Security Target

Juniper Networks Junos Pulse Access Control Service 4.2 R4

Document Version 1.3

5/30/2013 (updated)

Prepared For:

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

www.juniper.net

Prepared By:

Apex Assurance Group, LLC

530 Lytton Ave, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Juniper Networks Junos Pulse Access Control Service 4.2 R4. 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 Pulse Access Control Service 4.2 R4
ST Revision	1.3
ST Publication Date	5/30/2013
Author	Juniper Networks and Apex Assurance Group

1.2 TOE Reference

TOE Reference	Junos Pulse Access Control Service 4.2 R4

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
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
IC	Infranet Controller
IMC	Integrity Measurement Collectors
IMV	Integrity Measurement Verifier
LDAP	Lightweight Directory Access Protocol
NAC	Network Access Control
NTP	Network Time Protocol
OSP	Organizational Security Policy
RADIUS	Remote Authentication Dial-In User Service

TERM	DEFINITION
RFC	Request for Comment
RSA	Rivest Shamir Adelman
SA	Security Association
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
Syslog	System logging as specified in Request for Comment 5424
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UAC	Unified Access Control
VPN	Virtual Private Network

Table 2 – Acronyms Used in Security Target

1.6 TOE Overview

The TOE is the Junos Pulse Access Control Service 4.2 R4. The TOE is the central control point for Juniper Network's Unified Access Control (UAC) solution. Users can contact the TOE with a variety of clients in order to request network access. The TOE authenticates users and retrieves the access policies for those users. The TOE also assesses the health of a user's host machine and compares it to the policies in order to determine whether network access is allowed.

It then communicates with a variety of enforcement points (including Juniper endpoint clients filters, Juniper firewalls, and standard 802.1X enabled switches or wireless access points) to communicate the network access constraints based on the TOE's decision. The enforcement points will allow/deny access based on the TOE's result of authentication and policy compliance. The following figure shows the TOE (Infranet Controller) in a typical environment:

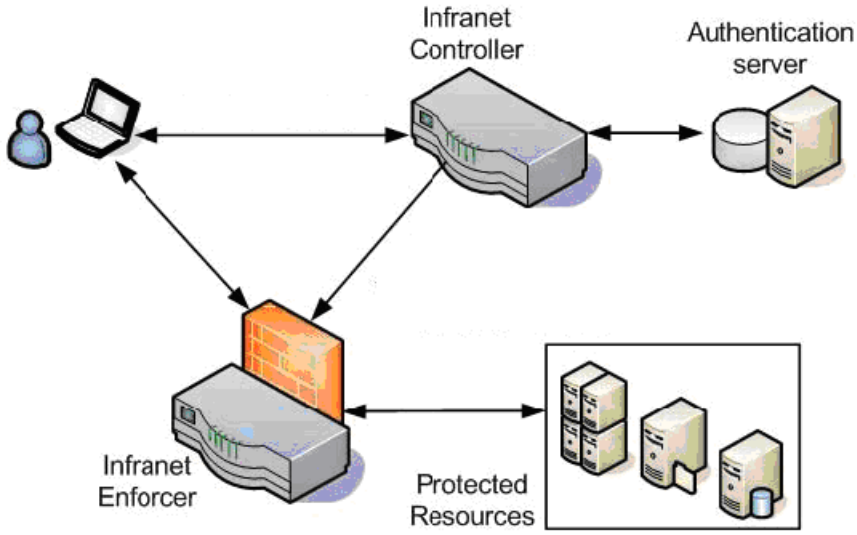

Figure 1 – The TOE in a Typical Environment

An Infranet Enforcer can be either a ScreenOS firewall device, or a J Series or SRX Series Services Gateway. The Infranet Enforcer is not part of the TOE as indicated in Figure 2 – TOE Boundary.

The TOE provides the following security functions: Security Audit, Cryptographic Support (including Cryptographic Operations), Information Flow Control, Identification and Authentication, Security Management. These security functions are described in Section 1.7.2 – Logical Boundary.

1.7 TOE Description

1.7.1 Physical Boundary

The TOE physical boundary is the appliance and software client running on a remote IT system. The appliance TOE component is completely self-contained, housing the software and hardware necessary to perform all functions. The TOE boundary is shown below:

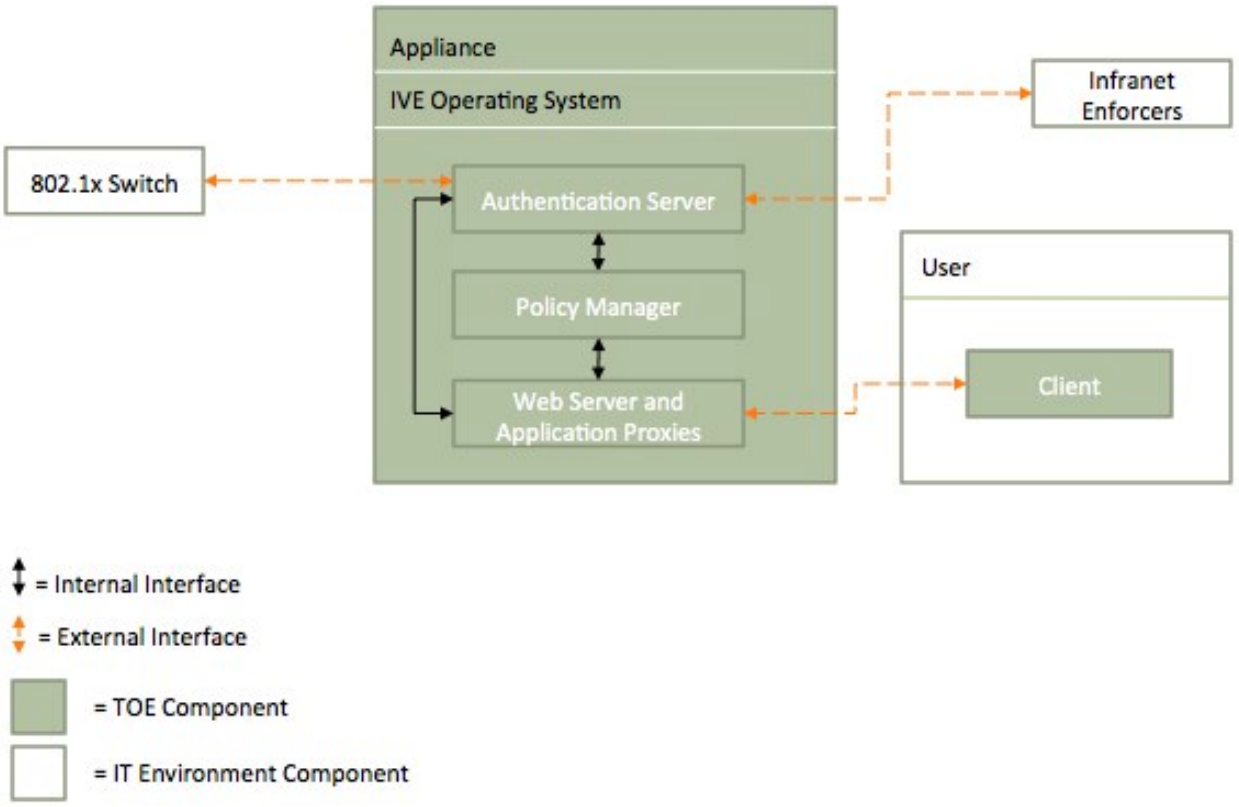

Figure 2 – TOE Boundary

The following hardware and software components comprise the TOE:

TOE COMPONENT	VERSION/MODEL NUMBER
Appliance Software	Version 4.2 R4
Appliance Hardware Note that not all appliances need to be installed in order for the TOE to run in evaluated configuration. One or more appliances can be used in the evaluated configuration.	• IC4000 Appliance • IC4500 Appliance • IC6000 Appliance • IC6500 Appliance • IC6500FIPS Appliance • MAG2600 • MAG4610 • MAG6610 with MAG-SM160 service module [and optional MAG-CM060 management module] • MAG6610 with MAG-SM360 service module [and optional MAG-CM060 management module] • MAG6611 with MAG-SM160 service module [and optional MAG-CM060 management module] • MAG6611 with MAG-SM360 service module [and optional MAG-CM060 management module]

TOE COMPONENT	VERSION/MODEL NUMBER
Client (note that all operating systems and the hardware running them are considered part of the IT Environment). Note that not all clients need to be installed in order for the TOE to run in evaluated configuration. One or more clients can be used in the evaluated configuration.	• Odyssey Access Client Version 5.3R2 o Windows Vista 32/64 bit o Windows 7 32/64 bit • Odyssey Access Client FIPS Edition Version 5.3R2 o Windows Vista 32/64 bit o Windows 7 32/64 bit • Agentless o Windows XP 32-bit o Windows Vista 32/64 bit o Windows 7 32/64 bit o Mac OS X 10.6 • Pulse Version 2.0R2 o Windows Vista 32/64 bit o Windows 7 32/64 bit

Table 3 – Evaluated Configuration for the TOE

The TOE interfaces comprise the following:

1. User client interfaces that handle user requests,
2. Authentication backend interfaces that consult external authentication servers,
3. Enforcer interfaces that apply access policies, and
4. Management interfaces that handle TOE administrative actions.

