Security Target

Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4

ST Version 3.2

January 11, 2013

Prepared By:

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

www.juniper.net

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

1 Introduction

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

1.1 ST Reference

ST Title	Security Target: Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4
ST Revision	3.2
ST Publication Date	January 11, 2013
ST Authors	Jane Medefesser, Seth Ross

1.2 TOE Reference

TOE Reference	Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4[1]

1.3 About This ST Document

1.3.1 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that comprise the security problem to be addressed by the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Security Requirements	Contains the functional and assurance requirements for this TOE
6	TOE Summary Specification	Identifies and describes the IT security functions implemented by the TOE to meet the functional requirements
7	Rationale	Demonstrates traceability and internal consistency
8	Audit Events	TOE audit events are listed here
9	Appendices	Supporting material

Table 1 – ST Organization and Section Descriptions

[1] Note: The label displayed by the TOE at its Command Line Interface is 'JUNOS Software Release [11.2S4] (FIPS edition)'. The TOE documentation may reference the evaluated version of Junos as either '11.2 R2S4', or '11.2S4' - these references are equivalent."

1.3.2 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Common Criteria version 3.1. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria defines several operations that can be performed on functional requirements, including *assignment, selection, refinement* and *iteration*.

The following applies to the operations performed by the Security Target author.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in bold text and in square brackets, i.e. [**assignment_value(s)**].
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. A selection operation is indicated by showing the value in italics and in square brackets, i.e. [*selection_value(s)*].
- An assignment within a selection is indicated by showing the value in bold italics and in square brackets, i.e. [***selected-assignment***].
- The refinement operation allows the addition of details or the narrowing of requirements components. A refinement operation is indicated by showing the value in bold text, i.e. **refinement_value(s)**.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement component and element identifiers from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1(1) and FMT_MTD.1(2) refer to separate instances of the FMT_MTD.1 security functional requirement component, where the corresponding requirement elements would be identified as FMT_MTD.1.1(1), and FMT_MTD.1.1(2), respectively.
- National Information Assurance Partnership (NIAP) interpretations are used and are presented with the text string “NIAP” and the NIAP interpretation number as part of the requirement identifier (e.g., FAU_GEN.1-NIAP-0429 for Audit data generation).
- In this document, extended requirements are indicated with the text string “(EXT)” following the component name.

1.3.3 Document Terminology

See Section 9.2 for the Glossary.

1.4 TOE Overview

The Target of Evaluation (TOE) includes two secure router products running Junos 11.2S4:

- LN1000-V Mobile Secure Router (abbreviated LN1000), and
- SRX650 Services Gateway (abbreviated SRX650)

These network boundary devices provide three basic services:

- Routing — forwarding data packets along networks in accordance with one or more routing protocols

- Firewalling — applying access rules to control connectivity between two or more network environments
- Intrusion detection — monitoring and analyzing a set of IT system resources for potential vulnerabilities or misuse

The devices run the same version of the Junos Software, and offer identical security functionality.

The LN1000 is intended for deployment in the following environments:

- Defense communities
- Public sector safety organizations, such as first responders

The SRX650 is intended for deployment at remote and branch locations in the network to provide all-in-one secure WAN connectivity, IP telephony, and connection to local PCs and servers via integrated Ethernet switching.

1.5 TOE Description

The Juniper Networks LN1000 and SRX650 devices are complete routing, firewalling, and IDS systems that support a variety of high-speed interfaces for network applications.

The secure routers share a common operating system, a common architecture, and a common “release train” for delivery to customers. The LN1000 and SRX650 share identical security functionality.

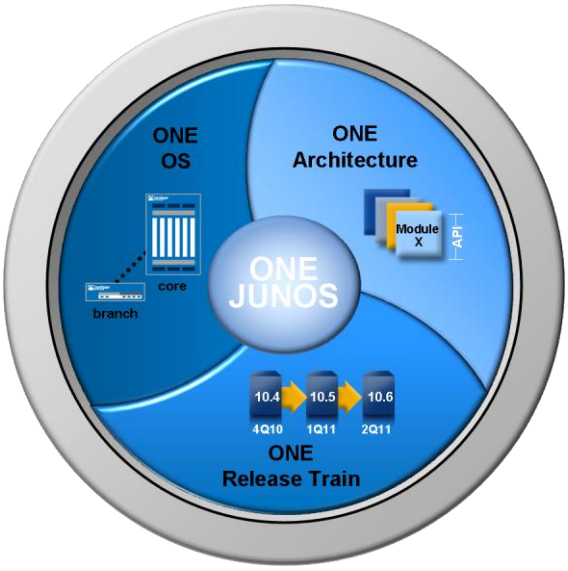

Figure 1 – One Junos

The secure routers are physically self-contained, housing the software, firmware and hardware necessary to perform all routing, firewalling, and intrusion detection functions.

The architecture of the secure routers cleanly separates routing and control functions from packet forwarding operations, thereby eliminating bottlenecks and permitting the router to maintain a high level of performance.

Each secure router includes the following major architectural components:

- The Routing Engine (RE) runs the Junos Software and provides Layer 3 routing services and networking;
- The Packet Forwarding Engine (PFE) provides all operations necessary for transit packet forwarding.

This architecture inherently enforces separation of control and forwarding, isolating each within its own security domain. For the SRX650, the RE and PFE reside on physically separate hardware planes. For the LN1000, the control and forwarding are still logically separate processes, but they run on the same hardware plane.

Traffic that enters and exits the secure routers running Junos Software is processed according to features the customer configures, such as packet filters, security policies, and pre-configured filters for common attacks (also known as “screens”). For example, the software can determine:

- Whether the packet is allowed into the device
- Which firewall screens to apply to the packet
- The route the packet takes to reach its destination
- Whether to apply Network Address Translation (NAT) to translate the packet’s IP address
- Whether the packet requires an Application Layer Gateway (ALG)

Packets that enter and exit the secure router undergo both packet-based and flow-based processing.

- Flow-based packet processing treats related packets, or a stream of packets, in the same way. Packet treatment depends on characteristics that were established for the first packet of the packet stream, which is referred to as a flow. This is also known as “stateful packet processing”.
- Packet-based, or stateless, packet processing treats packets discretely. Each packet is assessed individually for treatment.

Interfaces act as a doorway through which traffic enters and exits the secure router. Many interfaces can share exactly the same security requirements; however, different interfaces can also have different security requirements for inbound and outbound data packets. Interfaces with identical security requirements can be grouped together into a single security zone.

Security zones are the building blocks for policies; they are logical entities to which one or more interfaces are bound. Security zones provide a means of distinguishing groups of hosts (user systems and other hosts, such as servers) and their resources from one another in order to apply different security measures to them.

Security zones have the following properties:

- Interfaces — A list of interfaces in the zone.
- Policies — Active security policies that enforce rules for the transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall.
- Screens — A Juniper Networks stateful firewall secures a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another. For every security zone a set of predefined screen options can be enabled that detect and block various kinds of traffic that the device determines as potentially harmful. This is known as “Reconnaissance Deterrence”.
- Address books—An administrator defined rule-set containing the IP address or domain names of hosts and subnets whose traffic is either permitted, denied, encrypted, or user-authenticated. An address book is a management object that assists the administrator manage the IP addresses for the firewall ruleset. It does not play a direct role in the enforcement of the information flow policy.

To secure all connection attempts, Junos uses a dynamic packet-filtering method known as stateful inspection. Using this method, Junos identifies various components in the IP packet and TCP segment headers—source and destination IP addresses, source and destination port numbers, and packet sequence numbers—and maintains the state of each TCP session and pseudo UDP session traversing the firewall. Junos also modifies session states based on changing elements such as dynamic port changes or session termination.

When a responding TCP packet arrives, Junos Software compares the information reported in its header with the state of its associated session stored in the inspection table. If they match, the responding packet is allowed to pass the firewall. If the two do not match, the packet is dropped.

Junos Screen options secure a zone by inspecting, then allowing or denying, all connection attempts that require crossing an interface bound to that zone. Junos then applies firewall policies, which can contain content filtering and IDS components, to the traffic that passes the Screen filters.

The Junos IDS system selectively enforces various attack detection and prevention techniques on network traffic traversing the secure routers. It enables the definition of policy rules to match traffic based on a zone, network, and application, and then take active or passive preventive actions on that traffic.

The signature database is stored on the secure router and contains definitions of predefined attack objects and groups. These attack objects and groups are designed to detect known attack patterns and protocol anomalies within the network traffic. In response to new vulnerabilities, Juniper Networks periodically provides a file containing attack database updates on the Juniper web site.

The TOE supports IPsec to provide confidentiality and integrity services for network traffic transmitted between TOE devices and for traffic transmitted from a TOE device to an external IT system (e.g., a peer router). The TOE does not provide support for general-purpose VPN clients to connect to the TOE. The only

VPN connectivity in an evaluated configuration is between peer routers (per FTP_ITC.1(1) and FTP_ITC.1(2)).

The following figure shows a typical IPsec architecture:

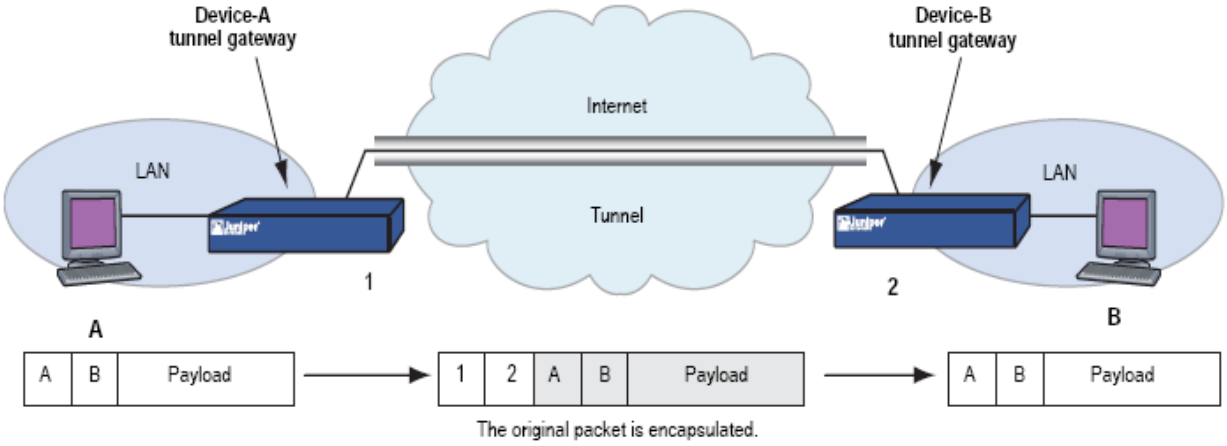

Figure 2 – Typical IPsec Configuration

The Junos Software performs all IPsec operations, and supports the Authentication Header (AH) and Encapsulating Security Payload (ESP) security protocols, the set-up and processing of Security Associations (SAs), the Internet Key Exchange (IKE) protocol, and the IPsec algorithms for authentication and encryption.

Each secure router is a hardware device that protects itself largely by offering only a minimal logical interface to the network and attached nodes. Junos is a special purpose OS that provides no general purpose programming capability. All network traffic from one network zone to another or between two networks within the same network zone passes through the TOE. The TOE also preserves its configuration for a trusted recovery in the event that the configuration has been modified and not saved or if the security router has been ungracefully shutdown. The TOE additionally protects the session table by enforcing destination-based session limits and applying procedures to limit the lifetime of sessions when the session table reaches the defined watermark.

1.5.1 Physical Boundary

1.5.1.1 The LN1000 Mobile Security Router

The LN1000 is an embedded router that operates identically in both wire-line and wireless environments and with communication nodes that are either mobile or stationary. The LN1000 is a single hardware card designed to operate in a VITA 46.0 chassis; the chassis is part of the IT environment. The card conforms to the VITA 46.0 IEEE 1101.2 specifications and is a 3U compact node slot interface. A single slot VITA 46 card is approximately 3”x 6”. It supports eight Gigabit Ethernet ports.

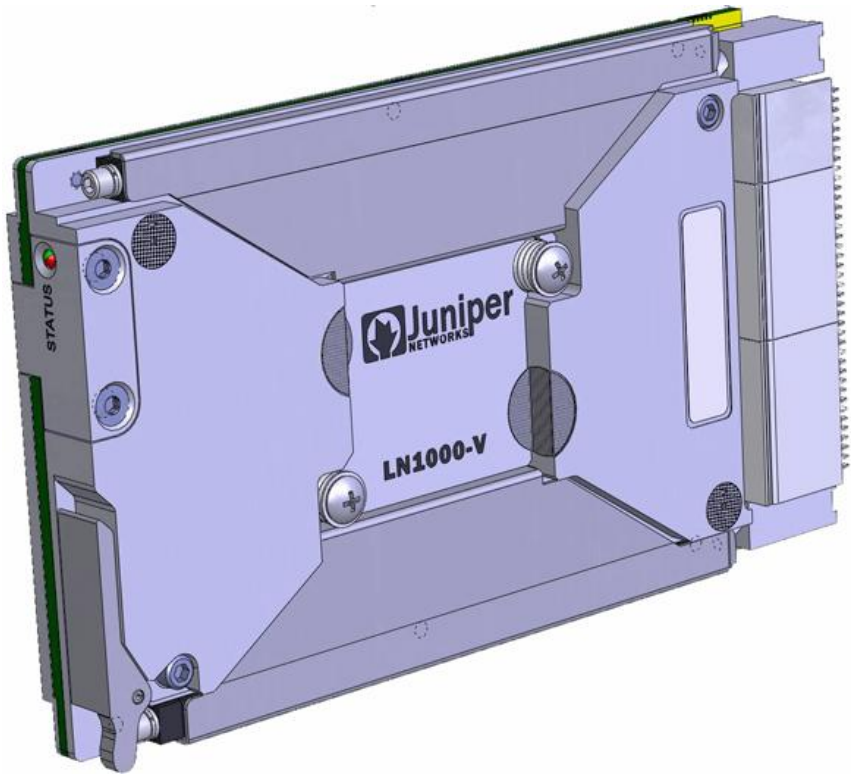

Figure 3 - The LN1000 Mobile Security Router

1.5.1.2 The SRX650 Services Gateway

The physical boundary of the SRX650 is the physical device. It features four fixed 10/100/1000 Ethernet LAN ports and eight Gigabit Ethernet-backplane Physical Interface Module (GPIM) slots. The exterior dimensions are 17.5 x 3.5 x 18.2 in (44.4 x 8.8 x 46.2 cm); it weighs 24.9 lbs (11.3 kg). The device has 2 GB DRAM, 2 GB compact flash, and an external compact flash slot for additional storage.

1.5.2 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Audit (FAU)	TOE auditable events are stored in an administrator-configurable memory buffer. Auditable events include start-up and shutdown of the audit functions, start-up and shutdown of the IDS audit functions, authentication events, and service requests, as well as the events listed in Table 20 in Section 8. Audit records include the date and time, event category, event type, username, and the outcome of the event (success or failure). The TOE provides the capability of analyzing potential intrusions via signature analysis, which uses patterns corresponding to known attacks, and by detecting protocol anomalies. The TOE enforces two roles related to audit: the Audit Administrator and the IDS Audit Administrator. The audit log can be viewed by all Administrators; the IDS audit log can be viewed only by the IDS Administrator. Search and sort facilities are provided, along with the ability for the the appropriate administrator to determine the amount of space dedicated to audit record storage. The oldest audit records in the buffer are overwritten when space available for audit storage is exhausted. In conjunction with the audit capabilities, the TOE provides an alarm mechanism that provides immediate notification of potential security violations and potential intrusions.
Cryptographic Support (FCS)	The TOE includes a baseline cryptographic module that provides confidentiality and integrity services for authentication and for protecting communications with adjacent systems. The cryptographic module fulfills the requirements of FIPS 140-2, and has been awarded certificates 1704 (SRX650) and 1718 (LN1000).
User Data Protection/Information Flow Control (FDP)	The TOE is designed to forward network packets (i.e., information flows) from source network entities to destination network entities based on available routing information. This information is either provided directly by TOE users or indirectly from other network entities (outside the TOE) configured by the TOE users. The TOE has the capability to regulate the information flow across its interfaces; traffic filters can be set in accordance with the presumed identity of the source, the identity of the destination, the transport layer protocol, the source service identifier, and the destination service identifier (TCP or UDP port number).

TSF	DESCRIPTION
Identification and Authentication (FIA)	The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The devices also require that applications exchanging information with them successfully authenticate prior to any exchange. This covers all services used to exchange information, including Secure Shell (SSH). Telnet, File Transfer Protocol (FTP), Secure Socket Layer (SSL) are out of scope. Authentication services can be handled either internally (user selected passwords) or through a RADIUS or TACACS+ authentication server in the IT environment. Note that in support of FIPS 140-2 compliance, external authentication servers are excluded from use in the evaluated configuration.
Security Management (FMT)	The TOE provides four distinct administrative roles: The Cryptographic Administrator is responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product; the Audit Administrator is responsible for the configuration and maintenance of the evaluated product's audit data; the IDS Administrator is solely responsible for regular review and management of the IDS audit data; the Security Administrator is responsible for all other administrative tasks (e.g., creating the security policy) not addressed by the other three administrative roles. The devices are managed through a Command Line Interface (CLI). The CLI is accessible through an SSH session, or via a local terminal console.
Protection of the TSF (FPT)	The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of routes. Another protection mechanism is that all routing functions of the TOE are confined to the device itself. The secure router is completely self-contained, and therefore maintains its own execution domain. Each sub-component of the Junos Software operates in an isolated execution environment, protected from accidental or deliberate interference by others. The TOE provides for both cryptographic and non-cryptographic self-tests, and is capable of automated recovery from failure states.
Resource Utilization (FRU)	The TOE can enforce traffic quotas based on source IP address and/or based on TCP protocol.
TOE Access (FTA)	The TOE can be configured to lock and/or terminate interactive user sessions, to present an access banner with warning messages prior to authentication, and to deny logon based on location, time, and day.
Trusted Path/Channels (FTP)	The TOE creates trusted channels between itself and remote trusted authorized IT product entities that protect the confidentiality and integrity of communications. The TOE creates trusted paths between itself and remote administrators and users that protect the confidentiality and integrity of communications.

Table 2 - Logical Boundary

1.5.3 Summary of Out-of-Scope Items

The following items are out of the scope of the evaluation:

- Use of telnet, since it violates the Trusted Path requirement set (see Section 5)
- Use of FTP, since it violates the Trusted Path requirement set (see Section 5)
- Use of SNMP, since it violates the Trusted Path requirement set (see Section 5)
- Management via J-Web, since it violates the Trusted Path requirement set (see Section 5)
- Media use (other than during installation of the TOE)
- Use of the LN1000-V RTM or SRX650 SRE
- RADIUS and TACACS+ authentication servers

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 extended and Part 3 conformant. The TOE is EAL4, augmented with ALC_FLR.2.

3 Security Problem Definition

The security problem definition (SPD) describes the security problem to be addressed. The statement of TOE security environment defines the following:

- Threats to be countered by the TOE, its operational environment, or a combination of the two;
- Assumptions made on the operational environment in order to be able to preserve security functionality;
- Organizational security policies with which the TOE, its' operational environment, or a combination of the two are to comply.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

A threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset.

- Threat agents are entities that can adversely act on assets – the threat agents in the threats below are unauthorized user, network attacker, and authorized user,
- Assets are entities that someone places value upon – the assets are access to network services,
- Adverse actions are actions performed by a threat agent on an asset – the adverse actions are: unauthorized changes to configuration, both network routing configuration and management configuration.

Table 15 - Threats Addressed by the TOE in Section 7.1 identifies each threat addressed by the TOE and provides rationale for its inclusion in the Security Target.

Table 3 - Threats Addressed by the TOE

THREAT	DESCRIPTION
T.ADDRESS_MASQUERADE	A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.
T.ADMIN_ROGUE	An administrator's intentions may become malicious resulting in user or TOE Security Functions (TSF) data being compromised.
T.AUDIT_COMPROMISE	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.CRYPTO_COMPROMISE	A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
	.
T.EAVESDROP	A malicious user or process may observe or modify user or TSF data transmitted between the TOE and another trusted IT entity
T.MALICIOUS_TSF_COMPROMISE	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.

THREAT	DESCRIPTION
T.REPLAY	A user may gain inappropriate access to the TOE by replaying authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or security attributes (e.g., captured as transmitted during the course of legitimate use).
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.RESOURCE_EXHAUSTION	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.SPOOFING	A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.
T.UNAUTHORIZED_PEER	An unauthorized IT entity may attempt to establish a security association with the TOE.
T.UNIDENTIFIED_ACTIONS	The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.UNIDENTIFIED_INTRUSIONS	The IDS Administrator may fail to notice potential intrusions, thus limiting the IDS Administrator's ability to identify and take action against a possible intrusion.
T.UNKNOWN_STATE	When the TOE is initially started or restarted after a failure, the security state of the TOE may be unknown.

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The TOE is required to meet the following organizational security policies.

Table 16 - Organizational Security Policies in Section 7.2 identifies each Organizational Security Policy addressed by the TOE and provides rationale for its inclusion in the Security Target.

POLICY NAME	POLICY DESCRIPTION
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
P.COMPATIBILITY	The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operation with other routers and network equipment using the same protocols.

POLICY NAME	POLICY DESCRIPTION
P.CRYPTOGRAPHY	The TOE shall use NIST FIPS-validated cryptography as a baseline with additional NSA-approved methods for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys), and for cryptographic operations (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).
P.IDS_DATA_COLLECTION	IDS audit events based on data collected from IT System resources will be created.

Table 4 - Organizational Security Policies

3.3 Assumptions

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

Table 17 - Assumptions Consistency Rationale in Section 7.3 identifies each assumption addressed by the TOE and provides rationale for its inclusion in the Security Target.

ASSUMPTION	DESCRIPTION
A.NO_GENERAL_PURPOSE	The administrator 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 IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
A.NO_TOE.BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

Table 5 - Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT Security Objectives for the TOE are stated below.

The tables in Sections 7.1 and 7.2 trace each Security Objective for the TOE to the threats and Organizational Security Policies specified in the Security Problem Definition, and provide rationale justifying why the Security Objectives for the TOE are suitable to counter the specified threats and satisfy the specified OSPs.

OBJECTIVE	DESCRIPTION
O.ADMIN_ROLE	The TOE will provide administrator roles to isolate administrative actions, and to make the administrative functions available locally and remotely.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information (i.e. audit records and IDS audit records).
O.AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.
O.CORRECT_ TSF_OPERATION	The TOE will provide a capability to test the TSF to ensure the correct operation of the TSF in its operational environment.
O.CRYPTOGRAPHIC_FUNCTIONS	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.CRYPTOGRAPHY_VALIDATED	The TOE shall use NIST FIPS 140-2 validated crypto modules for cryptographic services implementing FIPS-approved security functions and random number generation services used by cryptographic functions.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.

OBJECTIVE	DESCRIPTION
O.IDS_AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events from targeted IT System resource(s) and associate those events with component that created the record.
O.IDS_AUDIT_REVIEW	The TOE will provide the capability to selectively view IDS audit information, and alert the IDS Administrator of potential intrusions.
O.MAINT_MODE	The TOE shall provide a mode from which recovery or initial startup procedures can be performed.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE_INFORMATION_FLOW	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_AUTHENTICATION	The TOE will authenticate each peer TOE that attempts to establish a security association with the TOE.
O.PROTOCOLS	The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or Industry specifications to ensure interoperability.
O.PROTECT_IN_TRANSIT	The TSF shall protect TSF data when it is in transit between the TSF and another trusted IT entity.
O.REPLAY_DETECTION	The TOE will provide a means to detect and reject the replay of authentication data and other TSF data and security attributes.
O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated.
O.RESOURCE_SHARING	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).

OBJECTIVE	DESCRIPTION
O.ROBUST_TOE_ACCESS	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 administrator to set the time used for these time stamps.
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.

Table 6 - TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below.

The table in Section 7.3 traces Security Objectives for the Operational Environment to the assumptions specified in the Security Problem Definition, and provides rationale justifying why the Security Objectives for the Operational Environment are suitable to meet the assumptions.

OBJECTIVE	DESCRIPTION
OE.NO_GENERAL_PURPOSE	The Administrator 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 IT environment.
OE.MANAGEMENT	The environment will provide a secure communication path with the TSF for the purpose of remote administration of the TOE by authorized administrators.
OE.CRYPTANALYTIC	Cryptographic methods used in the IT environment shall be interoperable with the TOE, should be FIPS 140-2 validated and should be resistant to cryptanalytic attacks (i.e., will be of adequate strength to protect unclassified Mission Support, Administrative, or Mission Critical data).
OE.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

Table 7 - Operational Environment Security Objectives

5 Security Requirements

This section provides security functional and assurance requirements that must be satisfied by the TOE. These requirements consist of components from the CC Part 2 and Part 3, National Information Assurance Partnership (NIAP) interpreted requirements, and explicit requirements.

5.1 Security Functional Requirements

The table in Section 7.4 traces security functional requirements to the Security Objectives for the TOE and provides rationale why the SFRs are suitable to meet the Security Objectives.

