile subscriber credentials are authenticated by the RADIUS server.
O.PEER	FCS_IKE_EXT.1 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
O.PROTECT_IN_TRANSIT	FTP_ITC.1 ensures that all TSF data will be protected from disclosure while in transit from the TOE to another trusted IT product. FTP_TRP.1 will use cryptographic means to prevent disclosure and modification of TSF data.
O.RESOURCE	FRU_RSA.1 was used to mitigate potential resource exhaustion attempts and to reduce the impact of an attempt being made to exhaust the transport-layer representation (e.g., attempt to make the TSF unable to respond to connection-oriented requests, such as SYN attacks).
O.ROBUST_TOE	FIA_UID.2 plays a role in satisfying this objective by ensuring that every administrative-user is identified before the TOE performs any mediated functions. FIA_ATD.1a defines the attributes of users, including a userid that is used by the TOE to determine an administrative-user's identity and enforce what type of access the administrative-user has to the TOE FIA_ATD.1b defines the attributes of IT entities, including a subject ID that is used to by the TOE to determine an entity's identity and enforce what type of access the entity has to the TOE. FIA_UAU.2 requires that administrative-users and authorized IT entities authenticate themselves to the TOE before performing any TSF-mediated actions FIA_AFL.1 provides a detection mechanism for unsuccessful authentication attempts by remote administrative-users.

O.TIME_STAMPS	FPT_STM.1 requires that the TOE be able to provide reliable time stamps for its own use and therefore, satisfies this objective. FMT_MOF.1a satisfies the rest of this objective by providing the capability to configure NTP settings/time source settings used for generating time stamps.
O.TRUSTED_PATH	FTP_TRP.1 requires the TOE to provide a trusted path for administrative-user access to the TOE. The trusted path be the only means available for administrative-users to access TSF functions. FTP_ITC.1 requires a mechanism that creates a distinct communication path to protect communications between IT products.
O.UNATTEND_PROTECT	FTA_SSL.3 specifies that the TSF shall terminate an interactive CLI session after a Root or Network Manager configured value of inactivity.

6.4 Rationale For IT Security Requirement Dependencies

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

Functional Component	**Dependency**	**Included/Rationale**
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Yes, via FIA_UID.2
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SEL.1	FAU_GEN.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FCS_BCM_EXT.1	None	None
FCS_CKM.1a,b	FCS_COP.1a, FCS_CKM.4	Yes
FCS_CKM.4	FCS_CKM.1	Yes
FCS_COP.1a,b,c,d	FCS_CKM.1, FCS_CKM.4	Yes
FCS_IKE_EXT.1	FCS_COP.1, FCS_CKM.1, FCS_CKM.4	Yes
FDP_IFC.1a,b	FDP_IFF.1a,b	Yes
FDP_IFF.1a,b	FDP_IFC.1a,b, FMT_MSA.3	Yes
FIA_AFL.1	FIA_UAU.1	Yes, via FIA_UAU.2
FIA_ATD.1a,b	None	None
FIA_UAU.2	FIA_UID.1	Yes, via FIA_UID.2
FIA_UID.2	None	None
FMT_MOF.1a,b	FMT_SMF.1, FMT_SMR.1	Yes

Functional Component	**Dependency**	**Included/Rationale**
FMT_MSA.1a,b,c,d	FDP_IFC.1a,b, FMT_SMR.1, FMT_SMF.1	Yes
FMT_MSA.3a,b	FMT_SMR.1, FMT_MSA.1	Yes
FMT_MTD.1a,b,c,d,e,f	FMT_SMF.1, FMT_SMR.1	Yes
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	Yes
FPT_STM.1	None	None
FRU_RSA.1	None	None
FTA_SSL.3	None	None
FTP_ITC.1	None	None
FTP_TRP.1	None	None

Table 8: SFR Dependencies

6.5 TOE Security Assurance Requirements

EAL 2 + ALC_FLR.2 was chosen to provide a “low to moderate” level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than “basic” and the product will have undergone a search for obvious flaws and a vulnerability analysis.