The management interface to the TOE includes a web-based administrative interface[1]. The end user directly interfaces to the TOE using a Web-Based user interface. Alternatively, the end user may use an 802.1X supplicant. In the latter case, the user interface to the TOE is RADIUS over TCP between the 802.1X Authenticator (switch or access point, acting as a RADIUS client) and the Authentication Server (which is a RADIUS server). Note the end user interface only handles authentication traffic, including user credentials. End user application data does not pass through the TOE.

In addition to the software clients, the TOE is composed of the following appliance components:

1. Web server and Application Proxies
2. Authentication Server
3. Policy Manager
4. Operating system

The TOE includes a proprietary web server developed by Juniper which provides the main interface for both users and administrators of the TOE. The web server provides users an interface to submit connection requests via an HTTPS encrypted tunnel. The web server provides administrators an

[1] Note that the serial port of the appliances is used for initial setup only; any management actions via the serial console are excluded from use in the evaluated configuration as specified in the Operational Guidance and Preparative Procedures.

interface to administrate the TOE using a web browser. The web server component is included as part of the TOE, and this includes application proxies to govern the use of and access to applications on the protected network.

The Authentication Server in the TOE verifies the credentials presented by the user (or presented by the Authenticator on behalf of the user) and associates the user with an access policy. The Authentication Server may use its integrated database, or it may consult an external authentication server. The interface to an external database may be RADIUS, or it may be a more generic database interface (e.g., LDAP).

The Policy Manager interfaces with external enforcement points like Juniper firewalls. It uses proprietary interfaces to set the access privileges of users that connect through those enforcement points.

The TOE utilizes a Linux-based operating system that includes the 2.4 kernel. The operating system is relied upon for all access to the physical hardware devices connected to the TOE and for providing reliable time stamping for audit data. Note that this operating system is locked down and purpose-built; no foreign or untrusted applications may be run on the appliance.

1.7.2 Logical Boundary

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

TSF	DESCRIPTION
Security Audit	The TOE generates audit records for security events. The administrator and the read-only administrator are the only roles with access to the audit trail and have the ability to view the audit trail.
Cryptographic Support	The TOE supports secure communications between the TOE and other IT entities in order to authenticate users and to transmit authorizations to enforcement points. Encryption prevents modification and disclosure of this information.
Information Flow Control	The TOE is designed to help prevent unwanted and non-compliant endpoints from gaining access to the local area network. The TOE compares endpoint configuration with defined security policies; a non-compliant endpoint is not allowed full access to the network.
Identification and Authentication	All users are required to perform identification and authentication before any information flows are permitted. Additionally, administrators must be authenticated before performing any administrative functions.
Security Management	The TOE provides a wide range of security management functions. Administrators can configure the TOE, manage users, the information flow policy, and audit among other routine maintenance activities.

Table 4 – Logical Boundary Descriptions

2 Conformance Claims

2.1 CC Conformance Claim

The TOE and ST are Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant and augmented with ALC_FLR.2.

2.2 PP Claim

The TOE and ST are do not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE and ST are claim conformance to the EAL3 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009). The TOE and ST do 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.NOAUDIT	An unauthorized person may attempt to change the TOE configurations and other management information, and this activity may 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.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between a remotely located authorized administrator and the TOE.
T.UNAUTH_ENDPOINT	An unauthorized person or unauthorized external IT entity may attempt to access a protected internal network, resulting in malicious or unidentified activity that may compromise sensitive data on that network.
T.TOECOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between distributed components of the TOE.

Table 5 – Threats Addressed by the TOE

The IT Environment does not explicitly address 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.

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.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.ENCRYPT	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
O.PROTECT	The TOE must protect against unauthorized accesses and disruptions of TOE functions and data.
O.SECKEY	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows.
O.UNAUTH_ENDPOINT	The TOE will detect unauthenticated, unauthorized, or non-compliant endpoints and deny access to the network until the endpoint is authenticated, authorized, and compliant to internal security policies.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components.

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 administrators are trained to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.

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.UNAUTH_ENDPOINT	T.PRIVIL	T.OPS	T.NOAUDIT	T.PROCOM	T.TOECOM	A.LOCATE	A.NOEVIL
O.AMANAGE		✓						
O.AUDIT		✓		✓				
O.ENCRYPT					✓	✓		
O.PROTECT		✓	✓					
O.SECKEY					✓	✓		
O.UNAUTH_ENDPOINT	✓							
O.TOECOM						✓		
OE.ADMIN								✓
OE.PHYSICAL							✓	

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

4.3.1.1 Rationale for Security Objectives of the TOE

OBJECTIVE	RATIONALE
T.NOAUDIT	This threat is countered by • O.AUDIT which ensures that users are accountable for their actions in administering the TOE.
T.OPS	This threat is countered by • O.PROTECT, which ensures that the TOE protects against unauthorized accesses and disruptions of TOE functions and data.
T.PRIVIL	This threat is countered by • 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 that the TOE protects against unauthorized accesses and disruptions of TOE functions and data.
T.PROCOM	This threat is countered by • O.ENCRYPT, which ensures that administrator management sessions are encrypted. • O.SECKEY, which ensures that TOE provides a means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows.
T.UNAUTH_ENDPOINT	This threat is countered by • O.UNAUTH_ENDPOINT, which ensures that the TOE detects unauthenticated, unauthorized, or non-compliant endpoints and denies access to the network until the endpoint is authenticated, authorized, and complaint to internal security policies.

OBJECTIVE	RATIONALE
T.TOECOM	This threat is completely countered by • O.TOECOM which ensures the TOE protects the confidentiality of its dialogue between distributed TOE components • O.ENCRYPT, which ensures that administrator management sessions are encrypted. • O.SECKEY, which ensures that TOE provides a means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows.
A.LOCATE	This threat is supported by • OE.PHYSICAL, which ensures that those responsible for the TOE must ensure that the TOE is protected from any physical attack.
A.NOEVIL	This threat is supported by • OE.ADMIN, which ensures that TOE administrators are trained to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents.

Table 10 – Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Definition of Extended Components

There are no extended components in this Security Target.

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_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_STG.1	Protected Audit Trail Storage
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Distribution
	FCS_COP.1	Cryptographic Operation
User Data Protection	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	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
	FPT_STM.1	Reliable Time Stamps
	FPT_ITT.1	Basic internal TSF data transfer protection

Table 11 – TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 – Audit Data Generation

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

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

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

c) [The events in column two of Table 12 – Auditable Events]

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

a) Date and time of the event, type of event, subject identity (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, [information specified in column three of Table 12 – Auditable Events].

SFR	EVENT	DETAILS
FMT_SMR.1	Modifications to the group of users that are part of a role.	The identity of the Administrator performing the modification and the user identity being associated with a role
FIA_UID.2	All use of the user identification mechanism.	None
FIA_UAU.2	Any use of the user authentication mechanism.	None
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Changes to the time.	The identity of the Administrator performing the operation
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the Administrator performing the operation

Table 12 – Auditable Events

6.1.1.2 FAU_SAR.1 – Audit Review

FAU_SAR.1.1 The TSF shall provide [an Administrator] with the capability to read [all audit information] from the audit records.

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

6.1.1.3 FAU_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 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 – Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [ANSI X9.31] and specified cryptographic key sizes [128-, 192-, or 256-bit AES key and 168-bit TDES key] that meet the following: [FIPS 197 for AES and FIPS 46-3 for TDES].

Application Note: This requirement's dependency on FCS_CKM.4 is not met because FCS_CKM.4 is excluded from the Security Target. However, the architecture addresses this by not providing any commands to retrieve keys and not providing and functions pertaining to a general-purpose operating system. Additionally, the operational environment helps counter this by not providing unauthorized physical access to the TOE.

6.1.2.2 FCS_CKM.2 – Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [RSA] that meets the following: [RSA_WITH_3DES_CBC_SHA or RSA_WITH_AES_CBC_SHA in the TLS specification in RFC 2246].

Application Note: This requirement's dependency on FCS_CKM.4 is not met because FCS_CKM.4 is excluded from the Security Target. However, 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.

6.1.2.3 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)	128, 192, 256	FIPS 197
	TDES	168	FIPS 46-3
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 because FCS_CKM.4 is excluded from the Security Target. However, the architecture addresses this by not providing any commands to retrieve keys and not providing and functions pertaining to a general-purpose operating system. Additionally, the operational environment helps counter this by not providing unauthorized physical access to the TOE.

6.1.3 Information Flow Control (FDP)

6.1.3.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [NAC Information Flow Control SFP] on

[Subjects: External IT entities attempting to access a network in the IT Environment

Information: Information contained on the protected network

Operations: Information access requests].

Application Note: The TOE (Infranet Controller) provides the information flow control decision by first verifying the username and password of the user and then a Host Checker Policy. The TOE will forward results to enforcement endpoints on the network (e.g., firewalls, Infranet Enforcers, etc.) that will uphold the flow control policy decision of the TOE.

6.1.3.2 FDP_IFF.1 – Simple Security Attributes

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

[Subject Security Attributes:

- IP Address

- MAC Address
- User role

Windows Entities:

- Antivirus software update status
- Virus signature update status
- Firewall status
- Anti-malware status
- Anti-spyware status
- Operating System Checks

Macintosh, Linux, and Solaris Entities:

- Ports
- Processes
- Files.

].

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

[

A. Monitoring option is enabled for the service and information structure type and:

1. The user successfully authenticates to the TOE and
2. The endpoint is compliant to the Host Checker Policy or
3. The endpoint MAC address is contained within an exception list.

Or

B. Monitoring is disabled.

].

FDP_IFF.1.3 The TSF shall enforce the [following additional rule:

If the Monitoring option is enabled for the service and information structure type; and the user of the endpoint successfully authenticates to the TOE; and the endpoint is not compliant with the Host check policy; and the endpoint is NOT in an exception list: the host is remediated in an isolated area of the network to attain compliance with the Host Checker Policy].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [No explicit authorization rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [No explicit denial rules].

Application Note: The TOE (Infranet Controller) provides the information flow control decision by first verifying the username and password of the user and then a Host Checker Policy. The TOE will forward results to enforcement endpoints on the network (e.g., firewalls, Infranet Enforcers, etc.) that will uphold the flow control policy decision of the TOE.

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [identity/username, association of a human user with a role, password].

6.1.4.2 FIA_SOS.1 – Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

1. Minimum of eight (8) characters,
2. Minimum of three (3) numeric characters,
3. Minimum of three (3) alphabetic characters,
4. Combination of both uppercase and lowercase alphabetic characters,
5. Different from the username, and
6. Different from the previously used password].

6.1.4.3 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.

6.1.4.4 FIA_UID.2 – User Identification before Any Action

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

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MOF.1 – 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 [NAC Information Flow Control SFP] to [an Administrator].

6.1.5.2 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [NAC Information Flow Control SFP] to restrict the ability to [*modify, delete*] the security attributes [defined FDP_IFF.1] to [the Administrator].

6.1.5.3 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 NAC Information Flow Control SFP].

6.1.5.4 FMT_MSA.3 – Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [NAC 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 [Administrator] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.5 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to **control** the [data described in the table below] to [the Administrator]:

DATA	CHANGE DEFAULT	QUERY	MODIFY	DELETE
NAC Information Flow Control SFP	✓	✓	✓	✓
User Account Attributes	✓	✓	✓	✓

DATA	CHANGE DEFAULT	QUERY	MODIFY	DELETE
Audit Logs		✓	✓	✓
Date/Time			✓	
Rules that restrict the ability to establish management sessions			✓	
Cryptographic algorithms used in protected communications sessions with external IT entities		✓	✓	

Table 14 – Management of TSF data

6.1.5.6 FMT_SMF.1 Specification of Management Functions

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

a) Reboot the appliance, shut down the appliance, or restart services (all via management GUI);

b) Create, delete, modify, and view Host Checker Policies;

c) Create, delete, modify, and view user attribute values defined in FIA_ATD.1;

d) Enable and disable external IT entities from communicating to the TOE;

e) Modify and set the time and date;

f) Archive, clear, filter, and review the audit trail

g) Define cryptographic algorithms used in protected communications sessions with external IT entities].

6.1.5.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [User, Administrator, Read-Only Administrator].

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

6.1.5.8 FPT_ITT.1 – Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from [*disclosure* **and** *modification*] when it is transmitted between separate parts of the TOE.

6.1.5.9 FPT_STM.1 – Reliable Time Stamps

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

6.2 Security Functional Requirements for the IT Environment

There are no Security Functional Requirements for the IT Environment.

6.3 Security Assurance Requirements

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

6.4 Security Requirements Rationale

6.4.1 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.ENCRYPT	O.SECKEY	O.UNAUTH_ENDPOINT	O.PROTECT	O.AMANAGE	O.TOECOM	O.AUDIT
FAU_GEN.1							✓
FAU_SAR.1							✓
FAU_STG.1							✓
FCS_CKM.1	✓	✓					
FCS_CKM.2	✓	✓					
FCS_COP.1	✓	✓					
FDP_IFC.1			✓				
FDP_IFF.1			✓				
FIA_ATD.1				✓	✓		✓
FIA_SOS.1				✓	✓		
FIA_UAU.2				✓	✓		
FIA_UID.2				✓	✓		

SFR \ OBJECTIVE	O.ENCRYPT	O.SECKEY	O.UNAUTH_ENDPOINT	O.PROTECT	O.AMANAGE	O.TOECOM	O.AUDIT
FMT_MOF.1				✓	✓		
FMT_MSA.1			✓				
FMT_MSA.2			✓				
FMT_MSA.3			✓				
FMT_MTD.1			✓	✓	✓		✓
FMT_SMF.1			✓	✓	✓		✓
FMT_SMR.1			✓	✓	✓		✓
FPT_STM.1							✓
FPT_ITT.1						✓	

Table 15 – Mapping of TOE Security Functional Requirements and Objectives

6.4.2 Sufficiency of Security Requirements

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

SFR	RATIONALE
O.AMANAGE	This objective is met by • FIA_ATD.1, which specifies the list of security attributes belonging to individual users • FIA_SOS.1, which specifies minimum requirements for passwords • FIA_UAU.2, which requires operator authentication before any action • FIA_UID.2, which requires operator authentication before any action • FMT_MOF.1, which restricts configuration of the NAC Information Flow Control SFP to an Administrator • FMT_MTD.1, which restricts control of user and TOE data to an Administrator • FMT_SMF.1, which specifies management functions available in the TOE • FMT_SMR.1, which specifies roles available to TOE users

SFR	RATIONALE
O.AUDIT	This objective is met by • FAU_GEN.1, which specifies auditing requirements for the TOE • FAU_SAR.1, which ensures audit information can be read by the Administrator • FAU_STG.1, which ensures audit records are protected from unauthorized access or deletion • FIA_ATD.1, , which specifies the list of security attributes belonging to individual users • FMT_MTD.1, which restricts control of user and TOE data to an Administrator • FMT_SMF.1, which specifies management functions available in the TOE • FMT_SMR.1, which specifies roles available to TOE users • FPT_STM.1, which ensures the TOE provides reliable time stamps
O.ENCRYPT	This objective is met by • FCS_CKM.1, which specifies secure key generation methods • FCS_CKM.2, which specifies secure key distribution methods • FCS_COP.1, which specifies standards-based algorithms for cryptographic operations
O.PROTECT	This objective is met by • FIA_ATD.1, which specifies the list of security attributes belonging to individual users • FIA_SOS.1, which specifies minimum requirements for passwords • FIA_UAU.2, which requires operator authentication before any action • FIA_UID.2, which requires operator authentication before any action • FMT_MOF.1, which restricts configuration of the NAC Information Flow Control SFP to an Administrator • FMT_MTD.1, which restricts control of user and TOE data to an Administrator • FMT_SMF.1, which specifies management functions available in the TOE • FMT_SMR.1, which specifies roles available to TOE users
O.SECKEY	This objective is met by • FCS_CKM.1, which specifies secure key generation methods • FCS_CKM.2, which specifies secure key distribution methods • FCS_COP.1, which specifies standards-based algorithms for cryptographic operations

SFR	RATIONALE
O.UNAUTH_ENDPOINT	This objective is met by • FDP_IFC.1, which defines the subjects, information, and operations associated with the NAC Information Flow Control SFP • FDP_IFF.1, which defines the NAC Information Flow Control SFP • FMT_MSA.1, which restricts the ability to modify or delete the security attributes defined in NAC Information Flow Control SFP to the Administrator • FMT_MSA.2, which ensures that only secure values are accepted for the security attributes listed with NAC Information Flow Control SFP • FMT_MSA.3, which ensures the TOE provides restrictive default values for the NAC Information Flow Control SFP • FMT_MTD.1, which restricts control of user and TOE data to an Administrator • FMT_SMF.1, which specifies management functions available in the TOE • FMT_SMR.1, which specifies roles available to TOE users
O.TOECOM	This objective is completely satisfied by • FPT_ITT.1 which ensures that traffic transmitted between TOE components (client and appliance) is protected from disclosure and modification

Table 16 – Rationale for TOE SFRs to Objectives

6.4.3 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) augmented with ALC_FLR.2 Flaw Reporting Procedures. 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_FLR.2	Flaw Reporting Procedures
	ALC_LCD.1	Developer defined life-cycle model
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.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 17 – Security Assurance Requirements at EAL3

6.4.4 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 3 augmented with ALC_FLR.2. 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 Basic, 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.

6.4.5 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: Juniper Networks Junos Pulse Access Control Service 4.2R4
ADV_FSP.3 Functional Specification with Complete Summary	Functional Specification: Juniper Networks Junos Pulse Access Control Service 4.2R4
ADV_TDS.2 Architectural Design	Architectural Design: Juniper Networks Junos Pulse Access Control Service 4.2R4
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks Junos Pulse Access Control Service 4.2R4
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks Junos Pulse Access Control Service 4.2R4
ALC_CMC.3 Authorization Controls	Security Measures: Juniper Networks Junos Pulse Access Control Service 4.2R4
ALC_CMS.3 Implementation representation CM coverage	Security Measures: Juniper Networks Junos Pulse Access Control Service 4.2R4
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: Juniper Networks Junos Pulse Access Control Service 4.2R4

