Security Target

Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms

Document Version 2.0

July 13, 2011

Prepared For:

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

www.juniper.net

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, 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), the JUNOS 10.0 R4 for J-Series and SRX-Series Platforms. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

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 product.

1.1 ST Reference

ST Title	Security Target: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
ST Revision	2.0
ST Publication Date	July 13, 2011
Author	Apex Assurance Group, LLC

1.2 TOE Reference

TOE Reference	Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms

1.3 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	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- 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 square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BGP	Border Gateway Protocol
CC	Common Criteria version 3.1
DH	Diffie Hellman
EAL	Evaluation Assurance Level
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
JUNOS	Juniper Operating System
NAT	Network Address Translation
NTP	Network Time Protocol
OSP	Organizational Security Policy
PFE	Packet Forwarding Engine

TERM	DEFINITION
PIC/PIM	Physical Interface Card/Module
RE	Routing Engine
RFC	Request for Comment
RIP	Routing Information Protocol
SA	Security Association
SCEP	Simple Certificate Enrollment Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VPN	Virtual Private Network
VR	Virtual Router

Table 2 – Acronyms Used in Security Target

1.6 TOE Overview

The TOE is Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms, which primarily supports the definition of and enforces information flow policies among network nodes. The routers provide for stateful inspection of every packet that traverses the network and provide central management to manage the network security policy. All information flow from one network node to another passes through an instance of the TOE. Information flow is controlled on the basis of network node addresses, protocol, type of access requested, and services requested. In support of the information flow security functions, the TOE ensures that security-relevant activity is audited, that their own functions are protected from potential attacks, and provide the security tools to manage all of the security functions.

The J-series Services Routers are 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.

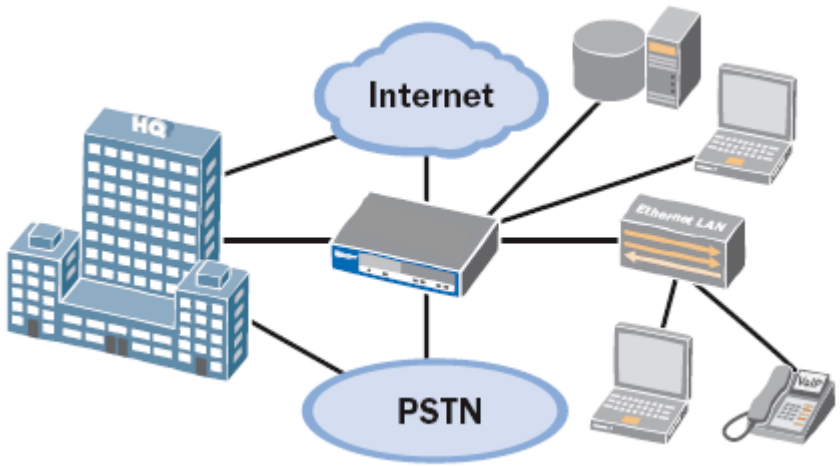

Figure 1 – Common TOE Deployment

JUNOS 10.0 R4 for J-Series and SRX-Series Platforms may also be referred to as the TOE in this document.

1.7 TOE Description

1.7.1 Overview

Each Juniper Networks J-Series and SRX-Series routing platform is a complete routing system that supports a variety of high-speed interfaces for medium/large networks and network applications. Juniper Networks routers share common JUNOS software, features, and technology for compatibility across platforms.

The routers are physically self-contained, housing the software, firmware and hardware necessary to perform all router functions. The hardware has two components: the router itself and various PIC/PIMs, which allow the routers to communicate with the different types of networks that may be required within the environment where the routers are used.

Each instance of the TOE consists of the following major architectural components:

- The Routing Engine (RE) runs the JUNOS software and provides Layer 3 routing services and network management for all operations necessary for the configuration and operation of the TOE and controls the flow of information through the TOE, including Network Address Translation (NAT) and all operations necessary for the encryption/decryption of packets for secure communication via the IPSec protocol;
- The Packet Forwarding Engine (PFE) provides all operations necessary for transit packet forwarding;

The Routing Engine and Packet Forwarding Engine perform their primary tasks independently, while constantly communicating through a high-speed internal link. This arrangement provides streamlined forwarding and routing control and the capability to run Internet-scale networks at high speeds.

The routers support numerous routing standards for flexibility and scalability as well as IETF IPSec protocols as defined in RFC2401- RFC2410. These functions can all be managed through the JUNOS software, either from a connected terminal console or via a network connection. Network management can be secured using SSL, SNMP v3, and SSH protocols. All management, whether from a user connecting to a terminal or from the network, requires successful authentication and is communicated using JUNOScript. Net conf is an IETF standardization effort which is closely aligned to JUNOScript. JUNOS only supports netconf via SSH transport, and authentication is handled by SSHD.

The TOE supports IPSec to provide confidentiality, integrity, and authenticity to network traffic transmitted from one TOE device and received by another TOE device.

The following figure shows a typical IPSec architecture:

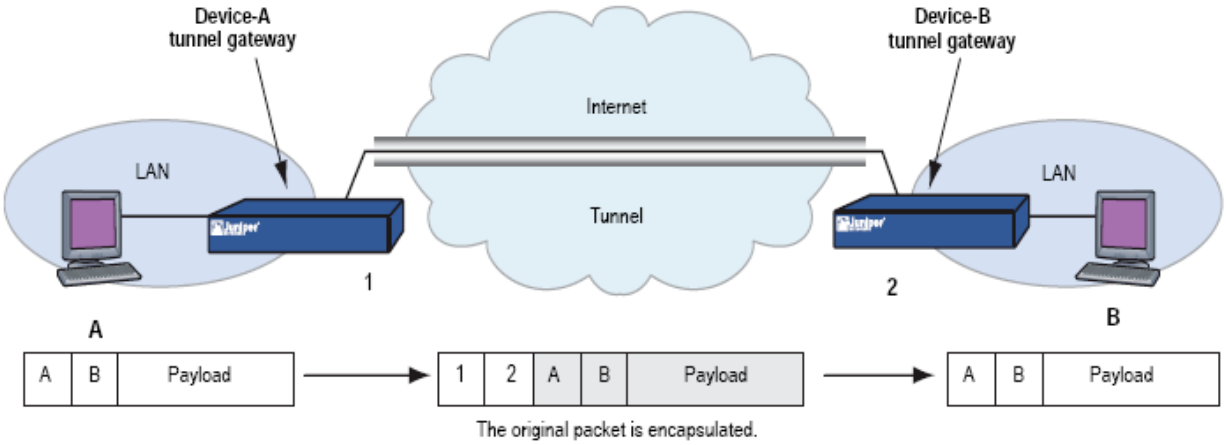

Figure 2 – Typical IPSec Configuration

IPSec supports the automated generation and negotiation of keys and security associations using the Internet Key Exchange (IKE) protocol. The JUNOS software performs all IPSec operations, including control of Security Associations and Key Management operations.

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.