"ST Notes" are intended to clarify the relationships between the SFR and the TOE design and implementation. All statements in the notes are normative and descriptive, rather than prescriptive. They are intended as aids to understanding for developers, evaluators, and customers.

The security functional requirements for this Security Target consist of the following components, which are summarized in the following table.

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_ARP.1(1)	Security alarms – security violations
	FAU_ARP.1(2)-IDS	Security alarms – IDS intrusion alarms
	FAU_ARP_ACK_(EXT).1	Security alarm acknowledgement
	FAU_ARP_ACK_ (EXT).2-IDS	Intrusion alarm acknowledgement
	FAU_GEN.1-NIAP-0429	Audit data generation
	FAU_GEN_(EXT).1-IDS	Audit data generation -- IDS audit records
	FAU_GEN.2-NIAP-0410	User identity association – human users
	FAU_SAA.1-NIAP-0407	Potential violation analysis
	FAU_SAA_(EXT).1-IDS	Analyzing capability intrusion analysis
	FAU_SAR.1(1)	Audit review – audit records
	FAU_SAR.1(2)-IDS	Audit review – IDS audit records
	FAU_SAR.2(1)	Restricted audit review – audit records
	FAU_SAR.2(2)-IDS	Restricted audit review – IDS audit records
	FAU_SAR.3(1)	Selectable audit review – audit records
	FAU_SAR.3(2)-IDS	Selectable audit review – IDS audit records
	FAU_SEL.1-NIAP-0407(1)	Selective audit – audit events
	FAU_SEL.1-NIAP-0407(2)-IDS	Audit event selection – IDS audit events
	FAU_STG.1-NIAP-0429	Protected audit event storage
	FAU_STG.2-NIAP-0429-IDS	Guarantees of audit data availability
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.NIAP-0414-1-NIAP-0429(1)	Site-configurable prevention of audit loss – audit records
	FAU_STG.NIAP-0414-1-NIAP-0429(2)-IDS	Site-configurable prevention of audit data loss -- IDS audit records
Cryptographic Support	FCS_BCM_(EXT).1	Baseline Cryptographic Module
	FCS_CKM.1(1)	Cryptographic key generation (for symmetric keys using Random Number Generator (RNG))
	FCS_CKM.1(2)	Cryptographic key generation (for asymmetric keys)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_CKM_(EXT).2	Cryptographic Key Handling and Storage

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	FCS_COP.1(1)	Cryptographic operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic operation (for cryptographic signature)
	FCS_COP.1(3)	Cryptographic operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic operation (for cryptographic key agreement)
	FCS_COP_(EXT).1	Random Number Generation
	FCS_IKE_(EXT).1	Internet Key Exchange
User Data Protection	FDP_IFC.1(1)	Subset information flow control (unauthenticated Information flow policy)
	FDP_IFC.1(2)	Subset information flow control (unauthenticated TOE services policy)
	FDP_IFF.1(1)	Simple security attributes (unauthenticated Information flow policy)
	FDP_IFF.1(2)	Simple security attributes (unauthenticated TOE services policy)
	FDP_RIP.2	Full residual information protection
Identification and Authentication	FIA_AFL.1-NIAP-0425	Authentication failure handling
	FIA_ATD.1(1)	User attribute definition (Human users)
	FIA_ATD.1(2)	User attribute definition (TOE to TOE Identification)
	FIA_UAU.1-FW	Timing of authentication (for TOE services)
	FIA_UAU_(EXT).2-FW	Specified User authentication before any action
	FIA_UAU_(EXT).5	Authentication mechanism
	FIA_UID.2	User Identification Before Any Action (Human Users)
	FIA_USB.1	User-subject binding (human user-subject binding)
Security Management	FMT_MOF.1(1)	Management of security functions behavior (TSF non-cryptographic self-test)
	FMT_MOF.1(2)	Management of security functions behavior (cryptographic self-test)
	FMT_MOF.1(3)	Management of security functions behavior (audit review)
	FMT_MOF.1(4)	Management of security functions behavior (audit selection)
	FMT_MOF.1(5)	Management of security functions behavior (alarms)
	FMT_MOF.1(6)	Management of security functions behavior (quota mechanism)
	FMT_MOF.1(6)-FW	Management of security functions behavior (available TOE-services for unauthenticated users)
	FMT_MOF.1(6)-IDS	Management of security functions behavior (IDS audit review)
	FMT_MOF.1(7)	Management of security functions behavior (unsuccessful authentication attempts)
	FMT_MOF.1(7)-IDS	Management of security functions behavior (IDS audit selection)
	FMT_MOF.1(8)-IDS	Management of security functions behavior (IDS intrusion alarms)
	FMT_MSA.1-FW	Management of security attributes

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	FMT_MSA.2	Secure security attributes
	FMT_MSA.3(1)	Static attribute initialization (unauthenticated services)
	FMT_MSA.3-NIAP-0409(1)-FW	Static attribute initialization (ruleset)
	FMT_MSA.3-NIAP-0409(2)-FW	Static attribute initialization (services)
	FMT_MTD.1(1)	Management of TSF data (non-cryptographic, non-time TSF data)
	FMT_MTD.1(2)	Management of TSF data (cryptographic TSF data)
	FMT_MTD.1(3)	Management of TSF data (time TSF data)
	FMT_MTD.1(4)	Management of TSF data (information flow policy ruleset)
	FMT_MTD.2(1)	Management of limits on TSF data (transport-layer quotas)
	FMT_MTD.2(2)	Management of limits on TSF data (controlled connection-oriented quotas)
	FMT_MTD.2(3)	Management of limits on TSF data (percentage of storage capacity for audit records)
	FMT_REV.1	Revocation
	FMT_REV.1-FW	Revocation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.2	Restrictions on security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_PRO_(EXT).1	Standard protocol usage
	FPT_RCV.2	Automated Recovery
	FPT_RPL.1	Replay detection
	FPT_STM.1	Reliable time stamps
	FPT_TDC.1	Inter-TSF basic TSF data consistency
	FPT_TST_(EXT).1	TSF testing
	FPT_TST.1(1)	TSF testing (for cryptography)
	FPT_TST.1(2)	TSF testing (for key generation)
Resource Utilization	FRU_RSA.1	Maximum quotas (controlled connection-oriented quotas)
TOE Access	FTA_SSL.1-FW/IDS	TSF-initiated session locking
	FTA_SSL.2-FW/IDS	User-initiated locking
	FTA_SSL.3(1)	TSF-initiated termination (interactive sessions)
	FTA_SSL.3(2)	TSF-initiated termination (remote sessions)
	FTA_TAB.1	Default TOE access banners
	FTA_TSE.1	TOE session establishment
Trusted Path/Channels	FTP_ITC.1(1)	Inter-TSF trusted channel (prevention of disclosure)
	FTP_ITC.1(2)	Inter-TSF trusted channel (detection of modification)
	FTP_TRP.1(1)	Trusted path (prevention of disclosure)
	FTP_TRP.1(2)	Trusted path (detection of modification)

Table 8 - TOE Security Functional Requirements

5.1.1 Security Audit (FAU)

5.1.1.1 Security alarms – security violation (FAU_ARP.1(1))

FAU_ARP.1.1(1) The TSF shall ~~take~~ [immediately display a message identifying the potential security violation, and make accessible the audit record contents associated with the auditable event(s) that generated the alarm, at the

a) local console;

b) remote Security Administrator sessions that exist;

c) remote Security Administrator sessions that are initiated before the alarm has been acknowledged; and

d) [*no other methods*]

upon detection of a potential security violation.

5.1.1.2 Security alarms – IDS intrusion alarms (FAU_ARP.1(2)-IDS)

FAU_ARP.1(2)-IDS The TSF shall [immediately generate an alarm message, identifying the potential intrusion, and make accessible the analytical result associated with the IDS auditable event(s) that generated the alarm, at the [**local console and the remote Security Administrator sessions**] and take [**no other actions**]] upon detection of a potential intrusion.

5.1.1.3 Security alarm acknowledgement (FAU_ARP_ACK_ (EXT).1)

FAU_ARP_ACK_(EXT).1.1

The TSF shall display the alarm message identifying the potential security violation and make accessible the audit record contents associated with the auditable event(s) until it has been acknowledged. If the Security Administrator configures the TOE to generate an optional audible alarm, the audible alarm will sound until acknowledged by an administrator. Once the alarm is acknowledged, it will be reset to zero.

FAU_ARP_ACK_(EXT).1.2

The TSF shall generate an acknowledgement message identifying a reference to the potential security violation, a notice that it has been acknowledged, the time of the acknowledgement and the user identifier that acknowledged the alarm. The TSF shall provide the capability to view alarm acknowledgements at the local console and at remote administrator sessions that received the alarm.

5.1.1.4 Intrusion alarm acknowledgement (FAU_ARP_ACK_ (EXT).2-IDS)

FAU_ARP_ACK_(EXT).2.1-IDS

The TSF shall display the alarm message identifying the potential intrusion and make accessible the analytical result associated with the IDS auditable event(s) until it has been acknowledged.

FAU_ARP_ACK_(EXT).2.2-IDS

The TSF shall generate an acknowledgement message identifying a reference to the potential intrusion, a notice that it has been acknowledged, the time of the acknowledgement and the user identifier that acknowledged the alarm. The TSF shall provide the capability to view alarm acknowledgements at the local console and at remote IDS administrator sessions that received the alarm.

5.1.1.5 Audit data generation (FAU_GEN.1-NIAP-0429)

FAU_GEN.1.1-NIAP-0429

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

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

b) All auditable events for the *basic* level of audit; and

c) [specifically defined auditable events listed in the table in Section 8].

FAU_GEN.1.2-NIAP-0429

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

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

b) For each audit event time, based on the auditable event definitions of the functional components included in the ST, [information specified in column three in the table in Section 8].

5.1.1.6 Audit data generation - IDS audit records (FAU_GEN_(EXT).1-IDS)

FAU_GEN_(EXT).1.1-IDS

The TSF shall be able to generate an IDS audit record by collecting the following information from the targeted IT System resource(s):

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

b) identification and authentication events, service requests, and network traffic;

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

FAU_GEN_(EXT).1.2-IDS

The TSF shall record within each IDS audit record at least the following information:

a) Date and time of the event, type of event.

b) For each IDS audit event type selected in FAU_GEN_(EXT).1.1, based on the IDS auditable event definitions of the functional components included in the ST, [none].

Application Note: In the context of this ST, "targeted IT System resource(s)" refers to the TOE itself. The IDS capability of the TOE monitors activity on the TOE itself and all network traffic received by the TOE.

5.1.1.7 User identity association – human users (FAU_GEN.2-NIAP-0410)

FAU_GEN.2.1-NIAP-0410

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

5.1.1.8 Potential violation analysis (FAU_SAA.1-NIAP-0407)

FAU_SAA.1.1-NIAP-0407

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicates a potential violation of the TSP.

FAU_SAA.1.2-NIAP-0407

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [

1. Security Administrator specified number of user authentication failures;
2. Any detected replay of TSF data or security attributes;
3. Any failure of the cryptographic self-tests;
4. Any failure of the other TSF self-tests;
5. Cryptographic Administrator specified number of encryption failures;
6. Cryptographic Administrator specified number of decryption failures; and
7. Security Administrator specified number of Information Flow policy violations by an individual presumed source network identifier (e.g., IP address) within an administrator specified time period;

8. Security Administrator specified number of Information Flow policy violations to an individual destination network identifier within an administrator specified time period;

9. Security Administrator specified number of Information Flow policy violations to an individual destination subject service identifier (e.g., TCP port) within an administrator specified time period;

10. Security Administrator specified Information Flow policy rule, or group of rule violations within an administrator specified time period;

] known to indicate a potential security violation;

b) ["*no additional rules*"]

5.1.1.9 Analyzing capability intrusion analysis (FAU_SAA_(EXT).1-IDS)

FAU_SAA_(EXT).1.1-IDS

The TSF shall perform the following analysis functions on all IDS audit data received:

a) Signature analysis which uses patterns corresponding to known attacks or misuses of a System,

then create an analytical result for each potential intrusion.

FAU_SAA_(EXT).1.2-IDS

The TSF shall create an IDS audit record for each analytical result with at least the following information:

a) Date and time of the result, type of analysis, outcome of analysis, Analyzer component ID, IDS audit records that generated potential intrusion; and

b) [**none**].

5.1.1.10 Audit review – audit records (FAU_SAR.1(1))

FAU_SAR.1.1(1) The TSF shall provide [the Administrators] with the capability to read [all audit data] from the audit records.

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

5.1.1.11 Audit review -- IDS audit records (FAU_SAR.1(2)-IDS)

FAU_SAR.1.1(2)-IDS The TSF shall provide [the IDS Administrator] with the capability to read [all IDS audit information] from the IDS audit records.

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

5.1.1.12 Restricted audit review – audit records (FAU_SAR.2(1))

FAU_SAR.2.1(1) The TSF shall prohibit all users read access to the audit records in the audit trail, except the administrators.

5.1.1.13 Restricted audit review -- IDS audit records (FAU_SAR.2(2)-IDS)

FAU_SAR.2.1(2)-IDS The TSF shall prohibit all users read access to the IDS audit records, except those users that have been granted explicit read-access.

5.1.1.14 Selectable audit review – audit records (FAU_SAR.3(1))

FAU_SAR.3.1(1) The TSF shall provide the ability to perform searches and sorting of audit data based on:

a. [user identity;

b. source subject identity;

c. destination subject identity;

d. ranges of one or more: dates, times, user identities, subject service identifiers, or transport layer protocol;

e. rule identity;

f. TOE network interfaces; and

g. [*no additional criteria*].

5.1.1.15 Selectable audit review -- IDS audit records (FAU_SAR.3(2)-IDS)

FAU_SAR.3.1(2)-IDS The TSF shall provide the ability to perform searches and sorting of IDS audit data based on [date and time, type of event, success or failure of related event].

5.1.1.16 Selective audit – audit events (FAU_SEL.1-NIAP-0407(1))

FAU_SEL.1.1-NIAP-0407(1)
The TSF shall allow only the Security Administrator to include or exclude auditable events from the set of audited events based on the following attributes:

a. user identity;

b. event type;

c. success of auditable security events;

d. failure of auditable security events; and

e. [***network identifier, policy name, subject service identifier***].

5.1.1.17 Selective audit -- IDS audit events (FAU_SEL.1-NIAP-0407(2)-IDS)

FAU_SEL.1.1-NIAP-0407(2)-IDS

The TSF shall allow only the IDS Administrator to include or exclude IDS auditable events from the set of IDS audited events based on the following attributes:

a) [Event type; and

b) [*no additional attributes*.]

5.1.1.18 Protected audit trail storage (FAU_STG.1-NIAP-0429)

FAU_STG.1.1-NIAP-0429

The TSF shall restrict the deletion of stored audit records in the audit trail to the Audit Administrator.

FAU_STG.1.2-NIAP-0429

The TSF shall be able to prevent modifications to the audit records in the audit trail.

5.1.1.19 Guarantees of IDS audit data availability (FAU_STG.2-NIAP-0429-IDS)

FAU_STG.2.1-NIAP-0429-IDS

The TSF shall restrict the deletion of stored IDS audit records in the IDS audit trail to the IDS Administrator.

FAU_ STG.2.2-NIAP-0429-IDS

The TSF shall be able to prevent unauthorized modifications to the IDS audit records in the IDS audit trail.

FAU_ STG.2.3-NIAP-0429-IDS

The TSF shall ensure that [**the most recent**] IDS audit records will be maintained when the following conditions occur: [*IDS audit storage exhaustion*].

5.1.1.20 Action in case of possible audit data loss (FAU_STG.3)

FAU_STG.3.1 The TSF shall [immediately alert the administrators by displaying a message at the local console, [and at the remote administrative console when an administrative session exists for each of the defined administrative roles, at the option of the Security Administrator generate an audible alarm] [**no other actions**] if the audit trail exceeds [a Security Administrator settable percentage of storage capacity].

5.1.1.21 Site-configurable prevention of audit data loss – audit records (FAU_STG.NIAP-0414-1-NIAP-0429(1))

FAU_STG.NIAP-0414-1.1-NIAP-0429

The TSF shall provide the Security Administrator the capability to select one or more of the following actions [*'overwrite the oldest stored audit records'*] and [**no other actions to be taken in case of audit storage failure**] to be taken if the audit trail is full.

FAU_STG.NIAP-0414-1.2-NIAP-0429

The TSF shall enforce the Security Administrator's [*"overwrite the oldest stored audit records"*] and [**no other actions to be taken in case of audit storage failure**] if the audit trail is full.

5.1.1.22 Site-configurable prevention of audit data loss -- IDS audit records (FAU_STG.NIAP-0414-1-NIAP-0429(2)-IDS)

FAU_STG.NIAP-0414-1.1-NIAP-0429(2)-IDS

The TSF shall provide the IDS Administrator the capability to select one or more of the following actions [*'overwrite the oldest stored IDS audit records'*] and [**no other actions to be taken in case of IDS audit store failure**] to be taken if the IDS audit trail is full.

FAU_STG.NIAP-0414.1.2-NIAP-0429(2)-IDS

The TSF shall [*"overwrite the oldest stored IDS audit records"*] and [**no other actions to be taken in case of IDS audit storage failure**] if the IDS audit trail is full.

5.1.2 Cryptographic Support (FCS)

5.1.2.1 Extended: Baseline Cryptographic Module (FCS_BCM_(EXT))

5.1.2.1.1 Extended: Baseline Cryptographic Module (FCS_BCM_(EXT).1)

FCS_BCM_(EXT).1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a cryptomodule 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 [*as a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-2, Level 2*

5.1.2.2 Cryptographic Key Management (FCS_CKM)

5.1.2.2.1 Cryptographic Key Generation (for symmetric keys) (FCS_CKM.1(1))

FCS_CKM.1.1(1) The TSF shall generate symmetric cryptographic keys using a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and provide integrity

protection to generated symmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.

5.1.2.2.2 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1(2))

FCS_CKM.1.1(2) The TSF shall generate asymmetric cryptographic keys in accordance with the mathematical specifications of the FIPS-approved or NIST-recommended standard [**ANSI X9.62-1998**], using a domain parameter generator and
[*(1) a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and/or*

(2) a prime number generator as specified in ANSI X9.80 "Prime Number Generation, Primality Testing, and Primality Certificates" using random integers with deterministic tests, or constructive generation methods]

in a cryptographic key generation scheme that meets the following:

- The TSF shall provide integrity protection and assurance of domain parameter and public key validity to generated asymmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.
- Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 128 bits using conservative estimates.

5.1.2.2.3 Cryptographic Key Distribution (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method[

- *Manual (Physical) Method, and*
- *Automated (Electronic) Method, and*
- *No other method*]

that meets the following:

- NIST Special Publication 800-57, "Recommendation for Key Management" Section 8.1.5
- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

5.1.2.2.4 Extended: Cryptographic Key Handling and Storage (FCS_CKM_(EXT).2)

FCS_CKM_(EXT).2.1 The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).

FCS_CKM_(EXT).2.2 The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

FCS_CKM_(EXT)_2.3 The TSF shall destroy non-persistent cryptographic keys after a cryptographic administrator-defined period of time of inactivity.

FCS_CKM_(EXT).2.4 The TSF shall prevent archiving of expired (private) signature keys.

5.1.2.2.5 Cryptographic Key Destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a cryptographic key zeroization method that meets the following:

a) Key zeroization requirements of FIPS PUB 140-2, "Security Requirements for Cryptographic Modules"

b) Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete.

c) The TSF shall zeroize each intermediate storage area for plaintext key/critical cryptographic security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/critical cryptographic security parameter to another location.

d) For non-volatile memories other than EEPROM and Flash, the zeroization shall be executed by overwriting three or more times using a different alternating data pattern each time.

e) For volatile memory and non-volatile EEPROM and Flash memories, the zeroization shall be executed by a single direct overwrite consisting of a pseudo random pattern, followed by a read-verify.

5.1.2.3 Cryptographic Operation (FCS_COP)

5.1.2.3.1 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))

FCS_COP.1.1(1) The cryptomodule shall perform encryption and decryption using the FIPS-approved security function AES algorithm operating in [**CBC mode**] and cryptographic key size of [*128 bits, 192 bits, or 256 bits*].

5.1.2.3.2 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))

FCS_COP.1.1(2) The TSF shall perform cryptographic signature services using the FIPS-approved security function [

*DSA Digital Signature Algorithm (DSA) with a key size (modulus) of [**2048 bits or greater**], and*

*RSA Digital Signature Algorithm (SHA-1) with a key size (modulus) of [**2048 bits or greater],** and*

none]

that meets NIST Special Publication 800-57, "Recommendation for Key Management."

5.1.2.3.3 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))

FCS_COP.1.1(3) The TSF shall perform cryptographic hashing services using the FIPS-approved security function Secure Hash Algorithm and message digest size of [*256 bits*].

5.1.2.3.4 Cryptographic Operation (for cryptographic key agreement) (FCS_COP.1(4))

FCS_COP.1.1(4) The TSF shall perform cryptographic key agreement services using the FIPS-approved security function as specified in NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"[

[Diffie Hellman (DH group 14)] and cryptographic key sizes (modulus) of [2048 bits]].

5.1.2.3.5 Extended: Random Number Generation (FCS_COP_(EXT).1)

FCS_COP_(EXT).1.1 The TSF shall perform all random number generation (RNG) services in accordance with a FIPS-approved RNG [**FIPS 186-2 with X-change notice**] seeded by [*a combination of hardware based and software based entropy sources*].

FCS_COP_(EXT).1.2 The TSF shall defend against tampering of the random number generation (RNG)/ pseudorandom number generation (PRNG) sources.

5.1.2.4 Internet key exchange (FCS_IKE_(EXT).1)

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 one of the following, as configured by the security administrator:

- Main Mode
- Aggressive Mode

New Group mode shall include the private group 14, 2048-bit MOD P, [*no other group modes*] for the Diffie-Hellman key exchange.

Phase 2, negotiation of security services for IPsec, shall be done using Quick Mode, using SHA-1 as the pseudo-random function. Quick Mode shall generate key material that provides perfect forward secrecy.

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 minimum size for the x should be 256 bits.

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

FCS_IKE_(EXT).1.4 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

- 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)*
]

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

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

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

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

[*none*]

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

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

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

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

a) Authentication with digital signatures: The TSF shall use [*RSA, DSA,* [***and none***]]]

b) [***X.509 certificates Version 3*** [*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 [*CRL*].

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

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

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

HASH(2) = sha(SKEYID_a, M-ID | Ni_b | [**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).1.9 The TSF shall compute new keying material during Quick Mode as follows:

[*when using perfect forward secrecy*

KEYMAT = sha(SKEYID_d, g(qm)^xy | protocol | SPI | Ni_b | Nr_b),

When perfect forward secrecy is not used

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

FCS_IKE_(EXT).1.10 The TSF shall at a minimum, support the following ID types: [*ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, [ID_IPV4_ADDR_SUBNET]*].

5.1.3 Information Flow Control (FDP)

5.1.3.1 Subset information flow control (unauthenticated policy) (FDP_IFC.1(1))

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

- [source subject: the TOE interface on which information is received;
- Destination subject: TOE interface to which information is destined;
- Information: network packets; and
- Operations:
    a) pass information without modifying

].

5.1.3.2 Subset information flow control (unauthenticated TOE services policy) (FDP_IFC.1(2))

FDP_IFC.1.1(2) The TSF shall enforce the [UNAUTHENTICATED TOE SERVICES SFP] on

a) source subject: TOE interface on which information is received;

b) destination subject: the TOE;

c) information: network packets; and

d) operations: accept or reject the packet].

5.1.3.3 Simple Security attributes (unauthenticated policy) (FDP_IFF.1(1))

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

a) [Source subject security attributes:

- set of source subject identifiers; and
- [*none*].

b) Destination subject security attributes:

- Set of destination subject identifiers; and
- [*none*].

c) Information security attributes:

- presumed identity of source subject[2];
- identity of destination subject;
- source zone membership;
- destination zone membership;
- transport layer protocol;
- source subject service identifier;
- destination subject service identifier (e.g., TCP or User Datagram Protocol (UDP) destination port number);
- [packet payload [3]].];

[2] The TOE can make no claim as to the real identity of any source subject; the TOE can only suppose that such identities are accurate. Therefore, a "presumed identity" is used to identify source subjects. Note, however, that the TOE can ensure that the identity is included in the set that is associated with the interface (see FDP_IFF.1.6(1)).

- Stateful packet attributes: [*for IP-based network stacks:*
    - *Connection-oriented protocols:*
        - *sequence number;*
        - *acknowledgement number;*
        - *Flags:*
            - *SYN;*
            - *ACK;*
            - *RST;*
            - *FIN; and*
        - *[none].*
    - *Connectionless protocols:*
        - *source and destination network identifiers;*
        - *source and destination service identifiers;*
        - *[none];,*

for non-IP-based network stacks: [none)].