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ALC_DVS.1 Identification of Security Measures	Security Measures: Juniper Networks Junos Pulse Access Control Service 4.2R4
ALC_LCD.1 Developer defined life-cycle model	Life Cycle Model: Juniper Networks Junos Pulse Access Control Service 4.2R4
ALC_FLR.2 Flaw Reporting Procedures	Flaw Reporting Procedures: Juniper Networks Junos Pulse Access Control Service 4.2R4
ASE_CCL.1 Conformance claims	Security Target: Juniper Networks Junos Pulse Access Control Service 4.2R4
ASE_ECD.1 Extended components definition	Security Target: Juniper Networks Junos Pulse Access Control Service 4.2R4
ASE_INT.1 ST introduction	Security Target: Juniper Networks Junos Pulse Access Control Service 4.2R4
ASE_OBJ.2 Security objectives	Security Target: Juniper Networks Junos Pulse Access Control Service 4.2R4
ASE_REQ.2 Derived security requirements	Security Target: Juniper Networks Junos Pulse Access Control Service 4.2R4
ASE_SPD.1 Security problem definition	Security Target: Juniper Networks Junos Pulse Access Control Service 4.2R4
ASE_TSS.1 TOE summary specification	Security Target: Juniper Networks Junos Pulse Access Control Service 4.2R4
ATE_COV.2 Analysis of Coverage	Testing Evidence: Juniper Networks Junos Pulse Access Control Service 4.2R4
ATE_DPT.1 Testing: Basic Design	Testing Evidence: Juniper Networks Junos Pulse Access Control Service 4.2R4
ATE_FUN.1 Functional Testing	Testing Evidence: Juniper Networks Junos Pulse Access Control Service 4.2R4

Table 18 – 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:

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

7.2 Security Audit

The TOE generates a fine-grained set of audit logs. These logs are stored locally, and the system can also send them to an external SYSLOG server for alternative storage. The logs are divided into the following categories and are maintained separately:

- Event logs – used to track system related events such as start-up and shutdown
- Admin access logs – used to record administrator generated events
- User access logs – record user access events such as retrieving a file.

Each log contains the following fields:

- Severity (Info/Minor/Major)
- ID
- Timestamp
- Date
- Event outcome (success or failure)
- Entity who initiated the activity: [initiating IP] initiator username if applicable, (user type if applicable),[user role if applicable]
- Description of the activity

The TOE generates logs for the following list of events:

- Modifications to the group of users that are part of a role, which includes the identity of the Administrator performing the modification and the user identity being associated with a role in each related log;

- All use of the user identification mechanism, which includes the user identities provided to the TOE in each related log;
- Any use of the authentication mechanism, which includes the user identities provided to the TOE in each related log;
- All decisions on requests for information flow;
- Changes to the time, which includes the identity of the Administrator performing the operation in each related log;
- Use of the functions listed in this requirement pertaining to audit with the exception for viewing information flow security policy rules, user attribute values, and audit trail data, which includes the identity of the Administrator performing the operation in each related log.

The logs are only accessible through the Web-Based administrative interface, in which only authenticated administrators are authorized to access. Administrators can view, clear, save the logs. When logs are saved from the TOE, they are transferred to the PC connected to the Web-Based administrative interface. The administrator also has the ability to change the log settings.

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

- FAU_GEN.1: The TOE generates all the audit events identified in this requirement. Within each event is the information listed above which addresses all required details.
- FAU_SAR.1: The Administrator has the ability to read all of the audit logs. Each log is presented to the administrator in a human-readable format.
- FAU_STG.1: Only the Administrator has access to the logs. The administrator is not permitted to modify any information in the logs. The only manipulations allowed on logs are to clear them, download them, save them, or view them.

7.3 Cryptographic Support

The TOE provides an encrypted path between users and itself. Users connect to the TOE using a secure connection using TDES or AES (with 128-, 192-, or 256-bit key sizes) encryption algorithms supported by the TOE. The secure connection ensures that user passwords and data are protected from modification and disclosure.

AES and TDES keys are generated with an ANSI X9.31 pseudo-random number generator and are used as session keys for TLS sessions. Cryptographic key distribution is implemented via the TLS protocol.

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

- FCS_CKM.1: This component ensures that cryptographic keys and parameters are generated with standards-based algorithms
- FCS_CKM.2: This component provides secure key distribution to remote trusted IT products
- FCS_COP.1: Robust algorithms are used to support cryptographic operations between users and the TOE.

7.4 Information Flow Control

The TOE enforces an information flow policy between authenticated users and protected resources logically behind the appliance. Subjects perform requests for information access (such as reading, writing, or deleting a file or accessing an internal Web server) to a network in the IT Environment, and they are granted access if the user successfully authenticates to the TOE and the endpoint is compliant to the Host Checker Policy or the endpoint MAC address is contained within an exception list. If the authentication is successful and the endpoint is not compliant to a Host Checker Policy, the endpoint may be remediated in an isolated area of the network to attain compliance with the Host Checker Policy then gain access.