1.7.2 Physical Boundary

The TOE is a combined hardware/software TOE and is defined as the JUNOS 10.0 R4 for J-Series and SRX-Series Platforms. The TOE boundary is shown below:

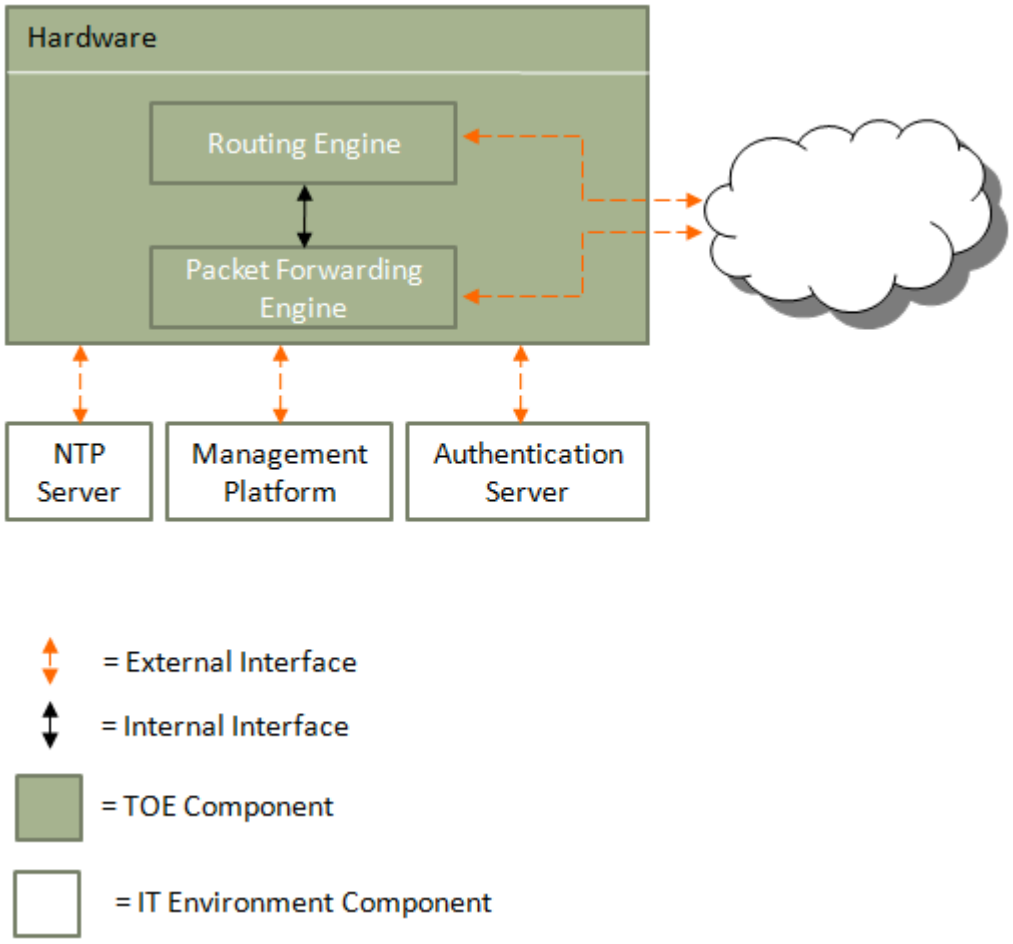

Figure 3 – TOE Boundary

The physical boundary is defined as the entire router chassis, as depicted below:

Figure 4 – J2320, J2350, J4350, J6350 (Top to Bottom)

The SRX series appliances are pictured below:

Figure 5 – SRX100, SRX210, SRX650, SRX3400, SRX3600, SRX5600, SRX5800 (Top to Bottom)

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

TOE COMPONENT	VERSION/MODEL NUMBER
Software Version	JUNOS US/Canada Version 10.0 R4 JUNOS-FIPS Version 10.0 R4
J-Series Hardware Version	J2320, J2350, J4350, J6350
SRX-Series	SRX100, SRX210, SRX240, SRX650, SRX3400, SRX3600, SRX5600, SRX5800

Table 3 – Evaluated Configuration for the TOE

The TOE interfaces are comprised of the following:

1. Network interfaces which pass traffic
2. Management interface through which handle administrative actions.

1.7.3 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 table:

TSF	DESCRIPTION
Audit	JUNOS auditable events are stored in the syslog files, and although they can be sent to an external log server, the requirements for auditing are met by local storage. Audit events cover authentication activity and configuration changes. Audit records include the date and time, event category, event type, username. An accurate time is gained by the router ntp daemon, acting as a client, from an NTP server in the IT environment. (The NTP server is considered outside the scope of the TOE.) This external time source allows synchronization the TOE audit logs with external audit log servers in the environment. The audit log can be viewed only by a super-user and custom-user with appropriate privileges.
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 also implements Internet Protocol Security (IPSec) support confidentiality, integrity, and authenticity of data transmitted from the TOE and received by the TOE in a VPN-configured state.

TSF	DESCRIPTION
Identification and Authentication	The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The TOE provides three levels of authority for users, providing administrative flexibility (additional flexibility is provided in JUNOS, but is outside the scope of the evaluation). Super-users and custom-users with appropriate privileges have the ability to define groups and their authority and they have complete control over the TOE. The routers also require that applications exchanging information with them successfully authenticate prior to any exchange. This covers all services used to exchange information, including telnet (out of scope), SSH, SSL, and FTP. Authentication services can be handled either internally (fixed user selected passwords) or through a RADIUS or TACACS+ authentication server in the IT environment (the external authentication server is considered outside the scope of the TOE).
Security Management	The router is managed using XML RPCs (JUNOScript), either through raw XML (API mode) as in the case of J-Web (over HTTP) and JUNOScope (over SSL) or through a Command Line Interface (CLI) protected by SSH. Both interfaces provide equivalent management functionality. Through these interfaces all management can be performed, including user management and the configuration of the router functions. The CLI interface is accessible through an SSH session, or via a local terminal console. Net conf is an IETF standardization effort which is closely aligned to JUNOScript.

Table 4 – Logical Boundary Descriptions

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.

2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE claims conformance to the EAL3 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009). The TOE does not claim conformance to any functional package.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

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*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.CONFLOSS	Failure of network components may result in loss of configuration data that cannot quickly be restored.
T.MANDAT	Unauthorized changes to the network configuration may be made through interception of in-band router management traffic on a network
T.NOAUDIT	Unauthorized changes to the router configurations and other management information will not be detected.
T.OPS	An unauthorized process or application may gain access to the TOE security functions and data, inappropriately changing the configuration data for the TOE security functions.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, inappropriately changing the configuration data for TOE security functions.
T.ROUTE	Network packets may be routed inappropriately due to accidental or deliberate misconfiguration.
T.UNTRUSTED_PATH	An attacker may attempt to disclose, modify or insert data within packet flows transmitted/received by the TOE over an untrusted network. If such an attack was successful, then the confidentiality, integrity and authenticity of packet flows transmitted/received over an untrusted path would be compromised.

Table 5 – Threats Addressed by the TOE

The IT Environment does not explicitly addresses any threats.

3.2 Organizational Security Policies

The TOE is not required to meet any organizational security policies.

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NOEVIL	The authorized users will be competent, and not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
AE.EAUTH	External authentication services will be available via either RADIUS, TACACS+, or both.
AE.TIME	External NTP services will be available.
AE.CRYPTO	In-band management traffic will be protected using SSL or SSH.

Table 6 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCESS	The TOE must only allow authorized users and processes (applications) to access protected TOE functions and data.
O.AMANAGE	The TOE management functions must be accessible only by authorized users.
O.AUDIT	Users must be accountable for their actions in administering the TOE.
O.AUTHENTICITY	The TOE must provide the means for ensuring that a packet flow has been received from a trusted source.
O.CONFIDENTIALITY	The TOE must protect the confidentiality of packet flows transmitted to/from the TOE over an untrusted network.
O.EADMIN	The TOE must provide services that allow effective management of its functions and data.
O.FLOW	The TOE must ensure that network packets flow from source to destination according to available routing information.
O.INTEGRITY	The TOE must ensure that any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected.
O.PROTECT	The TOE must protect against unauthorized accesses and disruptions of TOE functions and data.
O.ROLBAK	The TOE must enable rollback of router configurations to a known state.
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.

Table 7 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ADMIN	Authorized users must follow all guidance
OE.CRYPTO	SSL or SSH must be enabled for all in-band management traffic
OE.EAUTH	A RADIUS server, a TACACS+ server, or both must be available for external authentication services.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
OE.TIME	NTP server(s) will be available to provide accurate/synchronized time services to the router.

