Enterasys Networks, Inc. Netsight/Network Access Control v3.2.2

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 0.7

Prepared for:

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810
United States of America
Phone: +1 978 684 1000

http://www.enterasys.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America
Phone: +1 703 267 6050

http://www.corsec.com

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the Enterasys Netsight/Network Access Control v3.2.2, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-only network access control system.

1.1 Purpose

This ST provides mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats in the following sections:

- Security Target Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims.
- Security Problem Definition (Section 3) – Describes the threats, policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components Definition (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	Enterasys Networks, Inc. Netsight/Network Access Control v3.2.2 Security Target
ST Version	Version 0.7
ST Author	Corsec Security, Inc.
ST Publication Date	2011-3-8
TOE Reference	Enterasys Netsight/Network Access Control v3.2.2 Build 48
Keywords	NAC, network access control, NetSight, Controller, Gateway

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The Target of Evaluation (TOE) is the Enterasys Netsight/Network Access Control v3.2.2, and will hereafter be referred to as the TOE throughout this document. The TOE is a network access control system that provides detection, authentication, and authorization of devices attempting to access a network. The software-only TOE consists of the Network Access Control (NAC) software and the NetSight Suite management software.

Figure 1 shows a typical deployment configuration of the TOE:

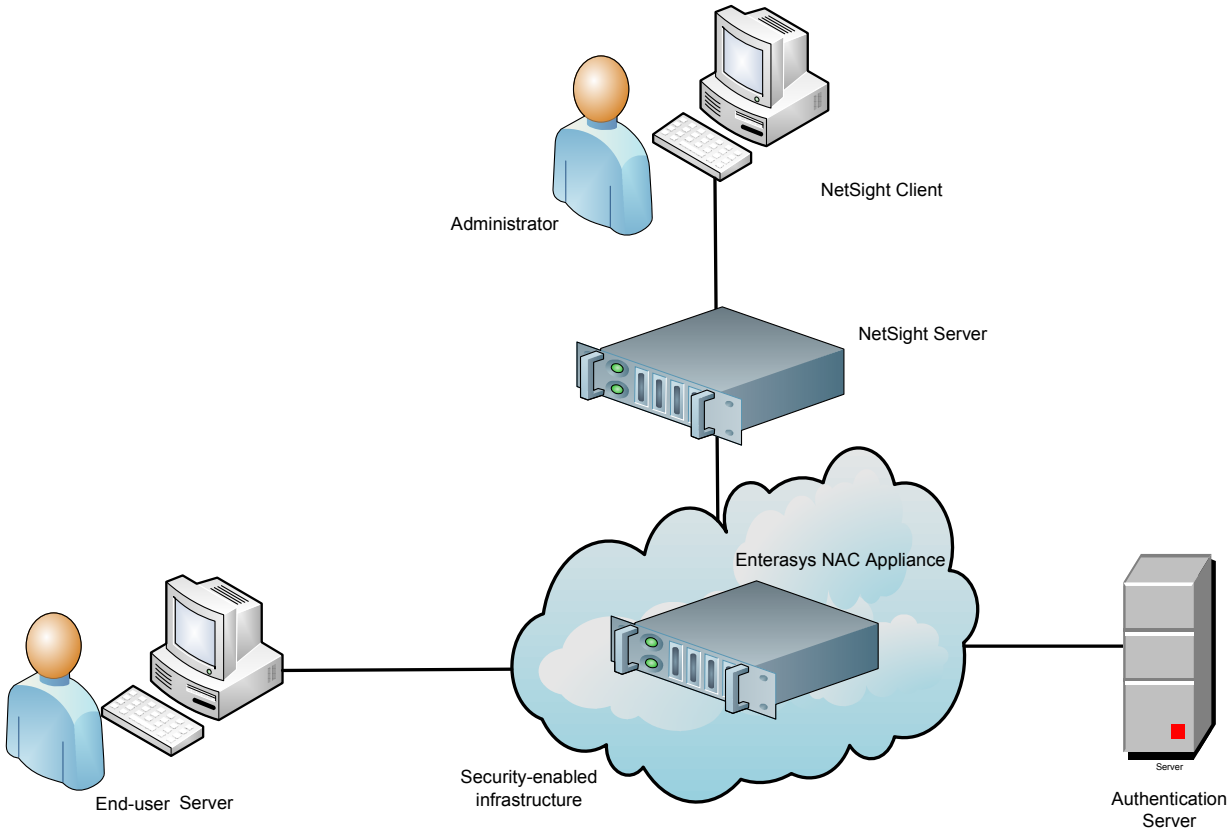

Figure 1 – Typical Deployment Configuration of the TOE

1.3.1 Brief Description of the Components of the TOE

The TOE is a centralized network access control system that authenticates and authorizes end-system access to network resources. It ensures that only valid users and devices are permitted to connect to the network from the proper location and at the right time. The TOE supports three network access control functions: detection, authentication, and authorization. These three functions can be deployed in various combinations, but only one deployment model is available for the evaluated configuration of the TOE, as described below in 1.3.1.4. The deployments vary based on licensable components within the TOE.

1.3.1.1 Detection

The detection functionality of the TOE identifies at what time and from what location a user or device attempts to connect to the network.

1.3.1.2 Authentication

The authentication functionality of the TOE verifies the identity of the user or device attempting to connect to the network.

1.3.1.3 Authorization

The authorization functionality of the TOE determines the appropriate network access for the connecting device based on authentication results, and enforces this authorization level to the end-system. Authorization level for an end-system can be determined by a combination of the device's location, MAC address, and identity of the user or device as validated through authentication. (Although the user guidance indicates that Port Web Authentication (PWA) and 802.1X authentication are also available, they are not part of the CC-evaluated configuration of the TOE.) End-system authorization can be accomplished by the TOE through either inline or out-of-band techniques, depending on the deployment of the TOE appliance.