The TOE supports predefined rules that check for antivirus software and up-to-date virus signatures, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders. Additionally, the TOE supports custom rules that use integrity measurement collectors (IMCs) and integrity measurement verifiers (IMVs) to perform customized client-side checks. Custom rules also allow the TOE to check for third party DLLs that perform customized clientside checks. Finally, custom rules can check for ports, processes, files, registry key settings, and the NetBIOS name, MAC addresses or certificate of the client machine.

The examples above apply to Windows-based machines. For Mac OS, Linux, and Solaris the TOE can check for ports, processes, and files.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE supports an authenticated user information flow policy that controls who can access a network in the IT Environment.
- FDP_IFF.1: The NAC Information Flow Control SFP limits information flow based on user roles and resource types. Administrators have the ability to establish rules that permit or deny information flows based on the combination of attributes listed.

7.5 Identification and Authentication

The TOE performs identification and authentication of all users and administrators accessing the TOE. The TOE has the ability to authenticate operators locally using a password or can integrate with a remote authentication server. In the evaluated configuration, The TOE will perform the authentication locally. Operators enter a username and password which is validated by The TOE against the information stored by the TOE. If the authentication succeeds, the operator receives a session token that is used for identification of subsequent requests during that session.

The Identification and Authentication security function is supported by FIA_SOS.1, FIA_UAU.2 and FIA_UID.2 and ensures authentication parameters meet the following:

- Minimum of eight (8) characters,

- Minimum of three (3) numeric characters,
- Minimum of three (3) alphabetic characters,
- Combination of both uppercase and lowercase alphabetic characters,
- Different from the username, and
- Different from the previously used password

The TOE associates an operator to a role by associating the username with the proper role once successful authentication occurs. 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 operator accounts used for management.

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

- FIA_ATD.1: For each registered user, the TOE stores the following information: user identity/username, user roles, and password.
- FIA_SOS.1: The TOE is equipped with a mechanism that can be configured by the administrator to verify that user authentication secrets meet a list of criteria for ensuring their strength. The following parameters for authentication secrets are required for the evaluated configuration: a minimum of eight (8) characters, a minimum of three (3) numeric characters, a minimum of three (3) alphabetic characters, a combination of both uppercase and lowercase alphabetic characters, different from the username, and different from the previously used password.
- FIA_UAU.2: ensures that users are authenticated to the TOE via fixed password meeting the requirements listed above.
- FIA_UID.2: ensures that users are identified to the TOE via username.

7.6 Security Management

The TOE provides security management functions via a browser interface. The Administrator logs onto the TOE from a protected network and performs all management functions through the browser interface. The administrator has the ability to control all aspects of the TOE configuration including: user management, information flow policy management, audit management, and system start-up and shutdown.

The TOE also provides a console port for certain management capabilities, such as configuring the network relevant information pertaining to the internal and external network interfaces. However, the console port does not provide the management capabilities necessary to utilize the security management functionalities claimed within this ST.

Administrators set the information flow policy rules on a per user basis. When the administrator adds a new user, the administrator defines the user access. Although users are grouped into roles, administrators can create rules that except specific users from the constraints of their role. By default, user access is restrictive but the administrator may override the default upon rule creation.

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

- FMT_MOF.1: The ability to determine the behavior of, disable, enable, modify the behavior of the NAC Information Flow Control SFP is restricted to the Administrator:
- FMT_MSA.1: This component restricts the ability to modify and delete the parameters for the NAC Information Flow Control SFP to the Administrator
- FMT_MSA.2: This component ensures that only secure values are accepted for the configuration parameters associated with the NAC Information Flow Control SFP
- FMT_MSA.3: The TOE allows restrictive access by default but the Administrator can assign more restrictive permissions.
- FMT_MTD.1: The TOE restricts the ability to modify the NAC 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, restricts the ability to modify the data relating to TOE access locations. All restrictions apply to the Administrator.
- FMT_SMF.1: The TOE supports the following security management functions:
  a) Reboot the appliance, shut down the appliance, or restart services (all via management GUI);
  b) Create, delete, modify, and view Host Checker Policies;
  c) Create, delete, modify, and view user attribute values defined in FIA_ATD.1;
  d) Enable and disable external IT entities from communicating to the TOE;
  e) Modify and set the time and date;
  f) Archive, clear, filter, and review the audit trail
  g) Define cryptographic algorithms used in protected communications sessions with external IT entities].
- FMT_SMR.1: The TOE supports the roles User, Administrator, Read-Only Administrator.

The TOE provides a timestamp for its own use. The timestamp is generated from the clock provided in the hardware. Communications between TOE components (client and appliance) are protected with cryptography provided by FCS_COP.1.

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

- FPT_STM.1: The TOE generates a reliable timestamp for its own use.
- FPT_ITT.1: All communications between TOE components is encrypted via a secure connection using encryption & decryption algorithms defined in FCS_COP.1. This protects the traffic from disclosure and modification