



Security Target

Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series

Document Version 1.5

Rev A

December 22, 2011

Prepared For:

Prepared By:



Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

www.juniper.net



Apex Assurance Group, LLC

530 Lytton Ave, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), JUNOS-FIPS 10.4R4 for SRX Series. 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

1	Introduction	5
1.1	<i>ST Reference</i>	<i>5</i>
1.2	<i>TOE Reference</i>	<i>5</i>
1.3	<i>About This ST Document</i>	<i>5</i>
1.3.1	<i>Document Organization</i>	<i>5</i>
1.3.2	<i>Document Conventions</i>	<i>6</i>
1.3.3	<i>Document Terminology</i>	<i>6</i>
1.4	<i>TOE Overview</i>	<i>7</i>
1.5	<i>TOE Description</i>	<i>7</i>
1.5.1	<i>Logical Boundary</i>	<i>12</i>
2	Conformance Claims	14
2.1	<i>CC Conformance Claim</i>	<i>14</i>
2.2	<i>PP Claim</i>	<i>14</i>
2.3	<i>Package Claim</i>	<i>14</i>
2.4	<i>Conformance Rationale</i>	<i>14</i>
3	Security Problem Definition	15
3.1	<i>Threats</i>	<i>15</i>
3.2	<i>Organizational Security Policies</i>	<i>17</i>
3.3	<i>Assumptions</i>	<i>18</i>
4	Security Objectives	19
4.1	<i>Security Objectives for the TOE</i>	<i>19</i>
4.2	<i>Security Objectives for the Operational Environment</i>	<i>20</i>
4.3	<i>Statement of Threats Consistency</i>	<i>21</i>
4.4	<i>Statement of Organizational Security Policies Consistency</i>	<i>24</i>
4.5	<i>Statement of Assumptions Consistency</i>	<i>25</i>
4.6	<i>Statement of Security Objectives for the TOE Consistency</i>	<i>26</i>
4.7	<i>Statement of Security Objectives for the Operational Environment Consistency</i>	<i>29</i>
5	Extended Components Definition	32
5.1	<i>IDS Class</i>	<i>32</i>
5.1.1	<i>IDS_SDC.1 System Data Collection</i>	<i>32</i>
5.1.2	<i>IDS_ANL.1 Analyzer Analysis</i>	<i>33</i>
5.1.3	<i>IDS_RDR.1 Restricted Data Review (EXT)</i>	<i>34</i>
5.1.4	<i>IDS_RCT.1 – Analyzer React</i>	<i>35</i>
5.1.5	<i>IDS_STG.1 Guarantee of System Data Availability</i>	<i>35</i>
5.1.6	<i>IDS_STG.2 Prevention of System Data Loss</i>	<i>36</i>
5.2	<i>FAU Class</i>	<i>36</i>
5.2.1	<i>FAU_STG_EXT.1 External Audit Trail Storage</i>	<i>36</i>
6	Security Requirements	38
6.1	<i>Security Functional Requirements</i>	<i>38</i>
6.1.1	<i>Security Audit (FAU)</i>	<i>39</i>
6.1.2	<i>Cryptographic Support (FCS)</i>	<i>42</i>
6.1.3	<i>Information Flow Control (FDP)</i>	<i>44</i>

6.1.4	Identification and Authentication (FIA)	47
6.1.5	Security Management (FMT)	48
6.1.6	Protection of the TOE Security Functions	50
6.1.7	Traffic Analysis Component Requirements.....	50
6.2	<i>Statement of Security Requirements Consistency</i>	51
6.3	<i>Security Functional Requirements Rationale</i>	53
6.3.1	Sufficiency of Security Requirements	53
6.3.2	CC Component Hierarchies and Dependencies	56
6.4	<i>Security Assurance Requirements</i>	57
6.5	<i>Security Assurance Rationale</i>	58
7	TOE Summary Specification	59
7.1	<i>Traffic Analysis and Audit</i>	59
7.2	<i>Cryptographic Support</i>	62
7.3	<i>Information Flow Control</i>	66
7.4	<i>Identification and Authentication</i>	68
7.5	<i>Security Management</i>	69
8	Appendices	72
8.1	<i>References</i>	72
8.2	<i>Glossary</i>	72
8.3	<i>Acronyms</i>	78

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 JUNOS-FIPS 10.4R4 for SRX Series
ST Revision	1.5
ST Publication Date	December 22, 2011
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
----------------------	---

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 affect 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 the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance 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

1.3.2 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; operations performed by Protection Profile authors are not subject to these conventions.

- 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 blue 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 selection allows the addition of details or the narrowing of requirements components. A refinement selection 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), FMT_MTD.1.1(2), and FMT_MTD.1.1, 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 “(EXP)” following the component name. All the extended requirements are derived from the Protection Profiles cited in Section 2. This Security Target relies on the extended component definitions in the Protection Profiles in Section 2.

1.3.3 Document Terminology

See Section 9.2 for the Glossary.

1.4 TOE Overview

The Target of Evaluation (TOE) includes the following secure router products running JUNOS-FIPS 10.4R4: SRX100, SRX210, SRX220, SRX240, SRX650, SRX3400, SRX3600, SRX5600, and SRX5800. The TOE includes a FIPS 140-2 validated cryptographic module.

These network devices provide the following basic services in the evaluated configuration:

- VPN Routing — securely 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 and prevention — monitoring and analyzing a set of IT system resources for potential vulnerabilities or misuse and taking action upon detection of potential vulnerabilities.

1.5 TOE Description

The TOE consists of the following components:

1. Appliances: purpose-built appliances deployed at branch and remote 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.
2. JUNOS 10.4: an operating system for security appliances.

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
- Which class of service (CoS) to apply to the packet, if any
- 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, and the management 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—Contains the IP address or domain names of hosts and subnets whose traffic is either permitted, denied, encrypted, or user-authenticated

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 following figure shows a typical IPsec architecture:

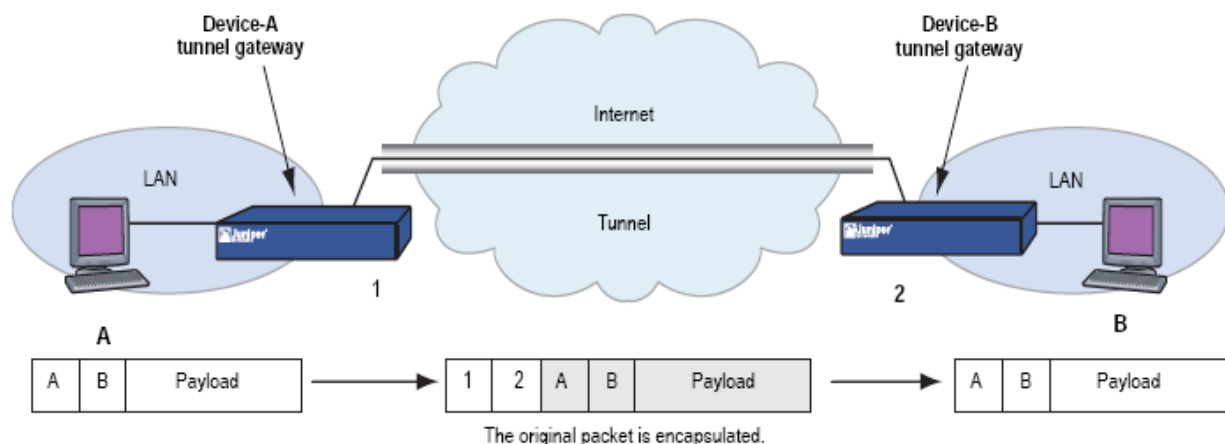


Figure 1 – Typical IPsec Configuration

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. JUNOS also enforces MAC address filtering, where the interface on a router may be configured to accept packets only from specified MAC addresses.

Juniper Networks security devices accomplish routing through a process called a virtual router (VR). A security device divides its routing component into two or more VRs with each VR maintaining its own list of known networks in the form of a routing table, routing logic, and associated security zones.

The JUNOS software Intrusion Detection and Prevention (IDP) policy enables the selective enforcement of various attack detections and prevention techniques on network traffic. It allows the definition of policy rules to match a section of traffic based on a zone, or network and then takes active or passive actions on that traffic. The TOE analyzes traffic for signature, Protocol Anomaly, Backdoor, Traffic Anomaly, Layer 2, and Denial of Service (DoS) attacks and, upon detection, can log the event, drop the packet, or block the originating address.

The TOE may be configured in either a transparent mode or an active gateway mode for IDP functions. When deployed as an active gateway, the TOE uses a policy to control what action to take when an attack is detected (e.g., log the event, or block/drop any identified malicious packets). When deployed in transparent mode, the TOE only detects and logs attacks. The TOE detection and prevention capabilities are rule-based, so rules can be specified within a Security Policy to define when and how packets or connections are dropped; the Security Policy configures the Sensor to log, send alarms, and even drop suspicious traffic.

The TOE is managed and configured via Command Line Interface.

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.