1.3.1.4 Deployment model

The three functions described above may be implemented concurrently, or separately, depending on the deployment desired by the purchaser. The only deployment model available for the evaluated configuration of the TOE is the End-system authorization model.

This deployment model implements the detection, authentication, and authorization functionality of the TOE. It controls access to network resources based on user and end-system identity and location. It also supports MAC address or guest registration, where new end-systems are required to provide a valid user identity in a web page form before being allowed access to the network, but this is not part of the evaluated configuration of the TOE.

1.3.1.5 NetSight Management

The TOE's NetSight Suite is accessed through a Graphical User Interface (GUI), and provides the means to manage the NAC functionality of the TOE. NetSight is used to monitor the health and status of switches, routers, and other security appliances in the network. It provides configurations for the authentication and authorization parameters for the NAC appliances. After an administrator[1] enforces these configurations, the NAC appliances can detect, authenticate, and authorize end-systems connecting to the network according to those configuration specifications. It also provides the ability to define and configure the authorization levels, or policies, for the NAC system. To implement this functionality, the NetSight product may be used in an inline NAC deployment, or may be used in an out-of-band deployment that includes policy-enabled switches in the access layer. NetSight provides central administration of policies throughout the network. Finally, NetSight provides comprehensive network inventory and change management capabilities for a network infrastructure.

1.3.2 TOE Environment

In the CC evaluated configuration of the TOE, the required non-TOE components include:

- NAC appliance running a Linux Operating System v2.6 (OS)
- NetSight appliance running a Linux OS v2.6
- Remote Authentication Dial In User Service (RADIUS) server

[1] Administrator – a user authorized to perform management functions on the TOE. Administrators are not end-users.

- Linux OS v2.6 for the NetSight Suite client software
- General-purpose computing hardware for the NetSight Suite client software

1.3.2.1 Appliances

The appliances are required components in the evaluated configuration of the TOE. There are two types of appliances: the NAC appliance and the NetSight Appliance. Each appliance comes in one or more hardware models or as a virtual appliance, as listed in Table 2 below.

1.3.2.1.1 The NAC Appliance

The NAC appliance can be deployed either inline or out-of-band. For inline deployments, the NAC Controller models are used. These appliances implement inline network access control and are used in deployments where non-intelligent wired or wireless edge devices are deployed in the network. Connecting end-systems are detected through the receipt of a packet from a new end-system. Based on the authentication results for a connecting device, the authorization of the end-system is implemented locally on the NAC Controller appliance by a set of traffic forwarding policies to all traffic sourced by the end-system.

For out-of-band deployments, the NAC Gateway models are used. These appliances implement out-of-band network access control and are used in deployments where intelligent wired or wireless edge devices are deployed in the network. Connecting end-systems are detected on the network through their RADIUS authentication interchange. Based on the authentication results for a connecting device, RADIUS attributes are added or modified during the authentication process to authorize the end-system on the authenticating edge switch.

The software installed on all models is identical. The appliances differ only in speed and capacity.

1.3.2.1.2 The NetSight Appliance

The NetSight appliance provides the management server software for the TOE, and must be deployed regardless of the deployment model used (see Section 1.3.1.4 above).

The appliance models are listed in Table 2 below. The Matrix Security Modules are the NAC engines for the NAC Controller appliances.

Table 2 - TOE Hardware Requirements

Part Number	Appliance Name	Description
2S4082-25-SYS	NAC Controller	24-Port Triple Speed, Uplink Small Form-factor Pluggable (SFP), 400 MegaHertz (MHz) processor, 256 MegaBytes (MB) Dynamic Random Access Memory (DRAM), 32 MB Flash Memory
7S4280-19-SYS	NAC Controller	18-Port SFP, Uplink SFP, 600 MHz processor, 256 MB DRAM, 32 MB Flash Memory
7S-NSTAG-01	Matrix Security Module	1,000 endpoints, 1.4 GigaHertz (GHz) processor, 400 MHz Front Side Bus, 2 MB Layer 2 Cache, 1 GB Memory, 60 GB Hard Drive
7S-NSTAG-01NPS	Matrix Security Module	1,000 endpoints, 1.4 GHz processor, 400 MHz Front Side Bus, 2 MB Layer 2 Cache, 1 GB Memory, 60 GB Hard Drive
SNS-TAG-HPA	NAC Gateway	3,000 endpoints, 2.13 GHz processor, 1066 MHz Front Side Bus, 2 MB Cache, 1 GB Memory, 80 GigaByte (GB) Hard Drive
SNS-TAG-LPA	NAC Gateway	2,000 endpoints, 1.8 GHz processor, 800 MHz Front Side Bus,1 MB Cache, 1 GB Memory, 80 GB Hard Drive
SNS-TAG-ITA	NAC Gateway	3,000 endpoints, 2.33 GHz processor, 1333 MHz Front Side Bus, 2 x 6 MB Cache, 8 GB Memory, 250 GB Hard Drive, 4 GB Minimum RAM, 8 GB Maximum RAM
NAC-A-20	NAC Gateway	E5506 Xeon 3,000 endpoints, E5506 Xeon Processor, 2.13 GHz 4M Cache, 4.86 GT/s, 12 GB Memory, (2) 250 GB Hard Drives
SNS-NSS-A	NAC NetSight Suite Appliance	2.66 GHz processor, 4 MB Cache, 4 GB Memory, 250 GB Hard Drive
2155328	NAC Virtual Appliance	VMWare .OVA file format for deployment on a VMWare ESX™ 4.0 server or ESXi™ 4.0 server with a vSphere™ 4.0 client. The VM has 12GB Memory, 4 Processors, 2 Network Adapters, 40GB thick-provisioned Hard Drive space.
	NAC NetSight Suite Virtual Appliance	VMWare .OVA file format for deployment on a VMWare ESX™ 4.0 server or ESXi™ 4.0 server with a vSphere™ 4.0 client. The VM has 8GB Memory, 4 Processors, 2 Network Adapters, 60GB thick-provisioned Hard Drive space.