Table 8 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

THREATS/ ASSUMPTIONS / OBJECTIVES	T.ROUTE	T.PRIVIL	T.OPS	T.MANDAT	T.CONFLOSS	T.NOAUDIT	T.UNTRUSTED_PATH	A.LOCATE	A.NOEVIL	A.TIME	A.EAUTH	A.CRYPTO
O.FLOW	✓											
O.PROTECT	✓	✓	✓									
O.EADMIN	✓				✓							
O.AMANAGE	✓	✓		✓								
O.ACCESS	✓	✓	✓	✓								
O.ROLBAK	✓	✓	✓		✓							
O.AUDIT	✓	✓	✓	✓		✓			✓			
O.AUTHENTICITY							✓					
O.CONFIDENTIALITY							✓					
O.INTEGRITY							✓					
O.SECURE_KEY							✓					
OE.EAUTH		✓									✓	
OE.TIME										✓		
OE.CRYPTO												✓
OE.PHYSICAL								✓				
OE.ADMIN									✓			

Table 9 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1.1 Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.CONFLOSS	This threat is completely countered by • O.EADMIN, which ensures that the TOE provides services that allow effective management of its functions and data • O.ROLBAK which ensures the TOE enables rollback of TOE configurations to a known state.

THREAT	RATIONALE
T.MANDAT	This threat is completely countered by • O.ACCESS which ensures the TOE only allows authorized users and processes (applications) to access protected TOE functions and data. • O.AMANAGE which ensures that the TOE management functions are accessible only by authorized users. • O.AUDIT which ensures users are accountable for their actions in administering the TOE.
T.NOAUDIT	This threat is completely countered by O.AUDIT, which ensures users are accountable for their actions in administering the TOE.
T.OPS	This threat is completely countered by • O.ACCESS which ensures the TOE only allows authorized users and processes (applications) to access protected TOE functions and data. • O.AUDIT which ensures users are accountable for their actions in administering the TOE. • O.PROTECT which ensures the TOE protects against unauthorized accesses and disruptions of TOE functions and data. • O.ROLBAK which ensures TOE enables rollback of TOE configurations to a known state.
T.PRIVIL	This threat is completely countered by • O.ACCESS which ensures the TOE only allows authorized users and processes (applications) to access protected TOE functions and data. • O.AMANAGE which ensures that the TOE management functions are accessible only by authorized users. • O.AUDIT which ensures users are accountable for their actions in administering the TOE. • O.PROTECT which ensures the TOE protects against unauthorized accesses and disruptions of TOE functions and data. • O.ROLBAK which ensures TOE enables rollback of TOE configurations to a known state.
T.ROUTE	This threat is completely countered by • O.ACCESS which ensures the TOE only allows authorized users and processes (applications) to access protected TOE functions and data. • O.AUDIT which ensures users are accountable for their actions in administering the TOE. • O.AMANAGE which ensures that the TOE management functions are accessible only by authorized users. • O.EADMIN which ensures that the TOE provides services that allow effective management of its functions and data • O.FLOW which ensures that network packets flow from source to destination according to available routing information in the TOE configuration. • O.PROTECT which ensures the TOE protects against unauthorized accesses and disruptions of TOE functions and data. • O.ROLBAK which ensures TOE enables rollback of TOE configurations to a known state.

THREAT	RATIONALE
T.UNTRUSTED_PATH	This threat is completely countered by • O.INTEGRITY which ensures that any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected. • O.AUTHENTICITY which ensures the TOE can ensure that a packet flow has been received from a trusted source. • O.CONFIDENTIALITY which ensures that the TOE protects the confidentiality of packet flows transmitted to/from the TOE over an untrusted network. • O.SECURE_KEY which ensures the TOE provides 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.

Table 10 – Mapping of Objectives to Threats

4.3.1.2 Rationale for Security Objectives of the TOE

OBJECTIVE	RATIONALE
O.ACCESS	This objective addresses the need to protect the TOE's operations and data. This helps counter the threats of incorrect routing (T.ROUTE), unauthorized access (T.PRIVIL and T.OPS), and interception (T.MANDAT).
O.AMANAGE	The objective to limit access to management functions helps ensure correct routing (T.ROUTE), and helps counter the threat of unauthorized access (T.PRIVIL), and interception (T.MANDAT).
O.AUDIT	This objective serves to discourage and detect inappropriate use of the TOE (T.NOAUDIT), and as such helps counter T.ROUTE, T.PRIVIL, T.OPS and T.MANDAT. It also helps to support the assumption A.NOEVIL, by recording actions of users.
O.AUTHENTICITY	This objective ensures that a packet flow has been received from a trusted source (T.UNTRUSTED_PATH)
O.CONFIDENTIALITY	This objective ensures the protection of confidentiality of packet flows transmitted to/from the TOE over an untrusted network (T.UNTRUSTED_PATH).
O.INTEGRITY	This objective ensures that any attempt to corrupt or modify a packet flow transmitted to/from the TOE is detected (T.UNTRUSTED_PATH).
O.EADMIN	This objective is to provide effective management tools that assist in the correct routing of packets (T.ROUTE) and help to recover from failures (T.CONFLOSS).
O.FLOW	This objective helps to counters the threat T.ROUTE through the use of routing tables to correctly route information.
O.PROTECT	This objective contributes to correct routing of information (T.ROUTE) and prevention of disruption to TOE functions by users (T.PRIVIL) or processes (T.OPS).
O.ROLBAK	The objective to restore previous configurations helps ensure correct routing of data (T.ROUTE), and helps recover from loss of configuration data (T.CONFLOSS) and unauthorized changes (T.PRIVIL, T.OPS).
O.SECURE_KEY	The objective mitigates the threat of data modification or disclosure by ensuring that cryptographic keys are generated sufficiently, kept confidential, and destroyed property (T.UNTRUSTED_PATH)

OBJECTIVE	RATIONALE
OE.ADMIN	The objective that users should follow guidance supports the assumption that they will not be careless, willfully negligent or hostile (A.NOEVIL).
OE.CRYPTO	The objective to use SSL or SSH to protect in-band management traffic supports the assumption that cryptography is used to protect management traffic (A.CRYPTO).
OE.EAUTH	The objective to have an authentication server in the TOE environment helps to counter the threat of unauthorized access (T.PRIVIL), and supports the assumption that such a server is present (A.EAUTH).
OE.PHYSICAL	The objective to provide physical protection for the TOE supports the assumption that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access (A.LOCATE).
OE.TIME	The objective to have an NTP server in the TOE environment supports the assumption (A.TIME) that time services are available to provide the router with accurate/synchronized time information.

Table 11 – Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Definition of Extended Components

FCS_CKM_SYM_EXP.1 Cryptographic Key Establishment for AES Symmetric Keys was created to define the details of ANSI X9.42 key establishment.

Management: FCS_CKM_SYM_EXP.1

There are no management activities foreseen.

Audit: FCS_CKM_SYM_EXP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of the activity.

b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

FCS_CKM_SYM_EXP.1 Cryptographic Key Establishment for AES Symmetric Keys

Hierarchical to: No other components

Dependencies: [FCS_CKM.1 Cryptographic Key Generation, FCS_COP.1 Cryptographic Operation]

FCS_CKM_SYM_EXP.1.1 The cryptomodule shall provide the following cryptographic key establishment using Discrete Logarithm Key Agreement that meets the following:

a) The cryptomodule shall provide the capability to act as the initiator or responder (that is, act as Party U or Party V as defined in the standard) to agree on cryptographic keys of all sizes using the [assignment: *key agreement scheme*] key agreement scheme where domain parameter p is a prime of [assignment: *size(s) in bits of P value(s)*] and domain parameter q is a prime of [assignment: *size(s) in bits of Q value(s)*], and that conforms with ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography.

b) The cryptomodule shall conform to a standard using a FIPS-approved Random Number generation function and a FIPS-approved Hashing function.

c) The choices and options used in conforming to the key agreement scheme(s) are as follows: [assignment: *prerequisites and other applicable standards*].