The TOE is a combined hardware/software TOE and is defined as JUNOS-FIPS 10.4R4 for SRX Series. The TOE boundary is shown below:

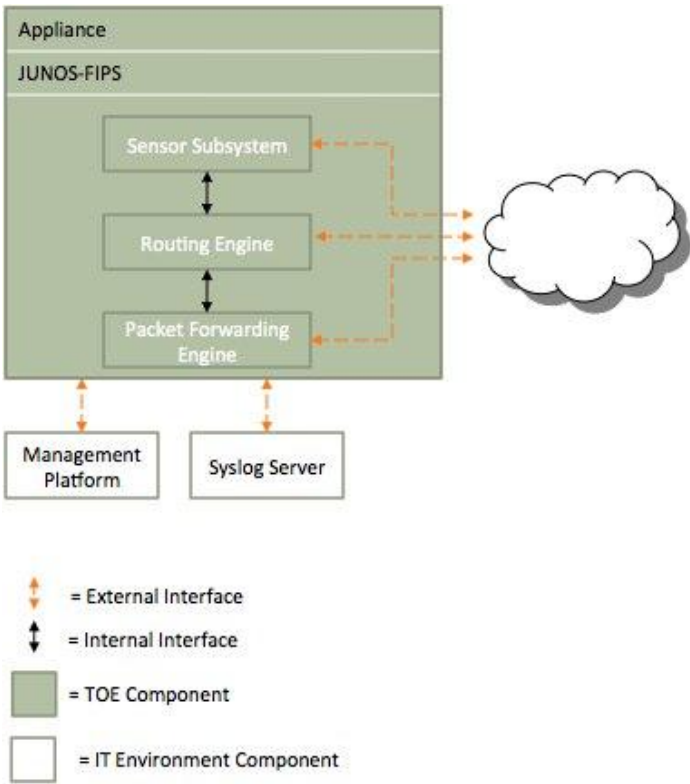


Figure 2 – TOE Boundary

In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Hardware	SRX100, SRX210, SRX220, SRX240, SRX650, SRX3400, SRX3600, SRX5600, SRX5800
TOE Software	JUNOS-FIPS 10.4R4

Table 2 – Evaluated Configuration for the TOE

The TOE interfaces are comprised of the following:

1. Network interfaces, which receive traffic for analysis and pass traffic for routing/VPN functions and transmission of generated audit data to an external IT entity.
2. Management interfaces exercised via CLI.

The following ports and services are excluded from the evaluation:

- 465/tcp (smtps - secure Simple Mail Transport Protocol)
- 636/tcp (ldaps - Secure Lightweight Directory Access Protocol)
- 989/tcp (ftps-data - Secure File Transfer Protocol Data port)

- 992/tcp (telnets - Secure TELNET Protocol)
- 443/tcp (supports management via J-Web GUI)
- 123/udp (Network Time Protocol)

The following options are not part of the evaluated configuration:

- TACACS+
- RADIUS

1.5.1 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
Traffic Analysis and Audit	JUNOS auditable events are stored in the syslog files. Auditable events include start-up and shutdown of the audit functions, network traffic events, authentication events, and service requests, as well as the events listed in Table 18 – Auditable Events. Audit records include the date and time, event type, username, and the outcome of the event (success or failure). IDS audit records also include component identity. 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 Administrator can review and delete audit data and IDS audit data. Search and sort facilities are provided via tools in the IT Environment, along with the ability for the appropriate administrator to determine how exhaustion of space for audit records is handled. 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	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 Overall Level 2.
User Data Protection/Information Flow Control	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).
Identification and Authentication	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

TSF	DESCRIPTION
	authenticate prior to any exchange. This covers all services used to exchange information, including telnet, File Transfer Protocol (FTP), Secure Shell (SSH), and Secure Socket Layer (SSL); both telnet and FTP are out of scope. Authentication services are handled internally by user-selected passwords. Note that in support of FIPS 140-2 compliance, external authentication servers are outside the scope of the evaluation.
Security Management	<p>The TOE provides an Administrator role that is responsible for:</p> <ul style="list-style-type: none"> the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product the regular review of all audit data; all administrative tasks (e.g., creating the security policy). <p>The devices are managed through a Command Line Interface (CLI). The CLI is accessible through remote administrative session, or via a local terminal console.</p>

Table 3 – Logical Boundary

1.5.1.1 TOE Guidance

The following guidance documentation will be provided as part of the TOE:

- Operational User Guidance and Preparative Procedures Supplement: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series¹*

1.5.1.2 IT Environment

The TOE boundary does not include the following IT Environment Components:

- Hardware and software for the syslog server. Note that the syslog server shall be able to perform searches and sorting of Firewall audit data based on: presumed subject address, ranges of dates, ranges of times, and ranges of addresses.
- Hardware platforms for the Management Platform, which can be any of the following:
 - Windows 2000 SP4, 2003 SP2, XP SP2 or later
 - Redhat Linux (2.6 Kernel) or later
 - Solaris (SPARC) 8 and 10 or later

¹ Note this document contains references to a broader set of public documentation available from Juniper's Techpubs website (<http://www.juniper.net/techpubs>)

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 at Evaluation Assurance Level 4 augmented with ALC_FLR.2 – Flaw Reporting Procedures.

2.2 PP Claim

The TOE claims conformance to the follow Protection Profiles:

- U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments Version 1.1, dated July 25, 2007 (FWPP)
- U.S. Government Protection Profile Intrusion Detection System - System for Basic Robustness Environments, Version 1.7, dated July 25, 2007 (IDSPP).

2.3 Package Claim

The TOE claims conformance to the EAL4 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009) augmented with ALC_FLR.2 – Flaw Reporting Procedures. The TOE does not claim conformance to any functional package.

2.4 Conformance Rationale

The TOE contains the security functionality described in the Protection Profiles in list Section 2.2. These Protection Profiles were chosen because the TOE is consistent with the functionality presented in those Protection Profiles.

In accordance with NIAP Precedent PD-0097, the following items have been deleted:

- FPT_ITA.1
- FPT_ITC.1
- FPT_ITI.1

Further modifications and refinements are presented in the following tables:

- Table 14 – Statement of Consistency for TOE Security Objectives
- Table 15 – Statement of Consistency for Operational Environment Security Objectives
- Table 21 – Statement of Security Requirements Consistency

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

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

Note that the assumptions, threats, and policies represent a superset of those found in each of the PPs such that this TOE serves to address the Security Problem for each of the PPs simultaneously. The assumptions, threats, and policies are drawn from one or more of the identified PPs as indicated in the tables below.

3.1 Threats

The following threats are addressed by the TOE.

The threats included in the Security Target represent a combination of the threats specified in the Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's statement of threats are included in the Security Target. The table in Section 4.3 identifies each threat included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

THREAT	DESCRIPTION
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

Table 4 – Threats Addressed by the TOE

The IT System addresses the following threats:

THREAT	DESCRIPTION
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.
T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

Table 5 – Threats Addressed by the IT System

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.

The Organizational Security Policies included in the Security Target represent a combination of the Organizational Security Policies specified in the Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's statement of Organizational Security Policies are included in the Security Target. The table in Section 4.4 identifies each Organizational Security Policy included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

POLICY NAME	POLICY DESCRIPTION
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.PROTECT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
P.IPSEC	The TOE shall support IPSec protocols.

Table 6 – Organizational Security Policies

3.3 Assumptions

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

The assumptions included in the Security Target represent a combination of the assumptions specified in the Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's statement of assumptions are included in the Security Target. The table in Section 4.5 identifies each assumption included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOTRST	The TOE can only be accessed by authorized users.
A.PHYSEC	The TOE is physically secure.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.

Table 7 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT Security Objectives for the TOE are addressed below.

The Security Objectives for the TOE included in the Security Target represent a combination of the Security Objectives for the TOE specified in the two Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's statement of Security Objectives for the TOE are included in the Security Target. The table in Section 4.6 identifies each Security Objective for the TOE included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

OBJECTIVE	DESCRIPTION
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDSCAN	The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.
O.MEDIAT	The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.

O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.ENCryp	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
O.SECURE_KEY	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows between instances of the TOE. The TOE must also provide a means of secure key distribution to other subjects.
O.CONFIDENTIALITY	The TOE must protect the confidentiality of packet flows transmitted to/from the TOE over an untrusted network.
O.AUTHENTICITY	The TOE must provide the means for ensuring that a packet flow has been received from a trusted source.
O.INTEGRITY	The TOE must ensure that any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.

Table 8 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below.

The Security Objectives for the Operational Environment included in the Security Target represent a combination of the Security Objectives for the Operational Environment specified in the relevant Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's statement of Security Objectives for the Operational Environment are included in the Security Target. The table in Section 4.7 identifies each Security Objective for the Operational Environment included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

OBJECTIVE	DESCRIPTION
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.

OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.INTROP	The TOE is interoperable with the IT System it monitors.
OE.PHYSEC	The TOE is physically secure.
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.PUBLIC	The TOE does not host public data.
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
OE.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.

Table 9 – Operational Environment Security Objectives

4.3 Statement of Threats Consistency

The threats included in the Security Target represent a combination of the threats specified in the Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's statement of threats are included in the Security Target. The following table identifies each threat included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

THREAT	PP Reference	DESCRIPTION
--------	--------------	-------------

T.COMINT	Reproduced exactly from IDS PP	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	Reproduced exactly from IDS PP	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	Reproduced exactly from IDS PP	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	Reproduced exactly from IDS PP	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	Reproduced exactly from IDS PP	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	Reproduced exactly from IDS PP	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	Reproduced exactly from IDS PP	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Reproduced exactly from IDS PP	Unauthorized attempts to access TOE data or security functions may go undetected.
T.NOAUTH	Satisfied by T.PRIVIL from IDS PP	Satisfied by T.PRIVIL. An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.REPEAT	Reproduced exactly from FW PP	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	Reproduced exactly from FW PP	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	Reproduced exactly from FW PP	An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.
T.MEDIAT	Reproduced exactly from FW PP	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.OLDINF	Reproduced exactly from FW PP	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

T.PROCOM	Reproduced exactly from FW PP	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE
T.AUDACC	Reproduced exactly from FW PP	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	Reproduced exactly from FW PP	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	Reproduced exactly from FW PP	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

Table 10 – Threats Addressed by the TOE

Threats addressed by the IT system:

THREAT	PP Reference	DESCRIPTION
T.SCNCFG	Reproduced exactly from IDS PP	Improper security configuration settings may exist in the IT System the TOE monitors.
T.SCNMLC	Reproduced exactly from IDS PP	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Reproduced exactly from IDS PP	Vulnerabilities may exist in the IT System the TOE monitors.
T.FALACT	Reproduced exactly from IDS PP	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	Reproduced exactly from IDS PP	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	Reproduced exactly from IDS PP	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Reproduced exactly from IDS PP	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Reproduced exactly from IDS PP	Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT	Reproduced exactly from IDS PP	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.
T.TUSAGE	Reproduced exactly from FW PP	The TOE may be inadvertently configured, used and administered in a insecure manner by either authorized or unauthorized persons.