1.4 TOE Description

This section will primarily address the physical and logical components of the TOE included in the evaluation.

1.4.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is a software-only network access control system which runs on Enterasys appliance models listed in Table 2, and on general-purpose computing hardware. The TOE is installed on the appliances and other hardware as depicted in Figure 2 below.

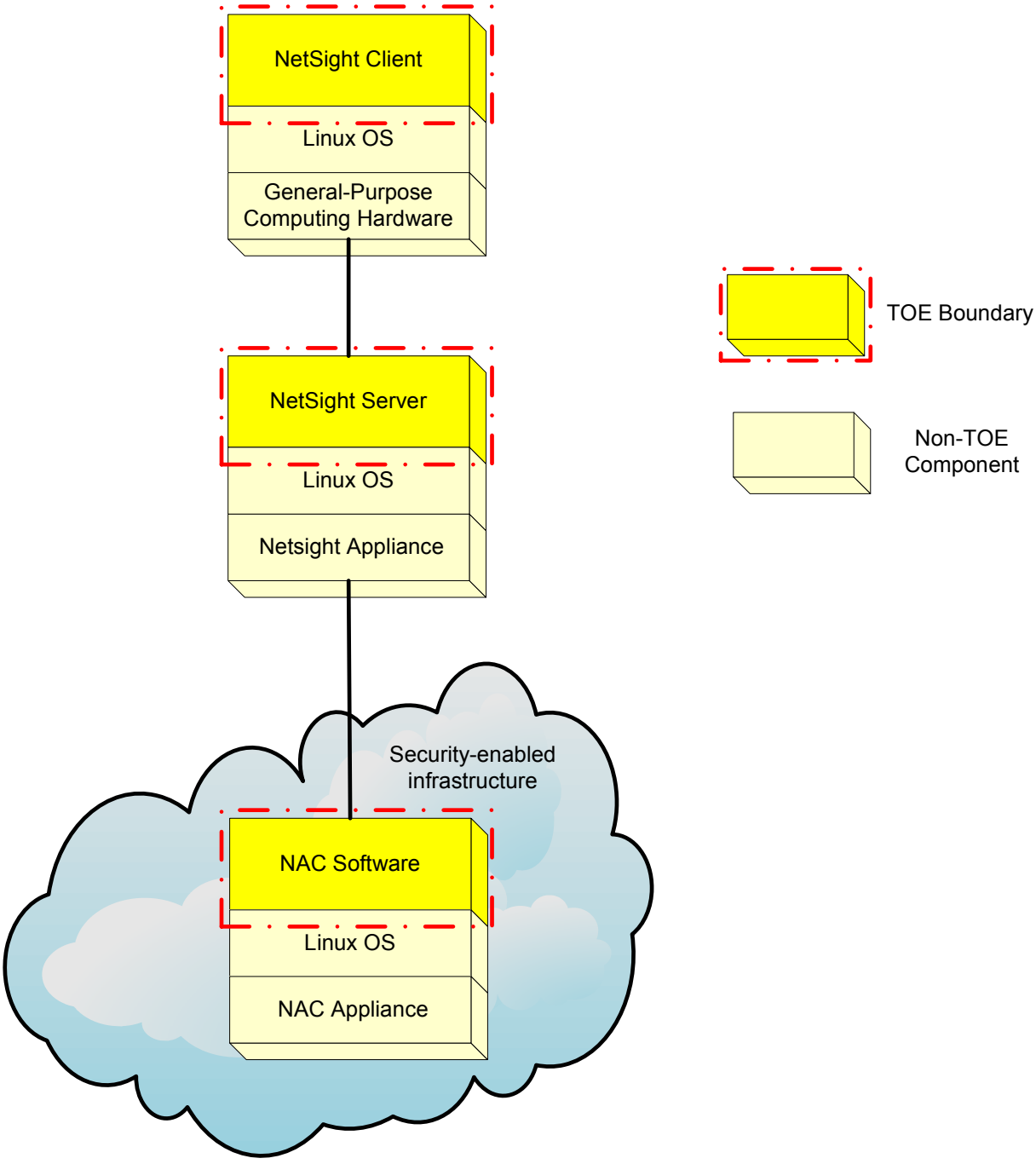

Figure 2 - Physical TOE Boundary

1.4.2 TOE Components

The TOE components include the Netsight Server software, the Netsight Client Software, and the NAC software. The Netsight Server and the Netsight Client make up the Netsight Suite. The Netsight Suite manages the NAC

software, which implements the detection, authentication, and authorization functionality of the TOE. The hardware appliances are required environmental components in the evaluated configuration of the TOE. All communications between TOE components are protected by SSL v2.x and v3.0, Transport Layer Security (TLS) v1.0 and v1.1, or SNMP v3.

1.4.3 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management

Each of these security functions is discussed below.

1.4.3.1 Security Audit

The TOE keeps track of auditable events through the Netsight Application Logs and the Netsight Server Log. The System Log records all auditable events in a human-readable format. Administrators can view and sort logs by any displayed field through the NetSight Management Suite GUI.

1.4.3.2 User Data Protection

User data protection defines how users of the TOE and end-systems connecting to the network are allowed to perform operations on objects.

The TOE provides authorized administrators with the ability to configure end-user[2] and end-system network access policies using the NetSight Management GUI. The Management GUI provides for the creation of rules that define actions the TOE is to take based on a set of conditions. The conditions and actions affect either the allowed access to network resources by end-users and end-systems (Failsafe Access Control Security Functional Policy (SFP), Quarantine Access Control SFP, or Accept Access Control SFP), or the way administrators interact with the TOE (Administrative Access Control SFP).