The security assurance requirements for the TOE are taken from Part 3 of the CC. The assurance requirements are summarized in the following table.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.4 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw Reporting Procedures
ASE: Security Target	ASE_CCL.1 Conformance claims

evaluation	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 9: Assurance Requirements: EAL 2 + ALC_FLR.2

7 TOE Summary Specification

The TOE security functional requirements are characterized through the following Security Functions:

- Security Audit
- Identification and Authentication
- User Data Protection: Flow Control
- Cryptographic Operations
- Security Management
- Protection of the TSF

7.1 Security Audit

7.1.1 Audit Record Generation – FAU_GEN, FPT_STM.1

The TOE generates Audit records for system configuration, administrative-user management, cryptographic operations and traffic events. Audit logs are sent from the local buffer to a Syslog server in the Operational Environment. The TOE can be configured to send audit logs to up to five syslog servers. The TOE maintains an internal time source and synchronizes time using an NTP server in the Operational Environment.

The log messages for administrative-user and security management include information such as:

- User logins and listens (logouts)
- Failed login or set privilege attempts
- Successfully executed configuration commands
- Invalid SNMP community strings
- SNMP configuration changes
- File operations
- System messages
- Reboot information

In addition, the AuditLog service can be configured to provide System Message logging to the syslog server that contains information regarding particular traffic flows. System log data includes:

- Date/Time of the event
- Interface
- Ingoing or Outgoing packet flow direction
- Packet Header summary
- Reason/Event summary

Cryptographic functions are logged in Local Audit logs and configured syslog servers that include Key Encryption Key (KEK) generation/zeroization and Virtual Private Network (VPN) related session data supporting FRF.17, IPsec and Internet Key Exchange (IKE).

7.1.1.1 <u>FRF.17 failures are logged by:</u>

- Date/Time

- SPI value
- Source/Destination IP
- Port
- Reason for discard (may include specifics such as authorization failure, cryptographic failure, unknown SPI/Peer, Invalid Packet or Clear text error)

IPsec failure logs follow the same format except that port is replaced by sequence number. IKE failure logs include cookie pair identification and the name of the payload responsible for the rejection.

Logs are coded using a severity level number based on the perceived importance of the event. The coding system follows the convention:

0=Emergency, 1=Alert, 2=Critical, 3=Error, 4=Warning, 5=Notice, 6=Info, 7=Debug

Logs may also be viewed directly from the local audit buffer by executing a SHow command from the network management console. The TOE allows filtering of audit logs based on service, severity, facility and/or message identifier.

Logs are formatted as follows:

<Priority> The priority of the message.

<SeqNumber> A number from 0 to 255. This is an identifier for the Syslog event.

<Hostname/IP Address> The resolved host name or IP address. When displaying the logfiles on the syslog server, this field is prepended to each log entry.

<Entity|Username> The entity or username that initiated the log message. Username specifies who initiated the command.

<Service> Service of the EOS that initiated the log message.

<Source> Source of the log message. Possible sources include:
CONSOLE — The console port.
EOS — The Enterprise OS system.
LoadConfig — The UI LoadConfig command. This source is visible only on locally logged messages.
xxx.xxx.xxx.xxx — The IP address of the SNMP management station that initiated an SNMP SET request. This source is visible only on locally logged messages.

<Text> A description of the event.

7.1.1.2 Firewall Logs

The TOE generates logs for Firewall related events. Log messages contain information about the system messages such as the date and time, interface, direction of the packets (ingoing or outgoing), packet header summary, and reason. Firewall logs contain the following information:

- Date/Time – Date & Time of the Event
- Transmit/Receive (direction) – Direction of traffic flow
- Interface – interface the traffic arrived on
- Source IP/Port – Source IP address and port number

- Destination IP/Port – Destination IP address and port number
- Protocol – the applicable traffic protocol - TCP, UDP, or ICMP. AH/ESP protocols are specified by name. Any other protocols are specified by numeric value
- Action – the action taken based on the event – packet permit/deny
- Filter type – the filter applied to result in the permit/deny action
- TOE Identifier – IP, MAC Address, SysName etc. (if applicable)

Services running on the TOE produce syslog messages based on the following service categories:

AuditLog, DHCP, System, Port, Firewall, OSPF/BGP, NAT, SNMP, MIP, PIM

Syslog logs are categorized by the following priority classes:

LogError, LogNotice, LogAlert, LogInfo, LogWarning, Log_Auth|LogAlert

7.1.2 Selective Audit Generation – FAU_SEL.1

The TOE allows the Network Manager and Root roles to configure which audit events are logged by configuring an “exclude” attribute that excludes events from audit generation. Audit events can be excluded based on the following attributes:

- service
- priority
- facility
- message identifier

7.1.3 Review of Audit Records – FAU_SAR.1

The TOE allows administrative-users with the Network Manager or Root privilege to view audit records through the CLI; however, routine audit review is expected to be conducted using a Syslog server.

7.1.4 Protection of Audit Records – FAU_STG.1, FAU_STG.4

Only the Network Manager or Root roles may delete audit records from the buffer on the device. The buffer is 64KB, so the TOE overwrites the oldest records when the buffer is filled.

7.2 Identification and Authentication

7.2.1 Administrative-user Authentication – FIA_UAU.2, FIA_UID.2, FIA_ATD.1a, FIA_AFL.1, FTA_SSL.3

The TOE requires positive identification and authentication of administrative-users prior to granting access the security management interface. Authentication may be performed either by the TOE itself using an internal database or using a RADIUS server in the Operational Environment. Upon the entry of authentication credentials, the TOE hashes the password. The hashed values of the entered credentials are checked against the internal database or passed to a RADIUS for validation. The TOE does not store the plaintext password.

An operator must enter a username and its password to log in. Passwords are alphanumeric strings consisting of 7 to15 characters chosen from the ASCII characters 0x20 thru 0x7E inclusive. Upon correct authentication, the role is selected from an internal lookup table based on the username of the user.

The TOE terminates inactive administrative sessions after an administrative-user configure time value. This value can be set to 2 minutes to 1440 minutes (24 hours).

After 1 to 6 consecutive failed login attempts, the TOE disables the account for between 2 minutes and 1440 minutes (24 hours). During this time additional login attempts are ignored. After the account lockout period has expired, login attempts may resume. The TOE does not maintain a failed login counter for failed login attempts to the RADIUS server.

7.2.2 SNMPv3 Passphrase Authentication – FIA_UAU.2, FIA_UID.2, FIA_ATD.1a

Access to the SNMPv3 User Manager Menu requires the entry of a SNMP username, authentication passphrase and an encryption passphrase in order to access the SNMPv3 user menu. SNMPv3 authentication is implemented per RFC 2574.

When a TOE device power cycles, sessions are terminated. An administrative-user must re-authenticate to access the TOE.

7.2.3 IKE Session Authentication – FIA_ATD.1b, FCS_IKE_EXT.1, FCS_COP.1d

For both IPsec and FRF.17, IKE is used to generate encryption and authentication keys. Internet Key Exchange (IKE) sessions are authenticated by the TOE using Pre-Shared keys. IKE uses Diffie-Hellman to negotiate the shared session keys. The Diffie-Hellman algorithm is used in conjunction with the encryption module to generate a shared secret with the peer. The shared secret is then used to generate an AES or TDES encryption key and an authentication key for use in the session. From that point forward, HMAC-SHA-1 is used with the authentication key to authenticate the packet. The AES or TDES encryption key is used to encrypt the packet for data confidentiality.

IKE negotiated session keys allow the FRF.17 protocol to further secure its data channel. IKE negotiation is initiated in one of two ways:

- Data-packet-triggered — When the TOE receives a packet to be transmitted on a port with Security enabled, it starts IKE negotiation and queues or drops the data packet. When IKE negotiation is complete, the queued data packets are transmitted.
- Pre-connect — Peers for which a Frame Relay port is specified using the PreSharedKey command are identified as pre-connect peers. The TOE attempts IKE negotiation as soon as it has a route to the IKE peer instead of waiting for a data packet to trigger IKE negotiation.

7.3 User Data Protection: Flow Control

The TOE uses a combination of statically configured routes and routes discovered through the OSPF, BGP and PIM protocols to determine how to forward traffic.

7.3.1 Packet Filtering – FDP_IFC.1a, FDP_IFF.1a

The Flow Control security function includes packet filtering which allows packet filters to be configured within the TOE that establish and enforce flow control rules. Packet parameters are established based on origin and destination IP address, direction of packet routing, protocol type and usage, and priority tags. For the Common Criteria evaluation configuration, traffic is denied by default through the device unless a permit rule allows its routing.

7.3.2 Protocol Authentication – FDP_IFC.1b, FDP_IFF.1b, FIA_ATD.1b

The TOE includes a configurable feature that performs protocol authentication through validation of messages using pre-shared keys (PSK). This applies to OSPF, BGP and PIM (Multicast) protocol traffic. Packets are authenticated upon receipt whereby the TOE validates the packets sent by peers; each holding secret keys. When the packet is received, the packet is hashed based on the protocol in use. If the two values match, the message is authenticated and routed accordingly. If the values do not match, the associated packets are dropped and a log entry is generated.

Protocol Independent Multicast (PIM) authentication uses an embedded IPsec Authentication Header with a manual authentication policy that uses static cryptographic key sets on configured peers. The SHA-1 algorithm is used for message integrity checking.

BGP and OSPF traffic is authenticated using a shared secret key and an HMAC-MD5. IPsec and FRF.17 sessions are authenticated using IKE and HMAC-SHA-1.

7.3.3 VPN support – FDP_IFC.1b, FDP_IFF.1b, FCS_IKE_EXT.1

Deployment options for VPNs supported by the TOE include:

7.3.3.1 IPsec Tunnel Mode

IPsec VPN traffic is supported though the IKE protocol in pre-shared key and manually configured Security Association mode.

7.3.3.2 FRF.17

Level 2 VPN support i.e.: FR link is protected with Layer 2 authentication and encryption using IKE in pre-shared mode as a key exchange protocol.

7.3.4 Firewall/Packet Filtering – FDP_IFF.1a

The TOE includes firewall features that allowing for the blocking of unwanted or potentially malicious traffic. The TOE is configured so everything not specifically permitted is denied. Firewall features are enabled by configuring filters within the TOE device based on connection or service type.

Filters can be created that are applied during packet inspection that can permit or deny traffic flows based on configured packet attributes. The following Firewall filter types can be applied using the TOE:

Service Independent Filter – allows TOE control through

- Filtering
- TCP/IP tiny fragment attacks (prevention)
- Packets that contain IP options such as source route, record route, and timestamp
- IP over IP tunnels
- ICMP messages (protection against denial of service attacks)

Pre-defined Service dependant filters – applies filters by service type including:

- SMTP, NNTP, FTP, HTTP, Gopher, and DNS services are filtered by the TOE by connection flow vs. packet flows. This approach allows the application of filter rules by threat type as applied to particular connection type.

FTP filter – applies filter to FTP connection types

TCP Stateful Firewall Filter - The TOE performs stateful packet inspection in which a range of IP addresses and TCP ports (source and destination) is defined over which a stateful packet inspection is performed on TCP packets. The TOE TCP stateful firewall feature mitigates the risk from the following types of attacks on TCP stacks:

- Rejecting or injecting malicious data on an existing TCP session.
- Denial of service (DoS) attacks in which the server is flooded with connection requests.

Generic Filters – allows for the creating of custom filter types using a Motorola filter drafting language. Through this, filters can be created based on rules that can be specified on a per interface basis, applied to incoming/outgoing traffic, provides logging for permit/deny packets, and can permit or deny packets based on any combination of source/destination address protocols, source/destination TCP/UDP port, ICMP message types, and TCP “Establish” keyword to differentiate the direction of TCP connections from the value of the SYN bit.

7.4 Cryptographic Operations

7.4.1 FIPS Validation summary – FCS_BCM_EXT.1

The TOE is validated as a FIPS 140-2 multi-chip standalone cryptographic module and provides cryptographic support used to encrypt message traffic for IPsec and VPN tunnel sessions, secure connections with peer router devices and establish SSHv2 encrypted sessions. The S2500 and S6000 are FIPS 140-2 Level 1 validated with certificates 1548 and 1547 respectively. The GGM 8000 is FIPS 140-2 Level 2 validated with certificate 1546.