Table 11 – Threats Addressed by the IT System

4.4 Statement of Organizational Security Policies Consistency

The Organizational Security Policies included in the Security Target represent a combination of the Organizational Security Policies specified in the Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's statement of Organizational Security Policies are included in the Security Target. The following table identifies each Organizational Security Policy included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

POLICY NAME	PP REFERENCE	POLICY DESCRIPTION
P.DETECT	Reproduced exactly from IDS PP	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.ANALYZ	Reproduced exactly from IDS PP	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.MANAGE	Reproduced exactly from IDS PP	The TOE shall only be managed by authorized users.
P.ACCESS	Reproduced exactly from IDS PP	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Reproduced exactly from IDS PP	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Reproduced exactly from IDS PP	Data collected and produced by the TOE shall be protected from modification.
P.PROTCT	Reproduced exactly from IDS PP	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
P.IPSEC	None	The TOE shall support IPSec protocols.
P.SYSTEM_MONITORING	None	The TOE shall support the capability to export generated audit data.

Table 12 – Organizational Security Policies

4.5 Statement of Assumptions Consistency

The assumptions included in the Security Target represent a combination of the assumptions specified in the relevant Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's statement of assumptions are included in the Security Target. The following table identifies each assumption included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

ASSUMPTION	PP REFERENCE	DESCRIPTION
A.ACCESS	Reproduced exactly from IDS PP	The TOE has access to all the IT System data it needs to perform its functions.
A.DYNMIC	Reproduced exactly from IDS PP	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.ASCOPE	Reproduced exactly from IDS PP	The TOE is appropriately scalable to the IT System the TOE monitors.
A.PROTCT	Satisfied by A.PHYSEC from FWPP	Satisfied by A.PHYSEC. The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	Satisfied by A.PHYSEC from FW PP	Satisfied by A.PHYSEC. The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	Reproduced exactly from IDS PP	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	Satisfied by A.NOEVIL from FW PP	Satisfied by A.NOEVIL. The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	Reproduced exactly from IDS PP	The TOE can only be accessed by authorized users.
A.PHYSEC	Reproduced exactly from FW PP	The TOE is physically secure.
A.LOWEXP	Reproduced exactly from FW PP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.GENPUR	Reproduced exactly from FW PP	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.PUBLIC	Reproduced exactly from FW PP	The TOE does not host public data.
A.NOEVIL	Reproduced exactly from FW PP	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Reproduced exactly from FW PP	Information can not flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Reproduced exactly from FW PP	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOREMO	Reproduced exactly from FW PP	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
A.REMACC	Reproduced exactly from FW PP	Authorized administrators may access the TOE remotely from the internal and external networks.

Table 13 – Assumptions

4.6 Statement of Security Objectives for the TOE Consistency

The Security Objectives for the TOE included in the Security Target represent a combination of the Security Objectives for the TOE specified in the relevant Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's statement of Security Objectives for the TOE are included in the Security Target. The following table identifies each Security Objective for the TOE included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

OBJECTIVE	PP REFERENCE	DESCRIPTION
O.PROTCT	Reproduced exactly from IDS PP	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDSCAN	Reproduced exactly from IDS PP	The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

O.IDSENS	Reproduced exactly from IDS PP	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	Reproduced exactly from IDS PP	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	Reproduced exactly from IDS PP	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	Reproduced exactly from IDS PP	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	Reproduced exactly from IDS PP	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	Reproduced exactly from IDS PP	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	Reproduced exactly from IDS PP	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	Reproduced exactly from IDS PP	The TOE must record audit records for data accesses and use of the System functions.
O.INTEGR	Reproduced exactly from IDS PP	The TOE must ensure the integrity of all audit and System data.
O.IDAUTH	Satisfied by O.IDAUTH from IDS PP	Satisfied by O.IDAUTH from IDS PP. The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
O.SINUSE	Reproduced exactly from FW PP	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.

O.MEDIAT	Reproduced exactly from FW PP	The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.SECSTA	Reproduced exactly from FW PP	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.ENCryp	Reproduced exactly from FW PP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
O.SELPRO	Reproduced exactly from FW PP	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.”
O.AUDREC	Reproduced exactly from FW PP	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ACCOUN	Reproduced exactly from FW PP	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.SECFUN	Satisfied by O.ACCESS from IDS PP	Satisfied by O.ACCESS. The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.LIMEXT	Reproduced exactly from FW PP	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

O.SECURE_KEY	To support P.IPSEC	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows between instances of the TOE. The TOE must also provide a means of secure key distribution to other subjects.
O.INTEGRITY	To support P.IPSEC	The TOE must ensure that any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected.
O.AUTHENTICITY	To support P.IPSEC	The TOE must provide the means for ensuring that a packet flow has been received from a trusted source.
O.CONFIDENTIALITY	To support P.IPSEC	The TOE must protect the confidentiality of packet flows transmitted to/from the TOE over an untrusted network.
O.SYSTEM_MONITORING	To support P.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.

Table 14 – Statement of Consistency for TOE Security Objectives

4.7 Statement of Security Objectives for the Operational Environment Consistency

The Security Objectives for the Operational Environment included in the Security Target represent a combination of the Security Objectives for the Operational Environment specified in the relevant Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's statement of Security Objectives for the Operational Environment are included in the Security Target. The following table identifies each Security Objective for the Operational Environment included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

OBJECTIVE	PP REFERENCE	DESCRIPTION
OE.AUDIT_PROTECTION	Reproduced exactly from IDS PP	The IT Environment will provide the capability to protect audit information.
OE.AUDIT_SORT	Reproduced exactly from IDS PP	The IT Environment will provide the capability to sort the audit information
OE.TIME	Reproduced exactly from IDS PP	The IT Environment will provide reliable timestamps to the TOE.
OE.INSTAL	Reproduced exactly from IDS PP	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

OE.PHYCAL	Reproduced exactly from IDS PP	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Reproduced exactly from IDS PP	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.PERSON	Reproduced exactly from IDS PP	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.INTROP	Reproduced exactly from IDS PP	The TOE is interoperable with the IT System it monitors.
OE.PHYSEC	Reproduced exactly from FW PP	The TOE is physically secure.
OE.LOWEXP	Reproduced exactly from FW PP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.GENPUR	Reproduced exactly from FW PP	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.PUBLIC	Reproduced exactly from FW PP	The TOE does not host public data.
OE.NOEVIL	Reproduced exactly from FW PP	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.SINGEN	Reproduced exactly from FW PP	Information can not flow among the internal and external networks unless it passes through the TOE.
OE.DIRECT	Reproduced exactly from FW PP	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
OE.NOREMO	Reproduced exactly from FW PP	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
OE.REMACC	Reproduced exactly from FW PP	Authorized administrators may access the TOE remotely from the internal and external networks.

OE.GUIDAN	Satisfied by OE.INSTAL from IDS PP	Satisfied by OE.INSTAL. The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.ADMTRA	Reproduced exactly from FW PP	Authorized administrators are trained as to establishment and maintenance of security policies and practices.

Table 15 – Statement of Consistency for Operational Environment Security Objectives

5 Extended Components Definition

5.1 IDS Class

All of the components in this section are taken from the *U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments*.

This class of requirements is taken from the IDS System PP to specifically address the data collected and analysed by an IDS scanner and analyzer. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of system data and provide for requirements about collecting, reviewing and managing the data.

5.1.1 IDS_SDC.1 System Data Collection

Management: IDS_SDC.1

The following actions could be considered for the management functions in FMT:

- a) Configuration of the events to be collected

Audit: IDS_SDC.1

There are no auditable events foreseen.

IDS_SDC.1 System Data Collection

Hierarchical to: No other components

Dependencies: No dependencies

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) [selection: *Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, detected known vulnerabilities*]; and

b) [assignment: *other specifically defined events*].

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

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

b) The additional information specified in the Details column of the table below:

COMPONENT	EVENT	DETAILS
IDS_SDC.1	Startup and shutdown	None
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC.1	Service requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDS, location of object, source address, destination address
IDS_SDC.1	Startup and shutdown of audit functions	None
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked passwords, account policy parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Table 16 – System Data Collection Events and Details

Application Note: The rows in this table must be retained that correspond to the selections in IDS_SDC.1.1 when that operation is completed. If additional events are defined in the assignment in IDS_SDC.1.1, then corresponding rows should be added to the table for this element.

5.1.2 IDS_ANL.1 Analyzer Analysis

Management: IDS_ANL.1

The following actions could be considered for the management functions in FMT:

- a) Configuration of the analysis to be performed

Audit: IDS_ANL.1

There are no auditable events foreseen.

IDS_ANL.1 Analyzer Analysis

Hierarchical to: No other components

Dependencies: IDS_SDC.1 System Data Collection

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:

- a) [selection: *statistical, signature, integrity*]; and
- b) [assignment: *other analytical functions*].

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:

- a. Date and time of the result, type of result, identification of data source; and
- b. [assignment: *other security relevant information about the result*]. (EXT)

5.1.3 IDS_RDR.1 Restricted Data Review (EXT)

Management: IDS_RDR.1

The following actions could be considered for the management functions in FMT:

- a) maintenance (deletion, modification, addition) of the group of users with read access right to the system data records.

Audit: IDS_RDR.1

There are no auditable events foreseen.

IDS_RDR.1 Restricted Data Review

Hierarchical to: No other components

Dependencies: IDS_SDC.1 System Data Collection
IDS_ANL.1 Analyzer Analysis

IDS_RDR.1.1 The System shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of System data*] from the System data.

IDS_RDR.1.2	The System shall provide the System data in a manner suitable for the user to interpret the information.
IDS_RDR.1.3	The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

5.1.4 IDS_RCT.1 – Analyzer React

Management: IDS_RCT.1

The following actions could be considered for the management functions in FMT:

- a) Configuration of the reaction operations to be performed

Audit: IDS_RCT.1

There are no auditable events foreseen.

IDS_RCT.1 Analyzer React

Hierarchical to:	No other components	
Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis
IDS_RCT.1.1	The System shall send an alarm to [assignment: <i>specified location</i>] and take [assignment: <i>specified actions</i>] when an intrusion is detected.	

5.1.5 IDS_STG.1 Guarantee of System Data Availability

Management: IDS_STG.1

The following actions could be considered for the management functions in FMT:

- b) maintenance of the parameters that control the system data storage capability.

Audit: IDS_STG.1

There are no auditable events foreseen.

IDS_STG.1 Guarantee of System Data Availability

Hierarchical to:	No other components	
Dependencies:	IDS_SDC.1	System Data Collection

IDS_STG.1.1	The System shall protect the stored System data from unauthorized deletion.
IDS_STG.1.2	<p>The System shall protect the stored System data from modification.</p> <p><i>Application Note: Authorized deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.</i></p>
IDS_STG.1.3	The System shall ensure that [assignment: <i>metric for saving System data</i>] System data will be maintained when the following conditions occur: [selection: <i>System data storage exhaustion, failure, attack</i>].

5.1.6 IDS_STG.2 Prevention of System Data Loss

Management: IDS_STG.2

The following actions could be considered for the management functions in FMT:

- a) maintenance (deletion, modification, addition) of actions to be taken in case system data storage capacity has been reached.

Audit: IDS_STG.2

There are no auditable events foreseen.

IDS_STG.2 Prevention of System data loss

Hierarchical to: No other components

Dependencies: IDS_SDC.1 System Data Collection

IDS_STG.2.1	The System shall [selection: ' <i>ignore System data</i> ', ' <i>prevent System data, except those taken by the authorized user with special rights</i> ', ' <i>overwrite the oldest stored System data</i> '] and send an alarm if the storage capacity has been reached.
-------------	--

5.2 FAU Class

5.2.1 FAU_STG_EXT.1 External Audit Trail Storage

Management: FAU_STG_EXT.1

The following actions could be considered for the management functions in FMT:

- a) Configuration of the TOE to transmit or receive audit data from an external source.

Audit: FAU_STG_EXT.1

There are no auditable events foreseen.

FAU_STG_EXT.1 External Audit Trail Storage

Hierarchical to: No other components

Dependencies: No dependencies

FAU_STG_EXT.1.1 The TSF shall be able to [selection: *'transmit the generated audit data to an trusted external IT entity', 'receive and store audit data from an trusted external IT entity'*] .

6 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.

6.1 Security Functional Requirements

The security functional requirements included in the Security Target represent a combination of the security functional requirements specified in the Protection Profiles for which conformance is claimed as well as VPN capabilities of the TOE. All concepts covered in each of the Protection Profile's statement of security functional requirements are included in the Security Target. The table in Section 7.6 identifies each security functional requirement included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

The IDS PP is the baseline for constructing this Security Target. When the FWPP significantly changes a requirement, the Security Target either 1) restates the requirement such that all aspects of all versions of the requirement are specified, or 2) levies an iterated requirement. Requirements that are iterated in order to cover the FWPP bear the suffix "-FW". This suffixing technique is also used for requirements that are unique to a given Protection Profile.

"Application Notes" are carried forward from the relevant Protection Profiles; in some instances, these are redacted for clarity. "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 functional security 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_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_SAR.3-IDS	Selectable Audit Review
	FAU_SAR.3-FW	Selectable Audit Review
	FAU_SEL.1	Selective Audit
	FAU_STG.2	Guarantees of Audit Data Availability
	FAU_STG.4	Prevention of Audit Data Loss
	FAU_STG_EXT.1	External Audit Trail Storage
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Distribution
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
User Data Protection	FDP_IFC.1(1)	Subset Information Flow Control
	FDP_IFF.1(1)	Simple Security Attributes
	FDP_IFC.1(2)	Subset Information Flow Control
	FDP_IFF.1(2)	Simple Security Attributes
	FDP_RIP.1	Residual Information Protection
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_AFL.1	Authentication failure handling
	FIA_UAU.1	Timing of Authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UID.2	User Identification before any action
Security Management	FMT_MOF.1-IDS	Management of Security Functions Behavior
	FMT_MOF.1-FW	Management of Security Functions Behavior
	FMT_MSA.3(1)	Management of Security Attributes
	FMT_MSA.3(2)	Management of Security Attributes
	FMT_MTD.1(1)	Management of TSF Data
	FMT_MTD.1(2)	Management of TSF Data
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_STM.1	Reliable Time Stamps
Traffic Analysis	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis
	IDS_RCT.1	Analyzer React (IDS)
	IDS_RDR.1	Analyzer React (IPS)
	IDS_STG.1	Restricted Data Review
	IDS_STG.2	Prevention of System data loss

Table 17 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 – Audit Data Generation

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

- Start-up and shutdown of the audit functions;
- All auditable events for the *[basic]* level of audit;
- [\[Access to the System and access to the TOE and System data.\]](#)

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

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

- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [the additional information specified in the Details column of Table 18 – Auditable Events.]

COMPONENT	EVENT	DETAILS
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FCS_COP.1	Success and failure, and the type of cryptographic operation as specified in the FWPP	The identity of the external IT entity attempting to perform the cryptographic operation
FDP_IFF.1	All decisions on requests for information flow	The presumed addresses of the source and destination subject.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the users capability to authenticate.	The identity of the offending user and the authorized administrator
FIA_UAU.1	All use of the authentication mechanism	User identity, location
FIA_UID.2	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF including archive, create, delete, empty, and review the audit trail;	The identity of the authorized administrator performing the operation
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a the authorized administrator role	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.
FPT_STM.1	Changes to the time	User identity

Table 18 – Auditable Events

Application Note: The auditable events described in Table 18 – Auditable Events are replicated from the FW PP and the IDS PP. Note that for the following SFRs, no level of audit is claimed: FAU_STG.4, FCS_CKM.1, FCS_CKM.2,

FCS_CKM.4, FIA_UAU.4 and FMT_MSA.3. As such, no auditable events are defined for those SFRs. The basic level of audit is maintained for conformance to the FW PP and IDS PP, and additional SFRs claim a not specified level of audit because of product capabilities and performance impacts.

Application Note: The IDS_SDC and IDS_ANL requirements in this ST address the recording of results from IDS scanning, sensing, and analysing tasks (i.e., System data). This follows the specification in the IDS PP.

Application Note: The TOE does not log success of cryptographic operations defined in FCS_COP.1 because given the number of connections and operations during use, any repository for this type of audit data would quickly be exhausted. Since the FWPP includes this to protect remote management sessions, any success is implicit in allowing the session to be setup and auditing use of the identification and authentication mechanism. In the event of a failure, the failure would be logged and a session would not be created

Application Note: Regarding FAU_GEN.1 for FAU_SAR.2, there is no syslog audit record when executing “show log syslog” command fail. However, the CLI is rejected with error message on the screen. However, since only an authorized Administrator role is defined in FMT_SMR.1, there is no use case for a non-authorized user attempting to read information from the audit records.

Application Note: For FAU_GEN.1 for FIA_AFL.1, the TOE implements an authentication-throttling mechanism discussed in FIA_AFL.1. As such, account restoration is not applicable since there is only one account (Administrator) which cannot restore its own account.

6.1.1.2 FAU_SAR.1 Audit Review

- | | |
|-------------|---|
| FAU_SAR.1.1 | The TSF shall provide [the Administrator] with the capability to read [all audit information] from the audit records. |
| FAU_SAR.1.2 | The TSF shall provide the audit records in a manner suitable for the user to interpret the information. |

6.1.1.3 FAU_SAR.2 – Restricted Audit Review

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

6.1.1.4 FAU_SAR.3-IDS – Selectable Audit Review (IDS)

- | | |
|-----------------|--|
| FAU_SAR.3.1-IDS | The TSF shall provide the ability to apply [sorting] of IDS audit data based on [date and time, subject identity, type of event, and success or failure of related event]. |
|-----------------|--|

Application Note: The TOE supports auditing as specified in FAU_GEN.1, and audit is provided via syslog. As such, the sorting of audit data is provided by tools in the IT Environment.

6.1.1.5 FAU_SAR.3-FW – Selectable Audit Review (FW)

- | | |
|----------------|---|
| FAU_SAR.3.1-FW | The TSF shall provide the ability to apply [searches and sorting] of Firewall audit data based on [|
|----------------|---|

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

Application Note: The TOE supports auditing as specified in FAU_GEN.1, and audit is provided via syslog. As such, the searching and sorting of audit data is provided by tools in the IT Environment.

6.1.1.6 FAU_SEL.1 – Selective Audit

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

- a) [event type]
- b) [no additional attributes].

6.1.1.7 FAU_STG.2 – Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [prevent] modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that [the most recent audit records limited by configured storage space] audit records will be maintained when the following conditions occur: [audit storage exhaustion.]

6.1.1.8 FAU_STG.4 – Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall [prevent auditable events, except those taken by the authorized user with special rights] and [shall limit the number of audit records lost and send an alarm] if the audit trail is full.

6.1.1.9 FAU_STG_EXT.1 – External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to [transmit the generated audit data to an trusted external IT entity].

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 – Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [FIPS 186-2] and specified cryptographic key sizes [128-, 192-,

or 256-bit AES key and 1024-, or 1536- bit P values for Diffie Hellman] that meet the following: [FIPS 197 for AES and ANSI X9.42 for Diffie-Hellman].

6.1.2.2 FCS_CKM.2 – Cryptographic Key Distribution

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]

that meets the following: [

- SCEP-IETF (Simple Certificate Enrollment Protocol -Internet Engineering Task Force
- ANSI X9.42 Agreement of Symmetric Keys Using Discrete Logarithm Cryptography]

6.1.2.3 FCS_CKM.4 – Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [Federal Information Processing Standard 140 requirements for key zeroization].

6.1.2.4 FCS_COP.1 – Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [the operations described below] in accordance with a specified cryptographic algorithm [multiple algorithms in the modes of operation described below] and cryptographic key sizes [multiple key sizes described below] that meet the following: [multiple standards described below].

OPERATION	ALGORITHM (MODE)	KEY SIZE IN BITS	STANDARDS
Encryption and Decryption	AES (CBC mode)	128, 192, 256	FIPS 197
Key agreement	Diffie-Hellman (ANSI X9.42 Hybrid 5 [concatenation])	g = 2 p = 1024, or 1536	ANSI X9.42
Hashing	SHS (SHA-1)	160 (size of digest)	FIPS 180-2
Random Number Generation	FIPS 186-2	Not Applicable	FIPS 186-2
Digital Signatures	RSA	Modulus Size: 1024	PKCS7

Table 19 – Cryptographic Operations

6.1.3 Information Flow Control (FDP)

6.1.3.1 FDP_IFC.1(1) – Subset information flow control

- FDP_IFC.1.1(1) The TSF shall enforce the [UNAUTHENTICATED INFORMATION FLOW SFP] on: [
- a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;
 - b) information: traffic sent through the TOE from one subject to another;
 - c) operation: pass information].

6.1.3.2 FDP_IFF.1(1) Simple security attributes

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

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

- FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold: [
- a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:
 - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

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

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

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

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

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

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

6.1.3.3 FDP_IFC.1(2) – Subset Information Flow Control

FDP_IFC.1.1 (2) The TSF shall enforce the [SECURE INFORMATION FLOW SFP] on

[Subjects: IT entities that send information through the TOE,

Information: network traffic, and

Operations: IP packet forwarding, encrypt, decrypt and authenticate].

6.1.3.4 FDP_IFF.1(2) – Simple Security Attributes

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

[Subject security attributes:

- TOE identity credentials (IP address)

Information security attributes:

- Presumed identifier of source subject
- Presumed identifier of destination subject
- IPSec attributes (parameters for Manual Key, AutoKey IKE with Preshared Keys, AutoKey IKE with Certificates, Pre-shared Key, route/policy-based VPNs)
- Port number of source subject
- Port number of destination subject
- Zone on which packet arrives and departs.

].

FDP_IFF.1.2 (2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [if one TOE instance (subject) can authenticate another TOE instance (subject) through the establishment of an IPSec Security Association using the configured policy and identity credentials of the TOE instances].

FDP_IFF.1.3 (2) The TSF shall enforce the [Network Address Translation operations with Destination IP address translation and/or Source IP address translation if configured to do so].

FDP_IFF.1.4 (2) The TSF shall provide the following [none].

FDP_IFF.1.5 (2) The TSF shall explicitly authorize an information flow based on the following rules: [no additional SECURE INFORMATION FLOW SFP rules].

FDP_IFF.1.6 (2) The TSF shall explicitly deny an information flow based on the following rules: [no additional denial rules].

6.1.3.5 FDP_RIP.1 – Subset residual information protection

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

Application Note: If, for example, the TOE pads information with bits in order to properly prepare the information before sending it out an interface, these bits would be considered a “resource”. The intent of the requirement is that these bits shall not contain the remains of information that had previously passed through the TOE. The requirement is met by overwriting or clearing resources, (e.g. packets) before making them available for use.

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_AFL.1 – Authentication failure handling

- FIA_AFL.1.1 The TSF shall detect when [an administrator-configurable non-zero integer] of unsuccessful authentication attempts occurs related to [external IT entities attempting to authenticate from an internal or external network].
- FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [prevent the offending external IT entity from successfully authenticating until an administrator-defined time period has elapsed].

Application Note: This requirement does not apply to the local administrators, since it does not make sense to lock a local administrator’s account in this fashion. This could be addressed by requiring a separate account for local administrators, which would be stated in the administrative guidance, or the TOE’s authentication mechanism implementation could distinguish login attempts that are made locally and remotely. Additionally, this functionality is only available to remote SSH sessions and is not applicable to VPN functionality.

6.1.4.2 FIA_ATD.1 – User Attribute Definition

- FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [
- a) User identity
 - b) Authentication Data
 - c) Role].

6.1.4.3 FIA_UAU.1 – Timing of Authentication

- FIA_UAU.1.1 The TSF shall allow [no actions] on behalf of the user to be performed before the user is authenticated.
- FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.4 FIA_UAU.4 – Single-use authentication mechanisms

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

- b) authorized external IT entities].

6.1.4.5 FIA_UID.2 – User Identification before Any Action

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

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MOF.1-IDS Management of Security Functions Behavior (IDS)

FMT_MOF.1.1-IDS The TSF shall restrict the ability to [*modify the behavior of*] the functions [*of IDS System data collection, analysis and reaction*] to [*the Administrator*].

6.1.5.2 FMT_MOF.1-FW Management of Security Functions Behavior (FW)

FMT_MOF.1.1-FW The TSF shall restrict the ability to perform the functions: [

- a) start-up and shutdown;
- b) create, delete, modify, and view information flow security policy rules that permit or deny information flows related to the UNAUTHENTICATED INFORMATION FLOW SFP;
- c) modify the behavior of IDS data collection, analysis, and reaction.
- d) create, delete, modify, and view user attribute values defined in FIA_ATD.1;
- e) enable and disable single-use authentication mechanisms in FIA_UAU.4;
- f) modify and set the threshold for the number of permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);
- g) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);
- h) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);
- i) modify and set the time and date;
- j) review the audit trail;
- k) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;
- l) recover to the state following the last backup;

- m) additionally, if the TSF supports remote administration from either an internal or external network:
 - a. enable and disable remote administration from internal and external networks;
 - b. restrict addresses from which remote administration can be performed;
 - n) no other security-relevant administrative functions].
- to [the Administrator].

6.1.5.3 FMT_MSA.3(1) – Static attribute initialization

- FMT_MSA.3.1(1) The TSF shall enforce the [UNAUTHENTICATED INFORMATION FLOW SFP] to provide [restrictive] default values for information flow security attributes that are used to enforce the SFP.
- FMT_MSA.3.2(1) The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

Application Note: The default values for the information flow control security attributes appearing in FDP_IFF.1 are intended to be restrictive in the sense that both inbound and outbound information is denied by the TOE until the default values are modified by an authorized administrator.

6.1.5.4 FMT_MSA.3(2) – Static Attribute Initialization

- FMT_MSA.3.1(2) The TSF shall enforce the [SECURE INFORMATION FLOW SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
- FMT_MSA.3.2(2) The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.5 FMT_MTD.1(1) – Management of TSF Data

- FMT_MTD.1.1(1) The TSF shall restrict the ability to [perform the functions FMT_MOF.1-IDS and FMT_MOF.1-FW] to [the Administrator].

6.1.5.6 FMT_MTD.1(2) – Management of TSF Data

- FMT_MTD.1.1(2) The TSF shall restrict the ability to [change default, query, modify, delete, clear] [the parameters associated with the SECURE INFORMATION FLOW SFP] to [the Administrator].

6.1.5.7 FMT_SMR.1 Security Roles

- FMT_SMR.1.1 The TSF shall maintain the roles [Administrator].
- FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6 Protection of the TOE Security Functions

6.1.6.1 FPT_STM.1 Reliable Time Stamps

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

6.1.7 Traffic Analysis Component Requirements

6.1.7.1 IDS_SDC.1 – System Data Collection (EXP)

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

- a) *[network traffic]* and
- b) *[no other specifically defined events]*.

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) The additional information specified in *[the Details column of Table 20 – System Events]*

COMPONENT	EVENT	DETAILS
IDS_SDC.1	Network traffic	Protocol, source address, destination address

Table 20 – System Events

6.1.7.2 IDS_ANL.1 – Analyzer Analysis (EXP)

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:

- a) *[signature]* and
- b) *[algorithm-based correlations]*.

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:

- a) Date and time of the result, type of result, identification of data source; and
- b) *[no other security relevant information about the result]*.

6.1.7.3 IDS_RCT.1 – Analyzer React (EXP)

IDS_RCT.1.1 The System shall send an alarm to [the audit log] and take [the following actions: notify the Administrator's designated personnel via log alert information to a saved file or displayed on the console,] when an intrusion is detected.

6.1.7.4 IDS_RDR.1 – Restricted Data Review (EXP)

IDS_RDR.1.1 The System shall provide [the Administrator] with the capability to read [event data] from the System data.

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

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

6.1.7.5 IDS_STG.1 – Guarantee of System Data Availability (EXP)

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

IDS_STG.1.2 The System shall protect the stored System data from modification.

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

6.1.7.6 IDS_STG.2 – Prevention of System data loss (EXP)

IDS_STG.2.1 The System shall [prevent auditable events, except those taken by the authorized user with special rights] and send an alarm if the storage capacity has been reached.

6.2 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent a combination of the Security Functional Requirements specified in the Protection Profiles for which conformance is claimed. All concepts covered in each of the Protection Profile's Statement of Security Requirements are included in the Security Target. The following table identifies each SFR included in the ST and provides rationale for its inclusion in the Security Target with regards to the relevant Protection Profiles.

SFR	PP	RATIONALE
FAU_GEN.1	IDS PP FW PP	Reproduced exactly from the PPs.
FAU_SAR.1	IDS PP FW PP	Reproduced exactly from the PPs.
FAU_SAR.2	IDS PP	Reproduced exactly from the IDS PP.
FAU_SAR.3-IDS	IDS PP	Reproduced exactly from the IDS PP.

FAU_SAR.3-FW	FW PP	Reproduced exactly from the FWPP.
FAU_SEL.1	IDS PP	Reproduced exactly from the IDS PP.
FAU_STG.2	IDS PP	Reproduced exactly from the IDS PP. Identified as FAU_STG.1 in the FWPP, which is superseded by this requirement. .
FAU_STG.4	IDS PP FW PP	Merged from the PPs. Assignment operations combined.
FAU_STG_EXT.1	N/A	Included to address transmission of generated audit data to an external IT entity (such as a syslog server)
FCS_CKM.1	N/A	Included to address IPSec operations.
FCS_CKM.2	N/A	Included to address IPSec operations.
FCS_CKM.4	N/A	Included to address IPSec operations.
FCS_COP.1	FW PP	Modified to address crypto operations in more detail to account for IPSec operations.
FDP_IFC.1(1)	FW PP	Reproduced exactly from the FWPP.
FDP_IFF.1(1)	FW PP	Reproduced exactly from the FWPP.
FDP_IFC.1(2)	N/A	Included to address flow control operations for IPSec operations.
FDP_IFF.1(2)	N/A	Included to address flow control operations for IPSec operations.
FDP_RIP.1	FW PP	Reproduced exactly from the FWPP.
FIA_AFL.1	FW PP IDS PP	Merged from the PPs.
FIA_ATD.1	IDS PP FW PP	Merged from the PPs.
FIA_UAU.1	IDS PP FW PP	Merged from the PPs
FIA_UAU.4	FW PP	Reproduced exactly from the FWPP.
FIA_UID.2	FW PP	Reproduced exactly from the FW PP.
FMT_MOF.1-IDS	IDS PP	Reproduced exactly from the IDS PP.
FMT_MOF.1-FW	FW PP	Reproduced exactly from the FWPP.
FMT_MSA.3(1)	FW PP	Reproduced exactly from the FWPP.
FMT_MSA.3(2)	N/A	Included to address IPSec feature
FMT_MTD.1(1)	IDS PP	Derived from the IDS PP to include both IDS and FW management functions.
FMT_MTD.1(2)	N/A	Included to address IPSec feature.
FMT_SMR.1	IDS PP FW PP	Merged from the PPs.
FPT_STM.1	IDS PP	Reproduced exactly from the IDS PP.
IDS_SDC.1	IDS PP	Reproduced exactly from the IDS PP.
IDS_ANL.1	IDS PP	Reproduced exactly from the IDS PP.
IDS_RCT.1	IDS PP	Reproduced exactly from the IDS PP.
IDS_RDR.1	IDS PP	Reproduced exactly from the IDS PP.
IDS_STG.1	IDS PP	Reproduced exactly from the IDS PP.
IDS_STG.2	IDS PP	Reproduced exactly from the IDS PP.

Table 21 – Statement of Security Requirements Consistency

6.3 Security Functional Requirements Rationale

All threats, Organizational Security Policies, assumptions, Security Objectives for the TOE, Security Objectives for the Operating Environment, and Security Functional Requirements have been copied from the validated Protection Profiles, and this Security Target relies on the mapping and rationale provided in those PPs.

Any changes to Security Functional Requirements are documented in Table 21 – Statement of Security Requirements Consistency. With regards to SFR changes, the more restrictive security requirement was chosen, in which the security objectives are still met and/or exceeded. The changes do not introduce any weakness or invalidate the PPs in any way.

For those requirements not specified in one of the PPs, the following table provides the correspondence mapping between security objectives or OSP for the TOE and the requirements that satisfy them.

OBJECTIVE / POLICY												
SFR	O.CONFIDENTIALITY	O.INTEGRITY	O.AUTHENTICITY	O.SECURE_KEY	O.MEDIAT	O.SECSTA	O.SECFUN	O.PROTCT	O.ACCESS	O.IDAUTH	O.SYSTEM_MONITORING	O.INTEGR
FCS_CKM.1				✓								
FCS_CKM.2				✓								
FCS_CKM.4				✓								
FCS_COP.1	✓	✓	✓									
FDP_IFC.1(2)	✓	✓	✓									
FDP_IFF.1(2)	✓	✓	✓									
FMT_MSA.3(2)					✓	✓	✓					
FMT_MTD.1(2)								✓	✓	✓		✓
FAU_STG_EXT.1											✓	

Table 22 – Mapping of TOE Security Functional Requirements and Objectives

6.3.1 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

SFR	RATIONALE
FCS_CKM.1	This component ensures that cryptographic keys and parameters are generated with standards-based algorithms (O.SECURE_KEY).
FCS_CKM.2	This component ensures that the establishment of the trust relationship and the key exchange operations are standards-based and cryptographically sound (O.SECURE_KEY).

SFR	RATIONALE
FCS_CKM.4	This component ensures that the cryptographic keys and parameters are safely destroyed when their lifetime ends or when the privileged operator forces generation of new keys. Keys are zeroized in accordance with FIPS 140-2 specifications (O.SECURE_KEY).
FCS_COP.1	This component ensures that the establishment of the trust relationship and the confidentiality operations are cryptographically sound (O.CONFIDENTIALITY), ensures that the establishment of the trust relationship and the integrity operations are cryptographically sound (O.INTEGRITY), and ensures that the establishment of the trust relationship and the digital signature operations are cryptographically sound (O.AUTHENTICITY).
FDP_IFC.1(2)	This component identifies and defines the SECURE INFORMATION FLOW SFP and the scope of control of the policies that form the secure information flow control portion of the TSP (O.CONFIDENTIALITY, O.INTEGRITY, O.AUTHENTICITY).
FDP_IFF.1(2)	This component states the rules for traffic exchange with a peer (e.g., identify which remote trusted IT product is providing integrity verification for which packet flow, and which packet flow is to be authenticated and protected when transmitted to a remote trusted IT product) (O.CONFIDENTIALITY, O.INTEGRITY, O.AUTHENTICITY).
FMT_MSA.3(2)	This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN
FMT_MTD.1(2)	This component restricts the ability to change default, query, modify, delete, clear TSF data related to SECURE INFORMATION FLOW SFP to authorized users. (O.PROTECT, O.ACCESS, O.IDAUTH, O.INTEGR).
FAU_STG_EXT.1	This component provides the capability for the TOE to export generated audit data to a trusted external IT entity, such as a syslog server. (O.SYSTEM_MONITORING).

Table 23 – Rationale for TOE SFRs to Objectives

The following table presents a mapping of the rationale of TOE Objectives to Security Requirements:

OBJECTIVE	RATIONALE
O.AUTHENTICITY	<p>This objective is completely satisfied by</p> <ul style="list-style-type: none"> FCS_COP.1 ensures that the establishment of the trust relationship and the digital signature operations are cryptographically sound. FDP_IFC.1(2) identifies and defines the SECURE INFORMATION FLOW SFP and the scope of control of the policies that form the secure information flow control portion of the TSP. FDP_IFF.1(2) states the rules for traffic exchange with a peer (e.g., identify which remote trusted IT product is providing integrity verification for which packet flow, and which packet flow is to be authenticated and protected when transmitted to a remote trusted IT product).

OBJECTIVE	RATIONALE
O.CONFIDENTIALITY	<p>This objective is completely satisfied by</p> <ul style="list-style-type: none"> • FCS_COP.1 ensures that the establishment of the trust relationship and the confidentiality operations are cryptographically sound. • FDP_IFC.1(2) identifies and defines the SECURE INFORMATION FLOW SFP and the scope of control of the policies that form the secure information flow control portion of the TSP. • FDP_IFF.1(2) states the rules for traffic exchange with a peer (e.g., identify which remote trusted IT product is providing integrity verification for which packet flow, and which packet flow is to be authenticated and protected when transmitted to a remote trusted IT product).
O.INTEGRITY	<p>This objective is completely satisfied by</p> <ul style="list-style-type: none"> • FCS_COP.1 ensures that the establishment of the trust relationship and the integrity operations are cryptographically sound. • FDP_IFC.1(2) identifies and defines the SECURE INFORMATION FLOW SFP and the scope of control of the policies that form the secure information flow control portion of the TSP. • FDP_IFF.1(2) states the rules for traffic exchange with a peer (e.g., identify which remote trusted IT product is providing integrity verification for which packet flow, and which packet flow is to be authenticated and protected when transmitted to a remote trusted IT product).
O.SECURE_KEY	<p>This objective is completely satisfied by</p> <ul style="list-style-type: none"> • FCS_CKM.1 ensures that cryptographic keys and parameters are generated with standards-based algorithms. • FCS_CKM.2 ensures that the establishment of the trust relationship and the key exchange operations are standards-based and cryptographically sound. • FCS_CKM.4 ensures that the cryptographic keys and parameters are safely destroyed when their lifetime ends or when the privileged operator forces generation of new keys. Keys are zeroized in accordance with FIPS 140-2 specifications.
O.MEDIAT	<p>This objective is completely satisfied by</p> <ul style="list-style-type: none"> • FMT_MSA.3(2) ensures that the default values of security attributes are appropriately restrictive in nature
O.SECSTA	<p>This objective is completely satisfied by</p> <ul style="list-style-type: none"> • FMT_MSA.3(2) ensures that the default values of security attributes are appropriately restrictive in nature
O.SECFUN	<p>This objective is completely satisfied by</p> <ul style="list-style-type: none"> • FMT_MSA.3(2) ensures that the default values of security attributes are appropriately restrictive in nature
O.PROTCT	<p>This objective is completely satisfied by</p> <ul style="list-style-type: none"> • FMT_MTD.1(2) restricts the ability to query, add or modify TSF data to authorized users.

OBJECTIVE	RATIONALE
O.ACCESS	This objective is completely satisfied by <ul style="list-style-type: none"> FMT_MTD.1(2) restricts the ability to query, add or modify TSF data to authorized users.
O.IDAUTH	This objective is completely satisfied by <ul style="list-style-type: none"> FMT_MTD.1(2) restricts the ability to query, add or modify TSF data to authorized users.
O.INTEGR	This objective is completely satisfied by <ul style="list-style-type: none"> FMT_MTD.1(2) restricts the ability to query, add or modify TSF data to authorized users.
O.SYSTEM_MONITORING	This objective is completely satisfied by <ul style="list-style-type: none"> FAU_STG_EXT.1, which provides the capability for the TOE to export generated audit data to a trusted external IT entity, such as a syslog server..

Table 24 – Rationale for TOE Objectives to SFRs

6.3.2 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale. Note that this table applies to SFRs that are not covered in the FW PP or the IDS PP.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_STG_EXT.1	No other components	None	N/A
FCS_CKM.1	No other components	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Satisfied
FCS_CKM.2	No other components	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Satisfied
FCS_CKM.4	No other components	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied
FCS_COP.1	No other components	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Satisfied
FDP_IFC.1(2)	No other components	FDP_IFF.1	Satisfied
FDP_IFF.1(2)	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied

FMT_MSA.3(2)	No other components	FMT_MSA.1 FMT_SMR.1	Satisfied ²
FMT_MTD.1(2)	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied ³

Table 25 – TOE SFR Dependency Rationale

6.4 Security Assurance Requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ADV_FSP.4 Complete Functional Specification	Functional Specification: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ADV_IMP.1 Implementation Representation of the TSF	Basic Design: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ADV_TDS.3 Basic Modular Design	Basic Design: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ALC_CMC.4 Production support, acceptance procedures and automation	Configuration Management Processes and Procedures: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ALC_CMS.4 Problem tracking CM coverage	Configuration Management Processes and Procedures: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ALC_DVS.1 Identification of security measures	Security Measures: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ALC_LCD.1 Developer defined life-cycle model	Product Development Lifecycle Model: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ALC_FLR.2 – Flaw Reporting Procedures	Flaw Reporting Procedures: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series

² Functional component FMT_MSA.3(2) depends on functional component FMT_MSA.1 Management of security attributes. In an effort to place all the management requirements in a central place, FMT_MTD.1(2) was used. Therefore FMT_MTD.1(2) more than adequately satisfies the concerns of leaving FMT_MSA.1 out of this Security Target

³ Functional component FMT_MTD.1(2) depends on functional component FMT_SMF.1 Specification of Management Functions. In an effort to place all the management requirements in a central place, FMT_MTD.1(2) was used. Therefore FMT_MTD.1(2) more than adequately satisfies the concerns of leaving FMT_SMF.1 out of this Security Target

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ALC_TAT.1 Well-defined development tools	Configuration Management Processes and Procedures: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ASE_CCL.1 Conformance claims	Security Target: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ASE_ECD.1 Extended components definition	Security Target: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ASE_INT.1 ST introduction	Security Target: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ASE_OBJ.2 Security objectives	Security Target: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ASE_REQ.2 Derived security requirements	Security Target: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ASE_SPD.1 Security problem definition	Security Target: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ASE_TSS.1 TOE summary specification	Security Target: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ATE_COV.2 Analysis of Coverage	Testing Evidence Supplement: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ATE_DPT.1 Testing: Basic Design	Testing Evidence Supplement: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ATE_FUN.1 Functional Testing	Testing Evidence Supplement: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
ATE_IND.2 Independent Testing - sample	Produced by Common Criteria Testing Laboratory
AVA_VAN.3 Focused Vulnerability Analysis	Produced by Common Criteria Testing Laboratory

Table 26 – Security Assurance Measures

6.5 Security Assurance Rationale

The ST security assurance requirements are from EAL 4 augmented with ALC_FLR.2 – Flaw Reporting Procedures. EAL 4 was selected for this TOE because it reflects good commercial practice expected of this type of TOE. EAL4 is augmented by ALC_FLR.2 to ensure that the customers can report the flaws and the flaws can be systematically corrected.

7 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.

7.1 Traffic Analysis and Audit

JUNOS creates and stores audit records for a large set of security-relevant events (see the table in Section 6). It supports both system audit records relevant to local events, and IDS audit records. The JUNOS IDS subsystem analyzes IDS audit data by using statistical analyses that identify deviations from normal patterns of behavior and by signature matching against known intrusions or misuses of the system. The JUNOS IDS subsystem does not perform integrity analysis in order to detect vulnerabilities or potential violations.

Auditing (both for local audit and IDS purposes) is performed using syslog. This can be configured to store the audit logs locally or to send them to one or more log servers, which are considered trusted IT entities. The syslogs are automatically deleted locally according to configurable limits on storage volume or number of days of logs to retain.

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) For each audit event type, based on the auditable event definitions of the functional components specified in Table 18 – Auditable Events.

The TOE audits all of the required events specified in Section 6 of this Security Target, and each audit record captures all of the required information as shown in column 3 of Table 18 – Auditable Events. For IDS audit events logged by identified sensing capabilities, the audit mechanism associate each auditable event with the identity of the sensing capability that logged the event.

JUNOS provides the Administrator with the ability to view audit data from the Command Line Interface (CLI) – the CLI is available via remote administrative sessions.

Using tools available in the IT Environment, the Administrator can search and sort the IDS audit data based on:

- date and time,
- subject identity,
- type of event, and

- success or failure of related event

The Administrator can search and sort the FW audit data based on:

- presumed subject address,
- ranges of dates,
- ranges of times,
- ranges of addresses

In terms of IDS, the TOE collects events associated with network traffic. The TOE records pertinent information for further analysis including: date and time of the event, type of event, and component identity (source/location). The entire content of network traffic is preserved temporarily while analysis occurs, but is not retained beyond the analysis and production of analysis conclusions. The TOE identifies known vulnerabilities using statistical analyses on available IDS audit data where deviations from normal patterns of behavior and signature matching against known vulnerability issues serve to identify security violations. Once the initial IDS data has been processed, analytical results are recorded as IDS data containing: date and time of the result, type of analysis, outcome of analysis, Analyzer component ID, and IDS audit records that generated potential intrusion.

The Administrator can search the IDS audit data by data and time, component identity, type of event, and success or failure of the related event as well as include or exclude events from the set of auditable events based on event type.

The TOE audits for the following events:

- Start-up and shutdown of audit functions
- Access to System
- Access to the TOE and System data
- Reading of information from the audit records
- Unsuccessful attempts to read information from the audit records
- All modifications to the audit configuration that occur while the audit collection functions are operating
- Success and failure, and the type of cryptographic operation
- The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the users capability to authenticate.
- All use of the authentication mechanism

- All use of the user identification mechanism
- All modifications in the behavior of the functions of the TSF
- All modifications to the values of TSF data
- Modifications to the group of users that are part of a the authorized administrator role
- Changes to the time

The Administrator can delete audit records (including those related to IDS), which are protected from unauthorized modification since the TOE does not allow for modification of audit data with the exception of deletion, which is an authenticated action.

The JUNOS software notifies administrators of pending potential audit data loss by displaying a message, when the used audit space exceeds an administrator-configurable percentage of available space, at the local console and by throwing an alarm, per the alarm mechanism described above, on any existing administrative sessions. The TOE will prevent auditable events if the storage capacity is reached. In any case, the most recent events are always preserved. The Administrator has the same option with the IDS audit records.

Each hardware appliance provides a reliable clock for a time source, and the JUNOS uses this clock to provide reliable time stamps.

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

- FAU_GEN.1
- FAU_SAR.1
- FAU_SAR.2
- FAU_SAR.3-IDS
- FAU_SAR.3-FW
- FAU_SEL.1
- FAU_STG.2
- FAU_STG.4
- FAU_STG_EXT.1
- IDS_SDC.1
- IDS_ANL.1

- IDS_RCT.1
- IDS_RDR.1
- IDS_STG.1
- IDS_STG.2
- FPT_STM.1

7.2 Cryptographic Support

All FIPS-approved cryptographic functions implemented by the secure routers are implemented in the JUNOS-FIPS cryptomodule, which is the entire appliance and will be designed for FIPS 140-2 Overall Level 2 compliance, and perform the specified cryptographic functions in a FIPS mode of operation. The FIPS 140-2 validation will include FIPS 140-2 validation certificates for the TOE as indicated in the table below.

CMVP #	MODELS
1613	SRX 100, 210, 220, 240 and 650
1611	SRX 3400, 3600
1602	SRX 5600, 5800

The FIPS 140-2 validation will include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE as indicated in the table below.

ALGORITHM	MODELS		
	SRX 100, 210, 220, 240, 650	SRX 3400, 3600	SRX 5600, 5800
Triple DES	1064	1032 & 1033	1030 & 1034
AES	1624	1575 & 1577	1573 & 1578
DSA	510	486	484
SHS	1433	1395 & 1396	1393 & 1397
RNG	871	849	847
RSA	802	768	766
HMAC	955	922 & 923	920 & 924

The Cryptographic Support security function is described in the context of how it satisfies the cryptographic security requirements.

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

distribution of private asymmetric keys uses NSA-approved certificate schemes with hardware tokens that meet the following:

1. PKI Roadmap for the DoD,
2. DoD X.509 Certificate Policy,
3. PKCS #8 v1.2 (Private-Key Information Syntax Standard),
4. PKCS #12 v1.0 (Personal Information Exchange Syntax),
5. PKCS #5 v2.0 (Password-Based Encryption Standard, 25 Mar 1999 - Final), and
6. PKCS #11 v2.11 (Cryptographic Token Interface Standard).

Support for manual distribution of public asymmetric key material also uses SA-approved certificate schemes that meet the 'PKI Roadmap for the DoD', 'DoD X.509 Certificate Policy', and PKCS #12 v1.0 (Personal Information Exchange Syntax). The TOE automatically distributes public asymmetric key material (certificates and/or keys) in accordance with NSA-certified DoD PKI for public key distribution using NSA-approved certificate schemes that meet the 'PKI Roadmap for the DoD', 'DoD X.509 Certificate Policy', and PKCS #12 v1.0 (Personal Information Exchange Syntax).

The cryptomodule only 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 FIPS 186-2. All cryptographic random numbers are drawn from this RNG.

The TSF generates symmetric cryptographic keys using a software RNG in connection with either pre-shared keys, or Diffie-Hellman key agreement. The TSF employs a FIPS 140-2 approved software RNG that complies with FIPS 186-2. The TSF also uses a mixing function that meets FIPS PUB 180-2. All cryptographic random numbers are drawn from this RNG. 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

Manually keyed VPNs do not draw upon the RNG; the Administrator explicitly configures the key values. Auto-key IKE VPNs draw upon the RNG during the key agreement process. The TOE supports only Diffie-Hellman key agreement.

The TSF generates DH keys Prime numbers are generated using a method that complies with ANSI X9.80 and X9.42. Support for distribution of symmetric keys is in accordance with NIST SP 800-57.

The TSF supports the manual and electronic distribution of cryptographic keys. 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 qualified 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. The Administrator 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 and resets it. 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-, or 256-bit keys.

The TOE supports the following digital signature algorithms:

- RSA with a key size of 1024 bits or greater

The TOE supports cryptographic hashing via the SHA-1 algorithm.

The TOE supports IKE v1 in Main and Aggressive modes as per RFC 2409. Authentication is available through pre-shared key and RSA certificates. All random values are generated using the FIPS-approved RNG.

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: $SKEYID = sha(Ni_b \parallel Nr_b, g^{xy})$
- Pre-shared keys: $SKEYID = sha(pre-shared-key, Ni_b \parallel Nr_b)$
- Authentication using Public key encryption, computing SKEYID as follows:

$= sha(sha(Ni_b \parallel Nr_b), CKY-I \parallel CKY-R)$

The TOE computes authenticated keying material as follows:

- $SKEYID_d = sha(SKEYID, g^{xy} \parallel CKY-I \parallel CKY-R \parallel 0);$
- $SKEYID_a = sha(SKEYID, SKEYID_d \parallel g^{xy} \parallel CKY-I \parallel CKY-R \parallel 1);$ and
- $SKEYID_e = sha(SKEYID, SKEYID_a \parallel g^{xy} \parallel CKY-I \parallel CKY-R \parallel 2).$

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 and as defined by the SFR in this security target.

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 as defined by the SFR in this security target. The TOE can also use X.509 Version 3 certificates.

The TOE computes hashes in the following way:

$\text{HASH}(1) = \text{sha}(\text{SKEYID_a}, \text{M-ID} \parallel [\text{any ISAKMP payload after HASH}(1) \text{ header contained in the message}])$

$\text{HASH}(2) = \text{sha}(\text{SKEYID_a}, \text{M-ID} \parallel \text{Ni_b} \parallel [\text{any ISAKMP payload after HASH}(2) \text{ header contained in the message}])$

$\text{HASH}(3) = \text{sha}(\text{SKEYID_a}, 0 \parallel \text{M-ID} \parallel \text{Ni_b} \parallel \text{Nr_b})$

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, ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN and ID_KEY_ID. 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 [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_CKM.1
- FCS_CKM.2

- FCS_CKM.4
- FCS_COP.1

7.3 Information Flow Control

The TOE supports the SECURE INFORMATION FLOW SFP and UNAUTHENTICATED INFORMATION FLOW SFP which are configured via security policies. The JUNOS security policies enforce rules for the transit traffic, in terms of what traffic can 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. Security zones have the following properties:

- Policies, which are active security policies that enforce rules for the transit traffic through the TOE. This includes
 - Interzone – routes traffic from one zone to another zone
 - Intrazone – routes traffic within one zone
 - Global – provides a storage area for static NAT addresses and can be used in policies like any other security zone
- Screens, which help secure a network by inspecting (then allowing or denying), all connection attempts that require passage from one security zone to another.

Management sessions are controlled in the same manner as just described. The administrator can configure the TOE to allow or deny the establishment of a management session by defining an access control policy specifying a source/destination IP address and source/destination TCP/UDP port number. Connection attempts that do not match the criteria in the access control policy will be denied.

The TOE supports IPSec to provide confidentiality, integrity, and authenticity for traffic transmitted for inbound/outbound traffic (when configured accordingly). This functionality is defined in the SECURE INFORMATION FLOW SFP, which includes support for routing via IPsec tunnels. 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. Each option is a configurable parameter of the SECURE INFORMATION FLOW SFP. 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
- SCEP-IETF (Simple Certificate Enrollment Protocol -Internet Engineering Task Force
- ANSI X9.42 Agreement of Symmetric Keys Using Discrete Logarithm Cryptography

JUNOS uses a single routing instance, referred to as the default virtual router (VR). A routing instance consists of a routing table and routing process that are linked to a specific security zone. Separate virtual routers are often configured for trusted and untrusted zones.

The Manual Key option allows both ends of an IPSec tunnel to be separately configured. 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.

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 SECURE INFORMATION FLOW SFP.

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

The TOE enforces the UNAUTHENTICATED INFORMATION FLOW SFP with stateful packet attributes which include the source and destination network identifiers as well as the source and destination service identifiers.

The Administrator can display the current 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.

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.

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

7.4 Identification and Authentication

The Administrator is responsible for provisioning user accounts. 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 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 Administrator can set a threshold for failed authentication attempts. By default, the TOE performs the following actions for Telnet or SSH sessions:

- Disconnects a session after a maximum of 3 consecutive password retries.
- After the second password retry, introduces a delay in multiples of 5 seconds between subsequent password retries (for example, the services router introduces a delay of 5 seconds between the third and fourth password retry, a delay of 10 seconds between the fourth and fifth password retry, and so on).
- Enforces a minimum session time of 20 seconds during which a session cannot be disconnected. Configuring the minimum session time prevents malicious users from disconnecting sessions before the password retry delay goes into effect, and attempting brute force and dictionary attacks with multiple logins.

The Administrator can configure the password retry limits for telnet and SSH access.

The TOE ensures that some one-time authentication mechanism is used in all attempts to authenticate to the TOE from an internal or external network. 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 type of connection being established to satisfy the SECURE INFORMATION FLOW SFP. For remote access of authorized administrators, the TOE's implementation of SSH prevents replay attacks by ensuring that each packet received is encrypted with the shared secret associated with that session. If the shared secret does not match, the packet will be discarded and the remote user will not be able to authenticate.

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

- FIA_AFL.1
- FIA_ATD.1
- FIA_UAU.1
- FIA_UAU.4
- FIA_UID.2

7.5 Security Management

The TOE supports and enforces the role of 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 through a Command Line Interface (CLI). The CLI is accessible through remote administrative session, 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 TOE implements an internal access control mechanism whereby specific roles are assigned permission to exercise specific CLI commands. These permissions are fixed by the developer and unchangeable by the product user. The following lists enumerate the CLI permissions in the evaluated configuration.

The following management functions are available to the Administrator role:

- Start-up and shutdown;
- Create, delete, modify, and view information flow security policy rules that permit or deny information flows related to the UNAUTHENTICATED INFORMATION FLOW SFP;
- Modify the behavior of IDS data collection, analysis, and reaction;
- Create, delete, modify, and view user attribute values defined in FIA_ATD.1;
- Enable and disable single-use authentication mechanisms in FIA_UAU.4;
- Modify and set the threshold for the number of permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);
- Restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);
- Enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);
- Modify and set the time and date;
- Backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;
- Recover to the state following the last backup;

Security Target: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series

- Enable and disable remote administration from internal and external networks;
- Restrict addresses from which remote administration can be performed;

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

- FMT_MOF.1-IDS
- FMT_MOF.1-FW
- FMT_MSA.3(1)
- FMT_MSA.3(2)
- FMT_MTD.1(1)
- FMT_MTD.1(2)
- FMT_SMR.1

8 Appendices

8.1 References

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

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.

8.2 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.

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 user – An authenticated 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 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.

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.

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).

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.

8.3 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

TERM	DEFINITION
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
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

TERM	DEFINITION
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
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 Resource Locator

TERM	DEFINITION
VPN	Virtual Private Network

Table 27 – Acronyms Used in Security Target