1.4.3.3 Identification and Authentication

The TOE provides the ability for end-users and end-systems to gain access to network resources. The identification and authentication security function ensures that access to network resources is restricted to authorized end-users and end-systems and access is protected by the entry of credentials. End-users and end-systems are assigned a role and a group to determine which network resources they are allowed to access.

Identification of administrators is performed by the TOE Environment.

1.4.3.4 Security Management

The Security Management function provides administrators with the ability to properly manage and configure the TOE. Administrators use the NetSight Management GUI to configure policies that grant access to network resources.

[2] End-user – any user attempting to access network resources. TOE Administrators are not end-users.

1.4.4 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Assessment (a licensable component of the software)
- Assisted remediation
- Operating System
- Hardware
- Simple Network Management Protocol v1 and v2 (i.e. SNMP must be used with v3 security features)
- Command Line Interface (CLI) on the appliances
- Access to the Command Line Interface (CLI) on the appliances via the GUI
- Telnet
- Unauthenticated MAC registration

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted CEM as of 2010-10-18 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation (ALC_FLR.1)

3 Security Problem Definition

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 - Security Objectives.

The following threats are applicable:

Table 4 – Threats[3]

Name	Description
T.MASQUERADE	A threat agent masquerading as the TOE or another entity may capture valid identification and authentication data for a legitimate administrator, end-user, or end-system of the TOE in order to gain unauthorized access to the TOE or network resources.
T.INT_CONF	An unauthorized user may attempt to disclose or compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.UNAUTH	A user or IT device may gain access to security data on the TOE or network resources, even though the user or device is not authorized in accordance with the TOE security policy.

[3] IT – Information Technology

Name	Description
T.DATALOSS	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NO_AUDIT	A threat agent may perform security-relevant operations on the TOE without being held accountable for it.
T.IA	A threat agent may attempt to compromise the TOE or network resources controlled by the TOE by attempting actions that it is not authorized to perform on the TOE or network resources.
T.INFO_CAPTURE	An external attacker or malicious insider may sniff the communication channel between the TOE and a remote administrator in order to capture or modify information sent between the two.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this Security Target.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 – Assumptions

Name	Description
A.LOCATE	The TOE resides in a physically controlled access facility that prevents unauthorized physical access.
A.NOEVIL	Authorized administrators who manage the TOE are non-hostile and are appropriately trained to use, configure, and maintain the TOE and follow all guidance.
A.PROTECT	The TOE and network devices shall be protected from MAC address spoofing and other disruptions of data and functions.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 6 - Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record the actions taken by administrators and provide the authorized administrators with the ability to review and sort the audit trail.
O.NETACCESS	The TOE must allow access to internal network resources as defined by the Accept Access Control SFP, the Failsafe Access Control SFP, and the Quarantine Access Control SFP when policy functionality has been configured on the TOE.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.USERAUTH	The TOE must be able to authenticate end-users and end-systems prior to allowing access to network resources.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 7 - IT Security Objectives

Name	Description

Name	Description
OE.ADMINAUTH	The TOE Environment must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.
OE.RADIUS	The TOE Environment must provide a RADIUS Server to assist in authentication of end-users and end-systems prior to the TOE granting or denying access to network resources.
OE.TIMESTAMP	The TOE Environment must provide reliable timestamps for the TOE's use.
OE.SECURECOMMUNICATION	The operational environment will provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.
OE.PROTECT	The TOE Environment must protect itself and the TOE from external interference or tampering.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 - Non-IT Security Objectives

Name	Description
NOE.TRUSTED_ENV	The TOE shall reside in a physically secure location, safe from compromise by malicious insiders or outsiders.

5 Extended Components Definition

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

5.1 Extended TOE Security Functional Components

There are no extended TOE Security Functional components defined for this Security Target.

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance components defined for this Security Target.

6 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Parts 2 and 3 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.

Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class.

Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review		✓		
FDP_ACC.1(a)	Subset access control		✓	✓	✓
FDP_ACC.1(b)	Subset access control		✓	✓	✓

Name	Description	S	A	R	I
FDP_ACC.1(c)	Subset access control		✓		✓
FDP_ACC.1(d)	Subset access control		✓		✓
FDP_ACF.1(a)	Security attribute based access control		✓		✓
FDP_ACF.1(b)	Security attribute based access control		✓		✓
FDP_ACF.1(c)	Security attribute based access control		✓		✓
FDP_ACF.1(d)	Security attribute based access control		✓		✓
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.2	User identification before any action			✓	
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1(a)	Management of security attributes	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes	✓	✓		✓
FMT_MSA.3(a)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(b)	Static attribute initialisation	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

- Start-up and shutdown of the audit functions;
- All auditable events, for the [*not specified*] level of audit; and
- [*management actions taken through the NetSight Suite*].

FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*authorized administrators*] 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.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1

The TSF shall provide the ability to apply [*ordering in ascending or descending order*] of audit data based on [*field values*].

Dependencies: FAU_SAR.1 Audit review

6.2.2 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1(a)

The TSF shall enforce the [*Failsafe Access Control SFP*] on

[

Subjects: end-systems attempting to access network resources,

Objects: specified network resources, and

Operations: all connectivity with and data transfers between the subjects and objects identified above

].

Dependencies: FDP_ACF.1(a) Security attribute based access control

FDP_ACC.1(b) Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1(b)

The TSF shall enforce the [*Accept Access Control SFP*] on

[

Subjects: end-systems attempting to access network resources,

Objects: specified network resources, and

Operations: all connectivity with and data transfers between the subjects and objects identified above

].

Dependencies: FDP_ACF.1(b) Security attribute based access control

FDP_ACC.1(c) Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1(c)

The TSF shall enforce the [*Quarantine Access Control SFP*] on

[

Subjects: end-systems attempting to access network resources,

Objects: specified network resources, and

Operations: all connectivity with and data transfers between the subjects and objects identified above

].

