Ceragon NetMaster

Security Target v1.4

Date: 2022-07-22

Created by

Change History

Version	Date	Author	Comment
0.1	2021/07/01	Ceragon Networks Ltd	Creation of the Document
0.2	2021/07/13	Ceragon Networks Ltd	Added changes proposed by the product architecture team
0.3	2021/08/02	Ceragon Networks Ltd	Added changes proposed by the product architecture team
0.4	2021/08/11	Ceragon Networks Ltd	Adjustments to the security problem and to the scope of secure channels
1.0	2021/09/08	Ceragon Networks Ltd	Change to the name of the TOE
1.1	2021/09/29	Ceragon Networks Ltd	The SNMP Agent sub-system is defined with more detail.
1.2	2021/12/03	Ceragon Networks Ltd	NCs by laboratory.
1.3	2022/01/20	Ceragon Networks Ltd	Fixing assignments.
1.4	2022/07/22	Ceragon Networks Ltd	Removing the SSH channel of the scope.

Table of contents

1 ST INTRODUCTION

1.1 ST REFERENCE

Title: Ceragon NetMaster Security Target

Version: v1.4

Author: Ceragon Networks Ltd

Evaluation Lab: jtsec Beyond IT Security

Date of publication: 2022-07-22

1.2 TOE REFERENCE

TOE Name: NetMaster

TOE Developer: Ceragon Networks Ltd

TOE Version: R21B00 - Build 1028

1.3 TOE OVERVIEW

1.3.1 INTRODUCTION

NetMaster is a Network Management System offering centralized operation and maintenance capability for a range of network elements. The TOE establishes secure communication channels with these elements: HTTPS with secure algorithms. In addition, Network Elements can communicate with the TOE through a secure SNMPv3 channel (which is configured from the TOE through the Connection Templates).

NetMaster offers complete range monitoring of all Ceragon and third-party network elements. NetMaster is designed for managing large-scale wireless backhaul networks.

Administrator users can manage NetMaster via the NetMaster Client. The NetMaster Client allows access through a graphical interface or a command-line interface; both interfaces require an authentication process.

1.3.2 TOE TYPE

NetMaster is a Network Management System (NMS) responsible for configuring, managing, and monitoring various network devices in a Wide Area or a Local Area Network. The TOE only consists of software (the NMS), not hardware.

1.3.3 TOE USAGE & MAJOR SECURITY FEATURES

NetMaster can receive traps from Network Elements and perform alarm synchronization; it receives fault alarms classified by severity (Critical, Major, Minor, Warning, Indeterminate, Info), with the capacity to filter by the kind of event. Moreover, it allows configuring Network Elements, backups, performing inventory reports, performance reports, and alarm reports.

Regarding users, NetMaster can perform group and user accounts administration, create new groups with defined permissions. As well as modifying security preferences, such as determining the maximum number of permitted authentication failure attempts or enabling protocols like SNMPv3. Finally, NetMaster performs audit logging and advanced log filtering, being able to associate events with users.

The TOE major security features are the following:

1. Security Audits.
2. User Data Protection.
3. Identification and Authentication.
4. Security Management.
5. TOE Access.
6. Trusted path/channels.

1.3.4 NON-TOE HARDWARE/SOFTWARE/FIRMWARE

1.3.4.1 ELEMENTS THAT ARE NOT PART OF THE TOE

It is necessary to consider that the TOE is connected to several network elements, monitoring them. The operational environment of the TOE can be divided into two groups; the element that are installed in the same machine as the TOE and the network elements.

Elements that are not part of the TOE:

- SFTP Server: NetMaster works with an external SFTP server that needs to be installed and configured by the user as defined in the manuals. Inside the NetMaster preferences view, the user configures the path and credentials for the SFTP servers. During file transfer, NetMaster sets these credentials on the Network Element and uploads the software file to the SFTP server. After getting the command from NetMaster, the Network Element connects to SFTP and downloads the file.

- Database Server: The database server stores all data used by the NetMaster system, except for large volumes of data handled by an Elasticsearch database.

Network Elements that are not part of the TOE:

- FibeAir IP-10, 20 and 50 Platforms are Network elements manufactured by Ceragon. The products consist of a wide range of elements, from routing products responsible for the backhaul of a network, to microwave radios responsible for communicating information over long distances from one point to another. All these elements can be managed by HTTPS through the TOE. In addition, they regularly send SNMPv3 messages to the TOE when requested by the TOE.

- Third-party network elements, such as power supplies, switches, and routers. These products can be configured to send SNMP messages to the TOE when requested by it; however, these products cannot be managed from the TOE.

1.3.4.2 TOE REQUIRED SOFTWARE

The TOE is delivered as software, which must be installed in one or more machines under a Windows operating system. In the evaluated configuration, the TOE and additional non-TOE software will be installed on the same Windows machine in a 1+0 Standalone configuration. Therefore, before installing the TOE software, it is necessary to install:

- **Database server**: NetMaster requires an Oracle or PostgreSQL database to be installed and available for NetMaster use. The database can be linked to the TOE through the System Manager wizard. Database systems supported: PostgreSQL version 11.5, Oracle 11g R2, 11.2.0.1.0, 64-bit edition, and Oracle 12c.

- **SFTP Server**: For using SFTP, the SFTP server software shall be installed on the same machine as the NetMaster Server. It is recommended to use the SolarWinds SFTP server 1.0.4.9 (freeware) or later. The SFTP server should be linked to NetMaster manually, as described in the manuals.

- **Java virtual Machine**. NetMaster is based on JAVA, therefore, it is necessary to install a Java Development Kit on the system. It is mandatory to install OpenJDK with version 8.

The TOE can be installed in the following operating systems:

- Windows Server 2016 64-bit.

- Windows Server 2019 64-bit.

- Windows 10 64-bit.

1.3.4.3 TOE REQUIRED HARDWARE

There are a number of factors affecting the requirements for NetMaster:

- The number of managed network elements and radio channels.
- The amount of information and number of alarms/events generated by the elements.
- The quantity and frequency of performance measurement data collected from the elements.
- Whether the NetMaster Client, NetMaster Server, and Database Server are co-located on the same computer or installed on separate computers.
- The number of concurrent clients running.
- Enabled NetMaster features and preferences.
- Load or interference from other applications on the same computers.
- Load or interference from other traffic in the DCN.

On each machine where NetMaster Server or NetMaster System Manager are installed, it is mandatory to keep a minimum of 30GB free disk space, the following table shows the recommended hardware specifications based on number of managed NEs for Standalone configurations:

Number of NEs	**CPU**	**RAM**	**Disk**
1-50 (Demo/Lab Tests)	2 Physical cores / 4 virtual cores	8GB	120GB
1-500	4 Physical cores / 8 Virtual cores	16GB	200GB SSD
500-2000	8 Physical cores / 16 Virtual cores	32GB	400GB SSD
2000-5000	16 Physical cores / 32 Virtual cores	64GB	800GB SSD

5000-10000	16 Physical cores / 32 Virtual cores	128GB	2x800GB SSD
10000-20000	20 Physical cores / 40 Virtual cores	128GB	4x800GB SSD RAID 0

**All CPU core numbers refer to X86-64 Server CPU architecture cores. All physical CPU core counts assume that Hyperthreading or equivalent is in place, hence they imply the doubled amount in virtual cores - (1 Physical x86-64 CPU with Hyper thread or equiv. = 2vCPUs).*

1.4 TOE DESCRIPTION

1.4.1 INTRODUCTION

NetMaster is a network management system that allows the management/monitoring of WAN/LAN networks.

This section describes the NetMaster configuration and environment for the evaluated configuration. Then, the logical scope of the TOE is defined, representing the various elements that make up the TOE, as well as the security functions it performs and the security-related functions that are not in the scope of the TOE. Lastly, the physical scope of the TOE is described.