7.4.2 Symmetric Encryption Operations – FCS_COP.1a

The TOE uses 128, 192, and 256 bit AES or 168 bit TDES to encrypt SSHv2, SNMPv3, IPsec, and FRF.17 sessions and 128 bit AES to encrypt persistent keys stored on the TOE.

7.4.3 Digital Signatures – FCS_COP.1b

RSA and DSA signatures with 1024 bit keys are used to authenticate SSHv2 sessions. An RSA digital signature is used for the FIPS firmware integrity test.

7.4.4 Hashing – FCS_COP.1c

The TOE uses SHA-1 and MD5 hashes.

HMAC-SHA-1-96 (truncated HMAC-SHA-1) is used for SSHv2, IKE, IPsec, and FRF.17 authentication and integrity checking.

HMAC-MD5 is used to authenticate BGP and OSPF traffic.

The TOE implements SNMPv3 authentication per RFC 2574. Key generation is per RFC 2274. In practice, per NMA Standards (2.8.2.1.1, 2.8.2.1.6) the authentication protocol is HMAC-

SHA-96 (truncated HMAC-SHA-1) and the privacy protocol is 128 bit AES. SHA-1 is used to derive the key from the encryption passphrase. The TOE utilizes an MD5 hash function for authentication of packets sent/received to a RADIUS Server.

7.4.5 Key Destruction – FCS_CKM.4

The zeroize command, executed from the CLI, zeroizes all plaintext FIPS CSPs according to FIPS 140-2. Plaintext FIPS CSPs are actively overwritten in RAM and flash memory.

7.5 Security Management

FMT_MOF.1a,b, FMT_MSA.1a,b,c,d, FMT_MSA.3a,b, FMT_MTD.1a,b,c,d,e,f, FMT_SMF.1, FMT_SMR.1

Security Management of the TOE is initiated via the local console, SSHv2, and SNMPv3.

The security management interface allows access to objects based on the role of the administrative-user. The TOE maintains a Root role with full read/write access to all security functions. The TOE maintains a Network Manager role with full read/write access to all security functions, except enable/disable of the audit function. The TOE maintains a User role with read only access to all functions except user management and the viewing of audit records. The Root, Network Manager, and User roles cannot be modified.

The Root role is the only role that can enable/disable the audit function. The Network Manager and Root can configure administrative-user accounts, audit functions, packet filtering, traffic routing, VPN attributes, and cryptographic settings. For managing information flow through the device, the TOE manages Source & Destination attributes for unauthenticated traffic flows. For authenticated traffic flows through the device Source and Destination attributes may be managed in addition to authentication information such as Pre-Shared Key or Shared Secret as applicable.

All TSF data managed by the TOE, except audit records and user data, may be queried by any administrative-user. User Management and Audit data can only be queried by the Network Manager and Root roles. Write access to TSF data requires the Network Manager or Root privilege.

The SNMPv3 User Manager menu allows administrative-users using SNMPv3 to create a USM User, set user privileges and manage authentication and encryption passphrases.

The TOE SNMPv3 interface supports two predefined access levels:

- MotoAdmin — Can issue any command from the SNMPv3 User Manager menu.
- MotoMaster — Can issue any command from the SNMPv3 User Manager Menu except for passphrase modification.

7.6 Protection of the TOE

FRU_RSA.1, FTP_ITC.1, FTP_TRP.1

All Administrative sessions with the TOE are conducted over encrypted channels establishing a trusted path using SSHv2 and AES encryption for SNMPv3 to prevent disclosure. These sessions also detect/prevent modifications to data transferred using a HMAC-SHA-1 to provide integrity checking of messages.

Sessions between the TOE and non-human users (IT Entities) are likewise protected against unauthorized disclosure or modification using either shared secret or shared key established cryptographic sessions using the AES or TDES algorithm and SHA-1 integrity checking.

The TOE provides mechanisms to limit the number of TCP connections that may be opened to mitigate Denial of Service SYN attacks. SYN attacks parameters are configured to limit the number of open connections that have not completed TCP initialization. In addition, the TOE provides configurable limits on the number of connection-oriented resources (i.e.: TCP, Frame Relay) a particular entity may consume to assure that TOE resources cannot be monopolized by a single or small group of IT entities. These quotas are set through firewall parameters that control the maximum number of connections to a particular server resource against a configured range of source addresses.