Dependencies: FDP_ACF.1(c) Security attribute based access control

FDP_ACC.1(d) Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1(d)

The TSF shall enforce the [*Administrative Access Control SFP*] on

[

Subjects: users attempting to establish an interactive session with the TOE,

Objects: User interface items, policies, NAC authentication and authorization configurations, and

Operations: all interactions between the subjects and objects identified above

].

Dependencies: FDP_ACF.1(d) Security attribute based access control

FDP_ACF.1(a) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(a)

The TSF shall enforce the [*Failsafe Access Control SFP*] to objects based on the following:

[

Subject attributes:

1. *MAC address*
2. *IP address*
3. *Switch Port*

Object attributes:

1. *IP address*
2. *Network service*

3. *Protocol*

].

FDP_ACF.1.2(a)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *If the subject's IP address cannot be determined from its MAC address, apply the Policy Role defined for the Failsafe Policy to the subject, and allocate the appropriate network resources;*

2. *If the above rule does not apply, and none of the restrictions defined by the Accept SFP applies, allocate full network access.*

].

FDP_ACF.1.3(a)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(a)

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

Dependencies: FDP_ACC.1(a) Subset access control
FMT_MSA.3(a) Static attribute initialization

FDP_ACF.1(b) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(b)

The TSF shall enforce the [*Accept Access Control SFP*] to objects based on the following:

[

Subject attributes:

1. *Authorization status as determined by the TOE*

Object attributes:

1. *IP address*

2. *Network service*

3. *Protocol*

].

FDP_ACF.1.2(b)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *If the subject has been authorized by the TOE, apply the Policy Role defined for the Accept Policy to the subject, and allocate the appropriate network resources;*

2. *If the Accept policy has been configured to replace the Filter-ID information returned in the RADIUS authentication messages, apply the Policy Role defined for the Accept Policy to the subject, and allocate the appropriate network resources;*

3. *If the above rules do not apply, deny network access.*

].

FDP_ACF.1.3(b)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(b)

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

Dependencies: **FDP_ACC.1(b) Subset access control**
FMT_MSA.3 (a) Static attribute initialization

FDP_ACF.1(c) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(c)

The TSF shall enforce the [*Quarantine Access Control SFP*] to objects based on the following:

[

Subject attributes:

1. MAC address

2. IP address

3. Switch Port

Object attributes:

1. IP address

2. Network service

3. Protocol

].

FDP_ACF.1.2(c)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *If a MAC Override and Quarantine Policy have been assigned on the TOE for the subject, apply the Policy Role defined for the Quarantine Policy to the subject, and allocate the appropriate network resources;*

2. *If the above rule does not apply, and none of the restrictions defined by the Accept SFP applies, allocate full network access.*

].

FDP_ACF.1.3(c)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(c)

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

Dependencies: FDP_ACC.1(c) Subset access control
FMT_MSA.3(a) Static attribute initialization

FDP_ACF.1(d) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(d)

The TSF shall enforce the [*Administrative Access Control SFP*] to objects based on the following:

[

Subject attributes:

1. *User role*
2. *User ID*
3. *Group ID*
4. *User's permissions*
5. *Group's permissions*

Object attributes:

1. *Permissions assigned to objects*
2. *Absence of permissions assigned to objects*

].

FDP_ACF.1.2(d)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *If the subject is the TOE Administrator, then access is granted;*
2. *If the subject requests access to an object that has no assigned permissions, then access is granted;*
3. *If a subject who is not a TOE Administrator requests access to an object that has assigned permissions, the permissions of the subject are examined to determine if the subject has permission to access the object. If a match is found, access is granted;*
4. *If none of the above rules apply, access is denied.*

].

FDP_ACF.1.3(d)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(d)

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

Dependencies: FDP_ACC.1(d) Subset access control
FMT_MSA.3(b) Static attribute initialization

6.2.3 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

The TSF shall require each **end-**user **and end-system** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **end-**user **or end-system**.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

The TSF shall require each **end-**user **and end-system** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **end-**user **or end-system**.

Dependencies: No dependencies

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*determine the behaviour of, disable, enable, modify the behaviour of*] the functions [*NAC authentication and authorization configurations*] to [*authorized administrators*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(a) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(a)

The TSF shall enforce the [*Failsafe Access Control SFP, Accept Access Control SFP, Quarantine Access Control SFP*] to restrict the ability to [*change_default, query, modify*] the security attributes [*Subject MAC address, Subject IP address, Subject Switch Port, Subject authorization status, Object IP address, Object Network Service, Object protocol*] to [*authorized administrators*].

Dependencies: FDP_ACC.1(a) Subset access control
FDP_ACC.1(b) Subset access control
FDP_ACC.1(c) Subset access control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MSA.1(b) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(b)

The TSF shall enforce the [*Administrative Access Control SFP*] to restrict the ability to [*change_default, query, modify, delete*] the security attributes [*User role, User ID, Group ID, User's permissions, Permissions assigned to objects*] to [*authorized administrators*].

Dependencies: FDP_ACC.1(d) Subset access control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MSA.3(a) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(a)

The TSF shall enforce the [*Failsafe Access Control SFP, Accept Access Control SFP, Quarantine Access Control SFP*] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(a)

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

Dependencies: **FMT_MSA.1(a) Management of security attributes**
FMT_SMR.1 Security roles

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(b)

The TSF shall enforce the [*Administrative Access Control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b)

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

Dependencies: **FMT_MSA.1(b) Management of security attributes**
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*management of security functions behavior, management of security attributes*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Administrator role, Limited Administrator roles as defined by Administrator, User roles as defined by Administrator*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.1. Table 10 - Assurance Requirements summarizes the requirements.