1.4.1.1 TOE EVALUATED CONFIGURATION

NetMaster supports multiple configurations in different scenarios:

- 1+0 Standalone: The operational environment (the database and SFTP servers) and all the TOE elements are in one machine (virtual or physical).
- 1+0 Split: Setup in which two machines are required. Part of the operational environment (SQL Database) is in one machine. The other part of the operational environment (SFTP Server) and all the TOE elements are in the second machine.
- 1+1 High Availability (1+1 HA): Two 1+0 Standalone, called mates, are configured so that one is the Primary Server, and the other is the Secondary Server.
- 2+2 High Availability (2+2 HA): Two 1+0 Split composed four machines; two machines host a NetMaster Server (+ SFTP Server), and two additional machines host a SQL database. The machines that host the NetMaster Server act like 1+1 High Availability; the machines that host the SQL database act like Active SQL Database and Failover Database, respectively.
- 1+1 Server High Availability: A setup in which two machines are required. In this setup, the SQL database is not managed by System Manager (NetMaster element, which provides a web interface for configuring the NetMaster database and shutting NetMaster down or turning it on), so it's not counted as part of the setup. In a 1+1 Server High Availability setup, only NetMaster Server high availability is managed by the NetMaster System Manager; database high availability remains the responsibility of the user.

The evaluated configuration is based on 1+0 Standalone. All TOE components (both server and client, plus other components) and the database and the SFTP server are installed in the same machine. Such TOE evaluated configuration is intended to provide a scenario with a basic setup with the indispensable settings required for the TOE to deploy the security functionality described in this Security Target.

Note: The access to the TOE's element "System Manager" is blocked after installing the TOE and configuring it for the first time. Therefore, this interface is not accessible during operational stage of the TOE and cannot be considered as a mean to manage the TOE or as an input interface for possible attempts to perform adverse actions on the TOE by a potential attacker. Furthermore, the

SNMP agent element (NetMaster element that allows forwarding SNMP messages received by NetMaster to other third-party applications) is disabled by default; unlike the System Manager, the SNMP agent is not used during [PRE] in the TOE installation. The SNMP Agent is disabled by default during the operational stage of the TOE and cannot be considered as a mean to manage the TOE or as a possible communication channel to perform adverse actions on the TOE by a potential attacker.

Moreover, the port 22 (SSH) is blocked in the machine where the TOE is installed in outbound connections, for disabling this channel and functionality of the TOE.

The installation will be performed on a machine with Windows Server 2019 64-bit as operating system (the Windows operating system is operational environment, not TOE), the TOE evaluated configuration can be described as follows:

- A PostgreSQL database version 11.5, which will be installed before the TOE.
- A SolarWinds SFTP Server with a minimum version of 1.0.4.9, which will be installed before the TOE.
- NetMaster (all its components) version referenced in *1.2 TOE Reference*, installed in a 1+0 Standalone configuration in the same machine as the SFTP and Database servers.

Note: For obtaining reliable time sources in the TOE evaluated configuration, the TOE is configured to synchronize its system clock with the clock of the host machine which has a secure and reliable time source according to TOE guidelines.

To achieve the above-described configuration, the TOE preparative guide must be thoroughly followed for the TOE installation and configuration.

1.4.2 TOE LOGICAL SCOPE

The following diagram depicts a typical scenario where the TOE is deployed in a network. All within the red figure is considered to be part of the TOE and is installed on the same machine according to the standalone 1+0 configuration. Likewise, the database and the SFTP server are installed on the same device, even though there are part of the operational environment (not TOE).

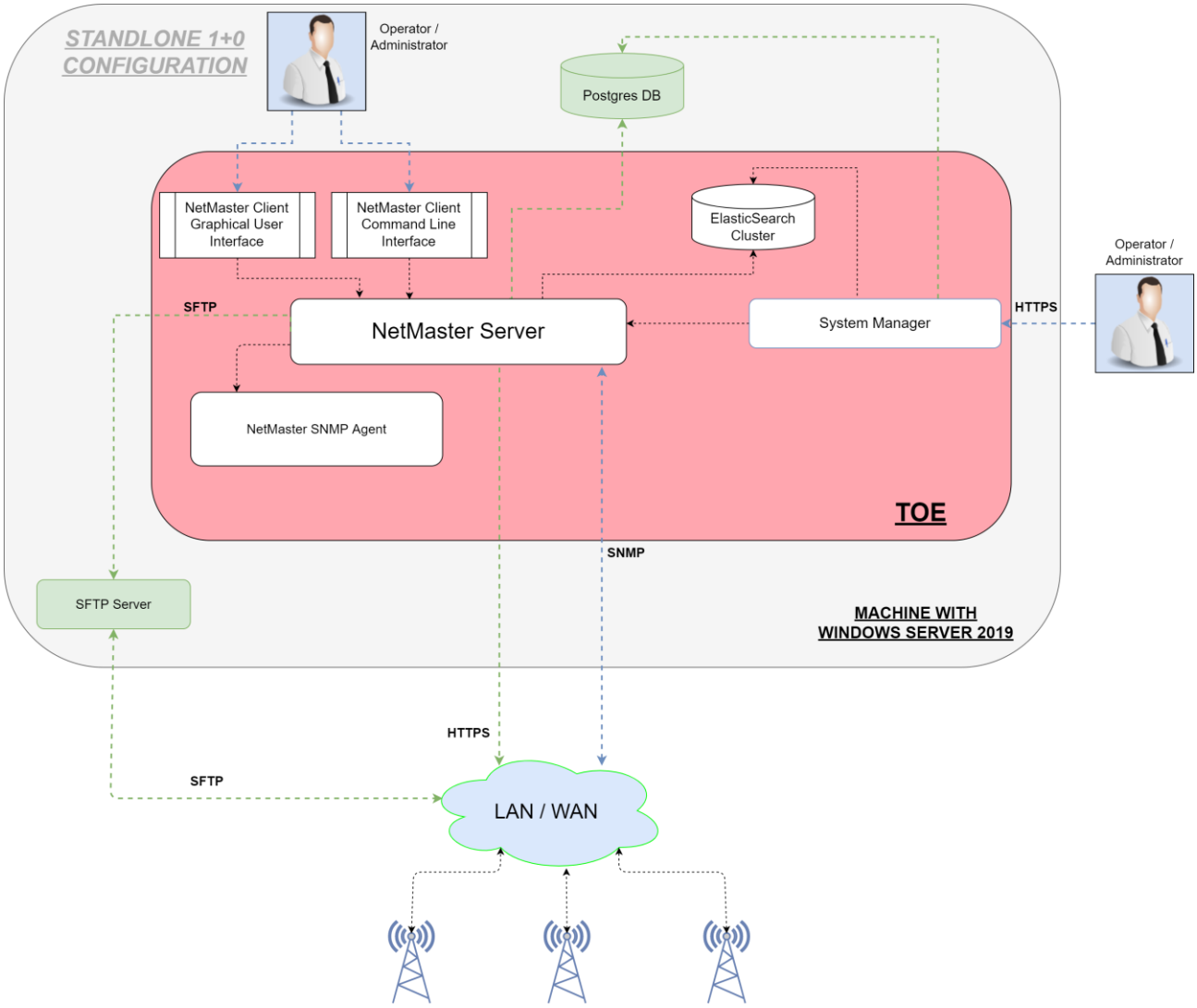

Figure 1. *Diagram of the TOE and its operational environment*

Note: In the Figure 1, the SFTP server (non-TOE) and the Postgres DB (non-TOE) are located inside the windows server 2019 machine; this is done in order to maintain the evaluated TOE configuration (1+0 Standalone, where the entire TOE operational environment and TOE elements are located on the same machine).

- **NetMaster Server**: The NetMaster server manages the interaction of all NetMaster system components and is the only entity that communicates with the network devices and performs the user-required management tasks. It runs continuously in the background as a service. It is based on JAVA technology.

- **NetMaster Client**: A client provides the user interface to the active services and the network managed by the server. Client and server are installed in the same machine in the 1+0 Standalone configuration. Interactions between client and server are based on JAVA RMI. Access to the NetMaster Client is local, since the NetMaster Client is installed on the same machine in the standalone configuration and access is through this application. NetMaster Client provides two interfaces to manage the TOE, a command line and a graphical interface, both within the scope of the TOE.

- **System Manager**: The purpose of the System Manager is to provide the NetMaster administrators a more accessible and more flexible way to deal with some NetMaster administrative tasks. NetMaster System Manager is a web application, and it uses wizards to schedule database back-up and database maintenance tasks (creation, high availability…), configure email notifications, and start/stop the NetMaster Server. System Manager is not remotely accessible during the operational stage of the TOE. After installing the TOE and configuring it for the first time, access to this element is not allowed for any remote user in the evaluated configuration. System manager is only locally accessible by entering its local IP address in a web browser in its evaluated configuration (but guidelines are imposed in [PRE] to prevent administrators from accessing this interface); System Manager continues to perform some tasks such as initializing the databases, even though its user access is disabled to prevent configuration changes.

- **NetMaster SNMP Agent**: Network Elements that NetMaster manages (Ceragon or 3rd party) communicate only with the NetMaster Server. SNMP Agent is used to forward the SNMP messages that NetMaster receives to 3rd party applications; however, this communication is disabled by default and it is not part of the TOE evaluation. SNMP Agent does not communicate with the Network Elements.

- **Elasticsearch Cluster**: Elasticsearch is a complementary database in which NetMaster stores large volumes of Performance Measurements (Traffic Queue Performance report, Ethernet Utilization report, Input voltage performance report…) collected from NEs. These measurements are sent by the NEs via SNMP to the NetMaster Server; due to the large size of these metrics, the NetMaster server stores the data in the Elasticsearch database. The NetMaster Installer automatically installs an Elasticsearch node.

While it is possible to have different setups and more complex scenarios, which are out of the scope of the evaluated configuration, the above summarizes the basic deployment case that illustrates how the TOE functions with its environment.

1.4.2.1 SECURITY AUDIT

The TOE generates audit data related to management events (administrative actions). The TOE associates audit events with the user who produced them if that is applicable. Finally, the TOE only allows authorized users to access the logs; however, the TOE protects the audit trails from being deleted or modified by any user.

1.4.2.2 USER DATA PROTECTION

The TOE implements an access control policy in which users are enabled by its group to execute certain objects. Each user belongs to a group, the objects that can be executed by that user are limited to those objects enable for its group. There are objects that can only be executed by certain groups that are created by default in the TOE and cannot be deleted (Security Officers and Administrators).

1.4.2.3 IDENTIFICATION AND AUTHENTICATION

The TOE does not allow to perform any action before a proper user successfully authenticated. Moreover, the TOE can lock users after a defined number of failed authentication attempts.

1.4.2.4 SECURITY MANAGEMENT

The TOE creates the following groups by default: Administrators, Security Officers, Services Manager, Services Viewer, and SNMP Agent. However, only Administrators and Security Officers groups cannot be removed from the TOE, as it always maintains them due to the functionality they provide.

The management functions involve: starting and stopping the NetMaster Server, reading and filtering logs, discovering and configuring Network Elements, configuring connection templates (creation, modification and deletion), connection templates assignment, defining a period of time for user's session termination by inactivity, configuring security preferences, performing backups and restoring NE's configurations, generating reports, and performing user and group administration. The different management functions provided via the TOE interfaces are available with different permissions depending on the user group.

1.4.2.5 TOE ACCESS

Users can terminate their own sessions; furthermore, after a defined period of inactivity time, the TOE ends the user's session.

1.4.2.6 TRUSTED PATH/CHANNELS

When the TOE manages the NEs, it communicates through HTTPS. Furthermore, the communication between the Network Elements and the TOE for functionalities as generating reports is done by SNMPv3.

1.4.3 TOE PHYSICAL SCOPE

The Target of Evaluation (TOE) is purely a software TOE and includes the following components:

Name	Type	Version	Distribution format	Description	Delivery
NetMaster	Software	R21B00 Build 1028	Installation package (.exe).	Executable file that allows to install the various elements of the TOE	Download from manufacturer's SharePoint server. The file is delivered inside a .zip.
NetMaster Installation Guide	Guidance	R21B00 Rev A	PDF Document	Installation guide of the TOE with all different kinds of installation setups.	Download from manufacturer's SharePoint server. The file is delivered inside a .zip.
NetMaster Technical Description	Guidance	R21B00 Rev A	PDF Document	Description of the various elements of NetMaster, as well as their functionality.	Download from manufacturer's SharePoint server. The file is delivered inside a .zip.
NetMaster User Guide	Guidance	R21B00 Rev A	PDF Document	User's guide to NetMaster, its views, configurations, etc.	Download from manufacturer's SharePoint server. The file is delivered inside a .zip.
Ceragon NetMaster - AGD_PRE	Guidance	0.6	PDF Document	Guidance for installation of the TOE and preparation of the operational environment.	Download from manufacturer's SharePoint server. The file is delivered inside a .zip.

Ceragon NetMaster - AGD_OPE	Guidance	0.5	PDF Document	Guide for operational use of the TOE.	Download from manufacturer's SharePoint server. The file is delivered inside a .zip.

2 CONFORMANCE CLAIMS

This Security Target and the TOE described are in accordance with the requirements of Common Criteria 3.1R5.

This Security Target claims conformance with the following parts of Common Criteria:

- Conformance with [CC31R5P2].
- Conformance with [CC31R5P3].

The methodology to be used for the evaluation is described in the "Common Evaluation Methodology" of the Common Criteria standard of April 2017, version 3.1 revision 5 with an evaluation assurance level of EAL2.

This Security Target does not claim conformance with any protection profile.

3 SECURITY PROBLEM DEFINITION

This section describes the security aspects of the operational environment and its expected use in said environment. It includes the declaration of the TOE operational environment that identifies and describes:

- The alleged known threats that will be countered by the TOE
- The organizational security policies that the TOE has to adhere to
- The TOE usage assumptions in the suggested operational environment.

First, the Assets and Agents of threats will be defined.

3.1 ASSETS

DATA IN TRANSIT: The TOE requests messages from the Network Elements for monitoring functions. Moreover, the TOE communicates with the Network Elements for management functions. This asset is referring to the data exchanged in the aforementioned communications. The security dimensions of this asset are INTEGRITY and CONFIDENTIALITY.

Application Note:

The SFTP server is installed on the same machine as the TOE, being local its communication with the TOE. Therefore, it is not necessary to protect this communication, being excluded from the asset DATA IN TRANSIT.

3.2 THREAT AGENTS

REMOTE_ATTACKER: An attacker trying to intercept or modify communications between the TOE and the Network Elements, or even act as a Network Element.

3.3 THREATS TO SECURITY

This section identifies the threats to assets that require protection by the TOE. The threats are defined in terms of assets concerned, attackers and the adverse action that materializes the threat.

T.NETWORK_EAVESDROP: A **REMOTE_ATTACKER** is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor, gain access, or modify without authorization **DATA IN TRANSIT** exchanged between the NetMaster Server and the Network Elements.

3.4 ORGANIZATIONAL SECURITY POLICIES

The organizational Security policies are defined as follows.

P.AUDIT: Audit data must be made available, thus the activities of users and their interaction with the TOE can be consulted and tracked.

P.MANAGEMENT: Identification and authorization must be ensured in the TOE, ensuring that authentication and authorization is performed on local access to the TOE for accessing to management functions, in accordance with the capabilities associated with each user's role, with these roles being established by the TOE.

3.5 ASSUMPTIONS

The assumptions when using the TOE are the following:

A.TRUSTED_ADMINS: Administrators of the TOE are appropriately trained to undertake the installation, configuration, and management of the TOE in a secure trusted manner as indicated in the TOE manuals. They are not careless, willfully negligent, or hostile.

A.SECURE_LOCATION: The machine on which the TOE resides is located within a facility that provides controlled access, ensuring only authorized personnel have physical access to the machine where the TOE is deployed.

A.SECURE_DB: All the data stored in the databases are protected by the platform on which they reside.

A.TIMECONFIG: The hardware and the hosting OS where the TOE runs provide accurate time to the TOE.

A.TRUSTED_PLATFORM: The platform administrators keep it updated and hardened. The platform ensures that only authorized personnel have logical access to the machine where the TOE is deployed.

A.TRUSTED_NES: Network Elements connected to the same network as the TOE are correctly configured and their operation allows them to communicate reliably with the TOE.

4 SECURITY OBJECTIVES

The security objectives are high level declarations, concise and abstract of the solution to the problem exposed in the former section, which counteracts the threats and fulfills the security policies and the assumptions. These consist of:

- the security objectives for the operational environment.
- the security objectives for the TOE.

4.1 SECURITY OBJECTIVES FOR THE TOE

The security objectives for the TOE must determine (to the desired extent) the responsibility of the TOE in countering the threats and in enforcing the OSPs. Each objective must be traced back to aspects of identified threats to be countered by the TOE and to aspects of OSPs to be met by the TOE.

OT.MANAGEMENT: The TOE shall enforce authentication and authorization to users on the TOE management interfaces in accordance with the capabilities associated with each role, and will establish and maintain those roles. Moreover, the TOE shall protect itself from brute force attacks (user's login block after various attempts) and should close interactive user's sessions after a determined period of time.

OT.AUDIT: The TOE shall generate audit data on management operations and start-up and shutdown of the audit functions. Furthermore, the TOE shall relate the audit events to the user who produce them (if applicable). Finally, the TOE shall protect the audit records from unauthorized deletion or modification; as well as only allowing access to these logs to authorized users.

OT.COMM: The outbound communication channels (HTTPS) for NEs administration between the TOE and the NEs shall be protected to avoid capturing sensitive data or unauthorized modification. In the same way, the communication channel (SNMP) whereby the NEs send SNMP messages to the TOE shall be protected to avoid capturing sensitive data or unauthorized modification.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The security objectives for the Operational Environment determine the responsibility of the environment in countering the threats, enforcing the OSPs and upholding the assumptions. Each objective must be traced back to aspects of identified threats to be countered by the environment, to aspects of OSPs to be enforced by the environment and to assumptions to be uphold by the environment.

OE.TRUSTED_ADMINS: Administrators of the TOE shall be appropriately trained to undertake the installation, configuration, and management of the TOE in a secure trusted manner as indicated in the TOE manuals. They shall not be careless, willfully negligent, or hostile.

OE.SECURE_LOCATION: The machine on which the TOE resides shall be located within a facility that provides controlled access, ensuring only authorized personnel have physical access to the machine where the TOE is deployed.

OE.SECURE_DB: All the data stored in the databases shall be protected by the platform on which they reside.

OE.TIMECONFIG: The hardware and the hosting OS where the TOE runs shall provide accurate time to the TOE.

OE.TRUSTED_PLATFORM: The platform (operating system) on which the TOE is installed is secure. The platform administrators shall keep it updated and hardened. The platform (operating system) shall ensure that only authorized personnel have logical access to the machine where the TOE is deployed by implementing secure access control methods.

OE.TRUSTED_NES: Network Elements connected to the same network as the TOE shall be correctly configured and their operation shall allow them to communicate reliably with the TOE.

4.3 SECURITY OBJECTIVES RATIONALE

The following table provides a mapping of security objectives tracing each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective. This illustrates that the security objectives counter all threats, the security objectives enforce all OSPs and the security objectives for the operational environment uphold all assumptions.

	OT.MANAGEMENT	OT.AUDIT	OT.COMM	OE.TRUSTED_ADMINS	OE.SECURE_LOCATION	OE.SECURE_DB	OE.TIMECONFIG	OE.TRUSTED_PLATFORM	OE.TRUSTED_NES
T.NETWORK_EAVESDROP			X						
P.AUDIT		X					X		
P.MANAGEMENT	X				X			X	
A.TRUSTED_ADMINS				X					
A.SECURE_LOCATION					X				
A.SECURE_DB						X			
A.TIMECONFIG							X		
A.TRUSTED_PLATFORM								X	
A.TRUSTED_NES									X

Table 1 *Security Objectives vs Security Problem Definition*

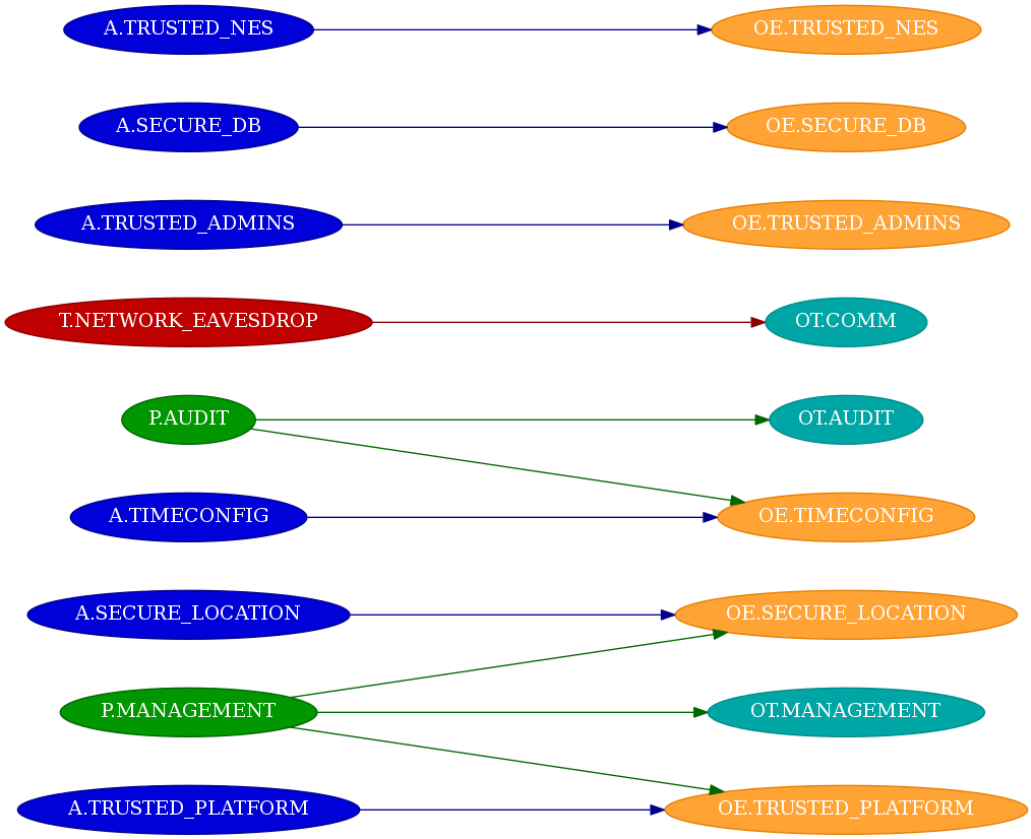

Figure 2 Mapping of Security Problem Definition to Security Objectives

4.3.1 THREATS

T.NETWORK_EAVESDROP: This threat is mitigated by **OT.COMM**, which ensures that the communications between the TOE and other IT trusted external entities occurs through trusted channels, not allowing attackers to access or modify information in transit without authorization.

The following table maps the threats of the security problem established to the security objectives of the TOE and the security objectives of the operational environment.

Threats	Security Objectives
T.NETWORK_EAVESDROP	OT.COMM

Table 2 Threats vs Security Objectives

4.3.2 ORGANIZATIONAL SECURITY POLICIES

P.AUDIT: This policy is addresses by **OT.AUDIT** and **OE.TIMECONFIG**

P.MANAGEMENT: This policy is addressed by **OT.MANAGEMENT**, **OE.SECURE_LOCATION**, and **OE.TRUSTED_PLATFORM**

The following table maps the organizational security policies of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

OSPs	Security Objectives
P.AUDIT	OT.AUDIT OE.TIMECONFIG
P.MANAGEMENT	OT.MANAGEMENT OE.SECURE_LOCATION OE.TRUSTED_PLATFORM OE.TRUSTED_NES

Table 3 OSPs vs Security Objectives

4.3.3 ASSUMPTIONS

A.TRUSTED_ADMINS: This assumption is upheld by **OE.TRUSTED_ADMINS**, which requires that the personnel configuring, managing, or monitoring the TOE are trusted and trained personnel that properly follow the TOE preparative guides.

A.SECURE_LOCATION: This assumption is upheld by **OE.SECURE_LOCATION**, which requires that the infrastructure where the TOE is deployed has physical control access.

A.SECURE_DB: This assumption is upheld by **OE.SECURE_DB**, which requires that all the data stored by the TOE in the databases is properly protected by the platform.

A.TIMECONFIG: This assumption is upheld by **OE.TIMECONFIG**, which requires that the environment provides a reliable time source to the TOE.

A.TRUSTED_PLATFORM: This assumption is upheld by **OE.TRUSTED_PLATFORM**, which requires that the platform where the TOE is installed is secure, and the platform's administrators keep it updated and hardened. Furthermore, the platform (OS) ensures that only authorized personnel have logical access to the machine where the TOE is deployed by implementing secure access control methods.

A.TRUSTED_NES: This assumption is upheld by **OE.TRUSTED_NES**, which requires that the Network Elements connected to the same network as the TOE are correctly configured and their operation allows them to communicate reliably with the TOE.

The following table maps the assumptions of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

Assumptions	Security Objectives
A.TRUSTED_ADMINS	OE.TRUSTED_ADMINS
A.SECURE_LOCATION	OE.SECURE_LOCATION
A.SECURE_DB	OE.SECURE_DB
A.TIMECONFIG	OE.TIMECONFIG
A.TRUSTED_PLATFORM	OE.TRUSTED_PLATFORM
A.TRUSTED_NES	OE.TRUSTED_NES

Table 4 Assumptions vs Security Objectives for the Operational Environment

5 EXTENDED COMPONENTS DEFINITION

No extended components have been defined.

6 SECURITY REQUIREMENTS

This section defines the Security functional requirements (SFRs) and the Security assurance requirements (SARs) that fulfill the TOE. Assignment, selection, iteration and refinement operations have been made, adhering to the following conventions:

- Assignments. They appear between square brackets. The word "assignment" is maintained and the resolution is presented in ***boldface, italic and blue color.***
- Selections. They appear between square brackets. The word "selection" is maintained and the resolution is presented in ***boldface, italic and blue color.***
- Iterations. It includes "/" and an "identifier" following requirement identifier that allows to distinguish the iterations of the requirement. Example: FCS_COP.1/XXX.
- Refinements: the text where the refinement has been done is shown ***bold, italic, and light red color.*** Where part of the content of a SFR component has been removed, the removed text is shown in ~~***bold, italic, light red color and crossed out.***~~

6.1 SECURITY FUNCTIONAL REQUIREMENTS

6.1.1 FAU: SECURITY AUDIT

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 ***[selection: not specified]*** level of audit; and

c) ***[assignment: server start-up, connection templates management (creation, modification and deletion), users logged in and logged out, user creation and deletion, group creation and deletion, user's password changes, user to group assignation, update group permissions, and lock/block and unblock users].***

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, ***[assignment: no other audit relevant information].***

6.1.1.2 FAU_GEN.2: USER IDENTITY ASSOCIATION

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

6.1.1.3 FAU_SAR.1: AUDIT REVIEW

FAU_SAR.1.1 The TSF shall provide ***[assignment: users inside the Administrators and Security Officers groups]*** with the capability to read ***[assignment: all the events listed in FAU_GEN.1.1]*** 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.

6.1.1.4 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 ***[selection: prevent]*** unauthorized modifications to the stored audit records in the audit trail.

6.1.2 FDP: USER DATA PROTECTION

6.1.2.1 FDP_ACC.1: SUBSET ACCESS CONTROL

FDP_ACC.1.1 The TSF shall enforce the ***[assignment: access control SFP]*** on ***[assignment: Subjects: users in groups; Objects: defined in Table 5; Operations: Execute the objects].***

Application Note

"Users in groups" refers to the users of any group created in the TOE. By default, the groups created are Administrators, Security Officers, Services Manager, Services Viewer, and SNMP Agent.

The TOE refers as Action Permissions to what is referred in this SFR as Objects.

Object	Description
User Administration	This object allows access to the “User Management” View, with the ability to manage users (list users, change passwords, create and delete users, change group users, and block and unblock users).
Group Administration	This object allows access to the “Group Management” View, with the ability to manage groups (list groups, create, clone, modify and delete groups, and assign objects to groups).
Audit Log	This object allows access to the “Audit Log” View, with the ability to read and filter the logs.
CLI Script Broadcast	This object allows access to execute commands on the NetMaster Client CLI for generating reports.
Backup and restore of configuration	This object allows access to the “Configuration File Management” View, with the ability to perform backups on NEs configurations or restore NEs.
Connection Templates	This object allows access to the “Connection Templates” View, with the ability to manage Connection Templates (list Connection Templates, create, modify, delete, and assign Connection Templates to NEs).
Inventory views	This object allows access to the “Hardware Inventory” and “Software Inventory” Views, with the ability to read the available hardware and software of the NEs managed by the TOE.
Launch External Applications	This object allows access to run External tools that can be added to NetMaster (not contemplated in the evaluated configuration).
Open SNMP Interface	This object allows access to the “Open SNMP Interface” View, with the ability to discover and manage third-party Network Elements.

NE software management	This object allows access to the "Element Software Management" View, with the ability to upload to the TOE NE's software updates. Moreover, it allows access to the "Software Download Jobs" View, with the ability to create and execute Software Download Jobs (downloading software updates to the NEs).
Discover and Manage Devices	This object allows access to the "Discover Settings", "Unmanaged Elements", and "Managed Elements" Views, with the ability to discover NEs in the network, manage or unmanage them. The group of the user who tries to access this object needs also to have assigned the objects: Logic Resource and Geographical Resource.
Ethernet service management	This object allows access to the "Ethernet Topology", "Ethernet Service Ports", and "Ethernet Service Path" Views, with the ability to manage the provisioning of end-to-end Ethernet Services.
Ethernet service viewing	This object allows access to the "Ethernet Topology", "Ethernet Service Ports", and "Ethernet Service Path" Views, with the ability to read the provisioning of end-to-end Ethernet Services.
Alarm management	This object allows access to the "Active Alarms" "Active Alarms Unacked Only", and "Active Alarms Acked Only" Views, with the ability to list and filter alarms, and to acknowledge or non-acknowledge alarms.
Alarm Template management	This object allows access to the "Alarm Templates" and "Alarm Templates Assignment" Views, with the ability to list, create, modify and delete alarm templates, and to assign Alarm Templates to Ceragon NEs.
Historical alarms	This object allows access to the "Historical Alarms" "Historical Alarms Unacked Only", and "Historical Alarms Acked Only" Views, with the ability to list and filter historical alarms, and to acknowledge or unacknowledge historical alarms.
Alarm notification	This object allows access to the "Alarm Notification" View, with the

management	ability to list, create, modify, or delete rules for generating sounds, e-mails or On-screen notifications when certain alarms occur in the network.
SNMP northbound interface	This object allows access to the “Northbound SNMP Settings” View, with the ability to list, create, modify, or delete a communication channel with third-party applications for forwarding SNMP data.
System Preferences	This object allows access to the “System Settings” Menu, with the ability to perform different configuration in the TOE such as defining the Session time out value, the password policies, or the maximum failed login attempts before user blocking.
Current performance monitoring	This object allows access to the “Current Performance” View, with the ability to list and delete active performances reports.
Performance monitoring control	This object allows access to the “Performance Collection Control” View, with the ability to list and generate various reports in the same way as the object CLI Script Broadcast, but from the NetMaster Client GUI.
Historical performance monitoring	This object allows access to the “Historical Performance” View, with the ability to list and delete historical performances reports.
Scheduled reports	This object allows access to the “Scheduled Reports” View, with the ability to list, create, delete, run and stop software and hardware inventory reports.
TDM service management	This object allows access to the “TDM Domains”, “TDM Topology”, “TDM Service Ports” and “TDP Service Path” Views, with ability to list and manage the provisioning end-to-end TDM trails.
TDM user link management	This object allows access to the “TDM Domains”, “TDM Topology”, “TDM Service Ports” and “TDP Service Path” Views, with ability to list the provisioning end-to-end TDM trails, and to run the User Link Wizard for enabling TDM trails between NEs.

TDM service viewing	This object allows access to the “TDM Domains”, “TDM Topology”, “TDM Service Ports” and “TDP Service Path” Views, with ability to list the provisioning end-to-end TDM trails.
Change topology attributes	This object allows access to modify Logical and Geographical Map’s Attributes. The group of the user who tries to access this object needs also to have assigned the objects: Logic Resource and Geographical Resource.
Administrative domain management	This object allows access to create new administrative domains in Logical and Geographical Maps. The group of the user who tries to access this object needs also to have assigned the objects: Logic Resource and Geographical Resource.
Link management	This object allows to access the User Link Wizard to enabling links between NEs. The group of the user who tries to access this object needs also to have assigned the objects: Logic Resource and Geographical Resource.
Map viewing	This object allows access to the “Geographical Map” and “Logical Map” Views. The group of the user who tries to access this object needs also to have assigned the objects: Logic Resource and Geographical Resource.
Map Management	This object allows access to the “Geographical Map” and “Logical Views”, to the ability to modify the location or position of the NEs in these maps. The group of the user who tries to access this object needs also to have assigned the objects: Logic Resource and Geographical Resource.
Geographical Map	This object allows access to the “Geographical Map” View, allowing to list all the connected NEs to the TOE in their geographical location.
Logic Map	This object allows access to the “Logical Map” View, allowing to list all the connected NEs to the TOE in their logical location.

Table 5. Objects in the TOE

Views are navigable windows that can be opened in the NetMaster Client GUI to perform management actions on the TOE or its operational environment. The Views to which a user has access are defined by the objects enabled to the group to which the user belongs.

The User Management, Group Management and Audit Log objects apply only to the Administrators and Security Officers group users (these objects cannot be disable for these groups or be assigned to other groups).

A NE connection template contains a list of attributes for defining communication between the NEs and NetMaster. This must be previously configured by the administrator from the NetMaster Client in order to establish communication between the TOE and the NEs.

6.1.2.2 FDP_ACF.1: SECURITY ATTRIBUTE BASED ACCESS CONTROL

FDP_ACF.1.1 The TSF shall enforce the ***[assignment: Access Control SFP]*** to objects based on the following: ***[assignment: Subjects: Users; Attributes: Group to which the users belong.***

Objects: listed in Table 5; Attributes: groups that are allowed to execute these objects].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[assignment: a user can execute an object when the group to which the user belongs has assigned such object, otherwise the object's execution is denied.].***

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***[assignment: none].***

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***[assignment: none].***

6.1.3 FIA: IDENTIFICATION AND AUTHENTICATION

6.1.3.1 FIA_AFL.1: AUTHENTICATION FAILURE HANDLING

FIA_AFL.1.1 The TSF shall detect when ***[selection: an administrator configurable positive integer within [assignment: 0 and 20]]*** unsuccessful authentication attempts occur related to ***[assignment: users, but not root user, trying to authenticate through the NetMaster Client].***

Application Note

The developer considers as 'administrator' who can define this value to the users in the Administrators/Security Officers groups, or users in groups with the “System Preferences” object enabled.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[selection: met]***, the TSF shall ***[assignment: prevent the offending user from successfully authenticating until a user of the Administrator or Security Officers groups request a password change].***

6.1.3.2 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.

6.1.3.3 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.

6.1.4 FMT: SECURITY MANAGEMENT

6.1.4.1 FMT_MSA.1: MANAGEMENT OF SECURITY ATTRIBUTES

FMT_MSA.1.1 The TSF shall enforce the ***[assignment: Access Control SFP]*** to restrict the ability to ***[selection: [assignment: list, add, modify or delete]]*** the security attributes ***[assignment: groups that are allowed to execute objects, and groups to which users belong]*** to ***[assignment: users belonging to the Administrators and Security Officers groups].***

6.1.4.2 FMT_MSA.3: STATIC ATTRIBUTE INITIALISATION

FMT_MSA.3.1 The TSF shall enforce the ***[assignment: Access Control SFP]*** to provide ***[selection: restrictive]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***[assignment: none]*** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 FMT_SMF.1: SPECIFICATION OF MANAGEMENT FUNCTIONS

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: ***[assignment: starting and stopping the NetMaster Server, reading and filtering logs, discovering and configuring Network Elements, configuring connection templates (creation, modification and deletion), connection templates assignment, defining a period of time for user's session termination by inactivity, configuring security preferences, performing backups and restoring NE's configurations, generating reports, and performing user and group administration].***

Application Note

"Performing backups" refers to performing backups of the NEs configuration through the NetMaster Server. This does not refer to performing database backups through the System Manager.

6.1.4.4 FMT_SMR.1: SECURITY ROLES

FMT_SMR.1.1 The TSF shall maintain the roles ***[assignment: Administrators, Security Officers, and user-defined groups].***

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

6.1.5 FTA: TOE ACCESS

6.1.5.1 FTA_SSL.3: TSF-INITIATED TERMINATION

FTA_SSL.3.1 The TSF shall terminate an interactive session after a ***[assignment: user-configurable period of time].***

Application Note

If this period of time value is not configured by the administrator, the default value is 60 minutes.

Any user in a group with the “System Preferences” object enabled can modify this value.

6.1.5.2 FTA_SSL.4: USER-INITIATED TERMINATION

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.1.6 FTP: TRUSTED PATH/CHANNELS

6.1.6.1 FTP_ITC.1/HTTPS: INTER-TSF TRUSTED CHANNEL

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

Application Note

By trusted IT product, it means NE. NEs are Network Elements such as radio devices, switches, and so forth, connected to the TOE.

FTP_ITC.1.2/HTTPS The TSF shall permit ***[selection: the TSF]*** to initiate communication via the trusted channel.

FTP_ITC.1.3/HTTPS The TSF shall initiate communication via the trusted channel for ***[assignment: managing network elements].***

Application Note

The TOE is connected to several network elements; these network elements can be configured through the TOE thanks to the Connection Templates. These connection templates are a kind of form kept by the TOE, where the connection type and the credentials to access the network element are detailed. The network elements can be configured to send certain types of SNMP traps, send performance reports, etc.

6.1.6.2 FTP_ITC.1/SNMP: INTER-TSF TRUSTED CHANNEL

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

Application Note

By trusted IT product, it means NE. NEs are Network Elements such as radio antennas, switches, and so forth, connected to the TOE.

FTP_ITC.1.2/SNMP The TSF shall permit ***[selection: the TSF]*** to initiate communication via the trusted channel.

FTP_ITC.1.3/SNMP The TSF shall initiate communication via the trusted channel for ***[assignment: requesting information to the NEs].***

6.2 SECURITY ASSURANCE REQUIREMENTS

The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements: **EAL2**

The following table shows the assurance requirements by reference the individual components in [CC31R5P3]

Assurance Class	Assurance Components
ASE: Security Target evaluation	ASE_CCL.1: Conformance claims ASE_ECD.1: Extended components definition ASE_INT.1: ST introduction ASE_TSS.1: TOE summary specification ASE_OBJ.2: Security objectives ASE_REQ.2: Derived security requirements ASE_SPD.1: Security problem definition
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
ADV: Development	ADV_TDS.1: Basic design ADV_ARC.1: Security architecture description ADV_FSP.2: Security-enforcing functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures
ATE: Tests	ATE_FUN.1: Functional testing ATE_COV.1: Evidence of coverage ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 6 Security Assurance Requirements

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 NECESSITY AND SUFFICIENCY ANALYSIS

SFR / TOE Security Objective	OT.MANAGEMENT	OT.AUDIT	OT.COMM
FAU_GEN.1		X	
FAU_GEN.2		X	
FAU_STG.1		X	
FIA_AFL.1	X		
FMT_SMF.1	X		
FMT_SMR.1	X		
FTA_SSL.3	X		
FTA_SSL.4	X		
FTP_ITC.1/HTTPS			X
FDP_ACC.1	X		
FDP_ACF.1	X		
FMT_MSA.1	X		

SFR / TOE Security Objective	OT.MANAGEMENT	OT.AUDIT	OT.COMM
FMT_MSA.3	X		
FTP_ITC.1/SNMP			X
FIA_UAU.2	X		
FIA_UID.2	X		
FAU_SAR.1		X	

Table 7 SFRs / TOE Security Objectives coverage

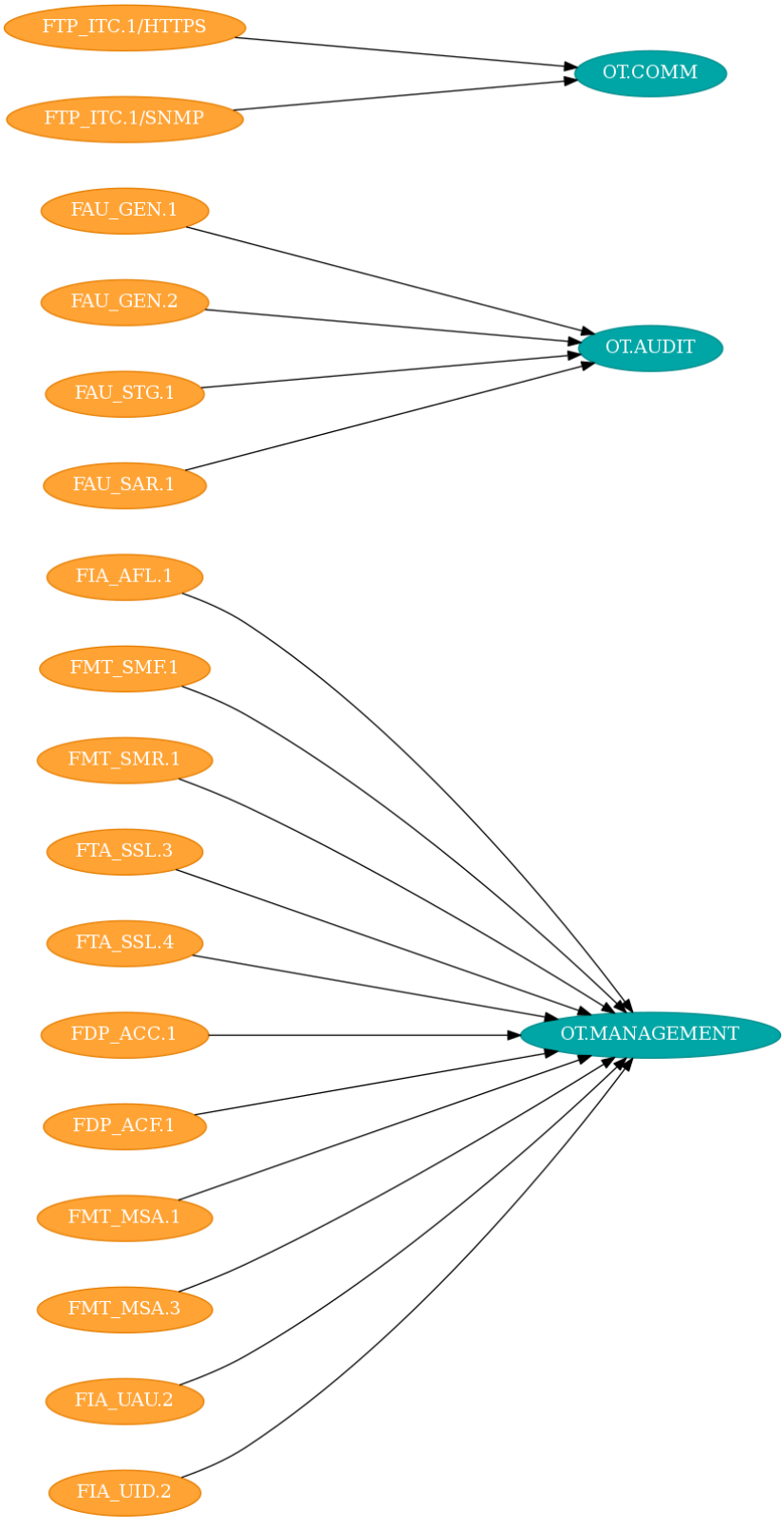

Figure 3 *Mapping of SFRs to TOE Security Objectives*

6.3.2 SECURITY REQUIREMENT SUFFICIENCY

OT.MANAGEMENT:

Several management functions can be executed in the TOE which are related to Objects, to model what management functions can be executed, **FMT_SMF.1** is included. Objects can be executed by users, which are limited to the objects enabled for the group to which the users belong. To model the latter, **FDP_ACF.1** and **FDP_ACC.1** are included.

Only certain groups (defined in the TOE by default) can execute certain objects. To define the functionality in this Security Target, the following SFRs are included: **FDP_ACF.1**, **FMT_MSA.1**, and **FMT_MSA.3**. Moreover, since the Administrators, Security Officers and other user-defined groups are maintained in the TOE, **FMT_SMR.1** is included to define it.

The TOE enforces identification and authentication to all users before allowing to perform any other action, **FIA_UID.2** and **FIA_UAU.2** are included to define that.

Finally, the TOE not only allows users to close their own sessions, but after a pre-defined time of inactivity, the TOE itself closes these sessions. **FTA_SSL.4** and **FTA_SSL.3** are included in the Security Target to define this functionality.

OT.AUDIT:

The TOE generates audit data in the start-up and shutdown of the audit functions, as well as on management operations, for this reason, **FAU_GEN.1** is included. The TOE relates all the audit data events to the user who produces them (if applicable), with the implication that **FAU_GEN.2** is necessary. Moreover, the TOE only allows users in the Administrator and Security Officer groups to access the logs (**FAU_SAR.1** is included by this reason) and does not allow users to delete or modify the log data; **FAU_STG.1** is defined to model this functionality.

OT.COMM:

The communication channel used for NE administration are protected by the use of a secure HTTPS channel, avoiding attackers to capture sensitive data or perform unauthorized modifications. To describe this functionality **FTP_ITC.1/HTTPS** is included.

On the other hand, the communication channel whereby the NEs send SNMP messages to the TOE is protected by the use of SNMPv3, avoiding in the same way attackers to capture sensitive data or perform unauthorized modifications. To describe this functionality, **FTP_ITC.1/SNMP** is included.

6.3.3 SFR DEPENDENCY RATIONALE

6.3.3.1 TABLE OF SFR DEPENDENCIES

The following table lists the dependencies for each requirement, indicating how they have been satisfied. The abbreviation "h.a." indicates that the dependency has been satisfied by a SFR that is hierarchically above the required dependency.

SFR	Required	Fulfilled	Missing
FAU_GEN.1	FPT_STM.1	None	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2 (h.a. FIA_UID.1)	None
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 (h.a. FIA_UAU.1)	None
FMT_SMF.1	None	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2 (h.a. FIA_UID.1)	None
FTA_SSL.3	None	None	None
FTA_SSL.4	None	None	None
FTP_ITC.1/HTTPS	None	None	None
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	None
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3	None
FMT_MSA.1	FMT_SMR.1, FMT_SMF.1, [FDP_ACC.1 or FDP_IFC.1]	FMT_SMR.1, FMT_SMF.1, FDP_ACC.1	None
FMT_MSA.3	FMT_MSA.1,	FMT_MSA.1,	None

SFR	Required	Fulfilled	Missing
	FMT_SMR.1	FMT_SMR.1	
FTP_ITC.1/SNMP	None	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2 (h.a. FIA_UID.1)	None
FIA_UID.2	None	None	None
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	None

Table 8 SFR Dependencies

6.3.3.2 JUSTIFICATION FOR MISSING DEPENDENCIES

FAU_GEN.1 dependency on FPT_STM.1

This dependency is covered by the assumption A.TIMECONFIG. The operational environment provides a reliable source of time to the TOE, which can produce Audit logs with reliable timestamps. Therefore, FPT_STM.1 is not needed.

6.3.4 SAR RATIONALE

The SARs were chosen according to the market expected evaluation assurance level for the TOE type.

6.3.5 SAR DEPENDENCY RATIONALE

6.3.5.1 TABLE OF SAR DEPENDENCIES

SAR	Required	Fulfilled	Missing
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.2 (hierarchically above ASE_REQ.1)	None
ASE_ECD.1	None	None	None
ASE_INT.1	None	None	None
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	None
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1	None

SAR	Required	Fulfilled	Missing
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.2 (hierarchically above ASE_REQ.1), ADV_FSP.2 (hierarchically above ADV_FSP.1)	None
ALC_CMC.2	ALC_CMS.1	ALC_CMS.2 (hierarchically above ALC_CMS.1)	None
ALC_CMS.2	None	None	None
ADV_FSP.2	ADV_TDS.1	ADV_TDS.1	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.2 (hierarchically above ADV_FSP.1)	None
AGD_PRE.1	None	None	None
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	None
AVA_VAN.2	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	None
ADV_TDS.1	ADV_FSP.2	ADV_FSP.2	None
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	ADV_FSP.2 (hierarchically above ADV_FSP.1), ADV_TDS.1	None
ATE_FUN.1	ATE_COV.1	ATE_COV.1	None
ATE_COV.1	ADV_FSP.2, ATE_FUN.1	ADV_FSP.2, ATE_FUN.1	None
ASE_SPD.1	None	None	None
ALC_DEL.1	None	None	None

Table 9 SAR dependencies

7 TOE SUMMARY SPECIFICATION

7.1 SF. SECURITY AUDIT

FAU_GEN.1 is implemented in the TOE through several JAVA libraries and functions that allow various events to be captured, catalogued (type of event and outcome), and registered. Then, these events are displayed in the NetMaster Client GUI and can be consulted as logs.

Furthermore, these JAVA libraries and functions use certain modules to get from the underlying O.S. the date and time (which are securely provided by **A.TIMECONFIG)**.

Certain actions performed in the TOE are done by users. When this happens, the TOE functions register the username of the user who perform these actions in the logs **(FAU_GEN.2).**

Finally, **FAU_STG.1** prevents unauthorized modifications or deletion to the stored audit records in the audit trail by not allowing unauthorized users to access or delete the logs (**FDP_ACC.1)**. **FAU_SAR.1** does not allow users who do not belong to the authorized groups to access the logs in the same way.

7.2 SF. USER DATA PROTECTION

The TOE defines several objects that can be executed. These objects are allowed or not in the different groups defined in the TOE. The objects can be performed by users, who can execute one object or another depending on the group they belong.

The objects, and the subjects and operations on these objects that are defined in **FDP_ACC.1** and enforced by **FDP_ACF.1** are implemented by means of several functions. These functions extract from the user database the group to which the user identified and authenticated belongs, and therefore, the objects available to this user.

There are objects only allowed to groups that are predefined in the TOE, such as user management, group management, and log files. New groups can be created in the TOE, but their users cannot access the objects described for the previous groups. By default, any group created will not have any object enabled (being the authorized user who must enable objects to this groups), following the least privilege principle.

The groups created in the TOE by default are Administrators, Security Officers, Services Manager, Services Viewer, and SNMP Agent.

7.3 SF. IDENTIFICATION AND AUTHENTICATION

Identification and authentication are required for accessing management and monitoring functions in the TOE. This identification/authentication is performed through the NetMaster client —graphical interface or command-line interface— for connecting to the NetMaster Server.

The TOE implements the functionality of registering every time a user fails to authenticate. Each consecutive unsuccessful attempt is recorded in a counter, which will trigger a function that will lock the user if he has reached a defined number of consecutive failed attempts. A user from the Administrators group can define the variable that will match the counter and trigger the locking function; this variable only allows values between 0 and 20. Only the users within the Administrators, Security Officers, or groups with the object "System Preferences" enabled can define this value. This is defined by **FIA_AFL.1**.

The TOE does not provide with the NetMaster Client GUI or CLI interface until the user is successfully authenticated; defined by **FIA_UAU.2**.

Once authenticated, each object requested by the user it is accompanied by the user identifier who requested it (it consists of a user session); otherwise, the object execution request is denied. Therefore, **FIA_UID.2** is met this way.

7.4 SF. SECURITY MANAGEMENT

All the objects that an user can execute are predefined by the group they belong to. There are certain objects that only can be executed by the Administrators and Security Officers groups; these objects cannot be disable from these groups. Since it is not possible to enable these objects to other groups, if the two groups mentioned previously were eliminated, the TOE would not be functional. Therefore, the TOE does not allow these groups to be modified or deleted, thus complying with **FMT_SMR.1**. Additional groups that the TOE administrators would like to maintain are included in this SFR too.

Only users in the Administrators or Security Officers groups can manage the relation between users and groups and between groups and objects. This is enforced by **FDP_ACC.1** and **FDP_ACF.1**, ensuring that **FMT_MSA.1** is fulfilled.

Moreover, the TOE functions define variables that can only take values from a set of valid values specified in the TOE code, or values between two defined valid limits. In this way, the TOE ensures that only secure values are accepted for the security attributed listed with Access Control SFP, meeting **FMT_MSA.3**.

The TOE management functions are defined by the operations that can be executed on some objects by a subject. This is enforced by **FDP_ACC.1** and **FDP_ACF.1**, supporting in this way **FMT_SMF.1**.

Users in the Administrators group have all the permissions. Users in the Security Officers group only have permissions to user management, group management and accessing the logs.

7.5 SF. TOE ACCESS

Users can perform management or monitoring functions in the TOE after being successfully authenticated through the NetMaster Client. Every time a user is successfully authenticated, a script is triggered that records in a counter how many minutes the user has been without performing any action. Each time the user performs an action, this counter returns to 0. If this counter reaches a defined number (variable defined by the authorized user, 60 by default), the TOE will terminate the user's session, meeting **FTA_SSL.3**.

On the other hand, users can terminate their session in the NetMaster Clients by logging out by pressing the X button of the NetMaster Client (located in the right-superior corner). Pressing the X button will terminate the user session, completing **FTA_SSL.4**.

7.6 SF. TRUSTED PATH/CHANNELS

The TOE can initiate a communication channel with the Network Elements for management and configuration purposes. This communication channel can be done through:

- HTTPS (TLS version 1.2). User authentication is done through user and password. For HTTPS, the TOE offers a total of 43 valid cipher suites such as TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.

This way, **FTP_ITC.1/HTTPS** is met.

On the other hand, the HTTPS channel allows limited administration of the NEs, only allowing to define the IP family to be used, configure the trap management and the NTP configuration in the NEs. This is achieved by modifying these parameters in the Connection Template associated to the NEs, since the TOE performs an HTTPS polling process with the NEs every 20 minutes, updating the configuration of the NEs.

Moreover, the Network Elements can communicate with the TOE (this communication is initiated by the TOE) for sending SNMP messages. Assured identification and confidentiality are achieved through SNMPv3, which requires identification/authentication and encrypts the communication; the TOE uses SNMPv3 authentication keys to identify the NEs. The authentication keys are generated from:

- The specified password.
- The IP of the Network Element.

This way, **FTP_ITC.1/SNMP** is met.

8 ACRONYMS

The following table shows the acronyms used in this document.

Acronym	Meaning
CC	Common Criteria
CPU	Central Processing Unit
DCN	Data Communication Network
EAL	Evaluation Assurance Level
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IT	Information Technology
JAVA RMI	Java Remote Method Invocation
KPI	Key Performance Indicator
LAN	Local Area Network
NE	Network Element
NMS	Network Management System
OSP	Organizational Security Policies
PM	Performance Monitoring
PP	Protection Profile
RAM	Random access memory
RMON	Remote Network Monitoring
SFP	Security Function Policy
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3
SQL	Structured Query Language
SSD	Solid State Drive
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

Acronym	Meaning
WAN	Wide Area Network

Table 10 *Abbreviations*

9 GLOSSARY OF TERMS

Term	Meaning
Augmentation	Addition of one or more requirement(s) to a package
Evaluation Assurance Level	Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
Operational Environment	Environment in which the TOE is operated
Protection Profile	Implementation-independent statement of security needs for a TOE type
Security Target	Implementation-dependent statement of security needs for a specific identified TOE
Target Of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance

Table 11 *Glossary of terms*

10 DOCUMENT REFERENCES

The following table shows the acronyms used in this document.

Reference	Document
[CC31R5P1]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 1: Introduction and general model
[CC31R5P2]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 2: Security functional components
[CC31R5P3]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 3: Security assurance components
[CEM31R5P3]	Common Criteria Evaluation methodology, Version 3.1, Revision 5
[PRE]	Ceragon NetMaster – AGD Preparative Procedures v0.6
[USER_GUIDE]	NetMaster User Guide R21B00 Rev A

Table 12 *List of document references*