FDP_IFF.1.2(1) 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 presumed identity of the source subject is in the set of source subject identifiers;
- The identity of the destination subject is in the set of destination subject identifiers;
- The network packet is not blocked by any configured screens, which apply checks to specific information security attributes that identify potential attacks;
- the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy ruleset defined by the Security Administrator) according to the following algorithm
  [**If the packet has source and destination addresses in different zones, the**

[3] An IP packet payload is the data which follows the header in a transmission

Inter-zone set of rules is applied. If a match is not found the default action is performed.

If the packet has source and destination addresses in the same zone, the Intra-zone set of rules is applied. If a match was not found the default action is performed.

Evaluation of a set of rules is done by evaluating rules sequentially within the set of rules searching for the first matching rule and performing the action specified by that rule to the packet.

A rule matches if all of the information security attributes are unambiguously permitted by the rule]; and

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

FDP_IFF.1.3(1) The TSF shall enforce the [following:

- fragmentation rule
  - prior to applying the information policy ruleset, the TOE completely reassembles fragmented packets;
- stateful packet inspection rules;
  - whenever a packet is received that is not associated with an allowed established session (e.g., the SYN flag is set without the ACK flag being set), the information flow policy ruleset, as defined in FDP_IFF.1.2(1), is applied to the packet;
  - otherwise, the TSF associates a packet with an allowed established session using the stateful packet attributes].

FDP_IFF.1.4(1) The TSF shall provide the following [

- the Security Administrator shall have the capability to view all information flows allowed by the information flow policy ruleset before the ruleset is applied;
- the TSF shall provide the capability to perform policy-based address translation on the presumed IPv4 address of the source subject and port, if a policy with a NAT source policy-based translation option is in place; and
- the TSF shall provide the capability to perform policy-based address translation on the presumed IPv4 address and port of the destination subject, if a policy with a NAT destination policy-based translation option is in place].

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

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

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

5.1.3.4 Simple security attributes (unauthenticated TOE Services policy) (FDP_IFF.1(2))

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

a) [Source subject security attributes:

- set of source subject identifiers; and
- [*none*].

b) Destination subject security attributes:

- TOE's network identifier; and
- [*none*].

c) Information security attributes:

- Presumed identity of source subject;
- identity of destination subject;
- transport layer protocol;
- destination subject service identifier (e.g., TCP destination port number);
- [*packet payload*]].

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

- [the presumed identity of the source subject is in the set of source subject identifiers;
- the identity of the destination subject is the TOE;
- the information security attributes match the attributes in an information flow control policy according to the following algorithm
  [**If the packet destined for the TOE has source and destination addresses in different zones, the Inter-zone set of rules is applied. If a match is not found the default action is performed.**

  If the packet destined for the TOE has source and destination addresses in the same zone, the Intra-zone set of rules is applied. If a match was not found the default action is performed.

  Evaluation of a set of rules is done by evaluating rules sequentially within the set of rules searching for the first matching rule and performing the action specified by that rule to the packet.

  A rule matches if all of the information security attributes are unambiguously permitted by the rule].

FDP_IFF.1.3(2) The TSF shall enforce the [following rules:

- The TOE shall allow source subjects to access TOE services [*for an IP-based network stack: ICMP, [**ARP**]; or for non-IP-based network stacks: [***none***]*] without authenticating those source subjects; and
- The TOE shall allow the list of services specified immediately above to be enabled (become available to unauthenticated users) or disabled (become unavailable to unauthenticated users)].

FDP_IFF.1.4(2) The TSF shall provide the following

- [the Security Administrator shall have the capability to view all information flows allowed by this information flow control policy before the policy is applied].

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

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

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

5.1.3.5 Full residual information protection (FDP_RIP.2)

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

5.1.4 Identification and Authentication (FIA)

5.1.4.1 Authentication failure handling (FIA_AFL.1-NIAP-0425)

FIA_AFL.1.1-NIAP-0425 The TSF shall detect when a Security Administrator-configurable positive integer of unsuccessful authentication attempts occurs related to user authentication, with the Security Administrator also able to configure increasing delays after each failed attempt before the user can reattempt authentication, up to the configured maximum number of unsuccessful attempts.

FIA_AFL.1.2-NIAP-0425 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [lock the user's account for a Security Administrator configurable amount of time].

5.1.4.2 User attribute definition (Human User Identity) (FIA_ATD.1(1))

FIA_ATD.1.1(1) The TSF shall maintain the following list of security attributes belonging to an authorized user:

a) [user identifier(s):

role;

[[***authentication data***]; and

b) [**none**]].

5.1.4.3 User attribute definition (TOE to TOE identification) (FIA_ATD.1(2))

FIA_ATD.1.1(2) The TSF shall maintain the following list of security attributes belonging to authorized IT entities:

a) [subject identity;

b) authentication data;

c) [**no other security attributes**].

5.1.4.4 Timing of authentication (for TOE services) (FIA_UAU.1-FW)

FIA_UAU.1.1(1)-FW The TSF shall allow [*for an IP-based network stack: ICMP,* [[***ARP***]*; or for a non-IP-based network stack:* [***none***]] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(1)-FW The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.4.5 Specified User authentication before any action (FIA_UAU_(EXT).2-FW)

FIA_UAU_(EXT).2.1-FW The TSF shall require the administrators and authorized IT entities to be successfully authenticated before allowing any other TSF-mediated actions on behalf of these authorized users.

5.1.4.6 Authentication mechanism (FIA_UAU_(EXT).5)

FIA_UAU_(EXT).5.1 The TSF shall provide a local authentication mechanism, [*none, no other authentication mechanisms*] to perform user authentication.

5.1.4.7 User Identification Before Any Action (Human Users)(FIA_UID.2(1))

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

5.1.4.8 User-subject binding (human user-subject binding) (FIA_USB.1)

FIA_USB.1.1(1) The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [all attributes listed in FIA_ATD.1(1)].

FIA_USB.1.2(1) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [none].

FIA_USB.1.3(1) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [only the Security Administrator can change security attributes].

5.1.5 Security Management (FMT)

5.1.5.1 Management of security functions behavior (TSF non-cryptographic self-test) (FMT_MOF.1(1))

FMT_MOF.1.1(1) The TSF shall restrict the ability to modify the behavior of the functions

[TSF Self-Test (FPT_TST_(EXT).1)]

to [the Security Administrator].

5.1.5.2 Management of security functions behavior (cryptographic self-test) (FMT_MOF.1(2))

FMT_MOF.1.1(2) The TSF shall restrict the ability to enable and disable the functions [TSF Self-Test (FPT_TST.1(1) and FPT_TST.1(2)] to [the Cryptographic Administrator] immediately after key generation.

5.1.5.3 Management of security functions behavior (audit review) (FMT_MOF.1(3))

FMT_MOF.1.1(3) The TSF shall restrict the ability to enable, disable, determine and modify the behavior of the functions

[Security Audit (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)] to [an Administrator].

5.1.5.4 Management of security functions behavior (audit selection) (FMT_MOF.1(4))

FMT_MOF.1.1(4) The TSF shall restrict the ability to enable, disable, determine and modify the behavior of the functions

[Security Audit Analysis (FAU_SAA); and

Security Audit (FAU_SEL)]

to [the Security Administrator].

5.1.5.5 Management of security functions behavior (alarms) (FMT_MOF.1(5))

FMT_MOF.1.1(5) The TSF shall restrict the ability to enable, or disable the functions

[Security Alarms (FAU_ARP)]

to [the Security Administrator].

5.1.5.6 Management of security functions behavior (quota mechanism) (FMT_MOF.1(6))

FMT_MOF.1.1(6) The TSF shall restrict the ability to determine the behavior of the functions

[Controlled connection-oriented resource allocation (FRU_RSA.1);

an administrator-specified network identifier;

set of administrator-specified network identifiers;

administrator-specified period of time]

to [the Security Administrator].

5.1.5.7 Management of security functions behavior (available TOE-services for unauthenticated users) (FMT_MOF.1(6)-FW)

FMT_MOF.1.1(6)-FW The TSF shall restrict the ability to enable, disable the functions

- [***ICMP***, [and ***ARP communications***] to [the Security Administrator].

5.1.5.8 Management of security functions behavior (IDS audit review) (FMT_MOF.1(6)-IDS)

FMT_MOF.1.1(6)-IDS The TSF shall restrict the ability to enable, disable, determine and modify the behavior of the functions [IDS Audit Review (FAU_SAR.1(2), FAU_SAR.2(2) and FAU_SAR.3(2))] to [the IDS Administrator].

5.1.5.9 Management of security functions behavior (authentication attempts) (FMT_MOF.1(7))

FMT_MOF.1.1(7) The TSF shall restrict the ability to enable, disable, determine and modify the behavior of the functions

[Authentication failure handling (FIA_AFL.1.2) configurable integer of unsuccessful authentication attempts that occurs related to a user's authentication to [the Security Administrator].

5.1.5.10 Management of security functions behavior (IDS audit selection)(FMT_MOF.1(7)-IDS)

FMT_MOF.1.1(7)-IDS The TSF shall restrict the ability to enable, disable, determine and modify the behavior of the functions [IDS Audit Selection (FAU_SEL.1-NIAP-0407(2))] to [the IDS Administrator].

5.1.5.11 Management of security functions behavior (IDS intrusion alarms)(FMT_MOF.1(8)-IDS)

FMT_MOF.1.1(8)-IDS The TSF shall restrict the ability to enable and disable the functions

- [Analyzing capability Intrusion Analysis (FAU_SAA_(EXT).1); and
- [IDS Intrusion Alarms (FAU_ARP.1(2))]

to [the IDS Administrator].

5.1.5.12 Management of security attributes (FMT_MSA.1-FW)

FMT_MSA.1.1-FW The TSF shall enforce the [UNAUTHENTICATED INFORMATION FLOW SFP, UNAUTHENTICATED TOE SERVICES SFP] to restrict the ability to manipulate the security attributes [referenced in the indicated polices] to [the Security Administrator].

5.1.5.13 Secure security attributes (FMT_MSA.2)

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

5.1.5.14 Static attribute initialization (unauthenticated services) FMT_MSA.3(1)

FMT_MSA.3.1(1) 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.3.2(1) The TSF shall allow the [Security Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.15 Static attribute initialization (ruleset) (FMT_MSA.3-NIAP-0409(1)-FW)

FMT_MSA.3.1-NIAP-0409(1)-FW

The TSF shall enforce the [UNAUTHENTICATED INFORMATION FLOW SFP] to provide restrictive default values for the information flow policy ruleset that is used to enforce the SFP.

FMT_MSA.3.2-NIAP-0409(1)-FW

The TSF shall allow the [Security Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.16 Static attribute initialization (services)(FMT_MSA.3-NIAP-0409(2)-FW)

FMT_MSA.3.1-NIAP-0409(2)-FW

The TSF shall enforce the [UNAUTHENTICATED TOE SERVICES SFP] to provide restrictive default values for the set of TOE services available to unauthenticated users.

FMT_MSA.3.2-NIAP-0409(2)-FW

The TSF shall allow the [Security Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.17 Management of TSF data (non-cryptographic, non-time TSF data) (FMT_MTD.1(1))

FMT_MTD.1.1(1) The TSF shall restrict the ability to [*modify* [***none***]] all the [TSF data except cryptographic security data and the time and date used to form the time stamps in FPT_STM.1] to [the administrators or authorized IT entities].

5.1.5.18 Management of TSF data (cryptographic TSF data) (FMT_MTD.1(2))

FMT_MTD.1.1(2) The TSF shall restrict the ability to modify the [cryptographic security data] to [the Cryptographic Administrator].

5.1.5.19 Management of TSF data (time TSF data) (FMT_MTD.1(3))

FMT_MTD.1.1(3) The TSF shall restrict the ability to [set] the [time and date used to form the time stamps in FPT_STM.1] to [the Security Administrator or authorized IT entity].

5.1.5.20 Management of TSF data (information flow policy ruleset) (FMT_MTD.1(4))

FMT_MTD.1.1(4) The TSF shall restrict the ability to query, modify, delete, create, [***none***] the [information flow policy rules] to [the Security Administrator].

5.1.5.21 Management of limits on TSF data (transport-layer quotas) (FMT_MTD.2(1))

FMT_MTD.2.1(1) The TSF shall restrict the specification of the limits for [quotas on transport-layer connections] to [the Security Administrator].

FMT_MTD.2.2(1) The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [**drops the packets and logs the event**].

5.1.5.22 Management of limits on TSF data (controlled connection-oriented quotas) (FMT_MTD.2(2))

FMT_MTD.2.1(2) The TSF shall restrict the specification of the limits for [quotas on controlled connection-oriented resources] to [the Security Administrator].

FMT_MTD.2.2(2) The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [**logs the connection attempt and then allows or denies the connection based upon the configuration specified by the Security Administrator**].

5.1.5.23 Management of limits on TSF data (percentage of storage capacity) (FMT_MTD.2(3))

FMT_MTD.2.1(3) The TSF shall restrict the specification of the limits for [percentage of storage capacity for audit records] to [the Security Administrator].

FMT_MTD.2.2(3) The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: ['**overwrite the oldest stored audit records**'].

5.1.5.24 Revocation (FMT_REV.1)

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the [users, [**no other additional resources**]] within the TSC to [Security Administrator].

FMT_REV.1.2 The TSF shall enforce the rules
[**The revocation of security-relevant authorizations by removing or modifying user security attributes (e.g., user name), which is effective from the next time the user attempts authentication.**

5.1.5.25 Revocation (FMT_REV.1-FW)

FMT_REV.1.1-FW The TSF shall restrict the ability to revoke security attributes associated with the [information flow policy ruleset, services available to unauthenticated users] within the TSC to [the Security Administrator].

FMT_REV.1.2-FW The TSF shall immediately enforce the:

- changes to the information flow policy ruleset when applied;
- disabling of a service available to unauthenticated users; and
- [*none*].

5.1.5.26 Specification of management functions (FMT_SMF.1)

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

1. invoke determine and modify the behavior of the functions TSF Self-Test (FPT_TST_(EXT).1);
2. enable, disable the functions TSF Self-Test (FPT_TST.1(1) and FPT_TST.1(2));
3. enable, disable, determine and modify the behavior of the functions Security Audit (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3);
4. enable, disable, determine and modify the behavior of the functions Security Audit Analysis (FAU_SAA); and Security Audit (FAU_SEL;
5. enable, or disable the functions Security Alarms (FAU_ARP) ;
6. enforce administrator-specified maximum quotas of the following resources: [controlled connection-oriented resources] that users associated with [an administrator-specified network identifier and a set of administrator-specified network identifiers] can use over an administrator-specified period of time.
7. enforce the [UNAUTHENTICATED INFORMATION FLOW SFP] to provide restrictive default values security attributes that are used to enforce the SFP;
8. enforce the [UNAUTHENTICATED TOE SERVICES SFP] to provide restrictive default values security attributes that are used to enforce the SFP;
9. modify the cryptographic security data;
10. set the time and date used to form the time stamps in FPT_STM.1.
11. query, modify, delete, create the information flow policy rules.

12. revoke security attributes associated with the user (FMT_REV.1)
13. specify the limits for quotas on transport-layer connections (FMT_MTD.2 (1));
14. specify the limits for quotas on controlled connection-oriented resources (FMT_MTD.2 (2));
15. specify the limits for percentage of storage capacity for audit records (FMT_MTD.2(3)).
16. enable, disable, determine and modify the behavior of the functions of Authentication failure handling (FIA_AFL.1.2) to configure an integer of unsuccessful authentication attempts that occurs related to a user's authentication.
17. Manage IDS intrusion alarms
18. Manage IDS audit selection
19. Manage IDS audit review.

5.1.5.27 Restrictions on security roles (FMT_SMR.2)

FMT_SMR.2.1 The TSF shall maintain the roles: [

- Security administrator role,
- Audit administrator role,
- Crypto administrator role,
- IDS Administrator].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- [All roles shall be able to administer the TOE locally;
- all roles shall be able to administer the TOE remotely;
- all roles are distinct; that is, there shall be no overlap of operations performed by each role, with the following exceptions:
    - all administrators can review the audit trail; and
    - all administrators can invoke the self-tests] are satisfied.

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [system panic, power failure].

5.1.6.2 Standard Protocol Usage (FPT_PRO_(EXT).1)

FPT_PRO_(EXT).1 The TSF shall utilize the standard protocol mechanisms within the standard protocols

[***a) BGP***

b) none].

5.1.6.3 Automated Recovery (FPT_RCV.2)

FPT_RCV.2.1 When automated recovery from [**a failure or service discontinuity**] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.2.2 For [**power failures**], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

5.1.6.4 Replay detection (FPT_RPL.1)

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [routing information, administrator sessions].

FPT_RPL.1.2 The TSF shall perform

[reject data;

audit event; and

[***no other actions***]

when replay is detected.

5.1.6.5 Reliable time stamps (FPT_STM.1)

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

5.1.6.6 Inter-TSF basic TSF data consistency (FPT_TDC.1)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [**BGP Open, Update, Notification, and Keepalive messages**] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [**RFC 4271**] when interpreting the TSF data from another trusted IT product.

5.1.6.7 Extended: TSF Testing (FPT_TST_EXP.1)

FPT_TST_EXP.1.1 The TSF shall run a suite of self tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.

FPT_TST_EXP.1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.

5.1.6.8 TSF Testing (for cryptography) (FPT_TST.1(1))

FPT_TST.1.1(1) The TSF shall run a suite of self tests in accordance with FIPS PUB 140-2 and Appendix C of this profile during initial start-up (on power on), at the request of the cryptographic administrator (on demand), under various conditions defined in section 4.9.1 of FIPS 140-2, and periodically (at least once a day) to demonstrate the correct operation of the following cryptographic functions:

a) key error detection;

b) cryptographic algorithms;

c) RNG/PRNG

FPT_TST.1.2(1) The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of TSF data related to the cryptography by using TSF-provided cryptographic functions.

FPT_TST.1.3(1) The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of stored TSF executable code related to the cryptography by using TSF-provided cryptographic functions.

5.1.6.9 TSF Testing (for key generation components) (FPT_TST.1(2))

FPT_TST.1.1(2) The TSF shall perform self tests immediately after generation of a key to demonstrate the correct operation of each key generation component. If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140-2 for failing a self-test, and this event will be audited.

FPT_TST.1.2(2) The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of TSF data related to the key generation by using TSF-provided cryptographic functions.

FPT_TST.1.3(2) The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of stored TSF executable code related to the key generation by using TSF-provided cryptographic functions.

5.1.7 Resource Utilization (FRU)

5.1.7.1 Maximum quotas (controlled connection-oriented quotas) (FRU_RSA.1)

FRU_RSA.1.1 The TSF shall enforce administrator-specified maximum quotas of the following resources: [controlled connection-oriented resources] that users associated with [an administrator-specified network identifier and a set of administrator-specified network identifiers] can use over an administrator-specified period of time.

5.1.8 TOE Access (FTA)

5.1.8.1 TSF-initiated session locking (FTA_SSL.1-FW/IDS)

FTA_SSL.1.1-FW/IDS The TSF shall lock a local interactive session after [a Security Administrator-specified time period of inactivity] by:

- disabling any activity of the user other than unlocking the session.

FTA_SSL.1.2-FW/IDS The TSF shall require the user to re-authenticate prior to unlocking the session.

5.1.8.2 User-initiated locking (FTA_SSL.2-FW/IDS)

FTA_SSL.2.1-FW/IDS The TSF shall allow user-initiated locking of the user's own local interactive session by

- disabling any activity of the user other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the user to re-authenticate prior to unlocking the session.

5.1.8.3 TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3(1) The TSF shall terminate an interactive session after a [**Security Administrator-configurable time interval of user inactivity**].

FTA_SSL.3(2) The TSF shall terminate **a** remote session after a [Security Administrator-configurable time interval of session inactivity].

5.1.8.4 Default TOE access banners (FTA_TAB.1)

FTA_TAB.1.1 Before establishing a user session that requires authentication, the TSF shall display only a Security Administrator specified advisory notice and consent warning message regarding unauthorized use of the TOE.

5.1.8.5 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny establishment of an authorized user session based on [location, time, and day].

5.1.9 Trusted Path/Channels (FTP)

5.1.9.1 Inter-TSF trusted channel (prevention of disclosure) (FTP_ITC.1(1))

FTP_ITC.1.1(1) The TSF shall use IPsec to provide a trusted communication channel between itself and remote trusted authorized IT product entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure.

FTP_ITC.1.2(1) The TSF shall permit the TSF, or the remote trusted authorized IT product entities to initiate communication via the trusted channel.

FTP_ITC.1.3(1) The TSF shall initiate communication via the trusted channel for [ntp, routing table updates, export of audit records].

5.1.9.2 Inter-TSF trusted channel (detection of modification) (FTP_ITC.1(2))

FTP_ITC.1.1(2) The TSF shall use IPsec to provide a trusted communication channel between itself and authorized IT product entities that is logically distinct from other communication channels and provides assured identification of its end points and detection of the modification of data.

FTP_ITC.1.2(2) The TSF shall permit the TSF, or the remote trusted authorized IT product entities to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The TSF shall initiate communication via the trusted channel for [ntp, routing table updates, export of audit records].

5.1.9.3 Trusted path (prevention of disclosure) (FTP_TRP.1(1))

FTP_TRP.1.1(1) The TSF shall use secure shell (SSH) to provide a secure communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure.

FTP_TRP.1.2(1) The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3(1) The TSF shall require the use of the trusted path for initial user authentication and all remote administration actions.

5.1.9.4 Trusted path (detection of modification) (FTP_TRP.1(2))

FTP_TRP.1.1(2) The TSF shall use secure shell (SSH) to provide a communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and detection of the modification of data.

FTP_TRP.1.2(2) The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3(2) The TSF shall require the use of the trusted path for initial user authentication, all remote administration actions.

5.2 Security Assurance Requirements

This section defines the assurance requirements for the TOE, which are summarized in the Table below.

The TOE assurance requirements for this Security Target map to Common Criteria EAL4 augmented with ALC_FLR.2.

ASSURANCE CLASS	COMPONENTS	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architectural Description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.4	Product support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.2	**Flaw Reporting Procedures**
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ATE: Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.3	Focused Vulnerability Analysis

Table 9 – Security Assurance Requirements

5.2.1 Class ADV: Development

5.2.1.1 ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

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

5.2.1.2 ADV_FSP.4 Complete semi-formal functional specification with additional error information

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall **describe all** actions associated with each TSFI.

ADV_FSP.4.5C **The functional specification shall describe all direct error messages that may result from an invocation of each TSFI**.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.4.1E The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

5.2.1.3 ADV_IMP.1 Implementation representation of the TSF

Dependencies:
ADV_TDS.3 Basic modular design
ALC_TAT.1 Well-defined development tools

Developer action elements:

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements:

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

5.2.1.4 ADV_TDS.3 Basic modular design

Dependencies:
ADV_FSP.4 Complete functional specification

Developer action elements:

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

Evaluator action elements:

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

ADV_TDS.3.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Class AGD: Guidance documents

5.2.2.1 AGD_OPE.1 Operational user guidance

Dependencies:

ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

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

5.2.2.2 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Class ALC: Life-cycle support

5.2.3.1 ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies:

ALC_CMS.1	TOE CM coverage
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_CMC.4.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.4.2D	The developer shall provide the CM documentation.
ALC_CMC.4.3D	The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.4.1C	The TOE shall be labeled with its unique reference.
ALC_CMC.4.2C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.4.3C	The CM system shall uniquely identify all configuration items.
ALC_CMC.4.4C	The CM system shall provide automated measures such that only authorized changes are made to the configuration items.
ALC_CMC.4.5C	The CM system shall support the production of the TOE by automated means.
ALC_CMC.4.6C	The CM documentation shall include a CM plan.
ALC_CMC.4.7C	The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.4.8C	The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ALC_CMC.4.9C	The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C	The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 ALC_CMS.4 Problem tracking CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

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

5.2.3.4 ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

5.2.3.5 ALC_FLR.2 Flaw reporting procedures

Dependencies: No dependencies.

Developer action elements:

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users' reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

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

5.2.3.6 ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

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

5.2.3.7 ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall identify each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of each development tool.

Content and presentation elements:

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

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

5.2.4 Class ATE: Tests

5.2.4.1 ATE_COV.2 Analysis of coverage

Dependencies:

ADV_FSP.2	Security-enforcing functional specification
ATE_FUN.1	Functional testing

Developer action elements:

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

Content and presentation elements:

ATE_COV.2.1C	The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.2.2C	The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

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

5.2.4.2 ATE_DPT.1 Testing: modular design

Dependencies:

ADV_ARC.1	Security architecture description
ADV_TDS.2	Architectural design
ATE_FUN.1	Functional testing

Developer action elements:

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

Content and presentation elements:

ATE_DPT.1.1C	The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.
ATE_DPT.1.2C	The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

Evaluator action elements:

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

5.2.4.3 ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

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

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

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

5.2.4.4 ATE_IND.2 Independent testing - sample

Dependencies:

ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.4.5 AVA_VAN.3 Focused vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.4 Complete functional specification

ADV_TDS.3 Basic modular design

ADV_IMP.1 Implementation representation of the TSF

AGD_OPE.1 Operational user guidance

ATE_DPT.1 Testing: Basic Design

6 TOE Summary Specification

This section provides summary information on how the security requirements are met. The objective is to give a high-level view of how the developer satisfies the security requirements; therefore, the descriptions are not overly detailed.

6.1 Security Audit

The TOE creates and stores audit records for a large set of security-relevant events (see the table in Section 8 below). It supports both system audit records relevant to local events, and IDS audit records.

Auditing (both for local audit and IDS purposes) is done using a process" [or daemon] "called eventd". Eventd generates an in-memory audit log of audit information and makes it available to administrators. No mechanism for resident or remote storage of audit records is provided by the TSF.

syslog can be configured to collect and store audit records locally on the SRX650 platform. The LN1000-v does not provide permanent local storage for non-operational system data. The use of syslog is outside the scope of this evaluation.

Junos will record within each audit record the following information:

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

b) Identity of the user that caused the event.

The TOE audits all of the required events specified in Section 8 of this Security Target, and each audit record captures all of the required information as shown in column 3 of the table in Section 8.

Junos provides authorized administrators with the ability to view audit data from the Command Line Interface (CLI) – the CLI is available via the console and remote administrative sessions. While any administrator can view audit data, only the IDS administrator can view IDS data collected and processed by the TOE. Commands are available to list entire files, or to select records that match or do not match a pattern. Administrators can search and sort the audit data based on:

- user identity;
- source subject identity;
- destination subject identity;
- ranges of one or more: dates, times, user identities, subject service identifiers, or transport layer protocol;
- rule identity; and
- network interfaces.

A Security Administrator can include or exclude events from the set of auditable events based on:

- user identity;
- event type;
- success of auditable security events;
- failure of auditable security events;
- policy name; [4]
- subject service identifier;
- and network interfaces.

IDS Administrators can view IDS audit data from the Command Line Interface (CLI) using the **'show security log idp'** command with arguments as follows:

```
show {
    security {
        log idp {
            active-policy <rule identity>
            alarms <alarm-type idp>
            idp-policy <rule identity>
            destination-address <destination-ip-address>
            destination-port <destination-port>
            detail
            event-id <ERRMSG event tag>

            interface <interface-name>
            older-than <show events older than this timestamp>
            process <process that generated event>
            protocol <tcp/udp>
            newer-than <show events newer than this timestamp>
            severity <severity of event>
            sort-by [ active-policy alarm-type idp-policy traceoptions ]
                                [ascending | descending]
            source-address <source-ip-address>
            source-port <source-port>
            traceoptions <flag options>
            username <username>
        }
    }
}
```

[4] The 'policy name' attribute identifies an IDS policy configured by the Security Administrator

An IDS Administrator can include or exclude events from the set of auditable IDS events based on the event type.

Eventd maintains its log data in a circular, in-memory buffer. When the buffer becomes full, the oldest contents of the buffer (i.e., the 1st record) is over-written. By default the buffer is capable of holding 10,000 records. The buffer limit can be configured by the Audit Administrator to hold any number of records. Eventd notifies administrators, by displaying an alarm, when a configurable percentage of the 10,000 records (or user-defined limit) have been generated.

Junos provides for an alarm mechanism that immediately displays potential security violations and potential intrusions at the CLI user prompt, which is available via remote administrative sessions, and at the local console. The security alarms are persistent in the user interface until acknowledged by the Security Administrator. The Security Administrator can also configure the TOE to generate an optional audible alarm, the audible alarm will sound until acknowledged by an administrator (at which time that alarm will be reset). The analytical result (i.e., the complete IDS record) associated with the IDS auditable event(s) that generated the alarm is made available through the audit viewing mechanism described above.

The alarm mechanism is invoked according to a set of rules that include an accumulation of the following:

- Security Administrator specified number of user authentication failures;
- Any detected replay of TSF data or security attributes;
- Any failure of the cryptographic self-tests;
- Any failure of the other TSF self-tests;
- Cryptographic Administrator specified number of encryption failures;
- Cryptographic Administrator specified number of decryption failures;
- Security Administrator specified number of Information Flow policy violations by an individual presumed source network identifier (e.g., IP address) within an administrator specified time period;
- Security Administrator specified number of Information Flow policy violations to an individual destination network identifier within an administrator specified time period;
- Security Administrator specified number of Information Flow policy violations to an individual destination subject service identifier (e.g., TCP port) within an administrator specified time period;
- Security Administrator specified Information Flow policy rule, or group of rule violations within an administrator specified time period

When an alarm is acknowledged, the TOE generates an acknowledgement message identifying a reference to the potential security violation or potential intrusion, a notice that it has been acknowledged, the time of the acknowledgement and the user identifier that acknowledged the alarm. The TSF provides the capability to view alarm acknowledgements at the local console and remote administrator sessions that received the alarm. If a Security Administrator establishes a new session after an alarm has occurred, but before it has been acknowledged, it will be displayed upon session establishment.

Only the Audit Administrator can delete audit records, which are protected from unauthorized modification. Similarly, only the IDS Administrator can delete stored IDS audit records, which are also protected from unauthorized modification.

The Junos software overwrites the oldest stored audit records in the event the space available for audit storage is exhausted. An alarm is generated when the size of the audit trail exceeds a percentage capacity configurable by the Security Administrator. There is no option to prevent auitable events, as this may expose the TOE to a denial-of-service attack. Similarly, the oldest stored IDS events are overwritten in the event the space available for storing IDS events is exhausted.

In support of IDS, the TOE collects events associated with start-up and shutdown of the IDS functions, identification and authentication events, service requests, and network traffic. The IDS Administrator can search the IDS audit data by date and time, type of event, and success or failure of the related event. In each case, the TOE records all pertinent information required by the IDS system for further analysis.

The TOE implements two separate IDS detection mechanisms;

- Potential violation analysis (FAU_SAA.1-NIAP-0407)
    - The TOE generates alarms on the collection and accumulation of specified events on the TOE (e.g., failed authentication attempts, replay attacks)
    - The TOE records results in IDS audit records (FAU_GEN_(EXT).1-IDS)
- Analyzing capability intrusion analysis (FAU_SAA_(EXT).1-IDS)
    - The TOE uses the following signature analysis techniques to identify intrusion attempts in network traffic
        - Application of screens to network traffic
        - Application of IDS policies to network traffic that passes through screens and firewall rules
    - The TOE records results in IDS audit records (FAU_GEN_(EXT).1-IDS)

The TOE uses a signature database to perform an analysis of IDS audit data against known intrusions or misuses of the system. The TOE includes a predefined attack object database that is periodically updated by Juniper Networks. Attack objects are specified in rules used to identify malicious activity. Whenever the TOE encounters a known pattern of attack in the monitored network traffic, the attack object is matched.

The TOE makes use of two attack objects described in the following table:

Table 10 - IDP Attack Objects Description

Attack Objects	Description
Signature Attack Objects	Signature attack objects detect known attacks using stateful attack signatures. An attack signature is a pattern that always exists within an attack; if the attack is present, so is the attack signature. With stateful signatures, IDP can look for the specific protocol or service used to perpetrate the attack, the direction and flow of the attack, and the context in which the attack occurs. Stateful signatures produce few false positives because the context of the attack is defined, eliminating huge sections of network traffic in which the attack would not occur.
Protocol Anomaly Attack Objects	Protocol anomaly attack objects identify unusual activity on the network. They detect abnormal or ambiguous messages within a connection according to the set of rules for the particular protocol being used. Protocol anomaly detection works by finding deviations from protocol standards, most often defined by RFCs and common RFC extensions. Most legitimate traffic adheres to established protocols. Traffic that does not, produces an anomaly, which may be created by attackers for specific purposes, such as evading an intrusion prevention system (IPS).

The Audit function is designed to satisfy the following security functional requirements:

- FAU_ARP.1(1)
- FAU_ARP.1(2)-IDS
- FAU_ARP_ACK_(EXT).1
- FAU_ARP_ACK_ (EXT).2-IDS
- FAU_GEN.1-NIAP-0429
- FAU_GEN_(EXT).1-IDS
- FAU_GEN.2-NIAP-0410
- FAU_SAA.1-NIAP-0407
- FAU_SAA_(EXT).1-IDS
- FAU_SAR.1(1)
- FAU_SAR.1(2)-IDS
- FAU_SAR.2(1)
- FAU_SAR.2(2)-IDS
- FAU_SAR.3(1)
- FAU_SAR.3(2)-IDS
- FAU_SEL.1-NIAP-0407(1)
- FAU_SEL.1-NIAP-0407(2)-IDS
- FAU_STG.1-NIAP-0429
- FAU_STG.2-NIAP-0429-IDS
- FAU_STG.3
- FAU_STG.NIAP-0414-1-NIAP-0429(1)
- FAU_STG.NIAP-0414-1-NIAP-0429(2)-IDS

6.2 Cryptographic Support

All FIPS-approved cryptographic functions implemented by the secure routers are implemented in the Junos-FIPS cryptomodule. The cryptomodule is the entire appliance and is FIPS 140-2 validated at Level 2 (certificate #1704 for the SRX650 and #1718 for the LN1000). The FIPS 140-2 validation includes an algorithm validation certificate for each FIPS-approved cryptographic function implemented by the TOE.

The FIPS-approved cryptomodule implements ECDSA using a base point of 256-bits or greater (as specified by the cryptographic administrator) for digital signature generation and verification. The FIPS-approved ECDSA algorithm is defined by ANSI X9.62-1998.

The TSF supports the manual and electronic distribution of cryptographic keys. Support for distribution of symmetric keys is in accordance with FIPS PUB 171 (Key Management Using ANSI X9.17). In the TOE private asymmetric keys are only distributed using manual distribution methods.

Support for manual and automatic distribution of public asymmetric key material also uses an X.509 certificate scheme that is compatible with usage specified in the 'PKI Roadmap for the DoD', and 'DoD X.509 Certificate Policy' The TOE is implemented as a combination of software and hardware.

The cryptomodule generates symmetric keys in the context of a Diffie-Hellman key agreement exchange. The TOE uses Diffie-Hellman key agreement for auto-key IKE. Auto-key IKE VPNs draw upon the RNG during this key agreement process.

The cryptomodule employs a FIPS 140-2 approved software RNG that complies with NIST SP 800-57 Section 6.1. The TSF also uses a mixing function that meets FIPS PUB 180-2. All cryptographic random numbers are drawn from this RNG. The TSF protects itself and the entropy sources used for generation of random numbers from tampering using by not providing a general purpose programming interface to users and through the mechanisms described in Section 6.6.

The TOE allows VPN connections to be configured in one of three ways:

1. Manual keys
2. Auto-key IKE with pre-shared keys for authentication
3. Auto-key IKE with certificates for authentication

The TSF generates 2048-bit DH keys and 256-bit ECDSA keys, which are equivalent or greater in strength to 112 bit symmetric keys. Prime numbers are generated using a method that complies with ANSI X9.80 and X9.42. The FIPS-approved ECDSA algorithm is defined by ANSI X9.62-1998. Support for distribution of symmetric keys is in accordance with NIST SP 800-57.

The TSF performs key input and output in accordance with FIPS 140-2, Level 2. Keys are associated with the correct entity through means such as a Security Parameters Index (SPI), a fully quality domain name (FQDN) or a connection index. A parity check is performed whenever a key is internally transferred. All keys are

encrypted when not in use. Administrators can define a period of inactivity, after which the TOE will destroy non-persistent cryptographic keys. When no longer needed, memory space used by a key is overwritten using a variable bit pattern. The TOE does not provide a mechanism to archive expired private signature keys.

The TSF supports a zeroization command line option that destroys all keying material, overwriting it three times with pseudo random bit pattern, followed by a read-verify. In addition, this command resets the device to the factory default configuration. Further, freed key storage memory is always zeroized whenever the key is moved, copied or deleted. The cryptomodule supports a FIPS-approved implementation of AES-CBC, using 128, 192 and 256 bit keys.

The TOE supports the following digital signature algorithms:

- DSA with a key size of 2048 bits
- RSA with a key size of 2048 bits, and
- ECDSA with a key size of 256 bits using the NIST curve, P-256.

The TOE supports cryptographic hashing via the SHA-256 algorithm.

The TOE supports a variation of the Diffie-Hellman protocol using Elliptic Curve-based cryptography – this supports SSHv2. The TOE uses Elliptic Curve Diffie-Hellman (ECDH) as a key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. ECDH provide a key agreement algorithm and cryptographic key sizes (modulus) of 256 bits, using the NIST P-256 curve as defined in FIPS PUB 186-3, that meet NIST SP 800-56A.

The TOE computes the value of SKEYID (as defined in RFC 2409), using SHA-1 as the pseudo-random function. The TOE authenticates using the methods for

- Signatures: SKEYID = sha(Ni_b | Nr_b, g^xy)
- Pre-shared keys: SKEYID = sha(pre-shared-key, Ni_b | Nr_b)
- Authentication using Public key encryption, computing SKEYID as follows:

  SKEYID = sha(sha(Ni_b | Nr_b), CKY-I | CKY-R)

The TOE computes 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); and
- SKEYID_e = sha(SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2).

To authenticate the Phase 1 exchange, The TOE generates HASH-I if it is the initiator and HASH-R if it is the responder, according to RFC 2409.

The TOE authenticates IKE Phase 1 using authentication with digital signatures or with a pre-shared key as defined by the SFR in this security target. For digital signatures, the TOE can apply an RSA signature to HASH-I or HASH-R if the signature is PKCS#1 encoded. The TOE can also use X.509 Version 3 certificates . CRL is used to handle revocation of certificates.

The TOE computes hashes in the following way

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

HASH(2) = sha(SKEYID_a, M-ID | Ni_b | [any ISAKMP payload after HASH(2) header contained in the message)]

HASH(3) = sha(SKEYID_a, 0 | M-ID | Ni_b | Nr_b)

The TOE computes keying material during quick mode using perfect forward secrecy. The TOE supports the following ID types: ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, and ID_IPV4_ADDR_SUBNET. The TOE provides cryptographic key establishment techniques in accordance with RFC 2409 as follows(s):

- Phase 1, the establishment of a secure authenticated channel between the TOE and another remote VPN endpoint, is performed using one of the following, as configured by the security administrator:

o Main Mode

o Aggressive Mode

New Group mode shall include the private group 14, 2048-bit MOD P for the Diffie-Hellman key exchange.

- Phase 2, negotiation of security services for IPsec, is done using Quick Mode, using SHA-1 as the pseudo-random function. Quick Mode generates key material that provides perfect forward secrecy. The TOE requires the nonce, and the x of g^xy be randomly generated using FIPS-approved random number generator when computation is being performed.

o The recommended nonce sizes are to be between 8 and 256 bytes;

o The minimum size for the x should be 256 bits.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_BCM_(EXT).1
- FCS_CKM.1(1)
- FCS_CKM.1(2)
- FCS_CKM.2
- FCS_CKM_(EXT).2
- FCS_CKM.4:
- FCS_COP.1(1)

- FCS_COP.1(2)
- FCS_COP.1(3):
- FCS_COP.1(4):
- FCS_COP_(EXT).1
- FCS_IKE_(EXT).1

6.3 Information Flow Control

The TOE is designed to route unauthenticated network traffic. Network traffic represents information flows between source and destination network entities. The specific routing of traffic is based on the routing configuration data that has been created by the TOE users or has been collected from network peers as defined by the TOE users. The routing decision is based on the destination address of the packet.

The TOE supports two information flow control policies: the UNAUTHENTICATED INFORMATION FLOW SFP, and the UNAUTHENTICATED TOE SERVICES SFP. Each SFP is configured via security policies. The Junos security policies enforce rules for the network traffic, in terms of what traffic can enter and pass through the TOE , and the actions that need to take place on the traffic as it passes through the TOE. From the perspective of security policies, the traffic enters one security zone and exits another security zone. This combination of a from-zone and to-zone is called a context. Each context contains an ordered list of policies. A security policy, which can be configured from the user interface, controls the traffic flow from one zone to another zone by defining the kind(s) of traffic permitted from specified IP sources to specified IP destinations. Policies can deny, permit, encrypt, decrypt, and authenticate the traffic attempting to cross from one security zone to another.

Interfaces with identical security requirements can be grouped together into a single security zone. Security zones are the building blocks for policies; they are logical entities to which one or more interfaces are bound. Security zones provide a means of distinguishing groups of hosts (user systems and other hosts, such as servers) and their resources from one another in order to apply different security measures to them. Security zones have the following properties:

- Policies, which are active security policies that enforce rules for the transit of traffic through the TOE. This includes
    - Interzone – routes traffic from one zone to another zone
    - Intrazone – routes traffic within one zone
- Screens, which can detect and block various kinds of traffic determined to be potentially harmful.

The Security Administrator configures screens to determine which attack events will trigger an alert and dropped packet. In the evaluated configuration, all screens are enabled. Following is a list of all the attacks that can be detected by screens and the packet information which will trigger them.

Table 11 - IP Packet Screen Configurable Options

Attack	Trigger
SYN Flood	When SYN Flood protection is enabled, the appliance will SYN-ACK each packet. If after certain time, there are no future packets received from the source, a SYN-flood will be detected. The appliance will remove the session from the session table and a TCP Reset will be sent to the source.
ICMP Flood	1000 ICMP echo requests in one second. The type is determined by the header of the packet.
UDP Flood	1000 UDP echo requests to the same destination in one second. The type is determined by the header of the packet.
Ping Of Death	Length of Offset plus the IP length is greater than 64K.
IP Spoofing	IP address is received on the untrust interface that belongs to the network being protected by the trust interface.
Port Scan	TCP SYN to 10 different ports with the same destination address in .3 seconds.
LAND Attack	A SYN attack is detected along with the source and destination IPs being the same.
TCP - Syn frag	A SYN packet contained in fragment packet
Tear Drop Attack	The sum of the offset and size of one fragmented packet differ from that of the next fragmented packet.
Filter IP Source Route Option	The header source and the source in the routing information are different.
Address Sweep Attack	ICMP echo request to 10 different addresses with the same destination address in .3 seconds.
Winnuke	Traffic sent to port 139.
IP options-Bad Option List	IP options do not conform to the RFC.
IP options-Record Packet Route	Option 7 is included in the IP header.
IP options-Timestamp	Option 4 is included in the IP header.
IP options-Provide security	Option 2 is included in the IP header.
IP options-Loose Source Route	Option 3 included in the IP header.
IP options-SAFNET ID	Option 8 included in the IP header.
IP options-Strict Source Route	Option 9 is included in the IP header.

Attack	Trigger
Deny Fragment Attack	All fragments are dropped. This is done by determining that the more fragments flag is set to 1 or an offset is indicated in offset field.
Unknown IP Protocol	Protocol field in IP header set to 101 or greater.
Fragmented ICMP Traffic	Protocol filed in IP header set to 1 and either the more fragments flag set to 1 or there is an offset indicated in the offset field.
Large ICMP Traffic	IP header set to 1 and IP length is greater than 1024.
TCP - no bits set in flags	No bits set in the flags field.
TCP - FIN and SYN	A TCP packet contains both FIN and SYN in flag field
TCP - FIN bit with no ACK bit in flags	Receive packet with FIN bit set and no ACK bit set.

All configured screens are applied prior to all configured policies. Only after a packet has passed through the configured screens is it eligible to be considered to match a policy rule.

Each security zone contains an address book that contains the IP address or domain names of hosts and subnets whose traffic is either allowed, blocked, encrypted, or user-authenticated. Before policies can be set between two zones, the addresses must be defined for each of the zone's address books. The address book of a security zone must contain all IP addresses that are reachable within that zone. Policies contain both source and destination zones and addresses. An address is referred to in a policy by the name you give it in its zone's address book.

- When traffic is sent to a zone, the zone and address to which the traffic is sent are used as the destination zone and address-matching criteria in policies.
- When traffic is sent from a zone, the zone and address from which it is sent are used as the matching source zone and address in policies.

To secure all connection attempts, the TOE uses a dynamic packet filtering method known as stateful inspection. Using this method, the TOE notes various components in a TCP packet header. State information recognized by the device includes: source and destination IP addresses, source and destination port numbers, packet sequence numbers, and packet length. The TOE maintains the state of each TCP session traversing the firewall. This means that the TOE keeps track of packet length and packet attributes such that each packet must be complete and correct for information to flow from source to destination. The stateful packet attributes maintained by the TOE for connection-oriented protocols (e.g., TCP) include sequence number, acknowledgement number, and flags (i.e., SYN, ACK, RST, and FIN). For connectionless protocols, the TOE maintains as stateful packet attributes the source and destination network identifiers as well as the source and destination service identifiers.

The TOE supports Network Address Translation (NAT) to control traffic flow. When a policy configuration includes Network Address Translation (NAT) in its match criteria, the TOE translates two components in the header of an outgoing IP packet destined for the external zone: its source IP address and source port number. The router replaces the source IP address of the originating host with the IP address of the external zone interface. When the reply packet arrives at the router, the router translates two components in the IP header of the incoming packet (the destination address and port number), which are translated back to the original numbers. The router then forwards the packet to its destination. NAT may be implemented in conjunction with the UNAUTHENTICATED INFORMATION FLOW SFP.

The TOE may also be configured to block or reassemble fragmented packets. When the first packet fragment arrives, it is sent to the fragmentation policy check. If it is denied, it will be dropped. If allowed, since it is not fully reassembled, the TOE places it into a fragment queue and sets a timeout. If all of the fragments arrive before the timeout, the TOE reassembles the packet and assures correct reassembly against a sequence of markers. If the assembly has been successful the packet is directed into the packet flow, where it is routed through information flow rules and policy checks to determine if it can pass through the TOE. Otherwise it is dropped from the queue and an error is reported.

The UNAUTHENTICATED TOE SERVICES SFP applies to traffic directed at the TOE (also referred to as “management traffic”). Management traffic is addressed to a TOE interface (i.e.. packets have the TOE’s interface IP address as the destination IP address), so when the TOE receives management traffic, it doesn't forward the traffic to another destination, but instead passes it to the appropriate system daemon for processing. Traffic that is destined for the TOE is handled this way:

1. The packet is delivered to the destination TOE interface.
2. If no services have been configured on that interface, the packet is dropped. (e.g., ICMP, SSH)”
3. If services have been configured, the type of traffic arriving on that interface compared against the services enabled. If they do not match, the packet is dropped.
4. If a traffic type match is found for the TOE interface, the packet is routed through information flow rules and policy checks to determine if it can be processed by the TOE.
5. If the packet passes the information flow rules and policy checks, it is delivered to the appropriate management daemon. Otherwise, it is dropped.

Unauthenticated ICMP echo and ARP communications directed at the TOE are received and acknowledged per the configuration defined by the security administrator.

A feature of both the UNAUTHENTICATED INFORMATION FLOW SFP and the UNAUTHENTICATED TOE SERVICES SFP is that the Security Administrator can display the current information flow rule set configuration using a CLI command, then configure a single new policy on the command line, which they can view in context of the whole configuration before entering the command for the new policy.

When enforcing both the UNAUTHENTICATED INFORMATION FLOW SFP and the UNAUTHENTICATED TOE SERVICES SFP, the TOE rejects requests for access or services where the presumed source identity of the information received by the TOE is not included in the set of source identifiers for the source subject, is a broadcast address, or is a loopback identifier. The TOE also rejects requests in which the information received by the TOE specifies the route (set of host network identifiers) for information flowing from the

source subject to the destination. These explicit information flow denial rules are provided by the IP Spoofing and Filter IP Source Route Option screens.

There are only two resources made available to information flowing through a TOE. One is the temporary storage of packet information when access is requested and when information is being routed. The second type of information is key material. All temporary storage is accounted for in that the size of a temporary storage relative to every packet is known. Therefore, no residual information from packets not associated with a specific information stream can traverse through the TOE.

Key material resources are distributed and managed using the security appliances IPSec capabilities. All temporary storage associated with key material is handled in the same manner since it is encapsulated within packets. Therefore, no residual information from packets not associated with a specific information stream can traverse through the TOE.

The Information Flow Control function is designed to satisfy the following security functional requirements:

- FDP_IFC.1(1)
- FDP_IFC.1(2)
- FDP_IFF.1(1)
- FDP_IFF.1(2)
- FDP_RIP.2

6.4 Identification and Authentication

The TSF enforces binding between human users and subjects. Security Administrator is responsible for provisioning user accounts, and only the Security Administrator can do so. User accounts in the TOE have the following attributes: user identity (user name), authentication data (password) and role (privilege). Locally stored authentication data for fixed password authentication is a case-sensitive, alphanumeric value. The password has a minimum length of 10 characters with at least one change of character set (upper, lower, numeric, punctuation), and can be up to 20 ASCII characters in length (control characters are not recommended).

The TOE retains a subject identity and authentication data for peer-routers that will authenticate to the TOE. The subject identity retained by the TOE can be either a hostname or network address. The authentication data will be a manually entered key, or certificate depending upon the types of services configured for the interface. (see section 6.6 for a discussion on IPSec authentication and a list of IPSec options)

The TOE requires users to provide unique identification and authentication data (passwords) before any access to the system is granted. A password is configured for each user allowed to log into the secure router. The TOE successfully authenticates if the authentication data provided matches that stored in conjunction with the provided identity.