Table 10 - Assurance Requirements[4]

Assurance Requirements	
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.1 Basic Flaw Remediation
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[4] CM – Configuration Management

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 11 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
User Data Protection	FDP_ACC.1(a)	Subset access control
	FDP_ACC.1(b)	Subset access control
	FDP_ACC.1(c)	Subset access control
	FDP_ACC.1(d)	Subset access control
	FDP_ACF.1(a)	Security attribute based access control
	FDP_ACF.1(b)	Security attribute based access control
	FDP_ACF.1(c)	Security attribute based access control
	FDP_ACF.1(d)	Security attribute based access control
Identification and Authentication	FIA_UAU.2	User authentication before any action

TOE Security Function	SFR ID	Description
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(a)	Management of security attributes
	FMT_MSA.1(b)	Management of security attributes
	FMT_MSA.3(a)	Static attribute initialisation
	FMT_MSA.3(b)	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles

7.1.1 Security Audit

The TOE keeps track of auditable events through the System Log. The System Log records all auditable events in a human-readable format. Management actions taken by administrators through the NetSight Suite GUI are captured and stored in the operating system's Syslog. Audited management actions include changes to network configurations, and startup and shutdown of the TOE. Startup and shutdown of the audit functions occurs when the TOE is started or shutdown. Administrators can view all logs through the NetSight Management Suite GUI, and sort them by any displayed field.

The TOE audit records contain the following information:

Table 12 - Audit Record Contents

Field	Content
Date/Time	Date and time the event occurred.
Origination IP	IP address of the IT device that caused the event.
Origination User	Username of the user that caused the event.
Category	Category of the event.

Field	Content
Severity	Severity of the event (e.g., Alert, Notice, Emergency, Informational, Warning, Error, etc.).
Description	Description of the event.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.3.

7.1.2 User Data Protection

User data protection defines how users of the TOE, and end-users and end-systems connecting to the network, are allowed to perform operations on objects.

The TOE provides authorized administrators with the ability to configure end-user and end-system network access policies using the NetSight Management GUI. The Management GUI provides for the creation of rules that define actions the TOE is to take based on a set of conditions. The conditions and actions affect either the allowed access to network resource by end-users and end-systems (Failsafe Access Control SFP or Accept Access Control SFP), or the way users interact with the TOE (Administrative Access Control SFP).

The Failsafe Access Control SFP determines which network resources are permitted for access by an end-user or end-system attempting to connect to the network whose IP address cannot be determined. The specific network resources to which an end-user or end-system is given access is determined by the administrator when the policy is configured.

The Accept Access Control SFP determines which network resources are permitted for access by an end-user or end-system attempting to connect to the network that has been authorized by the TOE. In some cases the administrator may configure the Accept Access Control SFP to replace the Filter-ID information returned by the RADIUS server. The specific network resources to which an end-user or end-system is given access is determined by the administrator when the policy is configured.

The Quarantine Access Control SFP determines which network resources are permitted for access by an end-user or end-system attempting to connect to the network for which a MAC Override and a Quarantine Policy has been configured. The specific network resources to which an end-user or end-system is given access is determined by the administrator when the policy is configured.

The Administrative Access Control SFP determines access to the management functions for users identifying and authenticating to the TOE through the NetSight Suite GUI. Administrators are given access to functions based on their User ID, User Role, Group ID, User's configured permissions, and Group's configured permissions. If the administrator's permissions match the permissions assigned to the object to which the administrator is attempting access, then that access is granted. Otherwise, it is denied.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACC.1(c), FDP_ACC.1(d), FDP_ACF.1(a), FDP_ACF.1(b), FDP_ACF.1(c), FDP_ACF.1(d).

7.1.3 Identification and Authentication

The TOE provides the ability for end-users and end-systems to gain access to network resources. The identification and authentication security function ensures that access to network resources is restricted to authorized users and access is protected by the entry of credentials. End-users and end-systems are assigned a User role and a group to determine what network resources they are allowed to access.

The TOE requires end-users and end-systems to authenticate to the network when end-user and end-system authentication has been configured for the network by an authorized administrator.

Administrators are identified and authenticated by the TOE environment. Once the administrator has been successfully identified and authenticated, the TOE assigns an Administrator or Limited Administrator role and a group to the administrator. The role and group to which the administrator is assigned determines the functions and data to which the administrator has access.

TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UID.2.

7.1.4 Security Management

The Security Management function provides administrators with the ability to properly manage and configure the TOE. Administrators use the NetSight Management GUI to configure policies that grant access to network resources. Only authorized administrators may configure the TOE's network authentication and authorization functionality, manage the security attributes of the network resources, and manage administrator permissions and accounts.

The TOE maintains an Administrator role that servers as the super user for the NAC system. In addition, an Administrator can define any number of Limited Administrator roles and assign permissions to them as appropriate.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3(a), FMT_MSA.3(b), FMT_SMF.1, FMT_SMR.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Parts 2 and 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1, revision 2.

There are no extended SFRs or SARs contained within this ST.

There are no protection profile claims for this Security Target.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 13 - Threats: Objectives Mapping

Threats	Objectives	Rationale
T.MASQUERADE A threat agent masquerading as the TOE or another entity may capture valid identification and authentication data for a legitimate administrator, end-user, or end-system of the TOE in order to gain unauthorized access to the TOE or network resources.	O.NETACCESS The TOE must allow access to internal network resources as defined by the Accept Access Control SFP, the Failsafe Access Control SFP, and the Quarantine Access Control SFP when policy functionality has been configured on the TOE.	O.NETACCESS ensures that the TOE allows access to internal network resources only as defined by policy, when such policy has been configured on the TOE. This prevents threat agents from gaining unauthorized access to the TOE or network resources.
T.INT_CONF An unauthorized user may attempt to disclose or compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.	O.AUDIT The TOE must record the actions taken by administrators and provide the authorized administrators with the ability to review and sort the audit trail.	O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded. This prevents unauthorized users from disclosing or compromising the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
	OE.ADMINAUTH The TOE Environment must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and	OE.ADMINAUTH requires that the TOE Environment be able to identify and authenticate administrators prior to allowing access to TOE data. This prevents unauthorized users from bypassing a security mechanism and disclosing or compromising the