6 Security Requirements

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

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_ARP.1	Security Alarms
	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAA.1	Potential Violation Analysis
	FAU_SAR.1	Audit Review
	FAU_STG.1	Protected Audit Trail Storage
Communication	FCO_NRO.2	Enforced Proof of Origin
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM_SYM_EXP.1	Cryptographic Key Establishment for AES symmetric keys
	FCS_CKM.2	Cryptographic Key Distribution
	FCS_COP.1	Cryptographic Operation
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_ROL.1	Basic Rollback
	FDP_UCT.1	Basic Data Exchange Confidentiality
	FDP_UIT.1	Data Exchange Integrity
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.2	Secure Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_STM.1	Reliable Time Stamps

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
TOE Access	FTA_TSE.1	TOE Session Establishment
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted Channel

Table 12 – TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_ARP.1 Security Alarms

FAU_ARP.1.1 The TSF shall take [the following configurable actions: create a log entry and drop connection] upon detection of a potential security violation.

6.1.1.2 FAU_GEN.1 Audit Data Generation

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

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

b) All auditable events for the [*not specified*] level of audit; and

c) [User login/logout;

d) Login failures;

e) Configuration is committed on a device;

f) Configuration is changed;

g) Errors during processing of the Routed Information Flow Control SFP and the Secure Information Flow Control SFP]

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other audit relevant information].

6.1.1.3 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.4 FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [failed authentication attempt events] known to indicate a potential security violation;

b) [no other rules].

6.1.1.5 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [super-users and custom-users with appropriate privileges] 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.

6.1.1.6 FAU_STG.1 Protected Audit Trail Storage

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

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

6.1.2 Communication (FCO)

6.1.2.1 FCO_NRO.2 Enforced Proof of Origin

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted [IP packets protected by the Secure Information Flow Control SFP] at all times.

FCO_NRO.2.2 The TSF shall be able to relate the [IPSec peer] of the originator of the information, and the [digital signature] of the information to which the evidence applies.

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to [the receiving TOE] given [the successful establishment of an IPSec security association with the transmitting TOE].

6.1.3 Cryptographic Support (FCS)

6.1.3.1 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 [ANSI X9.31] and specified cryptographic key sizes [128-, 192-, or 256-bit AES key and 728-, 1024-, or 1536-bit P values for Diffie Hellman] that meet the following: [FIPS 197 for AES and ANSI X9.42 for Diffie-Hellman].

Application Note: This requirement's dependency on FCS_CKM.4 is not met; FCS_CKM.4 is excluded from the Security Target because key destruction is implemented in hardware. However, as specified in the ADV_ARC.1 evidence, the architecture addresses this by not providing any commands to retrieve keys and not providing any functions pertaining to a general-purpose operating system. Additionally, the operational environment helps counter this by not providing unauthorized physical access to the TOE (see OE.PHYSICAL).

6.1.3.2 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 [Simple Certificate Enrollment Protocol (SCEP)] that meets the following: [SCEP-IETF, PKCS#7, X.509].

Application Note: This requirement's dependency on FCS_CKM.4 is not met; FCS_CKM.4 is excluded from the Security Target because key destruction is implemented in hardware. However, as specified in the ADV_ARC.1 evidence, the architecture addresses this by not providing any commands to retrieve keys and not providing any functions pertaining to a general-purpose operating system. Additionally, the operational environment helps counter this by not providing unauthorized physical access to the TOE (see OE.PHYSICAL).

6.1.3.3 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)	256	FIPS 197

OPERATION	ALGORITHM (MODE)	KEY SIZE IN BITS	STANDARDS
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	ANSI X9.31	Not Applicable	ANSI X9.31
Digital Signatures	RSA	Modulus Size: 1024	PKCS7

Table 13 – Cryptographic Operations

Application Note: This requirement's dependency on FCS_CKM.4 is not met; FCS_CKM.4 is excluded from the Security Target because key destruction is implemented in hardware. However, as specified in the ADV_ARC.1 evidence, the architecture addresses this by not providing any commands to retrieve keys and not providing any functions pertaining to a general-purpose operating system. Additionally, the operational environment helps counter this by not providing unauthorized physical access to the TOE (see OE.PHYSICAL).

6.1.3.4 FCS_CKM_SYM_EXP.1 Cryptographic Key Establishment for AES symmetric keys

Rationale for explicitly stated SFR: This SFR is necessary to define the details of ANSI X9.42 key establishment.

FCS_CKM_SYM_EXP.1.1 The cryptomodule shall provide the following cryptographic key establishment using Discrete Logarithm Key Agreement that meets the following:

a) The cryptomodule shall provide the capability to act as the initiator or responder (that is, act as Party U or Party V as defined in the standard) to agree on cryptographic keys of all sizes using the [dhHybrid5] key agreement scheme where domain parameter p is a prime of [1024/1536- bit P values] and domain parameter q is a prime of [160-bit Q value], and that conforms with ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography.

b) The cryptomodule shall conform to a standard using a FIPS-approved Random Number generation function and a FIPS-approved Hashing function.

c) The choices and options used in conforming to the key agreement scheme(s) are as follows: [prerequisites - domain parameters are validated

as they are received from a trusted entity, the CM, to have validated them in accordance with sec. 7.2; public keys (Yv and Tv) are validated locally be party V using trusted routines (sec. 7.4 option 3) and party U trusts that the public keys it receives have already been validated (sec. 7.4 option 4); concatenated mode is used (sec. 7.7.2)].

6.1.4 Information Flow Control (FDP)

6.1.4.1 FDP_IFC.1(1) – Subset Information Flow Control

FDP_IFC.1.1(1) The TSF shall enforce the [Routed Information Flow Control SFP] on

[Subjects: unauthenticated external IT entities that send and receive packets through the TOE to one another,

Information: network packets sent through the TOE from one subject to another, and

Operations: send and receive].

6.1.4.2 FDP_IFF.1(1) – Simple Security Attributes

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

[Subject security attributes:

- Presumed address

Information security attributes:

- Presumed address of source subject
- Presumed address of destination subject
- Network layer protocol (statically-defined routes, RIPv1, RIPv2, OSPF, BGP, filter-based Forwarding, ECMP)
- Zone on which packet arrives and departs].

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

[

- all the packet 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 packet security attributes, created by the authorized user;

- the presumed address of the source subject, in the packet, is consistent with the network interface it arrives on;
- and the presumed address of the destination subject, in the packet, can be mapped to a configured nexthop

].

FDP_IFF.1.3(1) 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(1) The TSF shall explicitly authorize an information flow based on the following rules: [no additional Routed Information Flow Control SFP rules].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [no additional denial rules].

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

FDP_IFC.1.1 (2) The TSF shall enforce the [Secure Information Flow Control SFP] on

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

Information: network traffic, and

Operations: IP packet forwarding].

6.1.4.4 FDP_IFF.1(2) – Simple Security Attributes

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

[Subject security attributes:

- Policy settings
- TOE identity credentials

Information security attributes:

- Presumed address of source subject
- Presumed address 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.

Operations: send and receive].

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 explicitly authorize an information flow based on the following rules: [no additional Secure Information Flow Control SFP rules].

FDP_IFF.1.5 (2) The TSF shall explicitly deny an information flow based on the following rules: [no additional denial rules].

6.1.4.5 FDP_ROL.1 Basic Rollback

FDP_ROL.1.1 The TSF shall enforce [the management access control policy[1]] to permit the rollback of the [committed configuration change] on the [router tables and access control lists].

FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the [limit of any of the last 50 committed configurations or a designated "rescue" configuration].

6.1.4.6 FDP_UCT.1 Basic Data Exchange Confidentiality

FDP_UCT.1.1 The TSF shall enforce the [Secure Information Flow Control SFP] to be able to [*transmit*, *receive*] user data in a manner protected from unauthorized disclosure.

6.1.4.7 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the [Secure Information Flow Control SFP] to be able to [*transmit*, *receive*] ~~user data~~ **packet flows** in a manner protected from [*modification*, *insertion*, *replay*] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of ~~user data~~ **packet flows**, whether [*modification*, *insertion*, *replay*] has occurred.

[1] As specified by FMT requirements

6.1.5 Identification and Authentication (FIA)

6.1.5.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Authentication Data, Privilege Level].

6.1.5.2 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [password minimum length of 6 characters with at least one change of character type (e.g., uppercase, lowercase, numeric, or special characters)].

6.1.5.3 FIA_UAU.2 User Authentication before Any Action

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

6.1.5.4 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide [internal fixed password mechanism and external server (RADIUS or TACACS+) gateway mechanism] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [authentication mechanism specified by an authorized user].

6.1.5.5 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.

6.2 Security Management (FMT)

6.2.1.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behavior of, disable, enable, modify the behavior of*] the functions [that implement the Routed Information Flow Control SFP and the Secure Information Flow Control SFP] to [super-users and custom-users with appropriate privileges].

6.2.1.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Routed Information Flow Control SFP and the Secure Information Flow Control SFP] to restrict the ability to [*query, modify, delete*]

the security attributes [TOE configuration (e.g., routing tables and access control lists)] to [super-users and custom-users with appropriate privileges].

6.2.1.3 FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [security attributes listed with Routed Information Flow Control SFP and the Secure Information Flow Control SFP].

6.2.1.4 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Routed Information Flow Control SFP and the Secure Information Flow Control SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [super-users and custom-users with appropriate privileges] to specify alternative initial values to override the default values when an object or information is created.

6.2.1.5 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to **control** the [data described in the table below] to [super-users and custom-users with appropriate privileges]:

DATA	CHANGE DEFAULT	QUERY	MODIFY	DELETE	CLEAR
Routed Information Flow Control SFP	✓	✓	✓	✓	✓
Secure Information Flow Control SFP	✓	✓	✓	✓	✓
User Account Attributes			✓		
Audit Logs				✓	
Date/Time			✓		
Rules that restrict the ability to establish management sessions			✓		

Table 14 – Management of TSF data

6.2.1.6 FMT_SMF.1 Specification of Management Functions

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

a) modify TOE configuration, including

a. rollback of configuration

b. control of management session establishment

c. configuration of Routed Information Flow Control SFP

d. configuration of Secure Information Flow Control SFP

b) modify user account attributes (including operation of identification and authentication),

c) delete audit logs,

d) modify the date/time,

e) modify security pattern matching for identification of potential violations].

6.2.1.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [read-only user, operator user, custom-user, super-user].

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

6.2.2 Protection of the TSF (FPT)

6.2.2.1 FPT_STM.1 Reliable Time Stamps

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

6.2.3 TOE Access (FTA)

6.2.3.1 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [access control policy specifying a source/destination IP address and source/destination TCP/UDP port number].

6.2.4 Trusted Path/Channels (FTP)

6.2.4.1 FTP_ITC.1 Inter-TSF trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF* and *another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [the secure transmission of traffic between trusted networks].

6.3 Security Functional Requirements for the IT Environment

6.3.1 Identification and Authentication (FIA)

6.3.1.1 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The ~~TSF~~ **IT Environment** shall provide [any necessary RADIUS or TACACS+ server] to support user authentication.

FIA_UAU.5.2 The ~~TSF~~ **IT Environment** shall authenticate any user's claimed identity according to the [authentication mechanism specified by an authorized user].

6.4 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.5.3 – Security Assurance Requirements.

6.5 Security Requirements Rationale

6.5.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

SFR \ OBJECTIVE	O.FLOW	O.PROTECT	O.EADMIN	O.AMANAGE	O.ACCESS	O.ROLBAK	O.AUDIT	O.CONFIDENTIALITY	O.INTEGRITY	O.AUTHENTICITY	O.SECURE_KEY
FAU_ARP.1		✓					✓				
FAU_GEN.1							✓				
FAU_GEN.2							✓				

SFR \ OBJECTIVE	O.FLOW	O.PROTECT	O.EADMIN	O.AMANAGE	O.ACCESS	O.ROLBAK	O.AUDIT	O.CONFIDENTIALITY	O.INTEGRITY	O.AUTHENTICITY	O.SECURE_KEY
FAU_SAA.1		✓					✓				
FAU_SAR.1							✓				
FAU_STG.1							✓				
FCO_NRO.2										✓	
FCS_CKM.1											✓
FCS_CKM_SYM_EXP.1											✓
FCS_CKM.2											✓
FCS_COP.1								✓	✓	✓	
FDP_IFC.1(1)	✓	✓									
FDP_IFF.1(1)	✓	✓									
FDP_IFC.1(2)								✓	✓	✓	
FDP_IFF.1(2)								✓	✓	✓	
FDP_ROL.1						✓					
FDP_UCT.1								✓			
FDP_UIT.1									✓		
FIA_ATD.1		✓		✓	✓		✓				
FIA_SOS.1		✓		✓	✓						
FIA_UAU.2		✓		✓	✓						
FIA_UAU.5		✓		✓	✓						
FIA_UID.2		✓		✓	✓						
FMT_MOF.1		✓		✓	✓						
FMT_MSA.1	✓		✓					✓	✓	✓	
FMT_MSA.2	✓		✓					✓	✓	✓	
FMT_MSA.3	✓		✓								
FMT_MTD.1	✓	✓		✓	✓		✓	✓	✓	✓	
FMT_SMF.1	✓	✓	✓	✓	✓		✓	✓	✓	✓	
FMT_SMR.1	✓	✓	✓	✓	✓		✓	✓	✓	✓	
FPT_STM.1							✓				
FTA_TSE.1				✓							
FTP_ITC.1								✓	✓	✓	

Table 15 – Mapping of TOE Security Functional Requirements and Objectives

6.5.2 Sufficiency of Security Requirements

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

SFR	RATIONALE
FAU_ARP.1	This component takes action following detection of potential security violations, and therefore contributes to meeting O.PROTECT and O.AUDIT.
FAU_GEN.1	This component outlines what events must be audited, and aids in meeting O.AUDIT.
FAU_GEN.2	This component required that each audit event be associated with a user, and aids in meeting O.AUDIT.
FAU_SAA.1	This component helps to detect potential security violations, and aids in meeting O.PROTECT and O.AUDIT.
FAU_SAR.1	This component requires that the audit trail can be read, and aids in meeting O.AUDIT.
FAU_STG.1	This component requires that unauthorized deletion of audit records does not occur, and thus helps to maintain accountability for actions, as required by O.AUDIT.
FCO_NRO.2	This component ensures that packet flows received by the TOE must have been digitally signed with key material associated with an identified remote trusted IT product (O.AUTHENTICITY).
FCS_CKM.1	This component ensures that cryptographic keys and parameters are generated with standards-based algorithms (O.SECURE_KEY).
FCS_CKM_SYM_EXP.1	This component ensures that the establishment of the trust relationship and the key exchange operations are standards-based and cryptographically sound (O.SECURE_KEY).
FCS_CKM.2	This component provides secure key distribution to remote trusted IT products (other instances of TOE), and between the TOE and a key server (CA). This enables the TOE to perform authentication using digital certificates, ensuring the source is trusted (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(1)	This component identifies the entities involved in the Routed Information Flow SFP (i.e. external IT entities sending packets), and aids in meeting O.FLOW and O.PROTECT.
FDP_IFF.1(1)	This component identifies the conditions under which information is permitted to flow between entities (the Routed Information Flow SFP), and aids in meeting O.FLOW and O.PROTECT.
FDP_IFC.1(2)	This component identifies and defines the Secure Information Flow Control 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).

SFR	RATIONALE
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).
FDP_ROL.1	This component allows previous router configurations to be restored, and aids in meeting O.ROLBAK.
FDP_UCT.1	This component provides confidentiality for packet flows received by, or transmitted from, the TOE using key material associated with an identified remote trusted IT product (O.CONFIDENTIALITY).
FDP_UIT.1	This component provides integrity for packet flows received by, or transmitted from, the TOE using key material associated with an identified remote trusted IT product (O.INTEGRITY).
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. The component aids in meeting O.PROTECT, O.AMANAGE, O.ACCESS and O.AUDIT.
FIA_SOS.1	This component specifies metrics for authentication, and aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).
FIA_UAU.2	This component ensures that users are authenticated to the TOE. As such it aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).
FIA_UAU.5	This component was selected to ensure that appropriate authentication mechanisms can be selected. As such it aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).
FIA_UID.2	This component ensures that users are identified to the TOE. As such it aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).

SFR	RATIONALE
FMT_MOF.1	This component relates to control of the functions that address detected security violations[2], and as such aids in meeting O.PROTECT`. This component relates to control of the functions that address identification and authentication (local or RADIUS/TACACS), and as such aids in meeting O.PROTECT, O.AMANAGE and O.ACCESS.
FMT_MSA.1	This component restricts the ability to modify, delete, or query the parameters for the Routed Information Flow Control SFP and the Secure Information Flow Control SFP to a privileged operator, and as such aids in meeting O.FLOW, O.CONFIDENTIALITY, O.INTEGRITY, and O.AUTHENTICITY. It also assists in effective management, and as such aids in meeting O.EADMIN.
FMT_MSA.2	This component ensures that only secure values are accepted for the configuration parameters associated with the Routed Information Flow Control SFP and the Secure Information Flow Control SFP, and as such aids in meeting O.FLOW, O.CONFIDENTIALITY, O.INTEGRITY, and O.AUTHENTICITY. It also assists in effective management, and as such aids in meeting O.EADMIN.
FMT_MSA.3	This component ensures that there is a *default deny* policy for the information flow control security rules. As such it aids in meeting O.FLOW. It also assists in effective management, and as such aids in meeting O.EADMIN.
FMT_MTD.1	This component restricts the ability to modify the Routed Information Flow Control SFP and the Secure Information Flow Control SFP, and as such aids in meeting O.FLOW, O.AMANAGE, O.PROTECT, O.CONFIDENTIALITY, O.INTEGRITY, and O.AUTHENTICITY. This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.PROTECT, O.AMANAGE and O.ACCESS. This component restricts the ability to delete audit logs, and as such contributes to meeting O.AUDIT and O.AMANAGE. This component restricts the ability to modify the date and time, and as such contributes to meeting O.AUDIT and O.AMANAGE. This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.AMANAGE.
FMT_SMF.1	This component lists the security management functions that must be controlled. As such it aids in meeting O.FLOW, O.PROTECT, O.EADMIN, O.AMANAGE, O.ACCESS, O.AUDIT, O.CONFIDENTIALITY, O.INTEGRITY, and O.AUTHENTICITY.

[2] For Login events (from the CLI) only as potential violations via all other authentication methods are hardcoded and cannot be modified.

SFR	RATIONALE
FMT_SMR.1	Each of the components in the FMT class listed above relies on this component (apart from FMT_MSA.3). It defines the roles on which access decisions are based. As such it aids in meeting O.FLOW, O.PROTECT, O.EADMIN, O.AMANAGE, O.ACCESS, O.AUDIT, O.CONFIDENTIALITY, O.INTEGRITY, and O.AUTHENTICITY.
FPT_STM.1	This component ensures that reliable time stamps are provided for audit records and aids in meeting O.AUDIT.
FTA_TSE.1	This component limits the range of locations from which a user session can be established, and hence reduces the chance of unauthorized access. As such it aids in meeting O.AMANAGE.
FTP_ITC.1	This component establishes a trust relationship with another remote instance of the TOE, meeting OCONFIDENTIALITY, O.INTEGRITY, and O.AUTHENTICITY.

Table 16 – Rationale for TOE SFRs to Objectives

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

OBJECTIVE	RATIONALE
O.ACCESS	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. • FIA_SOS.1 which specifies metrics for authentication, and aids in meeting objectives to restrict access. • FIA_UAU.2 which ensures that users are authenticated to the TOE. • FIA_UAU.5 which ensures that appropriate authentication mechanisms can be selected. • FIA_UID.2 which ensures that users are identified to the TOE. • FMT_MOF.1 which relates to control of the functions that address detected security violations. • FMT_MTD.1 which restricts the ability to modify identification and authentication data • FMT_SMF.1 which lists the security management functions that must be controlled. • FMT_SMR.1 which defines the roles on which access decisions are based.

OBJECTIVE	RATIONALE
O.AMANAGE	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. • FIA_SOS.1 which specifies metrics for authentication, and aids in meeting objectives to restrict access. • FIA_UAU.2 which ensures that users are authenticated to the TOE. • FIA_UAU.5 which ensures that appropriate authentication mechanisms can be selected. • FIA_UID.2 which ensures that users are identified to the TOE. • FMT_MOF.1 which relates to control of the functions that address detected security violations. • FMT_MTD.1 which restricts the ability to modify the Routed Information Flow Control SFP and the Secure Information Flow Control SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, and restricts the ability to modify the data relating to TOE access locations • FMT_SMF.1 which lists the security management functions that must be controlled. • FMT_SMR.1 which defines the roles on which access decisions are based. • FTA_TSE.1 which limits the range of locations from which a user session can be established, and hence reduces the chance of unauthorized access.
O.AUDIT	This objective is completely satisfied by • FAU_ARP.1 which takes action following detection of potential security violations. • FAU_GEN.1 which outlines what events must be audited. • FAU_GEN.2 which requires that each audit event be associated with a user. • FAU_SAA.1 which helps to detect potential security violations. • FAU_SAR.1 which requires that the audit trail can be read. • FAU_STG.1 which requires that unauthorized deletion of audit records does not occur • FIA_ATD.1 which provides users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. • FMT_MTD.1 restricts the ability to delete audit logs and restricts the ability to modify the date and time. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based. • FPT_STM.1 ensures that reliable time stamps are provided for audit records.

OBJECTIVE	RATIONALE
O.AUTHENTICITY	This objective is completely satisfied by • FCO_NRO.2 ensures that packet flows received by the TOE must have been digitally signed with key material associated with an identified remote trusted IT product. • 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 Control 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). • FMT_MSA.1 restricts the ability to modify, delete, or query the parameters for the Routed Information Flow Control SFP and the Secure Information Flow Control SFP to a privileged operator • FMT_MSA.2 ensures that only secure values are accepted for the configuration parameters associated with the Routed Information Flow Control SFP and the Secure Information Flow Control SFP. • FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules. • FMT_MTD.1 restricts the ability to modify the Routed Information Flow Control SFP and the Secure Information Flow Control SFP. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based. • FTP_ITC.1 establishes a trust relationship with another remote instance of the TOE.

OBJECTIVE	RATIONALE
O.CONFIDENTIALITY	This objective is completely satisfied by • 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 Control 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). • FDP_UCT.1 provides confidentiality for packet flows received by, or transmitted from, the TOE using key material associated with an identified remote trusted IT product. • FMT_MSA.1 restricts the ability to modify, delete, or query the parameters for the Routed Information Flow Control SFP and the Secure Information Flow Control SFP to a privileged operator • FMT_MSA.2 ensures that only secure values are accepted for the configuration parameters associated with the Routed Information Flow Control SFP and the Secure Information Flow Control SFP. • FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules. • FMT_MTD.1 restricts the ability to modify the Routed Information Flow Control SFP and the Secure Information Flow Control SFP. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based. • FTP_ITC.1 establishes a trust relationship with another remote instance of the TOE.
O.EADMIN	This objective is completely satisfied by • FMT_MSA.1 assists in providing effective management of the TOE. • FMT_MSA.2 assists in providing effective management of the TOE. • FMT_MSA.3 assists in providing effective management of the TOE. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based.

OBJECTIVE	RATIONALE
O.FLOW	This objective is completely satisfied by • FDP_IFC.1(1) identifies the entities involved in the Routed Information Flow SFP (i.e. external IT entities sending packets). • FDP_IFF.1(1) identifies the conditions under which information is permitted to flow between entities (the Routed Information Flow SFP). • FMT_MSA.1 restricts the ability to modify, delete, or query the parameters for the Routed Information Flow Control SFP and the Secure Information Flow Control SFP to a privileged operator • FMT_MSA.2 ensures that only secure values are accepted for the configuration parameters associated with the Routed Information Flow Control SFP and the Secure Information Flow Control SFP. • FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based.

OBJECTIVE	RATIONALE
O.INTEGRITY	This objective is completely satisfied by • 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 Control 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). • FDP_UIT.1 provides integrity for packet flows received by, or transmitted from, the TOE using key material associated with an • identified remote trusted IT product. • FMT_MSA.1 restricts the ability to modify, delete, or query the parameters for the Routed Information Flow Control SFP and the Secure Information Flow Control SFP to a privileged operator • FMT_MSA.2 ensures that only secure values are accepted for the configuration parameters associated with the Routed Information Flow Control SFP and the Secure Information Flow Control SFP. • FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules. • FMT_MTD.1 restricts the ability to modify the Routed Information Flow Control SFP and the Secure Information Flow Control SFP. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based. • FTP_ITC.1 establishes a trust relationship with another remote instance of the TOE.

OBJECTIVE	RATIONALE
O.PROTECT	This objective is completely satisfied by • FAU_ARP.1 takes action following detection of potential security violations. • FAU_SAA.1 helps to detect potential security violations. • FDP_IFC.1(1) identifies the entities involved in the Routed Information Flow SFP (i.e. external IT entities sending packets). • FDP_IFF.1(1) identifies the conditions under which information is permitted to flow between entities (the Routed Information Flow SFP). • FIA_ATD.1 exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. • FIA_SOS.1 specifies metrics for authentication, and aids in meeting objectives to restrict access. • FIA_UAU.2 ensures that users are authenticated to the TOE and as such it aids in meeting objectives to restrict access. • FIA_UAU.5 ensures that appropriate authentication mechanisms can be selected. • FIA_UID.2 ensures that users are identified to the TOE. • FMT_MOF.1 relates to control of the functions that address detected security violations and relates to control of the functions that address identification and authentication (local or RADIUS/TACACS). • FMT_MTD.1 restricts the ability to modify the Routed Information Flow Control SFP and the Secure Information Flow Control SFP to an authorized operator. • FMT_SMF.1 lists the security management functions available to authorized roles. • FMT_SMR.1 defines the roles on which authorized access decisions are based.
O.ROLBAK	This objective is completely satisfied by • FDP_ROL.1 allows previous router configurations to be restored.
O.SECURE_KEY	This objective is completely satisfied by • FCS_CKM.1 ensures that cryptographic keys and parameters are generated with standards-based algorithms. • FCS_CKM_SYM_EXP.1 ensures that the establishment of the trust relationship and the key exchange operations are standards-based and cryptographically sound. • FCS_CKM.2 provides secure key distribution to remote trusted IT products (other instances of TOE), and between the TOE and a key server (CA). This enables the TOE to perform authentication using digital certificates, ensuring the source is trusted.

Table 17 – Rationale for TOE Objectives to SFRs

6.5.3 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 (EAL3). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.3	Functional Specification with Complete Summary
	ADV_TDS.2	Architectural Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.3	Authorization Controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_LCD.1	Developer defined life-cycle model
ATE: Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 18 – Security Assurance Requirements at EAL3

6.5.4 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 3. EAL3 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL3 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

6.5.5 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements. Note that in some cases.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_FSP.3 Functional Specification with Complete Summary	Functional Specification: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
ADV_TDS.2 Architectural Design	Architectural Design: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
ALC_CMC.3 Authorization Controls	Security Measures: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
ALC_CMS.3 Implementation representation CM coverage	Security Measures: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
ALC_DVS.1 Identification of Security Measures	Security Measures: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
ALC_LCD.1 Developer defined life-cycle model	Life Cycle Model: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
ATE_COV.2 Analysis of Coverage	Testing Evidence Supplement: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
ATE_DPT.1 Testing: Basic Design	Testing Evidence Supplement: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms
ATE_FUN.1 Functional Testing	Testing Evidence Supplement: Juniper Networks JUNOS 10.0 R4 for J-Series and SRX-Series Platforms

Table 19 – Security Assurance Rationale and Measures

7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Audit
- Information Flow Control
- Identification and Authentication
- Security Management

7.2 Audit

JUNOS creates and stores audit records for the following events:

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

b) User login/logout;

c) Login failures;

d) Configuration is committed;

e) Configuration is changed;

f) Errors during processing of the Routed Information Flow Control SFP and the Secure Information Flow Control SFP

Auditing is done using syslog. This can be configured to store the audit logs locally or to send them to one or more log servers (note that the use of an external syslog server is not included as part of the evaluated configuration). The syslogs are automatically deleted locally according to configurable limits on storage volume or number of days of logs to retain. Only a super-user and custom-user with appropriate privileges can delete the local audit logs.

JUNOS will record within each audit record the following information:

a) Date and time of the event[3], type of event, subject identity, and the outcome (success or failure) of the event; and

[3] The TOE uses NTP to provide reliable time stamps.

b) Identity of the user that caused the event.

JUNOS provides super-users and custom-users with appropriate privileges with the ability to display audit data from the CLI. Commands are available to list entire files, or to select records that match or do not match a pattern. Records can also be saved to files for further analysis offline. Read only users cannot view the audit records. The TOE can be configured to display selected audit events as they occur.

The daemons authenticating users to JUNOS perform analysis of failed authentication attempts to identify activity indicating a potential violation. The following patterns of activity are defined to represent a potential violation and the action specified is triggered:

- 1 failed authentication attempt – the connection will be dropped and an audit event will be generated.
- After each successive login failure via login (for CLI) or SSH throttling will be applied progressively increasing the time delay enforced between login attempts until the configured number of login attempts (default is 10) is reached, at which point the connection will be dropped. An audit event will be generated reporting each failed login. If, after a number of failed authentication attempts, another authentication failure occurs using a different username, an audit record will be generated reporting the number of repeated failures of the original username.

The audit mechanism is automatically started up when the TOE is initialized and shut down when the TOE is powered down.

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

- FAU_ARP.1
- FAU_GEN.1
- FAU_GEN.2
- FAU_SAA.1
- FAU_SAR.1
- FAU_STG.1
- FPT_STM.1

7.3 Information Flow Control

The TOE supports two information flow control policies: one for unsecured data flows (the Routed Information Flow Control SFP) and one for secured data flows (the Secure Information Flow Control SFP). Each Information Flow Control SFP is 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.

In the default configuration, 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 (VLAN ID). Multiple virtual routers can exist within the JUNOS configuration; for example, separate virtual routers are often configured for trusted and untrusted zones. The zone/VLAN ID provides a logical interface to a virtual router's routing table. From there, traffic is routed as dictated by the associated VR routing table.

Management sessions are controlled in the same manner as just described. Privileged operators can configure the TOE to allow or deny the establishment of a management session by defining and 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 is designed to route unauthenticated network traffic. Network traffic represents information flows between source and destination network entities. The specific routing of traffic is based on the routing configuration data that has been created by the TOE users or has been collected from network peers as defined by the TOE users. The routing decision is based on the presumed source and destination address of the packet, the network layer protocol, service and the interface on which the packet arrives and is to depart on. The TOE supports statically-defined routes, RIPv1, RIPv2, OSPF, BGP, filter-based Forwarding, and ECMP. Each of these protocols implements the Routed Information Flow Control SFP.

Additionally, 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 Control SFP, which includes support for OSPF routing via IPSec tunnel. 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 Control SFP.

The Manual Key option allows both ends of a tunnel to be separately configured all IPSec security parameters. 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 Routed Information Flow Control SFP or the Secure Information Flow Control SFP.

Additionally, JUNOS maintains a history of up to 50 versions of the configuration, and can rollback to any of them on request. In addition a configuration can be saved as the rescue configuration, without risk of it scrolling off the rollback history. When the router is booting, if the primary configuration is missing or corrupt, the rescue configuration will be loaded if present, otherwise the first rollback will be loaded if possible. If all else fails a factory default configuration will be loaded.

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

- FCO_NRO.2
- FCS_CKM.1
- FCS_CKM_SYM_EXP.1
- FCS_CKM.2
- FCS_COP.1
- FDP_IFC.1(1)
- FDP_IFF.1(1)

- FDP_IFC.1(2)
- FDP_IFF.1(2)
- FDP_ROL.1
- FDP_UCT.1
- FDP_UIT.1
- FTA_TSE.1
- FTP_ITC.1

7.4 Identification and Authentication

User accounts in the TOE have the following attributes: user name, authentication data (password) and privilege (user class). The super-users and custom-users with appropriate privileges can export the authentication process to a RADIUS/TACACS+ server.

If a user is authenticated remotely, a template user account on the TOE may be used to determine the privileges, rather than specifying privileges for each user. In this instance, a template user account is configured on the TOE and an individual user account is configured on the external authentication server. When the authentication server successfully authenticates the user they pass the unique username and the template account the username is to be associated with back to the TOE. The user name that was authenticated is used when generating audit records regarding activity by that user.

Locally stored authentication data for fixed password authentication is a case-sensitive, alphanumeric value. The password has a minimum length of 6 characters with at least one change of character set (upper, lower, numeric, punctuation, other), and can be up to 1278 ASCII characters in length (control characters are not recommended).

The TOE requires users to provide unique identification and authentication data (passwords) before any administrative access to the system is granted. The TOE software supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, a password is configured for each user allowed to log into the TOE. RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router. Both are distributed client/server systems—the RADIUS and TACACS+ clients run on the router, and the server runs on a remote network system in the IT environment.

If the identity specified is defined locally, the TOE can successfully authenticate that identity if the authentication data provided matches that stored in conjunction with the provided identity. Alternately, if the TOE is configured to work with a RADIUS or TACACS+ server, the identity and authentication data is provided to the server and the TOE enforces the result returned from the server. Regardless, no administrative actions are allowed until successful authentication as a privileged operator.

It should be noted that when RADIUS and/or TACACS+ are used for authentication, the TOE can verify only that the remote authentication server has the correct credentials.

The TOE can be configured to allow users to be authenticated via RADIUS and/or TACACS+. The order in which authentication mechanisms are attempted is applied to all users. The configuration can also specify that local passwords can only be used when external authentication servers are unavailable, or as a general fallback. For example, some users (such as 'root') might only be able to authenticate using local password, if they do not have a RADIUS/TACACS+ account configured and password is in the authentication-order.

Regardless of what access method is used for management sessions, successful authentication is required prior to giving a user access to the system. These mechanisms are used for administration of the routing functions as well as the administration of the user accounts used for management.

For non-administrative functions no authentication is required. The primary non-administrative function of the TOE is to route IP packets between PICs/PIMs. This passes the packets from one network to a destination network, enabling network connectivity.

Authentication data can be stored either locally or on a separate server. The separate server must support either the RADIUS or TACACS+ protocol to be supported by the TOE.

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

- FIA_ATD.1
- FIA_SOS.1
- FIA_UAU.2
- FIA_UAU.5
- FIA_UID.2

7.5 Security Management

The functionality in the TOE requires management to ensure proper configuration control.

The router restricts to a super-user and custom-user with appropriate privileges the ability to modify the number of failed authentication attempts via CLI Login that occur before progressive throttling is enforced for further authentication attempts and before the connection is dropped.

The number of failed authentication attempts that represent a potential violation is hard-coded and cannot be configured. The router restricts to a super-user and custom-user with appropriate privileges the ability to add or delete users, modify their access permissions or manage authentication attributes. This is handled by the management Daemon (MGD).

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. (This can be achieved automatically on the J-series routers if there is a DHCP server in the network environment.)

The router will not route to an indirectly connected subnet (through another routing device) unless a route is configured in the router.

The router restricts the ability to administer the router configuration data, including rollback of configurations, to only super-users and custom-users with appropriate privileges. 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 BGP, RIP and MPLS protocols can be managed, as well as PIM /PIC configurations, TCP/IP configurations and date/time. The TOE automatically routes traffic based on available routing information, much of which is automatically collected from the TOE environment.

The router restricts the ability to administer user data to only super-users and custom-users with appropriate privileges. The CLI provides super-users and custom-users with appropriate privileges with a text-based interface from which all user data can be managed. From this interface new accounts can be created, and existing accounts can be modified or deleted. This interface also provides the super-user and custom-user with appropriate privileges with the ability to configure an external authentication server, such as a RADIUS or TACACS+ server. When this is assigned, a user can be authenticated to the external server instead of directly to the TOE. If authentication-order includes RADIUS and/or TACACS+, then these will be consulted in the configured order for all users. Typically, local password is only used as a fallback in such cases.

The router can be configured to automatically delete audit logs, or they can be deleted manually. Both operations can be carried out only by a super-user and custom-user with appropriate privileges. The router will allow only a super-user and custom-user with appropriate privileges to modify the date/time setting on the router. The router will allow only a super-user and custom-user with appropriate privileges to create, delete or modify the rules that control the presumed address from which management sessions can be established.

The TOE provides the ability to manage the following security functions:

a) User authentication (authentication data, roles);

b) Router information;

c) Audit management and review;

d) Modify the time;

e) Session establishment restrictions;

f) Parameters for Routed Information Flow Control SFP and the Secure Information Flow Control SFP

The TOE has three pre-defined roles; when a new user account is created, it must be assigned one of these roles:

a) Super-user: this role can perform all management functions on the TOE. A user with this role can manage user accounts (create, delete, modify), view and modify the TOE configuration information.

b) Operator user: this role can read some configuration data, and in addition can use the following commands:

- Can clear (delete) information learned from the network that is stored in various network databases (using the clear commands),
- Can access the network by entering the ping and traceroute commands,
- Can restart software processes using the restart command.
- Can view trace file settings in configuration and operational modes.

c) Read-only user: this role can view status and statistics only.

Additionally, the TOE supports the creation of custom user roles, which are configured by the super-user. This “custom-user” may have a subset of any of the privileges of the pre-defined roles discussed above. To ensure secure values for the Routed Information Flow Control SFP and the Secure Information Flow Control SFP are entered, only super-user and custom-user with appropriate privileges can configure those attributes. Additionally, use of the CLI or J-Web will ensure that proper syntax is used when configuring those attributes.

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

- FMT_MOF.1
- FMT_MSA.1
- FMT_MSA.2
- FMT_MSA.3
- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1