The Security Administrator can set a threshold for failed authentication attempts and can configure a throttling mechanism that increases the amount of time the TOE waits before prompting a user to enter a password after each failed authentication attempt in the same SSH session. Once the threshold has been reached, the user is prevented from making further attempts until a Security Administrator-defined period of time has elapsed. The following configuration values can be set by the Security Administrator to manage the behavior of the authentication failure mechanism and its associated throttling feature :

- backoff-factor — Sets the length of delay in seconds after each failed login attempt. When a user incorrectly logs in to the device, the user must wait the configured amount of time before attempting to log in to the device again. The length of delay increases by this value for each subsequent login attempt after the value specified in the backoff-threshold statement. The default value for this statement is five seconds, with a range of five to ten seconds.
- backoff-threshold — Sets the threshold for the number of failed login attempts on the device before the user experiences a delay when attempting to reenter a password. When a user incorrectly logs in to the device and hits the threshold of failed login attempts, the user experiences a delay that is set in the backoff-factor statement before attempting to log in to the device again. The default value for this statement is two, with a range of one through three.
- lockout-period — Sets the amount of time in minutes before the user can attempt to log in to the device after being locked out due to the number of failed login attempts specified in the tries-before-disconnect statement. When a user fails to correctly login after the number of allowed attempts specified by the tries-before-disconnect statement, the user must wait the configured amount of minutes before attempting to log in to the device again. The lockout-period must be

greater than zero. The range at which you can configure the lockout-period is one through 43,200 minutes.

- tries-before-disconnect — Sets the maximum number of times the user is allowed to enter a password to attempt to log in to the device through SSH. When the user reaches the maximum number of failed login attempts, the user is locked out of the device. The user must wait the configured amount of minutes in the lockout-period statement before attempting to log back in to the device. The tries-before-disconnect statement must be set when the lockout-period statement is set; otherwise, the lockout-period statement is meaningless. The default number of attempts is ten, with a range of one through ten attempts.

The TOE provides two services without authentication -- ICMP (i.e., ping) and ARP (Address Resolution Protocol) – since both of these services are essential for network operation.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1-NIAP-0425
- FIA_ATD.1(1)
- FIA_ATD.1(2)
- FIA_UAU.1(1)-FW
- FIA_UAU_(EXT).2-FW
- FIA_UAU_(EXT).5
- FIA_UID.2
- FIA_USB.1

6.5 Security Management

The TOE supports and enforces four distinct administrative roles: Audit Administrator, Cryptographic Administrator, IDS Administrator, and Security Administrator.

The TOE is delivered with restrictive default values such that no traffic can pass across the router until specific configuration changes are made. To enable forwarding between directly connected networks the IP addresses of the router interfaces must be configured. The secure router will not route to an indirectly connected subnet (through another routing device) unless a route is configured in the router.

The devices are managed through a Command Line Interface (CLI). The CLI provides the only mechanism for TOE management, access to the Unix shell is prohibited. The CLI is accessible through an SSH session (See section 6.9), or via a local terminal console. The CLI provides a text-based interface from which the router configuration can be managed and maintained. From this interface all router functions, such as the BGP, can be managed. The TOE automatically routes traffic based on available routing information, much of which is automatically collected from the TOE environment.

The revocation of authorizations occurring as a result of a security management operation occurs by removing or modifying user security attributes, policy rules, and available services. Changes to user security attributes that define the user's role take effect at the next login. Changes to information flow policy rules become effective immediately upon their being established as the current rules.

The TOE associates each command that is available at the CLI with one or more specific permissions. The association of permissions with CLI commands is static and cannot be modified by the product user. The TOE parses each command as it is entered at the CLI. At any point in the parsing, if the TOE determines the user does not have the appropriate permissions to invoke the command, the TOE cancels processing and presents the user with an error indication and a new CLI prompt. The guidance documentation provides instructions for creating login classes (roles) with the appropriate permissions to enforce the specified security management restrictions. When a user account is created, it must be assigned to a login class, so in the evaluated configuration, each user is associated with exactly one of the four specified roles.

The following lists enumerate the CLI permissions in the evaluated configuration.

Management functions available only to the Cryptographic Administrator role.

- The ability to execute the TSF Cryptographic Self-Test.
- The ability to modify the cryptographic security data parameters.

Management functions available only to the Audit Administrator role.

- The ability to manually delete audit logs.

Management functions available only to the Security Administrator role.

- The ability to invoke, determine and modify the behavior of the TSF Self-Test.
- The ability to enable, disable, determine and modify the behavior of the audit analysis and audit selection functions.
- The ability to enable or disable the security alarms.
- The ability to specify the limits for quotas on transport-layer connections.
- The ability to specify the limits, network identifiers and time period for quotas on controlled connection-oriented resources.
- The ability to specify the network addresses permitted to use ICMP or ARP.
- The ability to set the time and date used to form the time stamps in FPT_STM.1.
- The ability to query, modify, delete, create the information flow rules and attributes for the UNAUTHENTICATED INFORMATION FLOW SFP and the UNAUTHENTICATED TOE SERVICES SFP.
- The ability to specify initial values to override default values under the UNAUTHENTICATED INFORMATION FLOW SFP and the UNAUTHENTICATED TOE SERVICES SFP.
- The ability to create, delete or modify the rules that control the presumed address from which management sessions can be established.
- The ability to specify and revoke security attributes associated with the users, subjects, and objects within the TSC.
- The ability to specify the percentage of audit storage capacity at which the TOE alerts administrators.
- The ability to enable, disable, determine and modify the behavior of the functions of Authentication failure handling to configure an integer of unsuccessful authentication attempts that occurs related to a user's authentication to the Security Administrator.
- The ability to modify the number of failed authentication attempts via Login (for the CLI) or SSH that occur before progressive throttling is enforced for further authentication attempts and before the connection is dropped.
- The ability to manage basic network configuration of the router.

Management functions available only to the IDS Administrator role.

- The ability to specify IDS security alarms.
- The ability to specify IDS intrusion alarms.
- The ability to specify IDS audit selections.
- The ability to review IDS audit data.
- The ability to delete IDS records.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1(1)
- FMT_MOF.1(2)
- FMT_MOF.1(3)
- FMT_MOF.1(4)
- FMT_MOF.1(5)
- FMT_MOF.1(6)
- FMT_MOF.1(6)-FW
- FMT_MOF.1(6)-IDS
- FMT_MOF.1(7)
- FMT_MOF.1(7)-IDS
- FMT_MOF.1(8)-IDS
- FMT_MSA.1-FW
- FMT_MSA.2
- FMT_MSA.3(1)
- FMT_MSA.3(2)
- FMT_MSA.3-NIAP-0409(1)-FW
- FMT_MSA.3-NIAP-0409(2)-FW
- FMT_MTD.1(1)
- FMT_MTD.1(2)
- FMT_MTD.1(3)
- FMT_MTD.1(4)
- FMT_MTD.2(1)
- FMT_MTD.2(2)
- FMT_MTD.2(3)
- FMT_REV.1
- FMT_REV.1-FW
- FMT_SMF.1
- FMT_SMR.2

6.6 Protection of the TSF

The TOE is designed to fail securely. In the event of a transiently corrupt state or failure condition, the system will panic. A panic occurs when the operating system receives an unexpected instruction or handles an instruction improperly; for example if a cryptographic operation fails. The event will be logged and the system restarted, having ceased to process network traffic. When the system restarts, the system boot process does not succeed without passing all self-tests for cryptographic algorithms, RNG tests, and software integrity tests. This automatic recovery and self-test behavior, is discussed in Chapter 3 of the *Junos 11.2R2 Common Criteria Configuration Guide for LN1000 Mobile Secure Routers and SRX650 Services Gateways.*

When the TOE restarts, the system boot process will not succeed without passing all self-tests for cryptographic algorithms, RNG tests, and software integrity tests and will always bring the system to a known good state. Therefore, rebooting/restarting represents a failure remedy that brings the system back to a secure state. The TOE will run the following set of self tests during power on to check the correct operation of the TOE:

- Power on test – determines the boot-device responds, and performs a memory size check to confirm the amount of available memory.
- File integrity test –verifies integrity of all mounted signed packages, to assert that system files have not been tampered with.
- Crypto integrity test – checks integrity of major CSPs, such as SSH hostkeys and iked credentials, such as CAs, CERTS, and various keys.
- Authentication error – verifies that veriexec is enabled and operates as expected using /opt/sbin/kats/cannot-exec.real.

The power on self-tests may produce some or all of the output shown in Figure 4, below.

request system fips self-test

```
user@switch> request system fips self-test Testing file integrity:
File integrity Known Answer Test:                    Passed
Testing crypto integrity:
   Crypto integrity Known Answer Test:               Passed
Testing kernel KATS:
   DES3-CBC Known Answer Test:                       Passed
   HMAC-SHA1 Known Answer Test:                      Passed
   HMAC-SHA2-256 Known Answer Test:                  Passed
   SHA-2 Known Answer Test:                          Passed
   AES128-CMAC Known Answer Test:                    Passed
   AES-CBC Known Answer Test:                        Passed
Testing libmd KATS:
   HMAC-SHA1 Known Answer Test:                      Passed
   HMAC-SHA2-256 Known Answer Test:                  Passed
Testing OpenSSL KATS:
   FIPS RNG Known Answer Test:                       Passed
   FIPS DSA Known Answer Test:                       Passed
   FIPS ECDSA Known Answer Test:                     Passed
   FIPS ECDH Known Answer Test:                      Passed
   FIPS RSA Known Answer Test:                       Passed
   DES3-CBC Known Answer Test:                       Passed
   HMAC-SHA1 Known Answer Test:                      Passed
   SHA-2 Known Answer Test:                          Passed
   AES-CBC Known Answer Test:                        Passed
   ECDSA-SIGN Known Answer Test:                     Passed
   KDF-IKE-V1 Known Answer Test:                     Passed
Testing SSH IPsec KATS:
   DES3-CBC Known Answer Test:                       Passed
   HMAC-SHA1 Known Answer Test:                      Passed
   HMAC-SHA2-256 Known Answer Test:                  Passed
   SHA-2 Known Answer Test:                          Passed
   AES-CBC Known Answer Test:                        Passed
   SSH-RSA-ENC Known Answer Test:                    Passed
   SSH-RSA-SIGN Known Answer Test:                   Passed
   KDF-IKE-V1 Known Answer Test:                     Passed
Expect an exec Authentication error...
exec: /opt/sbin/kats/cannot-exec.real: Authentication error
```

Figure 4 - Fips Self-Test Example

After a power failure, the TOE automatically restarts to a secure state when power returns.

The TSF has the ability to perform a preconfigured action that is selected by the security administrator when a replay attack is detected. The configurable actions include rejection of session establishment in case of an administrative session. By default all the replay events are logged along with the timestamp, source address. The TSF provides replay detection on all the physical interfaces and tunnel interfaces as well, through the use of IPsec. For the remote administration sessions, the SSH daemon has a built-in replay detection mechanism. The TOE takes a conservative approach to identifying potential replay attacks. Specifically, the following two conditions will be flagged by the TOE as a potential replay and handled accordingly: invalid MAC (Message Authentication Code) on packet; received packet size exceeds maximum packet size.

The security router hardware provides a reliable clock, and the Junos uses this clock to provide reliable time stamps. The TOE also supports the use of the NTP protocol for clock synchronization. Both are part of the TSF.

For every command line operation that is entered at the command line interface, there is a command interpreter module which checks for the users privilege levels in real time before an action is taken.

The TSF runs self tests during initial start-up. Also, the security administrator can schedule the self tests to be executed or can invoke the self tests at any point during normal operation of the TOE. The TSF provides a command line operation that only the administrator can use to verify the integrity of the static code (including the TSF executable code). These tests demonstrate the integrity of the TSF executable code.

The TSF provides a suite of cryptographic module self-tests which are invoked every time the device boots up. These crypto self tests can be executed on demand only by the cryptographic administrator and as scheduled by the security administrator. Also, the TSF can be configured such that the self tests are run automatically after every key is generated. By default this is turned off and the administrator has to turn this on. These tests demonstrate the correct operation of the key error detection mechanism, the cryptographic algorithms, and the RNG/PRNG mechanism. The tests verify the integrity of TSF data and TSF executable code related to cryptography and key generation. The tests also demonstrate the correct operation of the TSF's key generation mechanism. The administrator is also instructed to schedule a self-test at least once per day. If a self-test fails the TOE generates an audit record.

As noted in the Cryptographic Support section above and the Trusted Path/Channels section below, the TOE supports IPsec, which provides for the confidentiality and integrity of communications between the secure router and external IT systems.

The TSF provides the ability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product using an integrity checksum built into the IPSec protocol (see Section 6.3, Information Flow Control). The TSF provides the ability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and to stop decryption if modifications are detected.

The TOE supports IPsec to provide confidentiality, integrity, and authenticity for traffic transmitted for inbound/outbound traffic (when configured accordingly). The TOE implements multiple configurations of IPsec, including route/policy-based VPNs, Manual Key, AutoKey IKE, AutoKey IKE with Preshared Keys, and AutoKey IKE with Certificates. The IPSec functionality supported by the TOE is described by the following set of RFCs.

- RFC 4301: Security Architecture for the Internet Protocol
- RFC 4302: IP Authentication Header
- RFC 4303: IP Encapsulating Security Payload
- RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 2409: The Internet Key Exchange

The Manual Key option allows both ends of a tunnel to separately configure all IPsec security parameters. The configurable options available during manual keying of a VPN are the same as those available in IKE Phase 1 VPN Configuration (See Table 12)[5]. AutoKey IKE facilitates the creation and management of numerous tunnels; each instance of the TOE does not have to be configured manually. Using AutoKey IKE with preshared keys to authenticate the participants in an IKE session, each side must configure and securely exchange the preshared key in advance. Once distributed, an autokey, unlike a manual key, can automatically change its keys at predetermined intervals using the IKE protocol. When using certificates to authenticate the participants during an AutoKey IKE negotiation, each side generates a public-private key pair and acquires a certificate. As long as the issuing certificate authority (CA) is trusted by both sides, the participants can retrieve the peer's public key and verify the peer's signature. There is no need to keep track of the keys and SAs; IKE does it automatically. Configuration options for Phase 1 and Phase 2 IKE are shown in the following tables.

Table 12 - IKE Phase 1 Configuration Options

IKE Phase 1 VPN Configuration	
Authentication Method The method the device uses to authenticate the source of Internet Key Exchange (IKE) messages. Options include:	• pre-shared-keys—Key for encryption and decryption that both participants must have before beginning tunnel negotiations. • rsa-key—Kinds of digital signatures, which are certificates that confirm the identity of the certificate holder.
Authentication Algorithm The Authentication Header (AH) algorithm the device uses to verify the authenticity and integrity of a packet. Supported algorithms include the following:	• sha1—Produces a 160-bit digest. • sha-256—Produces a 256-bit digest.

[5] The manual configuration options would include only pre-shared-keys (no rsa-key) and would not include the Diffie-Hellman groups.

IKE Phase 1 VPN Configuration	
Encryption Algorithm Supported encryption algorithms include the following:	• 3des-cbc—3DES-CBC encryption algorithm. • aes-128-cbc—AES-CBC 128-bit encryption algorithm. • aes-192-cbc—AES-CBC 192-bit encryption algorithm. • aes-256-cbc—AES-CBC 256-bit encryption algorithm.
Local Identity Type There are four identify types:	• IP Address • Host Name • Email Address • Distinguished Name

Table 13 - IKE Phase 2 Configuration Items

IKE Phase 2 IPsec Autokey Configuration	
Authentication Algorithm The Authentication Header (AH) algorithm the device uses to verify the authenticity and integrity of a packet. Supported algorithms include the following:	• Hmac-md5-96 –produces a 128 bit digest • Hmac-sha1-96—Produces a 160-bit digest
Encryption Algorithm Supported encryption algorithms include the following:	• 3des-cbc—Has a block size of 24 bytes; the key size is 192 bits long. • aes-128-cbc—AES 128-bit encryption algorithm. • aes-192-cbc—AES 192-bit encryption algorithm. • aes-256-cbc—AES 256-bit encryption algorithm.
Perfect Forward Secrecy The method the device uses to generate the encryption key. PFS generates each new encryption key independently from the previous key.	• Group 1 - Diffie-Hellman Group 1 • Group 2 - Diffie-Hellman Group 2 • Group 5 - Diffie-Hellman Group 5 • Group 14 – Diffie-Hellman Group 14

The TSF provides the capability to consistently interpret **BGP Open, Update, Notification, and Keepalive messages** when shared between the TSF and another trusted IT product. Junos supports the BGP protocol

in accordance with the relevant standards. The TSF uses **RFC 4271** when interpreting the TSF data from another trusted IT product.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_FLS.1
- FPT_PRO_(EXT).1
- FPT_RCV.2
- FPT_RPL.1
- FPT_STM.1
- FPT_TDC.1
- FPT_TST_(EXT).1
- FPT_TST.1(1)
- FPT_TST.1(2)

6.7 Resource Utilization

The TSF represents a transport-layer communication pathway as a connection. The TOE can defend itself and the resources it protects from various DoS and DDoS attacks by rate limiting these connections (i.e., applying a maximum quota to the number of connections). TCP SYN flood attack protection is one of them.

The TSF utilizes a session table to control connection-oriented resources. The TSF supports both source based session limiting and destination based session limiting to prevent session table flooding attacks. The thresholds for the same are configurable by the security administrator. Also, the Security Administrator has the ability to define the maximum number of resources a particular address or set of addresses can use over a specified time period. The TSF also provides SYN-ACK-ACK proxy flood, SYN flood and SYN cookie protection mechanisms. The default action taken by the TSF when a specific IT entity exceeds the quota is reject and log.

The Resource Utilization function is designed to satisfy the following security functional requirements:

- FRU_RSA.1

6.8 TOE Access

Junos enables Security Administrators to configure an access banner provided with the authentication prompt. The banner can provide warnings against unauthorized access to the secure router as well as any other information that the Security Administrator wishes to communicate.

Access to the secure routers can be denied based on time and date (e.g., users can only establish sessions between Monday and Friday). Access can also be denied based on the putative network location (IP address or subnet) of the in-bound access request.

User sessions can be locked or terminated by users. The Security Administrator can set the TOE so that a user is locked out after a period of inactivity.

The TSF overwrites the display device and makes the current contents unreadable after the local interactive session is locked due to inactivity, thus disabling any further interaction with the TOE. This mechanism is the inactivity timer for administrative sessions. The Security Administrator can configure this inactivity timer on administrative sessions after which the session will be logged out. The TOE requires the administrative user to re-authenticate after a timeout to unlock the session.

The local administrative user can logout of existing session by typing logout to exit the CLI admin session and the TSF makes the current contents unreadable after the admin initiates the locking and no user activity can take place until the user re-identifies and authenticates.

The TOE Access function is designed to satisfy the following security functional requirements:

- FTA_SSL.1-FW/IDS
- FTA_SSL.2-FW/IDS
- FTA_SSL.3(1)
- FTA_SSL.3(2)
- FTA_TAB.1
- FTA_TSE.1

6.9 Trusted Path/Channels

The TOE supports and enforces Trusted Channels that protect the communications between the TOE and peer systems from unauthorized disclosure or modification. It also supports Trusted Paths between itself and remote administrators so that the contents of administrative sessions are protected against unauthorized disclosure or modification.

The TOE achieves Trusted Channels through the IPsec secure tunneling standard, which ensures the confidentiality and integrity of network communications. The set-up of Trusted Channels is enforced by the Junos kernel. In the evaluated configuration, a setting in the kernel invokes the IP_IPSEC_POLICY and thereby forces the instantiation of IPsec for all connections with all adjacent IT systems. Junos does maintain an exclusion list of ports/services that are protected by either SSH or TLS/SSL and thus are not be required to use the IP_IPSEC_POLICY connection method.

The TOE achieves Trusted Paths by use of the SSHv2 protocol (all references to the use of SSH refer to the use of the SSHv2 protocol), which ensures the confidentiality and integrity of user sessions. The encrypted communication path between the TSF and a remote administrator is provided by the use of an SSH session. Remote administrators of the TSF initiate communication with the TSF through the SSH tunnel created by the SSH session. Assured identification is guaranteed by using public key certificate based authentication for SSH. The SSHv2 protocol ensures that the data transmitted over a SSH session cannot be disclosed or altered by using the encryption and integrity mechanisms of the protocol with the FIPS cryptographic module.

The Trusted Path/Channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1(1)
- FTP_ITC.1(2)
- FTP_TRP.1(1)
- FTP_TRP.1(2)

6.10 RFC Conformance Statements

This section identifies, for the critical RFCs, the options supported by the TOE.

Protocol	RFC	RFC synopsis	TOE Handling of Security-Related Protocol Options
IPSec/IKE	RFC 2409	The Internet Key Exchange	**Modes:** Junos supports both Main and Aggressive mode in phase 1, and Quick mode in phase 2. It does not support New Group mode. **Exchanges:** Authenticated with either pre-shared key, RSA or DSA signatures. **Informational exchanges:** Junos does not accept INITIAL-CONTACT messages unless they are authenticated. **Oakley groups:** Diffie-Hellman groups 2, 5 and 14 are supported. **Perfect Forward Secrecy:** May be configured on a per-tunnel basis.
	RFC 4301	Security Architecture for the Internet Protocol	**Security Association and Key Management:** Junos supports both manually keyed and automatically established VPNs using IKEv1. **Fragmentation:** Junos will reassemble a fragmented IPSec packet and will propagate the DF bit from the cleartext to the encapsulated packet.
	RFC 4302	IP Authentication Header	Junos supports AH in tunnel mode only. Transport mode is not supported. Junos does not support the use of AH without ESP.
	RFC 4303	IP Encapsulating Security Payload	Junos supports ESP in tunnel mode only. Transport mode is not supported. Junos supports the use of ESP with or without AH.
	RFC 4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	**Modes:** Junos supports both Main and Aggressive mode in phase 1, and Quick mode in phase 2. It does not support New Group mode. **Exchanges:** Authenticated with either pre-shared key, RSA or DSA signatures. **Informational exchanges:** Junos does not accept INITIAL-CONTACT messages unless they are authenticated. **Oakley groups:** Diffie-Hellman groups 2, 5 and 14 are supported. **Perfect Forward Secrecy:** May be configured on a per-tunnel basis.

Protocol	RFC	RFC synopsis	TOE Handling of Security-Related Protocol Options
SSH	RFC 4251	The Secure Shell (SSH) Protocol Architecture	**Host Keys:** The TOE has one RSA, one DSA, and one ECDSA Host Key for SSH v2, which are generated on initial setup of the TOE. Any of them can be deconfigured via the CLI and the relevant key will be deleted and thus unavailable during connection establishment. These keys are randomly generated to be unique to each TOE instance. The TOE presents the client with its public key and the client matches this key against its known_hosts list of keys. When a client connects to the TOE, the client will be able to determine if the same host key was used in previous connections, or if the key is different (per the SSHv2 protocol). **Policy Issues:** The TOE implements all mandatory algorithms and methods. The TOE can be configured to accept public-key based authentication and/or password-based authentication. The TOE does not require multiple authentication for users. The TOE allows port forwarding and sessions to clients. The TOE has no X11 libraries or applications and X11 forwarding is prohibited. **Confidentiality:** The TOE does not accept the "none" cipher. The TOE rekeys connections, after 2^27 blocks have been sent/received. The client may explicitly request a rekeying event as a valid SSHv2 message at any time and the TOE will honor this request. **Denial of Service:** When the SSH connection is brought down, the TOE does not attempt to re-establish it. The TOE can be configured with ACLs to control the clients that are able to connect to it via SSH. **Ordering of Key Exchange Methods:** The TOE orders key exchange algorithms as follows: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1. **Debug Messages:** The TOE sshd server does not support debug messages. **End Point Security:** The TOE permits port forwarding. **Proxy Forwarding:** The TOE permits proxy forwarding. **X11 Forwarding:** The TOE does not support X11 forwarding.

Protocol	RFC	RFC synopsis	TOE Handling of Security-Related Protocol Options
	RFC 4252	The Secure Shell (SSH) Authentication Protocol	**Authentication Protocol:** The TOE does not accept the "none" authentication method. The TOE disconnects a client after 30 seconds if authentication has not been completed. The TOE also allows authentication retries of six times before sending a disconnect to the client. **Authentication Requests:** The TOE does not accept authentication if the requested service does not exist. The TOE does not allow authentication requests for a non-existent username to succeed – it sends back a disconnect as it would for failed authentications and hence does not allow enumeration of valid usernames. The TOE denies "none" authentication method and replies with a list of permitted authentication methods. **Public Key Authentication Method:** The TOE supports public key authentication. Authentication succeeds if the correct private key is used. The TOE does not require multiple authentication (public key and password) for users. **Password Authentication Method:** The TOE supports password authentication. The TOE does not allow an expired password to be used for authentication. **Host-Based Authentication:** The TOE does not support the configuration of host-based authentication methods.
	RFC 4253	The Secure Shell (SSH) Transport Layer Protocol	**Encryption:** The TOE offers the following for encryption of SSH sessions: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, aes256-cbc, and 3des-cbc. The TOE permits negotiation of encryption algorithms in each direction. The TOE does not allow the "none" algorithm for encryption. **Data Integrity:** The TOE permits negotiation of MAC algorithms in each direction. **Key Re-Exchange:** The TOE performs a re-exchange when SSH_MSG_KEXINIT is received. However, it does not initiate a key re-exchange itself.

Table 14 - RFC Conformance Statements

7 Rationale

7.1 Statement of Threats Consistency

The following table identifies each threat included in the ST and maps to it the Security Objectives for the TOE and the operational environment that contribute to countering that threat.

Threat/Policy	Objectives Addressing the Threat / Policy	Rationale
T.ADDRESS_MASQUERADE	O.MEDIATE_INFORMATION_FLOW 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_INFORMATION_FLOW counters this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. The rules in each of the policies ensure that the network identifier in a network packet is in the set of network identifiers associated with a TOE's network interface. Therefore, if a user supplied a network identifier in a packet that was associated with a TOE network interface other than the one the user supplied the packet on, the packet would not be allowed to flow through the TOE, or access TOE services. This would, for example, prevent a user from sending a packet from the Internet claiming to be on a machine on the protected enclave.
T.ADMIN_ROGUE	O.ADMIN_ROLE The TOE will provide an administrator role to isolate administrative actions.	O.ADMIN_ROLE mitigates this threat to a limited degree by limiting the functions available to an administrator. This is somewhat different than the part this objective plays in countering T.ADMIN_ERROR, in that this presumes that separate individuals will be assigned separate roles. If the Audit Administrator's intentions become malicious they would not be able to render the TOE unable to enforce its information flow policies. On the other hand, if the Security Administrator becomes malicious they could affect the information flow policy, but the Audit Administrator may be able to detect those actions.

Threat/Policy	Objectives Addressing the Threat / Policy	Rationale
T.AUDIT_COMPROMISE	O.AUDIT_PROTECTION The TOE will provide the capability to protect audit information (i.e. audit records and IDS audit records).	contributes to mitigating this threat by controlling access to the audit and IDS audit trail. No one is allowed to modify audit or IDS Audit records, the Audit Administrator is the only one allowed to delete the audit trail while the IDS Administrator is the only role allowed to delete the IDS audit trail.
	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated.	O.RESIDUAL_INFORMATION prevents a user not authorized to read the audit trail from access to audit information that might otherwise be persistent in a TOE resource (e.g., memory). By ensuring the TOE prevents residual information in a resource, audit information will not become available to any user or process except those explicitly authorized for that data.
T.CRYPTO_COMPROMISE	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated.	O.RESIDUAL_INFORMATION mitigates the possibility of malicious users or processes from gaining inappropriate access to cryptographic data, including keys. This objective ensures that the cryptographic data does not reside in a resource that has been used by the cryptographic module and then reallocated to another process.
	OE.CRYPTANALYTIC Cryptographic methods used in the IT environment shall be interoperable with the TOE, should be FIPS 140-2 validated and should be resistant to cryptanalytic attacks (i.e., will be of adequate strength to protect unclassified Mission Support, Administrative, or Mission Critical data).	OE. CRYPTANALYTIC by ensuring that encryption is used on the communications channel between authorized IT entities and the TOE; and by ensuring that an administrator can be assured that they are communicating with the TOE.
T.EAVESDROP A malicious user or process may observe or modify user or TSF data transmitted between the TOE and another trusted IT entity.	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 counters this threat by ensuring protection of the communication between the TOE and trusted IT entities while transmitting data.

Threat/Policy	Objectives Addressing the Threat / Policy	Rationale
T.MALICIOUS_TSF_COMPROMISE	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated.	O.RESIDUAL_INFORMATION necessary to mitigate this threat by ensuring no TSF data remain in resources allocated to a user. Even if the security mechanisms do not allow a user to explicitly view TSF data, if TSF data were to inappropriately reside in a resource that was made available to a user, that user would be able to inappropriately view the TSF data
	O.MANAGE The TOE will provide all the functions and facilities necessary to support the administrators 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.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE	O.DISPLAY_BANNER helps mitigate this threat by providing the Administrator the ability to remove product information (e.g., product name, version number) from a banner that is displayed to users. Having product information about the TOE provides an attacker with information that may increase their ability to compromise the TOE
	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 various users (remote administrators, and trusted IT entities (for performing replication, for instance)). This ensures the transmitted data cannot be compromised or disclosed during the duration of the trusted path.

Threat/Policy	Objectives Addressing the Threat / Policy	Rationale
T.MASQUERADE	O.ROBUST_TOE_ACCESS 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_ACCESS mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanisms, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user.
T.REPLAY A user may gain inappropriate access to the TOE by replaying authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or security attributes (captured as it was transmitted during the course of legitimate use).	O.REPLAY_DETECTION The TOE will provide a means to detect and reject the replay of authentication data and other TSF data and security attributes	O.REPLAY_DETECTION prevents a user from replaying TSF data and security attributes (e.g., TSF data or security attributes transmitted between a remote administrator, an authorized IT entity and the TOE) that could leave the TOE in a configuration that the administrative staff did not intend (e.g., an administrator modifies the auditable events to be recorded and a user captures that traffic.
T.RESIDUAL_DATA A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.	O. RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated.	O.RESIDUAL_INFORMATION counters this threat by ensuring that TSF data and user data is not persistent when resources are released by one user/process and allocated to another user/process. This means that network packets will not have residual data from another packet due to the padding of a packet.
T.RESOURCE_EXHAUSTION 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.	O.RESOURCE_SHARING 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).	O.RESOURCE_SHARING mitigates this threat by requiring the TOE to provide controls over connection-oriented resources. These controls provide the administrator ability to specify which network identifiers have access to the TOE's connection-oriented resources over a time period that is specified by the administrator. 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).

Threat/Policy	Objectives Addressing the Threat / Policy	Rationale
T.SPOOFING A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.	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.	It is possible for an entity other than the TOE (a subject on the TOE, or another IT entity on the network between the TOE and the end user) to provide an environment that may lead a user to mistakenly believe they are interacting with the TOE, thereby fooling the user into divulging identification and authentication information. O.TRUSTED_PATH mitigates this threat by ensuring users have the capability to ensure they are communicating with the TOE when providing identification and authentication data to the TOE.
T.UNATTENDED_SESSION A user may gain unauthorized access to an unattended session.	O.ROBUST_TOE_ACCESS 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_ACCESS helps to mitigate this threat by including mechanisms that place controls on user's sessions. Local administrator's sessions are locked and remote sessions are dropped after a Security Administrator defined time period of inactivity. Locking the local administrator's session reduces the opportunity of someone gaining unauthorized access the session when the console is unattended.
T.UNAUTHORIZED_ACCESS A user may gain access to services (by sending data through the TOE) for which they are not authorized according to the TOE security policy.	O.MEDIATE_INFORMATION_FLOW 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_INFORMATION_FLOW works to mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. The TSF must ensure that all configured enforcement functions. The TOE restricts the ability to modify the security attributes associated with information flow control rules and access to authenticated and unauthenticated services, etc to the Security Administrator.
T.UNAUTHORIZED_PEER An unauthorized IT entity may attempt to establish a security association with the TOE.	O.PEER_AUTHENTICATION The TOE will authenticate each peer TOE that attempts to establish a security association with the TOE.	O.PEER_AUTHENTICATION mitigates this threat by requiring that the TOE implement the Internet Key Exchange protocol, as specified in RFC2409, to establish a secure, authenticated channel between the TOE and another remote router before establishing a security association with that router.

Threat/Policy	Objectives Addressing the Threat / Policy	Rationale
T.UNIDENTIFIED_ACTIONS The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.	O.AUDIT_REVIEW The TOE will provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.	O.AUDIT_REVIEW helps to mitigate this threat by providing the Security Administrator with a required minimum set of configurable audit events that could indicate a potential security violation.
T.UNIDENTIFIED_INTRUSIONS The IDS Administrator may fail to notice potential intrusions, thus limiting the IDS Administrator's ability to identify and take action against a possible intrusion.	O.IDS_AUDIT_REVIEW The TOE will provide the capability to selectively view IDS audit information, and alert the IDS Administrator of potential intrusions.	O.IDS_AUDIT_REVIEW helps to mitigate this threat by providing a variety of mechanisms for monitoring the targeted system resources. The two basic ways IDS audit review is performed is through analysis of the IDS audit trail produced by the IDS audit mechanism, and through the use of an automated analysis and alarm system.
T.UNKNOWN_STATE When the TOE is initially started or restarted after a failure, the security state of the TOE may be unknown.	O.MAINT_MODE The TOE shall provide a mode from which recovery or initial startup procedures can be performed. O.CORRECT_TSF_OPERATION The TOE will provide a capability to test the TSF to ensure the correct operation of the TSF in its operational environment.	O.MAINT_MODE helps to mitigate this threat by ensuring that the TOE does not continue to operate in an insecure state when a hardware or software failure occurs. After a failure, the TOE enters a state that disallows operations and requires an administrator to follow documented procedures to return the TOE to a secure state. O.CORRECT_TSF_OPERATION counters this threat by ensuring that the TSF runs a suite of tests to successfully demonstrate the correct operation of the TSF (hardware and software) and the TSF's cryptographic components at initial startup of the TOE. In addition to ensuring that the TOE's security state can be verified, an administrator can verify the integrity of the TSF's data and stored code and the TSF's cryptographic data and stored code using the TOE-provided cryptographic mechanisms.

Table 15 - Threats Addressed by the TOE

7.2 Statement of Organizational Security Policies Consistency

The following table identifies each Organizational Security Policy (OSP) included in the ST and maps to it each Security Objective for the TOE that contributes to meeting that OSP.

Threat/Policy	Objectives Addressing the Threat	Rationale
P.ACCESS_BANNER The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	O.DISPLAY_BANNER satisfies this policy by ensuring that the TOE displays a Security Administrator configurable banner that provides all users with a warning about the unauthorized use of the TOE.
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events associated with users.	O.AUDIT_GENERATION addresses this policy by providing the Security Administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE (e.g. access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.).
	O.TIME_STAMPS The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	O.TIME_STAMPS plays a role in supporting this policy by requiring the TOE to provide a reliable time stamp (configured locally by the Security Administrator or via an external NTP server). The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred.
	O.ROBUST_TOE_ACCESS 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_ACCESS supports this policy by requiring the TOE to identify and authenticate all authorized users prior to allowing any TOE access or any TOE mediated access on behalf of those users.

Threat/Policy	Objectives Addressing the Threat	Rationale
P.ADMIN_ACCESS Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.	O.ADMIN_ROLE The TOE will provide an administrator role to isolate administrative actions.	O.ADMIN_ROLE supports this policy by requiring the TOE to provide mechanisms (e.g., local authentication, remote authentication, means to configure and manage the TOE both remotely and locally) that allow remote and local administration of the TOE. This is not to say that everything that can be done by a local administrator must also be provided to the remote administrator. In fact, it may be desirable to have some functionality restricted to the local administrator (e.g., setting the ruleset).
	O.TRUSTED_PATH The TOE will provide a means to ensure users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.	O.TRUSTED_PATH satisfies this policy by requiring that each remote administrative session (all administrative roles) is authenticated and conducted via a secure channel. Additionally, all authorized IT entities (e.g. authentication/certificate servers, NTP servers) must adhere to the same requirements as the remote administrator.
P.COMPATIBILITY The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operation with other routers and network equipment using the same protocols.	O.PROTOCOLS The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or Industry specifications to ensure interoperability.	O.PROTOCOLS satifies this policy by requiring that standardized protocols are implemented in the TOE to ensure interoperatibility among peer TOEs therefore not compromising the secure state of the router.
P.CRYPTOGRAPHY The TOE shall use NIST FIPS-validated cryptography as a baseline with additional NSA-approved methods for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys), and for cryptographic operations (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).	O.CRYPTOGRAPHIC_FUNCTIONS The TOE shall use NIST FIPS validated cryptography as a baseline with additional NSA-approved methods for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys), and for cryptographic operations (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).	O.CRYPTOGRAPHIC_FUNCTIONS implements this policy, requiring a combination of FIPS-validation and non-FIPS-validated cryptographic mechanisms that are used to provide encryption/decryption services, and digital signature functions. Functions include symmetric encryption and decryption, digital signatures, and key generation and establishment functions.

Threat/Policy	Objectives Addressing the Threat	Rationale
	O.CRYPTOGRAPHY_VALIDATED The TOE shall use NIST FIPS 140-2 validated cryptomodules for cryptographic services implementing FIPS-approved security functions and random number generation services used by cryptographic functions.	O.CRYPTOGRAPHY_VALIDATED satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data in support of the TOE's trusted path and trusted channel functions.
	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated or upon completion of a function that residual biometric data could not be reused	O.RESIDUAL_INFORMATION satisfies this policy by ensuring that cryptographic data are cleared from resources that are shared between users. Keys must be zeroized according to FIPS 140-2
P.IDS_DATA_COLLECTION IDS audit events based on data collected from IT System resources will be created.	O.IDS_AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events from targeted IT System resource(s) and associate those events with the component that created the record.	O.AUDIT_GENERATION addresses this policy by providing an IDS audit mechanism to create records based on the actions from specific IT System resources, as well as the capability for an IDS Administrator to "pre-select" IDS audit events based on the component ID. The IDS audit event selection function is configurable during run-time to ensure the TOE is able to capture IDS security-relevant events given changes in threat conditions. Additionally, the IDS Administrator's ID is recorded when any security relevant change is made to the TOE (e.g., access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.). Attributes used in the audit record generation process are also required to be bound to the subject, ensuring components are bounded to the IDS audit records they create.

Table 16 - Organizational Security Policies

7.3 Statement of Assumptions Consistency

The following table identifies each assumption included in the ST and maps to it each Security Objective for the Operational Environment that contributes to upholding that assumption.

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.NO_GENERAL_PURPOSE The administrator ensures there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.	OE.NO_GENERAL_PURPOSE The Administrator ensures there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.	The Router must not include any general-purpose commuting or storage capabilities. This will protect the TSF data from malicious processes.
A.NO_TOE_BYPASS Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.	OE.NO_TOE_BYPASS The administrator configures the router configuration such that Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.	The router does not allow information flow between external and internal networks located in different enclaves without passing through the TOE.
A.PHYSICAL It is assumed that the IT 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 (e.g., theft, modification, destruction, or eavesdropping). 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.

Table 17 - Assumptions Consistency Rationale

7.4 Statement of Security Objectives for the TOE Consistency

The following table identifies each Security Objective for the TOE included in the ST and maps to it each Security Functional Requirement that contributes to meeting that objective.

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN_ROLE The TOE will provide administrator roles to isolate administrative actions, and to make the administrative functions available locally and remotely.	FMT_SMR.2	FMT_SMR.2 requires that three roles exist for administrative actions: the Security Administrator, who is responsible for configuring most security-relevant parameters on the TOE; the Cryptographic Administrator, who is responsible for managing the security data that is critical to the cryptographic operations; and the Audit Administrator, who is responsible for reading and deleting the audit trail. The TSF is able to associate a human user with one or more roles and these roles isolate administrative functions in that the functions of these roles do not overlap. It is true that the design of some systems could enable a rogue security administrator to manipulate cryptographic data by, for instance, writing directly to kernel memory. While this scenario is a security concern, this objective does not counter that aspect of T.ADMIN_ROGUE. If a security administrator were to perform such an action, the auditing requirements (along with the audit trail protection requirements) afford some measure of detectability of the rogue administrator's actions.

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events associated with users.	FAU_GEN.1- NIAP-0429	FAU_GEN.1-NIAP-0429 defines the set of events that the TOE must be capable of recording. This requirement ensures that an administrator 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. There is a minimum of information that must be present in every audit record and this requirement defines that, and the additional information that must be recorded for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to this ST.
	FAU_GEN.2- NIAP-0410	FAU_GEN.2-NIAP-0410 ensures that the audit records associate a user identity with the auditable event. Although the FIA_ATD.1 requirements mandate that a “userid” be used to represent a user identity, the TOE developer is able to associate different types of user-ids with different users in order to meet this objective.
	FIA_USB.1	FIA_USB.1 plays a role is satisfying this objective by requiring a binding of security attributes associated with users that are authenticated with the subjects that represent them in the TOE. This only applies to authenticated users, since the identity of unauthenticated users cannot be confirmed. Therefore, the audit trail may not always have the proper identity of the subject that causes an audit record to be generated.

Objective	Requirements Addressing the Objective	Rationale
	FAU_SEL.1-NIAP-0407	FAU_SEL.1-NIAP-0407 allows the selected administrator(s) to configure which auditable events will be recorded in the audit trail. This provides the administrator with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources consumed by the audit mechanism and providing the ability to focus on the actions of an individual user. In addition, the requirement has been refined to require that the audit event selection function is configurable during run-time to ensure the TOE is able to capture security-relevant events given changes in threat conditions.
O.AUDIT_PROTECTION The TOE will provide the capability to protect audit information (i.e., audit records and IDS audit records).	FMT_MOF.1(3)	FMT_MOF.1(3) restricts the ability to control the behavior of the audit and alarm mechanism to the Administrators.
	FMT_MOF.1(5)	FMT_MOF.1(5) restricts the ability to control the behavior of the audit and alarm mechanism to the Security Administrator. The Security Administrator is the only user that controls the behavior of the events that generate alarms and whether the alarm mechanism is enabled or disabled.
	FAU_SAR.2(1)	FAU_SAR.2(1) restricts the ability to read the audit trail to the administrators, thus, preventing the disclosure of the audit data to any other user. However, the TOE is not expected to prevent the disclosure of audit data if it has been archived or saved in another form (e.g., moved or copied to an ordinary file).
	FAU_SAR.2(2)	FAU_SAR.2(2) restricts the ability to read the IDS audit trail to the IDS Administrators, thus, preventing the disclosure of the IDS audit data to any other user. However, the TOE is not expected to prevent the disclosure of IDS audit data if it has been archived or saved in another form (e.g., moved or copied to an ordinary file).

Objective	Requirements Addressing the Objective	Rationale
	FAU_STG.NIAP-0414-1-NIAP-0429(1)	FAU_STG.NIAP-0414-1-NIAP-0429(1) allows the Security Administrator to configure the TOE so that if the audit trail does become full, either the TOE will prevent any events from being logged (other than actions taken by the administrator) that would generate an audit record or the audit mechanism will overwrite the oldest audit records with new records.
	FAU_STG.NIAP-0414-1-NIAP-0429(2)-IDS	FAU_STG.NIAP-0414-1-NIAP-0429(2) allows the IDS Administrator to configure the TOE so that if the IDS audit trail does become full, either the TOE will prevent any events from occurring (other than actions taken by the administrator) that would generate an IDS audit record or the IDS audit mechanism will overwrite the oldest IDS audit records with new records.
	FAU_STG.1-NIAP-0429	FAU_STG.1-NIAP-0429 primarily ensures only Audit Administrators can delete audit records. FAU_STG.1-NIAP-0429 also ensures that no one has the ability to perform unauthorized modifications to the audit records (e.g., edit any of the information contained in an audit record). This ensures the integrity of the audit trail is maintained.
	FAU_STG.2-NIAP-0429-IDS	FAU_STG.2-NIAP-0429-IDS restricts the ability to perform authorized deletion of IDS audit records to the IDS Administrator for maintenance purposes. FAU_STG.2-NIAP-0429-IDS also ensures that no one has the ability to modify audit records (e.g., edit any of the information contained in an audit record). This ensures the integrity of the IDS audit trail is maintained.

Objective	Requirements Addressing the Objective	Rationale
	FAU_STG.3	FAU_STG.3 requires that the administrators be alerted when the audit trail exceeds a capacity threshold established by the Security Administrator. In addition, an audit record is cut which will trigger the analysis performed in FAU_SAA, resulting in an FAU_ARP alarm being issued. When the audit trail is full, the TOE begins to re-use storage by writing new records over the oldest data. FAU_STG.3 ensures that an administrator has the opportunity to manage the audit trail before it becomes full and the avoiding the possible loss of audit data
O.AUDIT_REVIEW The TOE will provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.	FAU_ARP.1	FAU_ARP.1 requires that the alarm be displayed at the local administrative console and at the remote administrative console(s) when auditor and security administrative session(s) exists. For alarms at remote consoles, the alarm is sent either during an established session or upon session establishment (as long as the alarm has not been acknowledged). This is required to increase the likelihood that the alarm will be received as soon as possible. This requirement also dictates the information that must be displayed with the alarm. The potential security violation is identified in the alarm, as are the contents of the audit records of the events that accumulated and triggered the alarm. The information in the audit records is necessary; it allows the administrators to react to the potential security violation without having to search through the audit trail looking for the related events.
	FAU_ARP_ACK_(EXT).1	FAU_ARP_ACK_(EXT).1 requires that an alarm generated by the mechanism that implements the FAU_ARP requirement be maintained until an administrator acknowledges it. This ensures that the alarm message will not be obstructed and the administrators will be alerted of a potential security violation. Additionally, this requires that the acknowledgement be transmitted to users that received the alarm, thus ensuring that that set of administrators knows that the user specified in the acknowledgement message has addressed the alarm.

Objective	Requirements Addressing the Objective	Rationale
	FAU_SAA.1-NIAP-0407	FAU_SAA.1-NIAP-0407 defines the events (or rules) that indicate a potential security violation and will generate an alarm. The triggers for these events are largely configurable by the Security Administrator. Some rules are not configurable, or configurable by the cryptographic administrator.
	FAU_SAR.1	FAU_SAR.1 (both iterations) is used to provide both the auditor and an external audit analysis function 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 end user (auditor or external system) to interpret the audit trail. It is expected that the audit information be presented in such a way that the end user can examine an audit record and have the appropriate information (that required by FAU_GEN.2-NIAP-410) presented together to facilitate the analysis of the audit review. Ensuring the audit data are presented in an interpretable format will enhance the ability of the entity performing the analysis to identify potential security violations.
	FAU_SAR.3	FAU_SAR.3 complements FAU_SAR.1 by providing the administrators the flexibility to specify criteria that can be used to search or sort the audit records residing in the audit trail. FAU_SAR.3 requires the administrators be able to establish the audit review criteria based on a userid and role so that the actions of a user can be readily identified and analyzed. Allowing the administrators to perform searches or sort the audit records based on dates and times provides the capability to facilitate the administrator's review of incidents that may have taken place at a certain time. It is important to note that the intent of sorting in this requirement is to allow the administrators the capability to organize or group the records associated with a given criteria.

Objective	Requirements Addressing the Objective	Rationale
O.CORRECT_ TSF_OPERATION The TOE will provide a capability to test the TSF to ensure the correct operation of the TSF in its operational environment	FPT_TST_(EXT).1, FPT_TST.1(1) FPT_TST.1(2)	O_CORRECT_TSF_OPERATION requires two security functional requirements in the FPT class, FPT_TST. These functional requirements provide the end user with the capability to ensure the TOE's security mechanisms continue to operate correctly in the field. FPT_TST_(EXT).1 has been created to ensure end user tests exist to demonstrate the correct operation of the security mechanisms required by the TOE that are provided by the hardware and that the TOE's software and TSF data has not been corrupted. Hardware failures could render a TOE's software ineffective in enforcing its security policies and this requirement provides the end user the ability to discover any failures in the hardware security mechanisms. FPT_TST.1(1) and FPT_TST.1(2) are necessary to ensure the correctness of the TSF software and TSF data. If TSF software is corrupted it is possible that the TSF would no longer be able to enforce the security policies. This also holds true for TSF data, if TSF data is corrupt the TOE may not correctly enforce its security policies.
O.CRYPTOGRAPHIC_FUNCTIONS 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.	FCS_BCM_(EXT).1	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. The level specifies the degree of testing of the module. The higher the level, the more extensive the module is tested.
	FCS_CKM.1(1)	FCS_CKM.1(1) is a requirement that a cryptomodule generate symmetric keys. Such keys are used by the TDEA or AES encryption/decryption functionality specified in FCS_COP.1(1).
	FCS_CKM.1(2)	FCS_CKM.1(2) is a requirement that a cryptomodule generate asymmetric keys. Such keys are used for cryptographic signatures as specified in FCS_COP.1(2).

Objective	Requirements Addressing the Objective	Rationale
	FCS_CKM.2	Key distribution (FCS_CKM.2) occurs when the key is transmitted from one entity to the TOE. If the entity is electronic and a protocol is used to distribute the key, it is referred to in the ST as "Key Transport". If the key is loaded into the TOE it can be loaded electronically (e.g., from a floppy drive, smart card, or electronic keyfill device) or manually (e.g., typed in). One or more of these methods must be selected.
	FCS_CKM.4	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_CKM_(EXT).2	FCS_CKM_(EXT).2 requires that keys are handled appropriately and associated with the correct entities, and that transfer of keys is done with error detection. Storage of persistent secret and private keys must be done in a secure fashion.
	FCS_COP.1(1)	FCS_COP.1(1) specifies that TDEA or AES be used to perform encryption and decryption operations.
	FCS_COP.1(2)	FCS_COP.1(2) gives three options for providing the digital signature capability; these requirements reference the appropriate standards for each digital signature option.
	FCS_COP.1(3)	FCS_COP.1(3) requires that the TSF provide hashing services using a NIST-approved implementation of the Secure Hash Algorithm
	FCS_COP.1(4)	FCS_COP.1(4) requires the TSF's message authentication services be compliant with either of the NIST-approved approaches, HMAC or CCM.
O.CRYPTOGRAPHY_ VALIDATED The TOE shall use NIST FIPS 140-2 validated cryptomodules for cryptographic services implementing FIPS-approved security functions and random number generation services	FCS_BCM_(EXT).1	FCS_BCM_(EXT).1 is an extended requirement that specifies not only that cryptographic functions that are FIPS-approved, but also what NIST FIPS rating level the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensive the module is tested.

Objective	Requirements Addressing the Objective	Rationale
used by cryptographic functions.	FCS_CKM.1(1) FCS_CKM.1(2)	FCS_CKM.1(1) and (2) mandate that the cryptomodule must generate keys, and that this key generation must be part of the FIPS-validated cryptomodule.
	FCS_COP_(EXT).1 FCS_COP.1(3)	FCS_COP_(EXT).1 and FCS_COP.1(3) are similar in that they require that any random number generation and hashing functions, respectively, are part of a FIPS-validated cryptographic module. These requirements do not mandate that the functionality is generally available, but only that it be implemented in a FIPS-validated module if other cryptographic functions need these services.
O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	FTA_TAB.1	FTA_TAB.1 meets this objective by requiring the TOE display a Security Administrator-defined banner before an administrator can establish an interactive session. This banner is under complete control of the Security Administrator.
O.IDS_AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events from targeted IT System resource(s) and associate those events with component that created the record.	FAU_GEN_(EXT).1	FAU_GEN_(EXT).1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the IDS Administrator has the ability to audit any IDS security relevant events that takes place in the targeted IT System resources. This requirement also defines the information that must be contained in the IDS audit record for each auditable event. There is a minimum set of information that must be present in every IDS audit record and this requirement defines that, as well as the additional information that must be recorded for each IDS auditable event.

Objective	Requirements Addressing the Objective	Rationale
	FAU_SEL.1-NIAP-0407(2)	FAU_SEL.1-NIAP-0407(2) allows the IDS Administrator to configure which IDS auditable events will be recorded in the IDS audit trail. This provides the IDS Administrator with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources consumed by the IDS audit mechanism and providing the ability to focus on the actions of an individual component. In addition, the requirement has been refined to require that the IDS audit event selection function is configurable during run-time to ensure the TOE is able to capture security-relevant events given changes in threat conditions.
O.IDS_AUDIT_REVIEW The TOE will provide the capability to selectively view IDS audit information, and alert the IDS Administrator of potential intrusions.	FAU_SAA_(EXT).1	FAU_SAA_(EXT).1 defines the analyses that indicate a potential intrusion and will generate an alarm and an analytical result to be created. The triggers for these analyses to occur are largely configurable by the IDS Administrator
	FAU_ARP.1(2)	FAU_ARP.1(2) requires that the alarm be displayed at the local IDS Administrative console(s) and at the remote IDS Administrative console(s) when IDS Administrative session(s) exists. For alarms at remote consoles, the alarm is sent either during an established session or upon session establishment (as long as the alarm has not been acknowledged). This is required to increase the likelihood that the alarm will be received as soon as possible. This requirement also dictates the information that must be displayed with the alarm. The potential intrusion is identified in the alarm, as are the analytical results of the events that accumulated and triggered the alarm. The analytical result is necessary, it allows the IDS Administrators to react to the potential intrusion without having to search through the IDS audit trail looking for the what analysis produced the alarm.

Objective	Requirements Addressing the Objective	Rationale
	FAU_ARP_ACK_(EXT).2	FAU_ARP_ACK_(EXT).2 requires that an intrusion alarm generated by the mechanism that implements the FAU_ARP requirement be maintained until an IDS Administrator acknowledges it. This ensures that the alarm message will not be obstructed and the IDS Administrators will be alerted of a potential intrusion. Additionally, this requires that the acknowledgement be transmitted to users that received the alarm, thus ensuring that that set of administrators knows that the user specified in the acknowledgement message has addressed the alarm.
	FAU_SAR.1(2)	FAU_SAR.1(2) is used to provide the IDS Administrator the capability to read all the IDS audit data contained in the IDS audit trail. This requirement also mandates the IDS audit information be presented in a manner that is suitable for the end user to interpret the IDS audit trail. It is expected that the IDS audit information be presented in such a way that the end user can examine an IDS audit record and have the appropriate information presented together to facilitate the analysis of the IDS audit review. Ensuring the IDS audit data are presented in an interpretable format will enhance the ability of the entity performing the analysis to identify potential intrusions.
	FAU_SAR.3(2)	FAU_SAR.3(2) complements FAU_SAR.1(2) by providing the IDS Administrators the flexibility to specify criteria that can be used to search or sort the IDS audit records residing in the IDS audit trail. FAU_SAR.3(2) requires the IDS Administrator be able to establish the IDS audit review criteria based on a component so that the events logged by the component can be readily identified and analyzed. Allowing the IDS Administrators to perform searches or sort the IDS audit records based on dates and times provides the capability to facilitate the IDS Administrator's review of incidents that may have taken place at a certain time. It is important to note that the intent of sorting in this requirement is to allow the IDS Administrators the capability to organize or group the records associated with a given criteria.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MOF.1(8)-IDS	FMT_MOF.1(8)-IDS restricts the ability to control the behavior of the IDS audit and alarm mechanism to the IDS Administrator. The IDS Administrator is the only user that controls the behavior of the events that generate alarms and whether the alarm mechanism is enabled or disabled.
O.MAINT_MODE The TOE shall provide a mode from which recovery or initial startup procedures can be performed.	FPT_RCV.2	This objective is met by using the FPT_RCV.2 requirement, which ensures that the TOE does not continue to operate in an insecure state when a hardware or software failure occurs. Upon the failure of the TSF self-tests the TOE will no longer be assured of enforcing its security policies. Therefore, the TOE enters a state that operations cease and requires an administrator to follow documented procedures that instruct them on to return the TOE to a secure state.
O.MANAGE The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_MSA.1-FW	FMT_MSA.1-FW provides the Security Administrator the capability to manipulate the security attributes of the objects in their scope of control that determine the information flow control policies.
	FMT_MSA.2	FMT_MSA.2 Ensures that the TSF will accept only secure values for security attributes.
	FMT_MSA.3(1) FMT_MSA.3(1)-FW FMT_MSA.3(2)-FW	FMT_MSA.3(1) and FMT_MSA.3(1)-FW together require 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_MSA.3(2)-FW requires that these services by default are disabled. Since the Security Administrator must explicitly enable these services it ensures the Security Administrator is aware that they are running. This requirement does afford the Security Administrator the capability to override this restrictive default and allow the services to be started whenever the TOE reboots or is restarted.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MOF.1(1)	FMT_MOF.1(1) is used to ensure the administrators have the ability to invoke the TOE self-tests at any time. The ability to invoke the self-tests is provided to all administrators. The Security Administrator is able to modify the behavior of the tests (e.g., select when they run, select a subset of the tests).
	FMT_MOF.1(2)	FMT_MOF.1(2) and FMT_MSA.3(2) are related to the services provided by FAU_UAU.1(1) and provide the Security Administrator control as to the availability of these services
	FMT_MOF.1(3)	FMT_MOF.1(3) specifies the ability of the administrators to control the security functions associated with audit and alarm generation. The ability to control these functions has been assigned to the appropriate administrative roles.
	FMT_MOF.1(4)	FMT_MOF.1(4) provides the administrators “read only” access to the audit records and prohibits access to all other users. Additionally, the administrators are provided the capability to “search and sort” audit on defined criteria. This capability expedites problem resolution analysis.
	FMT_MOF.1(5)	FMT_MOF.1(5) ensures that only an administrators can “enable or disable” the security alarms. This requirement works with FMT_MOF.1(5) to provide detailed granularity to the administrator when determining which actions constitute a security violation.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MOF.1(6)	FMT_MOF.1(6) This requirement limits the ability to manipulate the values that are used in the FRU_RSA.1 requirements to the Security Administrator. The Security Administrator is provided the capability to assign the network identifier(s) they wish to place resource restrictions on and allows them to also specify over what period of time those quota limitations are in place. FMT_MOF.1(6) provides the Security Administration configuration control of the allocation of connection-oriented TOE resources. This requirement provides the Security Administrator with a capability to thwart possible external "resource allocation" attacks on the TOE.
	FMT_MOF.1(6)-FW	FMT_MOF.1(6)-FW limits the ability to enable or disable unauthenticated TOE services for both IP based networks and non-IP based networks to the Security Administrator. These TOE services would be available to appropriate network users at the discretion of the Security Administrator.
	FMT_MOF.1(6)-IDS	FMT_MOF.1(6)-IDS allows only the IDS Administrator to view the IDS audit log. It also allows the IDS Administrator to search and sort through the IDS audit records based on certain criteria (e.g., time of day, component identifier, type of event).
	FMT_MOF.1(7)	FMT_MOF.1(7) provides the Security Administration configuration control of unsuccessful authentication attempts
	FMT_MOF.1(7)-IDS	FMT_MOF.1(7)-IDS allows the IDS Administrator to set which IDS auditable events are logged. This is done at run-time so the IDS Administrator can change the events based on particular threats.
	FMT_MOF.1(8)-IDS	FMT_MOF.1(8)-IDS restricts the capability of managing the behavior of the IDS alarms to the IDS Administrator

Objective	Requirements Addressing the Objective	Rationale
	FMT_MTD.1(1)	The requirement FMT_MTD.1(1) is intended to address TSF data that has not already been specified by other FMT requirements. This requirement specifies that the manipulation of these data be restricted to the security administrator.
	FMT_MTD.1(2)	FMT_MTD.1(2) provides the Cryptographic Administrator, and only the Cryptographic Administrator, the ability to modify the cryptographic security data.
	FMT_MTD.1(3)	FMT_MTD.1(3) provides the capability of setting the date and time that is used to generate time stamps to the Security Administrator or a trusted IT entity (authorized data manager). It is important to allow this functionality, due to clock drift and other circumstances, but the capability must be restricted. A trusted IT entity is allowed in the selection made by the ST author to take in account the use of an NTP server or some other service that provides time information without human intervention.
	FMT_MTD.1(4)	FMT_MTD.1(4) addresses the capabilities of data managers, who have responsibilities for security data management for sub-portions of the set of TSF data (for example, the platform clock time, sub-hierarchies of the directory). The scope of a data manager's responsibility is set by a security administrator, but they are expected to manage the entities in their scope of control without reliance on the security administrator.
	FMT_MTD.2(3)	FMT_MTD.2(3) restricts the specification of audit system storage capacity to the Security Administrator.
	FMT_REV.1	FMT_REV.1 is a management requirement that affords the Security Administrator the ability to revoke a user's authorizations on the TOE. It enables the Security Administrator to protect the TOE from unauthorized use of functions and facilities.

Objective	Requirements Addressing the Objective	Rationale
	FMT_SMF.1	The requirement FMT_SMF.1 was introduced as an international interpretation. This requirement specifies functionality that must be provided to administrators of the TOE.
O.MEDIATE_INFORMATION_FLOW The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself and also protect user data in accordance with its security policy.	FDP_IFC.1(1) FDP_IFC.1(2)	FDP_IFC.1(1), and FDP_IFC.1(2) define the subjects, information and the operations that are performed with respect to the two information flow policies. FDP_IFC.1(2) defines subjects for the unauthenticated access to any services the TOE provides. FDP_IFC.1(1), the subjects are the TOE's network interfaces. The information is defined as the network IP packets on which the TOE performs routing operations.
	FDP_IFF.1(1)	FDP_IFF.1(1) specifies the attributes on which unauthenticated information flow decisions are made.
	FDP_IFF.1(2)	FDP_IFF.1(2) provides the rules that apply to the unauthenticated use of any services provided by the TOE. ICMP is the only service that is required to be provided by the TOE, and the security attributes associated with this protocol allow the Security Administrator to specify what degree the ICMP traffic is mediated (i.e., the ICMP message type and code).
	FMT_REV.1-FW	FMT_REV.1 is a management requirement that affords the Security Administrator the ability to immediately revoke user's ability to send network traffic to or through the TOE.
O.PEER_AUTHENTICATION	FCS_IKE_(EXT).1	The O.PEER_AUTHENTICATION objective is satisfied by the requirement FCS_IKE_(EXT).1, which specifies that the TOE must implement the Internet Key Exchange protocol defined in RFC 2409.
O.PROTOCOLS The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or Industry specifications to ensure interoperability.	FPT_FLS.1 FPT_PRO_(EXT).1	The O.PROTOCOLS objective is satisfied by FPT_PRO_(EXT).1, which requires that the TOE be implemented with standardized protocols to ensure interoperability among peer TOEs. Implementing the standardized protocols will ensure that a secure state (FPT_FLS.1) of the TOE is maintained.

Objective	Requirements Addressing the Objective	Rationale
	FPT_TDC.1	FPT_TDC.1 supports O.PROTOCOL by specifying the use of BGP Open, Update, Notification and Keepalive Messages when sharing data between the TSF and another trusted IT product. FPT_TDC.1 provides further support by requiring the use of [RFC 4271] when interpreting data from another trusted IT product.
O.PROTECT_IN_TRANSIT The TSF shall protect TSF data when it is in transit between the TSF and another trusted IT entity.	FTP_TRP.1(1) FTP_TRP.1(2)	FTP_TRP.1(1) and FTP_TRP.1(2) will use cryptographic means to provide prevention of disclosure and detection of modification of TSF data.
O.REPLAY_DETECTION The TOE will provide a means to detect and reject the replay of authentication data and other TSF data and security attributes.	FPT_RPL.1	The O.REPLAY_DETECTION objective is satisfied by FPT_RPL.1, which requires the TOE to detect and reject the attempted replay of authentication data and security attributes from a remote user. This is sufficient to meet the objective because no untrusted users have local access to the TOE, thus there is no way to capture and replay authentication data or security attributes for a local session.
O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated.	FDP_RIP.2 FCS_CKM.4	FDP_RIP.2 is used to ensure the contents of resources are not available to subjects other than those explicitly granted access to the data. For this TOE it is critical that the memory used to build network packets is either cleared or that some buffer management scheme be employed to prevent the contents of a packet being disclosed in a subsequent packet (e.g., if padding is used in the construction of a packet, it must not contain another user's data or TSF data). FCS_CKM.4 applies to the destruction of cryptographic keys used by the TSF. This requirement specifies how and when cryptographic keys must be destroyed. The proper destruction of these keys is critical in ensuring the content of these keys cannot possibly be disclosed when a resource is reallocated to a user

Objective	Requirements Addressing the Objective	Rationale
O.RESOURCE_SHARING 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).	FRU_RSA.1 FMT_MTD.2(1)	While an availability security policy does not explicitly exist, FRU_RSA.1 was used to mitigate potential resource exhaustion attempts. It was used 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). This requirement allows the administrator to specify the time period in which when maximum quota (which is defined by the ST) is met or surpassed, an ST defined action is to take place, which is specified in FMT_MTD.2(1). These two requirements together help limit the resources that can be utilized by the general population of users as a whole. An issue with treating all the users the same is that legitimate users may not be able to establish connections due to the connection table entries being exhausted.
	FMT_MTD.2(2)	FRU_RSA.1 has the advantage of providing the Security Administrator with the ability to define the maximum number of resources a particular address or set of addresses can use over a specified time period. This requirement works in conjunction with FMT_MTD.2(2) which restricts the ability to set the quotas to the security administrator and allows for the ST author to assign what actions will take place once the quotas are met or surpassed.
	FMT_MOF.1 (6)	FMT_MOF.1(6) restricts the ability to assign the single network address or set of network addresses used in FRU_RSA.1 to the Security Administrator. This is in keeping with the TOE's notion of the Security Administrator is responsible for configuring the TOE's policy enforcement mechanisms.
O.ROBUST_TOE_ACCESS 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.	FIA_AFL.1-NIAP-0425	FIA_AFL.1-NIAP-0425 provides a detection mechanism for unsuccessful authentication attempts by remote users. The requirement enables a Security Administrator settable threshold that prevents unauthorized users from gaining access to authorized user's account by guessing authentication data by locking the targeted account, thus limiting an unauthorized user's ability to gain unauthorized access to the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FIA_ATD.1(1)	FIA_ATD.1(1) defines the attributes of users, including a userid that is used by the TOE to determine a user's identity and enforce what type of access the user has to the TOE (e.g., the TOE associates a userid with any role(s) they may assume).
	FIA_ATD.1(2)	FIA_ATD.1(2) defines the attributes of IT entities, including a subject ID that is used by the TOE to determine an entity's identity and enforce what type of access the entity has to the TOE.
	FIA_UAU.1-FW	FIA_UAU.1-FW contributes to this objective by limiting the services that are provided by the TOE to unauthenticated users. Management requirements and the unauthenticated information flow policy requirement provide additional control on these services.
	FIA_UID.2	FIA_UID.2 plays a small role in satisfying this objective by ensuring that every user is identified before the TOE performs any mediated functions.
	FIA_UAU_(EXT).2 FIA_UAU_(EXT).5	FIA_UAU.2 requires that administrators and authorized IT entities authenticate themselves to the TOE before performing any TSF-mediated actions. In order to control logical access to the TOE an authentication mechanism is required. The extended requirement FIA_UAU_(EXT).5 mandates that the TOE provide a local authentication mechanism.
	FTA_TSE.1	FTA_TSE.1.1 contributes to this objective by limiting a user's ability to logically access the TOE. This requirement provides the Security Administrator the ability to control when (e.g., time and day(s) of the week) and where (e.g., from a specific network address) remote administrators, as and authorized IT entities can access the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FTA_SSL.1-FW/IDS FTA_SSL.2-FW/IDS FTA_SSL.3(1) FTA_SSL.3(2)	The FTA_SSL family partially satisfies the O.ROBUST_TOE_ACCESS objective by ensuring that user's sessions are afforded some level of protection. FTA_SSL.3 takes into account remote sessions. After a Security Administrator defined time interval of inactivity remote sessions will be terminated. This includes user remote administrative sessions. This component is especially necessary; since remote sessions are not typically afforded the same physical protections those local sessions are provided.
O.TIME_STAMPS The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	FPT_STM.1	FPT_STM.1 requires that the TOE be able to provide reliable time stamps for its own use and therefore, partially satisfies this objective. Time stamps include date and time and are reliable in that they are always available to the TOE, and the clock must be monotonically increasing.
	FMT_MTD.1(3)	FMT_MTD.1(3) satisfies the rest of this objective by providing the capability to set the time used for generating time stamps to either the Security Administrator, authorized IT entity, or both.

Objective	Requirements Addressing the Objective	Rationale
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.	FTP_TRP.1(1) FTP_TRP.1(2)	FTP_TRP.1.1 requires the TOE to provide a mechanism that creates a distinct communication path that protects the data that traverses this path from disclosure or modification. This requirement ensures that the TOE can identify the end points and ensures that a user cannot insert themselves between the user and the TOE, by requiring that the means used for invoking the communication path cannot be intercepted and allow a “man-in-the-middle-attack” (this does not prevent someone from capturing the traffic and replaying it at a later time – see FPT_RPL.1). Since the user invokes the trusted path (FTP_TRP.1.2) mechanism they can be assured they are communicating with the TOE. FTP_TRP.1.3 mandates that the trusted path be the only means available for providing identification and authentication information, therefore ensuring a user’s authentication data will not be compromised when performing authentication functions. Furthermore, the remote administrator’s communication path is encrypted during the entire session.
	FTP_ITC.1(1) FTP_ITC.1(2)	FTP_ITC.1(1) and FTP_ITC.1(2) are similar to FTP_TRP.1(1) and FTP_TRP.1(2), in that they require a mechanism that creates a distinct communication path with the same characteristics, however FTP_ITC.1(1) and FTP_ITC.1(2) is used to protect communications between IT entities, rather than between a human user and an IT entity. FTP_ITC.1.3 requires the TOE to initiate the trusted channel, which ensures that the TOE has established a communication path with an authorized IT entity and not some other entity pretending to be an authorized IT entity.

`Table 18 - TOE Security Objectives

7.5 Rationale for Extended Requirements

The following table presents the rationale for the inclusion of the extended functional requirements found in this Security Target. The extended requirements that are included as NIAP interpretations do not require a rationale for their inclusion per CCEVS management.

SFR	DESCRIPTION	RATIONALE
FAU_ARP_ACK_(EXT).1 FAU_ARP_ACK_ (EXT).2-IDS	Security alarm acknowledgement	This extended requirement is necessary since a CC requirement does not exist to ensure an administrator will be aware of the alarm. The intent is to ensure that if an administrator is logged in and not physically at the console or remote workstation the message will remain displayed until the administrators have acknowledged it. The message will not be scrolled off the screen due to other activity-taking place (e.g., the auditor is running an audit report).
FAU_GEN_(EXT).1-IDS	Audit data generation -- IDS audit records	This extended requirement is created to capture security functionality specific to the IDS TOE. The CC requires more in FAU_GEN.1 than is needed here.
FAU_SAA_(EXT).1-IDS	Analyzing capability intrusion analysis	This extended requirement in necessary because the CC does not provide a means to perform analyses and what information must be contained in the analytical result.
FCS_BCM_(EXT).1	Baseline Cryptographic Module	The CC does not provide a means of specifying a cryptographic module baseline for implementations developed in hardware, in software, or in hardware/software combinations. FCS_BCM_(EXT).1 provides for the specification of the required FIPS certification based on the implementation baseline.
FCS_CKM_(EXT).2	Cryptographic Key Handling and Storage	The CC does not provide components for key handling and storage. Key access and key destruction components do not address keys being transferred within the device nor key archiving when key is not in use. FCS_CKM_(EXT).2 addresses internal key transfer and archiving. It also addresses the handling of storage areas where keys reside.
FCS_COP_(EXT).1	Random Number Generation	The CC cryptographic operation components are focused on specific algorithm types and operations requiring specific key sizes. The generation of random numbers can be better stated as an extended component. Neither algorithms nor keys are required to generate random numbers. Random number generators can use any combination of software-based or hardware-based inputs as long as the RNG/PRNG design requirements are met and the required RNG/PRNG tests are successful.

SFR	DESCRIPTION	RATIONALE
FCS_IKE_(EXT).1	Internet Key Exchange	This extended requirement is necessary since the CC does not include requirements for this specific key enchange protocol. This protocol is specified in RFC 2409, but there are specific configurable setting that must be specified that are documented in the extended requirement.
FIA_UAU_(EXT).2-FW	Specified User authentication before any action	Extends FIA_UAU.1.2 to enforce all user actions be mediated. The requirement is levied to clearly enforce the user set required to authenticate to the TOE. Note that the authentication is required only when the specified user is performing a function related to the authentication; for instance, if a user that happens to be an administrator wants to utilize an unauthenticated service from the list in FIA_UAU.1.1(1), they are not required to authenticate to that service.
FIA_UAU_(EXT).5	Authentication mechanism	This extended requirement is needed for local administrators because there is no CC requirement that requires the TSF provide authentication. Because this ST allows the IT environment to provide an authentication server to be used for the single-use authentication mechanism for remote users, it is important to specify that the TSF provide the means for local administrator authentication in case the TOE cannot communicate with the authentication server.
FPT_PRO_(EXT).1	Standard protocol usage	This extended requirement is necessary since the CC does not provide requirements of choosing a standard protocol mechanism from the standard protocols being used by a particular IT product .
FPT_TST_(EXT).1	TSF testing	This extended requirement is necessary to capture the notion of the TOE to verify the integrity of the TSF software. Additionally, the TSF data set that is subject to these tests was reduced to address the notion that it does not make sense to test the integrity of some TSF data (e.g., audit data) and this extended requirement address that.

Table 19 - Statement of Security Requirement Consistency

8 Audit Events

Audit Events

The table below maps security requirements to auditable events and audit record contents, in support of FAU_GEN.1.1-NIAP-0429.

REQUIREMENT	AUDITABLE EVENTS	AUDIT RECORD CONTENTS
FAU_ARP.1 (1)	Actions taken due to potential security violations.	Identification of what caused the generation of the alarm.
FAU_ARP.1 (2)-IDS	Actions taken due to imminent security intrusions.	Identification of what caused the generation of the alarm.
FAU_ARP_ACK_(EXT).1	Acknowledgement of alarm.	The identity of the administrator that acknowledged the alarm.
FAU_ARP_ACK_(EXT).2-IDS	Acknowledgement of alarm.	The identity of the IDS Administrator that acknowledged the alarm.
FAU_GEN.1-NIAP-0429	None.	
FAU_GEN.2-NIAP-0410	None.	
FAU_GEN_(EXT).1-IDS	None.	
FAU_SAA.1-NIAP-0407	a) Enabling and disabling of any of the analysis mechanisms; b) Automated responses performed by the tool.	The identity of the Security Administrator performing the function.
FAU_SAA_(EXT).1-IDS	a) Enabling and disabling of any of the analysis mechanisms; b) Automated responses performed by the tool.	The identity of the IDS Administrator performing the function.
FAU_SAR.1(1)	Reading of information from the audit records.	The identity of the Audit Administrator performing the function.
FAU_SAR.1(2)-IDS	Reading of information from the IDS audit records.	The identity of the IDS Administrator performing the function.
FAU_SAR.2(1)	Unsuccessful attempts to read information from the audit records.	The identity of the administrator performing the function.
FAU_SAR.2(2)-IDS	Unsuccessful attempts to read information from the audit records.	The identity of the IDS Administrator performing the function.
FAU_SAR.3(1)	None.	
FAU_SAR.3(2)-IDS	None.	
FAU_SEL.1-NIAP-0407(1)	All modifications to the audit configuration that occur while the audit collection functions are operating.	The identity of the Security Administrator performing the function.

REQUIREMENT	AUDITABLE EVENTS	AUDIT RECORD CONTENTS
FAU_SEL.1-NIAP-0407(2)-IDS	All modifications to the audit configuration that occur while the audit collection functions are operating.	The identity of the IDS Administrator performing the function.
FAU_STG.NIAP-0414-1-NIAP-0429(1)	Actions taken due to the audit storage failure.	The identity of the Security Administrator performing the function.
FAU_STG.NIAP-0414-1-NIAP-0429(2)-IDS	Actions taken due to the IDS audit storage failure.	The identity of the IDS Administrator performing the function.
FAU_STG.1-NIAP-0429	None.	
FAU_STG.2-NIAP-0429-IDS	None.	
FAU_STG.3	Actions taken due to exceeding the audit threshold.	The identity of the Security Administrator performing the function.
FCS_BCM_(EXT).1	None.	
FCS_CKM.1(1)	a) Failure of the activity; b) Generation and loading of key.	Identify the failed activity and the data that caused the failure.
FCS_CKM.1(2)	a) Failure of the activity; b) Generation and loading of key pair for digital signatures.	Identify the failed activity and the data that caused the failure.
FCS_CKM.2	a) Failure of the activity; b) Generation and loading of key.	Identify the failed activity and the data that caused the failure.
FCS_CKM.4	a) Failure of the activity; b) Generation and loading of key.	Identify the failed activity and the data that caused the failure.
FCS_CKM_(EXT).2	a) Failure of the activity; b) Generation and loading of key.	Identify the failed activity and the data that caused the failure.
FCS_COP.1(1)	Failure of cryptographic operation.	Type of cryptographic operation. Any applicable cryptographic mode(s) of operation, excluding any sensitive information.
FCS_COP.1(2)	Failure of cryptographic operation.	Type of cryptographic operation Any applicable cryptographic mode(s) of operation, excluding any sensitive information.
FCS_COP.1(3)	Failure of cryptographic operation.	Type of cryptographic operation. Any applicable cryptographic mode(s) of operation, excluding any sensitive information.

REQUIREMENT	AUDITABLE EVENTS	AUDIT RECORD CONTENTS
FCS_COP.1(4)	Failure of cryptographic operation.	Type of cryptographic operation. Any applicable cryptographic mode(s) of operation, excluding any sensitive information.
FCS_COP_(EXT).1	Failure of cryptographic operation	Type of cryptographic operation. Any applicable cryptographic mode(s) of operation, excluding any sensitive information.
FCS_IKE_(EXT).1	If failure occurs, record descriptive reason for the failure.	a) Generation and loading of key pair for digital signatures; b) Changes to the pre-shared key used for authentication; c) All modifications to the key lifetimes; d) Failure of the authentication in If failure occurs, record a descriptive reason for the failure. Phase 1; e) Failure to negotiate a security association in Phase 2.
FDP_IFC.1(1)	None.	
FDP_IFC.1(2)	None.	

REQUIREMENT	AUDITABLE EVENTS	AUDIT RECORD CONTENTS
FDP_IFF.1(1)	a) Decisions to permit/deny information flows; b) Failure to reassemble fragmented packets	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 firewall interface associated on which the TOE received the packet Identity of the rule that allowed or disallowed the packet flow Reason why fragmented packets could not be reassembled (i.e., invalid fragment identifier, invalid offset, invalid fragment data length)
FDP_IFF.1(2)	Decisions to permit or deny information flows.	Presumed identity of source subject.
FDP_RIP.2	None	
FIA_AFL.1-NIAP-0425-IDS	a) The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g., disabling of an account) taken and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal).	a) Identity of the unsuccessfully authenticated user. b) The actions (e.g., disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal).
FIA_ATD.1(1)	None.	
FIA_ATD.1(2)	None.	

REQUIREMENT	AUDITABLE EVENTS	AUDIT RECORD CONTENTS
FIA_ATD.1(3)-IDS	None.	
FIA_UAU.1-FW	All use of authentication mechanisms	Claimed identity of the user using the authentication mechanism
FIA_UAU_(EXT).2-FW	Successful and unsuccessful use of authentication mechanisms	Claimed identity of the user using the authentication mechanism
FIA_UAU_(EXT).5	a) The final decision on authentication; b) The result of each activated mechanism together with the final decision.	Claimed identity of the user attempting to authenticate.
FIA_UID.2(1)	a) Unsuccessful use of the user identification mechanism, including the user identity provided; b) All use of the user identification mechanism, including the user identity provided (that is, those that authenticate to the TOE).	Claimed identity of the user using the identification mechanism.
FIA_USB.1(1)	Success and failure of binding of user security attributes to a subject (e.g., success and failure to create a subject).	The identity of the user whose attributes are attempting to be bound.
FMT_MOF.1(1)	All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the function, the function being performed and the data being used to perform the function (if available).
FMT_MOF.1(2)	a) Enabling or disabling of the key-generation self-tests. b) All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the function, the function being performed and the data being used to perform the function (if available).
FMT_MOF.1(3)	All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the function, the function being performed and the data being used to perform the function (if available).
FMT_MOF.1(4)	All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the function, the function being performed and the data being used to perform the function (if available).
FMT_MOF.1(5)	All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the function, the function being performed and the data being used to perform the function (if available).

REQUIREMENT	AUDITABLE EVENTS	AUDIT RECORD CONTENTS
FMT_MOF.1(6)	All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the function, the function being performed and the data being used to perform the function (if available).
FMT_MOF.1(6)-FW	All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the function, the function being performed and the data being used to perform the function (if available).
FMT_MOF.1(6)-IDS	All modifications in the behavior of the functions in the TSF.	The identity of the IDS Administrator performing the function
FMT_MOF.1(7)	All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the function, the function being performed and the data being used to perform the function (if available).
FMT_MOF.1(7)-IDS	All modifications in the behavior of the functions in the TSF.	The identity of the IDS Administrator performing the function.
FMT_MOF.1(8)-IDS	All modifications in the behavior of the functions in the TSF.	The identity of the IDS Administrator performing the function.
FMT_MSA.2	All offered and rejected values for a security attribute.	The identity of the administrator performing the function
FMT_MSA.1-FW	All modifications of the values of security attributes	The identity of the administrator performing the function
FMT_MSA.3(1)	a) Modifications of the default setting of permissive or restrictive rules; b) All modifications of the initial values of security attributes.	The identity of the administrator performing the function, the function being performed and the security attributes being used to perform the function (if available).
FMT_MSA.3-NIAP-0409(1)-FW	a) Modifications of the default setting of permissive or restrictive rules; b) All modifications of the initial values of security attributes.	The identity of the administrator performing the function, the function being performed and the security attributes being used to perform the function (if available).
FMT_MSA.3-NIAP-0409(2)-FW	a) Modifications of the default setting of permissive or restrictive rules; b) All modifications of the initial values of security attributes.	The identity of the administrator performing the function, the function being performed and the security attributes being used to perform the function (if available).
FMT_MTD.1(1)	All modifications of the values of TSF data by the administrator.	The identity of the administrator performing the function, the function being performed and the values of TSF data being modified during the performance the function (if available).

REQUIREMENT	AUDITABLE EVENTS	AUDIT RECORD CONTENTS
FMT_MTD.1(2)	All modifications of the values of cryptographic security data by the cryptographic administrator.	The identity of the administrator performing the function, the function being performed and the values of TSF data being modified during the performance the function (if available).
FMT_MTD.1(3)	All modifications to the time and date used to form the time stamps by the administrator.	The identity of the administrator performing the function, the function being performed the values of data being modified and the modifying data used during the performance the function.
FMT_MTD.1(4)	All modifications to the information flow policy ruleset by the Security Administrator.	The identity of the administrator performing the function, the function being performed the values of data being modified and the modifying data used during the performance the function.
FMT_MTD.2(1)	a) All modifications of the limits on TSF data b) All modifications in the actions to be taken in case of violation of the limits.	The identity of the administrator performing the function, the function being performed the values of data being modified and the modifying data used during the performance the function.
FMT_MTD.2(2)	a) All modifications of the limits on TSF data. b) All modifications in the actions to be taken in case of violation of the limits.	The identity of the administrator performing the function, the function being performed the values of data being modified and the modifying data used during the performance the function.
FMT_MTD.2(3)	a) All modifications of the limits on TSF data. b) All modifications in the actions to be taken in case of violation of the limits.	The identity of the administrator performing the function, the function being performed the values of data being modified and the modifying data used during the performance the function.
FMT_REV.1	a) Unsuccessful revocation of security attributes; b) All attempts to revoke security attributes.	List of security attributes that were attempted to be revoked. The identity of the administrator performing the function.
FMT_REV.1-FW	All attempts to revoke security attributes	List of security attributes that were attempted to be revoked The identity of the administrator performing the function
FMT_SMF.1	Use of the management functions.	The identity of the administrator performing the function. Identify the management function being performed

REQUIREMENT	AUDITABLE EVENTS	AUDIT RECORD CONTENTS
FMT_SMR.2	a) Modifications to the group of users that are part of a role; b) Unsuccessful attempts to use a role due to given conditions on the roles.	User IDs which are associated with the modifications. The identity of the administrator performing the function.
FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FPT_PRO_(EXT).1	None.	
FPT_RCV.2	a) The fact that a failure or service discontinuity occurred; b) Resumption of the regular operation; c) Type of failure or service discontinuity.	Identify the failure, and that the TSF was able to recover to a secure state. If it is not possible to recover, enter maintenance mode.
FPT_RPL.1 (including replay of authentication data notification from the authentication server)	Detected replay attacks.	Identity of the user that was the subject of the reply attack
FPT_STM.1	Changes to the time.	Identify that the time has been changed and the administrator that took the action.
FPT_TDC.1	a) Use of the TSF data consistency mechanisms b) Identification of which TSF data have been interpreted c) Detection of modified TSF data	BGP routing protocol Open, Update, Notification, and Keepalive messages.
FPT_TST_(EXT).1	Execution of this set of TSF self tests and the results of the tests.	The identity of the administrator performing the test, if initiated by an administrator. Report any results from the test.
FPT_TST.1(1)	Execution of this set of TSF self tests for Cryptography and the results of the tests.	The identity of the administrator performing the test, if initiated by an administrator. Report any results from the test.
FPT_TST.1(2)	Execution of this set of TSF self tests for key generation and the results of the tests.	The identity of the administrator performing the test, if initiated by an administrator. Report any results from the test.
FRU_RSA.1	a) Rejection of allocation operation due to resource limits. b) All attempted uses of the resource allocation functions for resources that are under control of the TSF.	Identify the controlled resources (controlled connection-oriented resources) that caused the rejection, and the user.

REQUIREMENT	AUDITABLE EVENTS	AUDIT RECORD CONTENTS
FTA_SSL.1-FW/IDS	Locking of an interactive session by the session locking mechanism. Any attempts at unlocking of an interactive session.	The identity of the user associated with the session being locked or unlocked.
FTA_SSL.2-FW/IDS	Locking of an interactive session by the session locking mechanism. Any attempts at unlocking of an interactive session.	The identity of the user associated with the session being locked or unlocked.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	The identity of the user associated with the session that was terminated.
FTA_TAB.1	None.	
FTA_TSE.1	a) Denial of a session establishment due to the session establishment mechanism. b) All attempts at establishment of a user session.	The identity of the user attempting to establish the session. For unsuccessful attempts, the reason for denial of the establishment attempt.
FTP_ITC.1(1)	a) Failure of the trusted channel functions. b) Identification of the initiator and target of failed trusted channel functions. c) All attempted uses of the trusted channel functions. d) Identifier of the initiator and target of all trusted channel functions.	Indicated that the trusted channel failed and identification of the initiator and target of all trusted channels.
FTP_ITC.1(2)	a) Failure of the trusted channel functions. b) Identification of the initiator and target of failed trusted channel functions. c) All attempted uses of the trusted channel functions. d) Identifier of the initiator and target of all trusted channel functions.	Indicated that the trusted channel failed and identification of the initiator and target of all trusted channels.

REQUIREMENT	AUDITABLE EVENTS	AUDIT RECORD CONTENTS
FPT_TRP.1(1)	a) Failure of the trusted channel functions. b) Identification of the user associated with all trusted path failures, if available. c) All attempted uses of the trusted path functions. d) UIdentification of the user associated with all trusted path invocations, if available.	Indicated that the trusted channel failed and Identification of the claimed user identity.
FPT_TRP.1(2)	a) Failure of the trusted channel functions. b) Identification of the user associated with all trusted path failures, if available. c) All attempted uses of the trusted path functions. d) UIdentification of the user associated with all trusted path invocations, if available.	Indicated that the trusted channel failed and Identification of the claimed user identity.

Table 20 - Audit Events

9 Appendices

Section 9 of this document contains the appendices that accompany the Security Target and provide clarity and/or explanation for the reader.

9.1 References

Common Criteria for Information Technology Security Evaluation, CCMB-2006-09, Version 3.1, September 2006.

Consistency Instruction Manual for Development of US Government Protection Profiles for Medium Robustness Environments, Release 2.0, March 1, 2004.

Federal Information Processing Standard Publication (FIPS-PUB) 140-2, Security Requirements for Cryptographic Modules, May 25, 2001. (Change notice (12-03-2002))

Federal Information Processing Standard Publication (FIPS-PUB) 197, Advanced Encryption Standard (AES), November 2001.

Internet Engineering Task Force, ESP CBC-Mode Cipher Algorithms, RFC 2451, November 1998.

Internet Engineering Task Force, Internet Key Exchange (IKE), RFC 2409, November 1998.

Internet Engineering Task Force, IP Encapsulating Security Payload (ESP), RFC 2406, November 1998.

Internet Engineering Task Force, Use of HMAC-SHA-1-96 within ESP and AH, RFC 2404, November 1998.

NSA Glossary of Terms Used in Security and Intrusion Detection, Greg Stocksdale, NSA Information Systems Security Organization, April 1998.

The AES Cipher Algorithm and Its Use with IPsec <draft-ietf-ipsec-ciph-aes-cbc.03.txt>, Internet draft, November 2001.

9.2 Glossary

Access – Interaction between an entity and an object that results in the flow or modification of data.

Access Control – Security service that controls the use of resources and the disclosure and modification of data.

Accountability – Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Active – (scanning capability) – to gain understanding of the IT environment through means that illuminate the environment being scanned.

Administrator – A user who has been specifically granted the authority to manage some portion or the entire TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Assurance – A measure of confidence that the security features of an IT system are sufficient to enforce its' security policy.

Asymmetric Cryptographic System – A system involving two related transformations; one determined by a public key (the public transformation), and another determined by a private key (the private transformation) with the property that it is computationally infeasible to determine the private transformation (or the private key) from knowledge of the public transformation (and the public key).

Asymmetric Key – The corresponding public/private key pair needed to determine the behavior of the public/private transformations that comprise an asymmetric cryptographic system

Attack – An intentional act attempting to violate the security policy of an IT system.

Authenticated User - An administrative user who has accessed a computer system with a valid identifier and authentication combination.

Authentication – Security measure that verifies a claimed identity.

Authentication data – Information used to verify a claimed identity.

Authorization – Permission, granted by an entity authorized to do so, to perform functions and access data.

Authorized IT Entity - A certificate or ntp server; or peer TOE.

Authorized user – An authenticated administrative user who may, in accordance with the TSP, perform an operation.

Availability – Timely, reliable access to IT resources.

Component – A single scanning capability, sensing capability or analyzing capability, operating within the TOE configuration

Compromise – Violation of a security policy.

Confidentiality – A security policy pertaining to disclosure of data.

Critical Security Parameters (CSP) – Security-related information (e.g., cryptographic keys, authentication data such as passwords and pins, and cryptographic seeds) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.

Cryptographic Administrator – An authorized user who has been granted the authority to perform cryptographic initialization and management functions. These users are expected to use this authority only in the manner prescribed by the guidance given to them.

Cryptographic boundary – An explicitly defined contiguous perimeter that establishes the physical bounds (for hardware) or logical bounds (for software) of a cryptographic module.

Cryptographic key (key) – A parameter used in conjunction with a cryptographic algorithm that determines:

- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data, or
- a digital authentication code computed from data.

Cryptographic Module – The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Cryptographic Module Security Policy – A precise specification of the security rules under which a cryptographic module must operate, including the rules derived from the requirements of this PP and additional rules imposed by the vendor.

Defense-in-Depth (DID) – A security design strategy whereby layers of protection are utilized to establish an adequate security posture for an IT system.

Discretionary Access Control (DAC) – A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. Those controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Embedded Cryptographic Module – On that is built as an integral part of a larger and more general surrounding system (i.e., one that is not easily removable from the surrounding system).

Enclave – A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.

Entity – A subject, object, user or another IT device, which interacts with TOE objects, data, or resources.

External IT entity – Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.

Identity – A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Integrity – A security policy pertaining to the corruption of data and TSF mechanisms.

Integrity level – The combination of a hierarchical level and an optional set of non-hierarchical categories that represent the integrity of data.

Intrusion – Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusion Detection – Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

Intrusion Detection System (IDS) – A combination of one or more sensing capabilities, and one or more analyzing capabilities and an optional but recommended scanning capability that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.

Intrusion Detection System Analyzing Capability – The components of an IDS that accepts data from sensing capabilities and scanning capabilities and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future).

Intrusion Detection System Data (IDS data) – Data collected and produced by the IDS functions. This could include digital signatures, policies, permissions, and IDS audit data.

Intrusion Detection System Sensing Capability – The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources.

Mandatory Access Control (MAC) – A means of restricting access to objects based on subject and object sensitivity labels.

Mandatory Integrity Control (MIC) – A means of restricting access to objects based on subject and object integrity labels.

Multilevel – The ability to simultaneously handle (e.g., share, process) multiple levels of data, while allowing users at different sensitivity levels to access the system concurrently. The system permits each user to access only the data to which they are authorized access.

Named Object – An object that exhibits all of the following characteristics:

- The object may be used to transfer information between subjects of differing user identities within the TSF.
- Subjects in the TOE must be able to require a specific instance of the object.
- The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to require the same instance of the object.

Non-Repudiation – A security policy pertaining to providing one or more of the following:

- To the sender of data, proof of delivery to the intended recipient,
- To the recipient of data, proof of the identity of the user who sent the data.

Object – An entity within the TSC that contains or receives information and upon which subjects perform operations.

Operating Environment – The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

Operating System (OS) – An entity within the TSC that causes operations to be performed. Subjects can come in two forms: trusted and untrusted. Trusted subjects are exempt from part or all of the TOE security policies. Untrusted subjects are bound by all TOE security policies.

Operational key – Key intended for protection of operational information or for the production or secure electrical transmissions of key streams

Passive – (sensing capability) – To gain understanding of the IT environment through means that do not effect or impact the environment being sensed.

Packet Contents - IP packets are composed of a header and payload. The IPv4 packet header consists of:

1. 4 bits that contain the *version*, that specifies if it's an IPv4 or IPv6 packet,
2. 4 bits that contain the *Internet Header Length*, which is the length of the header in multiples of 4 bytes (e.g., 5 means 20 bytes).
3. 8 bits that contain the *Type of Service*, also referred to as Quality of Service (QoS), which describes what priority the packet should have,
4. 16 bits that contain the *length* of the packet in bytes,
5. 16 bits that contain an *identification tag* to help reconstruct the packet from several fragments,
6. 3 bits. The first contains a zero, followed by a flag that says whether the packet is allowed to be *fragmented* or not (DF: Don't fragment), and a flag to state whether more fragments of a packet follow (MF: More Fragments)
7. 13 bits that contain the *fragment offset*, a field to identify position of fragment within original packet
8. 8 bits that contain the Time to live (TTL), which is the number of hops (router, computer or device along a network) the packet is allowed to pass before it dies (for example, a packet with a TTL of 16 will be allowed to go across 16 routers to get to its destination before it is discarded),
9. 8 bits that contain the *protocol* (TCP, UDP, ICMP, etc.)
10. 16 bits that contain the *Header Checksum,* a number used in error detection,
11. 32 bits that contain the *source IP address*,
12. 32 bits that contain the *destination address*.

After those 160 bits, optional flags can be added of varied length, which can change based on the protocol used, then the data that packet carries is added. An IP packet has no trailer. However, an IP packet is often carried as the payload inside an Ethernet frame, which has its own header and trailer.

Peer TOEs – Mutually authenticated TOEs that interact to enforce a common security policy.

Public Object – An object for which the TSF unconditionally permits all entities “read” access. Only the TSF or authorized administrators may create, delete, or modify the public objects.

Release Train -- The technique of planning software releases on regular or cyclic time period, for example, the last day of every quarter, or every 9 weeks, etc. The "train" metaphor of a release train is likely based on the concept of railroad train schedules (planned arrival and departure times) and that trains carry multiple types of rolling stock (different types of features are included in a release).

Remote Administrator - any authenticated user with elevated privileges capable of monitoring and/or controlling a device over a network, be it local or wide area.

Robustness – A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. DoD has three levels of robustness:

- Basic: Security services and mechanisms that equate to good commercial practices.
- Medium: Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.
- High: Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

Secure State – Condition in which all TOE security policies are enforced.

Security attributes – TSF data associated with subjects, objects, and users that are used for the enforcement of the TSP.

Security level – The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity of the information.

Sensitivity label – A security attribute that represents the security level of an object and that describes the sensitivity (e.g., Classification) of the data in the object. Sensitivity labels are used by the TOE as the basis for mandatory access control decision.

Split key – A variable that consists of two or more components that must be combined to form the operation key variable. The combining process excludes concatenation or interleaving of component variables.

Subject – An entity within the TSC that causes operation to be performed.

Symmetric key – A single, secret key used for both encryption and decryption in symmetric cryptographic algorithms.

Threat – Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

Threat Agent – Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorized operation with the TOE.

User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Vulnerability – A weakness that can be exploited to violate the TOE security policy.

9.3 Acronyms

TERM	DEFINITION
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Program Interface
ATM	Asynchronous Transfer Method
BGP	Border Gateway Protocol
CC	Common Criteria version 3.1
CCEVS	Common Criteria Evaluation Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CLNP	Connectionless Network Protocol
CLNS	Connectionless Network Service
CM	Configuration Management
CSP	Cryptographic security parameter
DES	Data Encryption Standard
DH	Diffie Hellman
DMZ	Demilitarized Zone
DoD	Department of Defense
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FIPS-PUB 140-2	Federal Information Processing Standard Publication
FTP	File Transfer Protocol
GIG	Global Information Grid
GUI	Graphical User Interface
HMAC	Keyed-Hash Authentication Code
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IATF	Information Assurance Technical Framework
ICMP	Internet Control Message Protocol
ID	Identification
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPsec ESP	Internet Protocol Security Encapsulating Security Payload
IPv6	Internet Protocol Version 6
IPX	Internetwork Packet Exchange

TERM	DEFINITION
ISAKMP	Internet Security Association and Key Management Protocol
IS-IS	Intermediate System-to-Intermediate System
ISO	International Organization for Standardization
IT	Information Technology
Junos	Juniper Operating System
LDP	Label Distribution Protocol
MAC	Mandatory Access Control
MRE	Medium Robustness Environment
NAT	Network Address Translation
NBIAT&S	Network Boundary Information Assurance Technologies and Solutions Support
NIAP	National Information Assurance Program
NIST	National Institute of Standards Technology
NSA	National Security Agency
NTP	Network Time Protocol
OSI	Open Systems Interconnect
OSP	Organizational Security Policy
OSPF	Open Shortest Path First
PFE	Packet Forwarding Engine
PIC/PIM	Physical Interface Card/Module
PKI	Public Key Infrastructure
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RE	Routing Engine
RFC	Request for Comment
RIP	Routing Information Protocol
RNG	Random Number Generator
RNG	Random Number Generator
RSA	Rivest, Shamir, Adelman
SA	Security Association
SCEP	Simple Certificate Enrollment Protocol
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol

TERM	DEFINITION
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TBD	To Be Determined
TCP/IP	Transmissions Control Protocol/ Internet Protocol
TDEA	Triple Data Encryption Algorithm
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSFI	TSF interfaces
TSP	TOE Security Policy
TTAP/CCEVS	Trust Technology Assessment Program/ Common Criteria Evaluation Standard Scheme
UDP	User Datagram Protocol
URL	Uniform Research Locator
VPN	Virtual Private Network

Table 21 - Acronyms Used in the Security Target