Threats	Objectives	Rationale
	data.	integrity of the data on the TOE.
	OE.RADIUS The TOE Environment must provide a RADIUS Server to assist in authentication of end-users and end-systems prior to the TOE granting or denying access to network resources.	OE.RADIUS requires that the TOE Environment provide a RADIUS Server to assist in authentication of end-users and end-systems prior to granting or denying access to network resources. This prevents unauthorized end-users or end-systems from disclosing or compromising the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN requires that the TOE allow only authorized users to configure the TOE security mechanisms. This prevents unauthorized users from disclosing or compromising the integrity of data collected and produced by the TOE.
	O.USERAUTH The TOE must be able to authenticate end-users and end-systems prior to allowing access to network resources.	O.USERAUTH ensures that end-users and end-systems are authenticated prior to being given access to network resources. This prevents unauthorized users from disclosing or compromising the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.UNAUTH A user or IT device may gain access to security data on the TOE or network resources, even though the user or device is not authorized in accordance with the TOE security policy.	OE.ADMINAUTH The TOE Environment must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.	OE.ADMINAUTH requires that the TOE Environment be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data. This prevents unauthorized users or IT devices from gaining access to security data on the TOE.
	O.NETACCESS The TOE must allow access to internal network resources as defined by the Accept Access Control SFP, the Failsafe Access Control SFP, and the Quarantine Access Control SFP when policy functionality has been configured on the TOE.	O.NETACCESS requires that the TOE allow access to internal network resources as defined by policy. This prevents unauthorized users or IT devices from gaining access to network resources.

Threats	Objectives	Rationale
	OE.RADIUS The TOE Environment must provide a RADIUS Server to assist in authentication of end-users and end-systems prior to the TOE granting or denying access to network resources.	OE.RADIUS requires that the TOE Environment provide a RADIUS Server to assist in authentication of end-users and end-systems prior to granting or denying access to network resources. This prevents unauthorized end-users or IT devices from gaining access to security data on the TOE.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN requires that only authorized administrators have privileges to manage the TOE functions and data. This prevents unauthorized users or IT devices from gaining access to security data on the TOE.
	O.USERAUTH The TOE must be able to authenticate end-users and end-systems prior to allowing access to network resources.	O.USERAUTH requires that end-users and end-systems be authenticated prior to gaining access to network resources. This prevents unauthorized users or IT devices from gaining access to network resources.
T.DATALOSS An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.	OE.ADMINAUTH The TOE Environment must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.	OE.ADMINAUTH requires that all administrators be identified and authenticated prior to being given access to TOE administrative functions and data. This prevents unauthorized users from removing or destroying data collected and produced by the TOE.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN requires that only users with appropriate privileges be allowed to exercise control over the TOE's functions and data. This prevents unauthorized users from removing or destroying data collected and produced by the TOE.
T.NO_AUDIT A threat agent may perform security-relevant operations on the TOE without being held accountable for it.	O.AUDIT The TOE must record the actions taken by administrators and provide the authorized administrators with the ability to review and sort the audit trail.	O.AUDIT requires that the TOE record actions taken by administrators. This ensures that all security-relevant events performed on the TOE are recorded, and provides accountability for them.

Threats	Objectives	Rationale
	OE.TIMESTAMP The TOE Environment must provide reliable timestamps for the TOE's use.	OE.TIMESTAMP requires that the TOE Environment provide timestamps for the TOE's use. These timestamps are recorded in all audit events. This ensures that all security-relevant events performed on the TOE are recorded with a date and time stamp, providing accountability.
T.IA A threat agent may attempt to compromise the TOE or network resources controlled by the TOE by attempting actions that it is not authorized to perform on the TOE or network resources.	OE.ADMINAUTH The TOE Environment must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.	OE.ADMINAUTH requires that all administrators be identified and authenticated prior to being allowed to access TOE administrative functions and data. This prevents unauthorized users from compromising the TOE.
	OE.RADIUS The TOE Environment must provide a RADIUS Server to assist in authentication of end-users and end-systems prior to the TOE granting or denying access to network resources.	OE.RADIUS requires that the TOE Environment provide a RADIUS Server to assist in authentication of end-users and end-systems prior to granting or denying access to network resources. This prevents unauthorized end-users or end-systems from compromising the TOE.
	O.USERAUTH The TOE must be able to authenticate end-users and end-systems prior to allowing access to network resources.	O.USERAUTH requires that the TOE be able to authenticate end-users and end-systems prior to allowing access to network resources. This prevents unauthorized users from compromising the TOE.
T.INFO_CAPTURE An external attacker or malicious insider may sniff the communication channel between the TOE and a remote administrator in order to capture or modify information sent between the two.	OE.SECURECOMMUNICATION The operational environment will provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.	OE.SECURECOMMUNICATION requires that information being transmitted between the TOE and TOE administrators never be modified or disclosed. This prevents external attackers and malicious insiders from capturing or modifying that data.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no policies defined for this Security Target.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 14 - Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.LOCATE The TOE resides in a physically controlled access facility that prevents unauthorized physical access.	NOE.TRUSTED_ENV The TOE shall reside in a physically secure location, safe from compromise by malicious insiders or outsiders.	NOE.TRUSTED_ENV ensures that the TOE shall reside in a physically secure location, thereby preventing unauthorized physical access.
A.NOEVIL Authorized administrators who manage the TOE are non-hostile and are appropriately trained to use, configure, and maintain the TOE and follow all guidance.	NOE.TRUSTED_ENV The TOE shall reside in a physically secure location, safe from compromise by malicious insiders or outsiders.	NOE.TRUSTED_ENV ensures that authorized administrators shall not compromise the TOE.
A.PROTECT The TOE and network devices shall be protected from MAC address spoofing and other disruptions of data and functions.	OE.PROTECT The TOE Environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT upholds this assumption by ensuring that the TOE Environment provides protection from external interference and tampering, thereby preventing MAC address spoofing and other disruptions of data and functions.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

No extended Security Functional Requirements have been defined for this Security Target.

8.4 Rationale for Extended TOE Security Assurance Requirements

No extended Security Assurance Requirements have been defined for this Security Target.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 15 - Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must record the actions taken by administrators and provide the authorized administrators with the ability to review and sort the audit trail.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of management events, including relevant details about the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FAU_SAR.3 Selectable audit review	The requirement meets the objective by ensuring that the TOE provides the ability to sort the audited events by any field value.
O.NETACCESS The TOE must allow access to internal network resources as defined by the Accept Access Control SFP, the Failsafe Access Control SFP, and the Quarantine Access Control SFP when policy functionality has been configured on the TOE.	FDP_ACC.1(a) Subset access control	The requirement meets the objective by defining the subjects, objects, and operations controlled by the Failsafe Access Control SFP.
	FDP_ACC.1(b) Subset access control	The requirement meets the objective by defining the subjects, objects, and operations controlled by the Accept Access Control SFP.
	FDP_ACC.1(c) Subset access control	The requirement meets the objective by defining the subjects, objects, and operations controlled by the Quarantine Access Control SFP.

Objective	Requirements Addressing the Objective	Rationale
	FDP_ACF.1(a) Security attribute based access control	The requirement meets the objective by defining the subject and object attributes, and the rules by which subjects can operate on objects under the Failsafe Access Control SFP.
	FDP_ACF.1(b) Security attribute based access control	The requirement meets the objective by defining the subject and object attributes, and the rules by which subjects can operate on objects under the Accept Access Control SFP.
	FDP_ACF.1(c) Security attribute based access control	The requirement meets the objective by defining the subject and object attributes, and the rules by which subjects can operate on objects under the Qurantine Access Control SFP.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FDP_ACC.1(d) Subset access control	The requirement meets the objective by defining the subjects, objects, and operations controlled by the Administrative Access Control SFP, which defines administrative access to the management functions of the TOE.
	FDP_ACF.1(d) Security attribute based access control	The requirement meets the objective by defining the subject and object attributes, and the rules by which subjects can operate on objects under the Administrative Access Control SFP.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MSA.1(a) Management of security attributes	The requirement meets the objective by ensuring that only authorized administrators are permitted to manage the security attributes of the Failsafe Access Control SFP, the Accept Access Control SFP, and the Quarantine Access Control SFP.
	FMT_MSA.1(b) Management of security attributes	The requirement meets the objective by ensuring that only authorized administrators are permitted to manage the security attributes of the

Objective	Requirements Addressing the Objective	Rationale
		Administrative Access Control SFP.
	FMT_MSA.3(a) Static attribute initialisation	The requirement meets the objective by ensuring that only authorized administrators are permitted to manage the default security attributes of the Failsafe Access Control SFP, the Accept Access Control SFP, and the Quarantine Access Control SFP.
	FMT_MSA.3(b) Static attribute initialisation	The requirement meets the objective by ensuring that only authorized administrators are permitted to manage the default security attributes of the Administrative Access Control SFP.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the security functions and security attributes.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.USERAUTH The TOE must be able to authenticate end-users and end-systems prior to allowing access to network resources.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by requiring that all TSF-mediated actions be denied prior to authentication to the TOE, when end-user and end-system authentication has been configured on the TOE.
	FIA_UID.2 User identification before any action	The requirement meets the objective by requiring that all TSF-mediated actions be denied prior to identification to the TOE, when end-user and end-system authentication has been configured on the TOE.

8.5.2 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable

software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2+, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 16 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 16 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	This dependency is met by the TOE Environment, which provides the timestamps for the TOE's use, as defined by OE.TIMESTAMP.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FDP_ACC.1(a)	FDP_ACF.1(a)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	
FDP_ACC.1(c)	FDP_ACF.1(c)	✓	
FDP_ACC.1(d)	FDP_ACF.1(d)	✓	
FDP_ACF.1(a)	FDP_ACC.1(a)	✓	
	FMT_MSA.3(a)	✓	
FDP_ACF.1(b)	FMT_MSA.3(a)	✓	
	FDP_ACC.1(b)	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACF.1(c)	FMT_MSA.3(a)	✓	
	FDP_ACF.1(c)	✓	
FDP_ACF.1(d)	FDP_ACC.1(d)	✓	
	FMT_MSA.3(b)	✓	
FIA_UAU.2	FIA_UID.1	✓	Because FIA_UID.2 is hierarchical to FIA_UID.1, and is included in this Security Target, this dependency is met.
FIA_UID.2	No dependencies		
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(a)	FMT_SMF.1	✓	
	FDP_ACC.1(b)	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1(a)	✓	
	FDP_ACC.1(c)	✓	
FMT_MSA.1(b)	FDP_ACC.1(d)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(a)	FMT_MSA.1(a)	✓	
	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FMT_MSA.3(b)	FMT_SMR.1	✓	
	FMT_MSA.1(b)	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.1	✓	The dependency for the User role is met by FIA_UID.2, which is hierarchical to FIA_UID.1. The dependency for the Administrator role and the Limited Administrator role is met by the TOE Environment, as defined by the OE.ADMINAUTH objective.

9 Acronyms

Table 17 - Acronyms

Acronym	Definition
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DRAM	Dynamic Random Access Memory
EAL	Evaluation Assurance Level
GB	Gigabyte
GHz	GigaHertz
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
MAC	Media Access Control
MB	MegaBytes
MHz	MegaHertz
NAC	Network Access Control
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
PWA	Port Web Authentication
RADIUS	Remote Authentication Dial In User Service

Acronym	Definition
SAR	Security Assurance Requirement
SFP	Small Form-factor Pluggable
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation