>scop NET

v7

Common Criteria Evaluation
Security Target Lite

MAY CYBER TECHNOLOGY

Document Name	**:**	>scopNET V7 Security Target Lite
Document ID	**:**	>scopNET_V7_Security Target Lite_(v.1.1)
Dissemination Level	**:**	Public
Status	**:**	Final Version
Document Version	**:**	1.1
Version Date	**:**	11.03.2019
Author	**:**	Volkan NERGİZ

Revision History

Version No	Reason for Change	Release Date	Prepared By	Approved By
1.0	Initial Version	07.02.2019	Volkan NERGİZ	Berivan ARSLAN KAVGAOĞLU
1.1	Final Version	11.03.2019	Volkan NERGİZ	Berivan ARSLAN KAVGAOĞLU

TABLE OF CONTENTS

1. Introduction

Due to the increase in the importance of information contained in computer networks, corporations need to track their systems and computer infrastructure for unauthorized access. One of the major security problems common to organizations are unauthorized access attempts of computers, which are not compliant to the organization security policy.

Guest computers, mobile devices, computers using out of date antivirus software creates important security risks for enterprises. In order to minimize this risk, it is critical to only permit authorized devices for network access. >scopNET is the solution to protect network from unauthorized access.

This Security Target is for evaluation of >scopNET at Evaluation Assurance Level 3. This section presents Security Target Identification, TOE Overview and Description. It also includes Document Conventions and Document Terminology.

1.1. Security Target Reference

ST Title	:	>scopNET V7 Security Target Lite
Version	:	v.1.1

1.2. TOE Reference

Target of Evaluation	:	>scopNET
Version	:	V7
Vendor	:	MAY Cyber Technology, Inc.

1.3. TOE Overview

The Target of Evaluation (TOE) is the >scopNET V7 and will hereafter be referred to as the TOE through this document. The TOE is a network access control system that provides detection, authentication and authorization of devices attempting to access a network. These devices may be Guest Computers, Mobile Devices, PDA, Smart Phones or Tablets.

>scopNET controls the device compliance to the company policy and authenticates this device. Compliance policies are defined by the company and introduced to >scopNET during setup and configuration processes. For example; out of date antivirus update or activeness of the firewall, being a domain member can be defined as compliance policies.

>scopNET is 802.1X independent solution to prevent unauthorized computer access to corporate networks. >scopNET offers different methods for controlling network access of endpoint devices. The system is able to integrate with routers, switches and firewalls for device detection and access control.

The opportunity to use techniques like ARP Poisoning or TCP-Reset enables organizations to deploy a NAC solution without any dependency to network infrastructure. When a new machine accesses the network, an enumeration is performed. Windows WMI, Windows RPC, SNMP and SSH protocols are used for device enumeration. Windows, Linux and Mac Operating Systems are supported. The enumeration process enables organizations to manage their IT Inventory. Real time visibility on inventory information is provided.

The built-in captive portal offers a unique end-user experience for external devices. Through integration with Short Message Services, these devices can be audited, and a restricted network access is provided to the requester.

1.3.1. Usage and Main Security Features

The TOE is a software-only product and consists of the >scopNET software components: >scopNET GUI, >scopNET Server, >scopNET Detector, >scopNET Captive Portal GUI & Engine, >scopNET Agent.

>scopNET and its components have the following functions;

- ***>scopNET Detector***; detects the Target Device and redirect the target device to the >scopNET Captive Portal GUI & Engine.

- ***>scopNET Server***; gives Authorization to the Target Device. If there is an unauthorized device or incompliance to the policy, it sends necessary commands for performing the attack. >scopNET Server detects the MAC Address - IP Address of Target Device through network scanning.

- ***>scopNET Health Check***; checks and controls the >scopNET Component's status (>scopNET Server and >scopNET Detector), if one of them down, it is restarted. It also provides emergency status action to stop or start all system via >scopNET GUI.

- ***>scopNET Captive Portal GUI & Engine***; defines the authorization procedures referred for the authorization of the Target Device and provides access to the network with limitations.

- ***>scopNET GUI***; provides Management and Configuration functions of all the >scopNET System.

- ***>scopNET Agent***; performs inventory collection on computers.

Roles:

>scopNET GUI Roles

- **Root User:** Uses >scopNET GUI Module, defines new user, makes the configuration, has access for each and every menu and action in >scopNET GUI.

- **>scopNET Admin:** Has a read only access to each menu in >scopNET GUI. In addition is allowed to discard host, add network device and credential.

- **>scopNET Read Only User:** Has access to each menu (except settings and audit review) but is not allowed to execute any operation. Only monitors the system.

>scopNET Captive Portal GUI & Engine Roles:

- **Requester:** Target device that requests network access and accesses the network over Captive Portal GUI & Engine. The terms requester and target device may be used interchangeably throughout this document. There are three kinds of authorization type for a requester;
    - Guest: has only internet access and he/she cannot access any internal network resource.
    - Corporate Employee: has both internet and intranet access.
    - Company Employee: is a custom created authorization type and his/her access rights are allocated upon request.

>scopNET should contain 9 main Security Functions which are described in the following table. All of these security functions will be examined in detail on Chapter 6.

Security Functions	DESCRIPTION
Security Audit	The TOE generates audit records for security events. Only the Root User role is allowed to view the audit trail.
Cryptographic Support	The TOE supports cryptographic security functions for storing crucial information for user like User Password.
User Data Protection	The TOE provides specifying requirements for TOE security functions and TOE security function policies related to protecting user data.
Identification and Authentication	All users are required to perform identification and authentication before any information flows are permitted.
Security Management	The TOE provides a wide range of security management functions. Root User can configure the TOE, manage users and audit among other routine maintenance activities.

Protection of the TSF	TOE preserves a secure state in the event of certain types of failures.
Resource Utilisation	The availability of required resources provide protection against unavailability of capabilities caused by failure of the TOE.
TOE Access	An interactive user session is terminated after a period of user inactivity. The user is also allowed to terminate his/her own interactive session.
Trusted Path/Channels	The TOE uses trusted path/channels to provide confidence that a user is communicating directly with the TSF whenever it is invoked. A user's response via the trusted path guarantees that untrusted applications cannot intercept or modify the user's response.

1.3.2. TOE Type

The TOE belongs to the "Network and Network-Related Devices and Systems" category. TOE type is a software-based Network Access Control System.

1.3.3. Required non-TOE Hardware, Software or Firmware

The TOE is software product that runs on a host computer. The host computer must run the operating system platform on which the TOE can execute. >scopNET has 5 main modules; >scopNET GUI, >scopNET Server (includes >scopNET Health Check), >scopNET Detector, >scopNET Captive Portal GUI & Engine, >scopNET Agent.

The table below shows the system requirements which enable >scopNET components to run properly. Before >scopNET components are installed, it should be checked that the required software is found on the system.

>scopNET Component	.NET Framework	Debian	IIS	MSSQL	NMAP	Winpcap
>scopNET GUI	✓		✓	✓		
>scopNET Server	✓			✓	✓	
>scopNET Detector	✓					✓
>scopNET Captive Portal GUI & Engine		✓ (Optional)				
>scopNET Agent Web Service	✓		✓			
>scopNET Agent Client Setup	✓					

The minimum operating system (O/S) and hardware requirements for the >scopNET GUI host computer are:

O/S	Windows 7 or higher, preferably Windows Server 2012 64-bit, or higher
CPU	Intel Pentium Core 2 Duo 2.6 GHz, or faster
RAM	At least 4GB, preferably 8GB
Connectivity	TCP/IP network interfaces
Disk space for TOE and logs	At least 1 GB / Subject to Log details

The minimum operating system (O/S) and hardware requirements for the >scopNET Server host computer are:

O/S	Windows 7 or higher, preferably Windows Server 2012 64-bit, or higher
CPU	Intel Pentium Core 2 Duo 2.6 GHz, or faster
RAM	At least 4GB, preferably 8GB
Connectivity	TCP/IP network interfaces
Disk space for TOE and logs	At least 2 GB / Subject to Log details

The minimum operating system (O/S) and hardware requirements for the >scopNET Detector host computer are:

O/S	Windows 7 or higher, preferably Windows Server 2012 64-bit, or higher
CPU	Intel Pentium Core 2 Duo 2.6 GHz, or faster
RAM	At least 2GB, preferably 4GB
Connectivity	TCP/IP network interfaces
Disk space for TOE and logs	At least 1 GB / Subject to Log details

The minimum operating system (O/S) and hardware requirements for the >scopNET Captive Portal GUI & Engine host computer are:

O/S	Linux Distributions (Ubuntu, Redhat, Pardus, preferred Debian)
CPU	Intel Pentium Core 2 Duo 2.6 GHz, or faster
RAM	At least 1GB, preferably 2GB
Connectivity	TCP/IP network interfaces
Disk space for TOE and logs	At least 3 GB / Subject to Log details

1.3.4. Operating Environment

This section describes the general environment in which the TOE is expected to perform. The environment of operation for the TOE is expected to be a facility that is physically secure from unauthorized intrusion. Personnel with explicit physical access to the hardware storing log data and application execution files must be authorized, trained and competent. At a minimum, a monitor, keyboard and mouse must be locally collected to the server machine in which the TOE is deployed or operated on. In addition to this the operational environment must include:

For >scopNET GUI;

• A web browser (offered Internet Explorer 8.0 or higher, or Mozilla Firefox 20.0 or higher, Google Chrome 21.0 or higher) to be used by users of the TOE as a medium of communication with the TOE's web GUI.

•.NET Framework 4.5 and IIS 7.0 or higher

• The database MSSQL 2008 or higher

• Either Windows 2008 or Windows 2012

For >scopNET Server;

•.NET Framework 4.5

• The database MSSQL 2008 or higher

• Either Windows 2008 or Windows 2012

For >scopNET Detector;

•.NET Framework 4.5

• The database MSSQL 2008 or higher

• Either Windows 2008 or Windows 2012

For >scopNET Captive Portal GUI & Engine;

• A web browser (offered Internet Explorer 8.0 or higher, or Mozilla Firefox 20.0 or higher, Google Chrome 20.0 or higher) to be used by users of the TOE as a medium of communication with the TOE's web GUI.

• Minimum Java 1.7, PHP and Apache Web Server Package

• The database MSSQL 2008 or higher

• Linux distributions (Ubuntu, Pardus, and preferred Debian 7.0)

• Below software packages;

Snort – Intrusion Detection Prevention

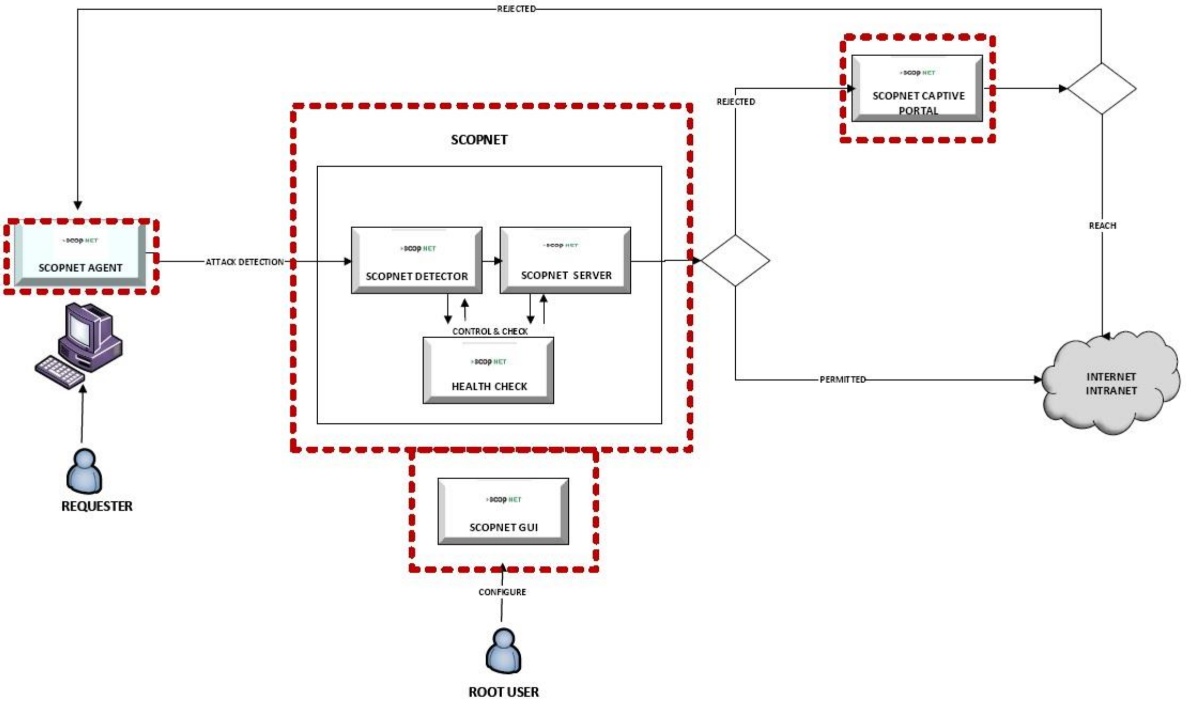
ULogD – Logs

Squid – Web Traffic Logs

1.4. TOE Description

This section provides the detailed information and description of TOE including physical and logical boundaries of the system. The TOE boundary is represented with the red dotted lines in the following figure.

The TOE Boundary



1.4.1. Physical Boundary

The TOE composed of multiple software modules that run as a complete IT product on required host computers. The host computers must run with an operating system platform on which the TOE executes (Please refer to the “Operating Environment).

>scopNET consists of the following components:

- **>scopNET GUI :** Graphical User Interface of >scopNET provides management and configuration functions of all >scopNET System. (Network and Attack Configurations, Logs, Reports)
- **>scopNET Server:** This component manages the system. It is responsible for managing network devices (VLAN & ACL Management), agentless enumeration and applying policies.
- **>scopNET Detector:** This component performs ARP sniffing & ARP Blocking.
- **>scopNET Captive Portal GUI & Engine:** This component is a portal for user registration of requesters. It can be a gateway in the guest VLAN or used by wireless controllers for authentication.
- **>scopNET Agent:** Performs inventory collection on computers. This component is installed to the target devices in case of customer’s request (customer decides whether to install Agent or not).

A brief description of required settings of TOE is provided in this section.

- Account with local administrative privileges in personal computers for enumeration is required.
- SNMP Credentials is required for enumeration.
- ARP trust in switches should be configured.
- SSH Credentials are required for enumerating Linux devices.
- Trunk port for >scopNET Detector is required if ARP blocking will be used.
- Router & Switch information is required if ACL or VLAN management to be used.
- SNMP RO permission on routers is required if ARP Table is to be tracked.
- SNMP RW permission on switches is required if VLAN management will be activated.
- SSH permission on Switches / Routers is required if ACL management will be activated.
- Server for scopNET Server Windows 2003/2008/2012 Supported with MS- SQL Server should be installed.
- Server for scopNET Detector Windows 2003/2008/2012 Supported with MS- SQL Server should be installed.
- Server for Captive Portal GUI & Engine is required.
- >scopNET Captive Portal GUI & Engine should be integrated with wireless controllers.
- Active directory credentials are required.

MAY Cyber R&D Manager checks the version of >scopNET product against the TOE version for compatibility before delivery. After this verification it is handled to MAY Cyber Service Team Product Responsible. Delivery and installation of the TOE is done by MAY Cyber Service Team Product Responsible and technical team. Right after the installation and customer's verification setup files and guidance documentation are delivered to the customer.

The physical boundary also includes the following guidance documentation:

- >scopNET Installation Guide
- >scopNET Administration Guide
- >scopNET Getting Started Guide

1.4.2. Logical Boundary

This section outlines the boundaries of the security functions of the TOE. The Logical Boundary of the TOE includes the security functionality described here.

1.4.2.1. Security Audit

The TOE provides for a comprehensive auditing layer, which will monitor activities and executions occurring with the system. Activities in this context are defined as operations occurring within the system that might or might not be initiated by a user. Each auditable event marks the exact time the event occurs, the account associated with that action as well as parametric details that are specific to that activity.

1.4.2.2. Cryptographic Support

In >scopNET System, authentication and identification is performed via a username password combination that will not only identify a specific user to the system but also define the level of access permitted to that particular user account. On top of it, SNMP and requester account passwords are encrypted by system automatically using AES_256 algorithm when saved into the database. Moreover timestamp value of audit logs in TOE is hashed using MD5 algorithm when saved into the database. Passwords of Root User, >scopNET Admin and >scopNET Read Only User are hashed with SHA-256 when saved into the database.

1.4.2.3. User Data Protection

In >scopNET system there are two SFPs for user data protection. One of them is Administrative Access Control SFP which is enforced by the TOE on >scopNET users (Root User, >scopNET Admin and >scopNET Read Only User) and all operations among these users and user interface items, policies, >scopNET authentication and authorization configurations are covered by this SFP based on user role, user ID and user permission.

>scopNET also enforces MAY Cyber Access Control SFP on requesters attempting to access network resources and information of the requesters like MAC Address, IP Address, Network Services and Resources, Protocol, Domain Information, Antivirus Information are controlled based on authorization type (corporate employee, guest, company employee) of the requester. If the requester has been authorized according to defined rules, then the TOE allocates the appropriate network resources otherwise denies network access.

1.4.2.4. Identification and Authentication

The TOE provides an identification and authentication layer independent from that of the Operating System it executes on. This security feature acts to protect and prevent access by unauthorized users to the system. In addition, it will also require each user to be identified and authorized before any access to security functions and data is granted. In the case of an authentication or identification failure, the TOE will disregard any request made an issue a forward redirection to the login page.

TOE provides multiple authentication and identification mechanisms. Authentication of LDAP users is performed via a username password combination that will not only identify a specific user to the system but also define the level of access permitted to that particular user account.

Authentication for the requester is done on >scopNET Captive Portal GUI & Engine and the user is authenticated in the TOE by username, password and captcha wants related information from requester (name, surname, e-mail address and department in addition to a username password combination). Also, a mechanism is provided by the TOE to verify the password strength.

1.4.2.5. Security Management

The TOE maintains three security roles by default; Root User, >scopNET Admin and >scopNET Read Only User for the management and monitoring of TOE. In addition to this there is “requester” role when >scopNET Captive Portal GUI & Engine is in question which is the target device that requests network access and accesses the network over Captive Portal GUI & Engine. There are three kinds of authorization type for a requester; Guest, Corporate Employee and Company Employee.

The TOE provides the Root User the ability to perform management functions like monitor system and service status, enable and disable External IT entities from communicating to the TOE, configure authorization rules, configure attack rules and access requests, deny access based on IP Address, enter record in White List/Black List.

1.4.2.6. Protection of the TSF

The TOE preserves its secure state if >scopNET Server or >scopNET Detector is down unexpectedly. >scopNET Health Check controls the status of >scopNET Detector and >scopNET Server, if one of them is down it is restarted. >scopNET Health Check also provides emergency status action to stop or start all system via >scopNET GUI.

1.4.2.7. Resource Utilisation

The availability of required resources provides protection against unavailability of capabilities caused by failure of the TOE. For this purpose, >scopNET Health Check which is a sub-system of >scopNET Server monitors system health and performs corrective actions when necessary. Network devices in critical state are tracked. Network devices are assigned critical state when they don’t respond to SNMP queries. >scopNET Health Check restarts >scopNET components (>scopNET Server or >scopNET Detector) which are down unexpectedly and by doing this it ensures the interchangeable operation of >scopNET Server and >scopNET Detector if one of them is not reachable. It also provides emergency stop/start actions. If more than one >scopNET Detectors are available, depending on the size of the organization, it allows them to operate in back-up.

1.4.2.8. TOE Access

After the logout or a specified time interval of user inactivity, TOE terminates interactive session. The session timeout value is by default 1 (one) hour and set by Root User.

1.4.2.9. Trusted Path/Channels

A trusted path provides a means for users to perform functions through an assured direct interaction with the TSF. It is usually desired for user actions such as initial identification and/or authentication, but may also be desired at other times during a user's session. In >scopNET System, credentials are protected between the >scopNET users and >scopNET GUI application server. SSL (Secure Socket Layer), cryptographic protocols designed to provide communications security over a computer network, is used for communication between >scopNET Users and >scopNET GUI. It provides “HTTPS” connection.

1.5. Document Conventions

The notation formatting and conventions used in this Security Target are consistent with those used in Version 3.1 Revision 5 of the Common Criteria. Selected section choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in part 2 of the Common Criteria are selection and assignment.

- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *[italicized text]*.
- The assignment operation is used to assign a specific value to an unspecified parameter to a component element. Assignments are denoted by [Blue-Colored Text]
- The iteration operation is used to denote using SFR's more than one. Iteration is denoted by SFR component title (letter). For example, FCS_COP.1(A)

1.6. Document Terminology

The table below defines the acronyms used in this Security Target document of >scopNET.

ABBREVIATION	MEANING
ACL	Access Control List
ARP	Address Resolution Protocol
CC	Common Criteria
DAU	Data Authentication
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
IT	Information Technology
MAC	Media Access Control
MOF	Management of Security
MSA	Management of Security Attribute
NAC	Network Access Control
OS	Operating System
OSP	Organization Security Policy
PP	Protection Profile
RPC	Remote Procedure Call
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMF	Specification of Management Functions
SNMP	Simple Network Management Protocol
SSDP	Simple Service Discover Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
USB	User Subject Binding
WMI	Windows Management Instrumentation

2. Conformance Claims

This section provides the identification for any CC, Protection Profile (PP) and EAL Package Conformance Claims.

2.1. CC Conformance Claim

The ST is Common Criteria Version 3.1 Revision 5 (April 2017) Part 2 conformant and Part 3 conformant.

2.2. PP Claim

The ST does not claim Conformance to any registered Protection Profile.

2.3. Package Claim

The TOE claims conformance to the EAL 3 assurance Package defined in Part 3 of the Common Criteria Version 3.1 Revision 5 (April 2017). The TOE does not claim conformance to any Functional Package.

2.4. Conformance Rationale

This Security Target conforms to Parts 2 and 3 of the Common Criteria Standard for Information Technology

Security Evaluations, Version 3.1, Revision 5, April 2017.

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

There are no Protection Profile claims for this Security Target.

3. Security Problem Definition

Assets:

- Configuration and device data stored in the Database1. These data are directly stored to the database.
- Audit data
- User information data such as role, ticket data related to GUI.
- Resources on the internal network

Threat Agents:

- Attacker from the internal network: A company user that is a domain member and has authorization but, try to attack without permission.
- Attacker from the outside network: An evil user that is not a domain member but tries to be authorized.

3.1. Threats

- ✓ **T.ACCOUNT AUDIT-T.ACC_AUD:** An attacker from the internal network could try to modify the Configuration and device data store in the Database1, audit data and user information data stored in Database4 and Database2. If the audits are not controlled regularly or the audit control could be bypassed, this action may not be noticed. Thus, the attacker succeeds without being detected.

- ✓ **T.DENIAL OF SERVICE-T.DOS:** An attacker could execute commands, send data, or perform other operations that make resources on the internal network unavailable to system users.

- ✓ **T.FULL AUDIT-T.FUL_AUD:** An attacker from the internal network could take actions resulting in low importance audits so as to exhaust audit storage capacity. If the audit storage capacity is exhausted, future audits are lost since no further audit could be recorded.

- ✓ **T.INFLUX:** An attacker may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

- ✓ **T.LOSS AND MODIFY OF DATA-T.DATALOSS/MODIFY:** An attacker from the outside or internal network may attempt to remove, destroy or modify configuration, device and user information data stored in the Database1, Database2 and Database3.

- ✓ **T.MASQUERADE-T.MASQ:** An attacker may masquerade as another entity in order to gain access to data or TOE resources.

- ✓ **T.MEDIATE-T.MEDIAT:** An attacker from the outside network may send impermissible information through the TOE which results in the exploitation of resources on the internal network.

- ✓ **T.NO AUTHORIZATION-T.NOAUTH:** An attacker from internal network may attempt to bypass the security services of the TOE so as to access and use resources on the internal network. Attempts by user to gain unauthorized access to the TOE, thus limiting the Root User's ability to identify and take action against a possible security breach.

- ✓ **T.UNSECURE_CONFIGURATION-T.UNSECCONF:** An attacker from internal network may cause attack surface by using unsecure configurations.

3.2. Organizational Security Policy

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 is one OSP defined for this Security Target.

- ✓ **OSP.SECURE TRANSFER:** The policy is about operational environment which provides a secure channel so that credentials are protected between the >scopNET users (Root User and >scopNET Admin) and >scopNET GUI application server. SSL (Secure Socket Layer) which is a cryptographic protocol designed to provide communication's security over a computer network, is used for communication between >scopNET Users and >scopNET GUI. It provides "HTTPS" connection.

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.

- ✓ **A.ACCESS DATA-A.ACCDATA:** The TOE has access to all the IT System data it needs to perform its functions.

- ✓ **A.NO EVIL USER-A.NOEVIL:** Root User, who manages the TOE is a non-hostile user, configures and maintains the TOE and follows all guidance.

- ✓ **A.EDUCATED USER-A.EDUCUSER:** Root User and end users are educated so as to use the >scopNET system suitably and correctly. Root User will install and configure the TOE according to the management guide.

- ✓ **A.PHYSICAL ACCESS AND PROTECTION-A.PYHPROT:** The TOE resides in a physically controlled access facility that prevents unauthorized physical access. Therefore, the physical hardware and software in which the TOE is deployed will be protected from unauthorized physical modification.

- ✓ **A.SECURE ENVIRONMENT-A.SECENV:** The Operating Systems, Database, Application and Web Server, on which the TOE is running are, fixed against all security bugs and protected against all threats.

- ✓ **A.TRUSTED PERSON-A.TRUST:** Creation of architecture, coding and administrative functions are done by trusted persons. The designer, programmer (coder) and Root User are responsible for these operations respectively.

4. Security Objectives

4.1. Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

- ✓ **O.ACCOUNTABILITY-O.ACCOUN:** The TOE will provide user accountability for information flows through the TSF and TSF data.

- ✓ **O.ADMINISTRATION-O.ADMIN:** The TOE will include a set of functions that allow efficient management of TSF and TSF data, ensuring that TOE users with appropriate privileges exist.

- ✓ **O.AUDIT RECORD-O.AUDREC:** The TOE will provide a means to record a readable audit trail of security related events, and means to the search the audit trail based on relevant attributes.

- ✓ **O.IDENTIFY AND AUTHENTICATE-O.IDAUTH:** The TOE will uniquely identify and authenticate the claimed identity of all users before granting a user access to TOE functions. Besides, the TOE shall define the rules for user authentication that forces users to have strong password policy.

- ✓ **O.MEDIATE-O.MEDIAT:** The TOE will mediate the flow of information from users on an external network to resources on an internal network, and will ensure that residual information from a previous information flow is protected and not transmitted in any way.

- ✓ **O.DATA STORAGE-O.DATASTOR:** The TOE will provide user and audit data storage including user account passwords and audit timestamp value in a secure manner. When it will be out of memory, the audit data will be deleted or stored or transferred to a suitable data storage according to the Root User's decision.

- ✓ **O.RESOURCE ACCESS-O.RESACC:** The TOE will control access to resources based on the identity of users. The TSF must allow Root User to specify which resources may be accessed by which users.

- ✓ **O.SECURITY FUNCTIONS-O.SECFUN:** The TOE will provide functionality that enables Root User to use the TOE security functions and will ensure that only Root User is able to access such functionality.

4.2. Security Objectives for the Operational Environment

The security objectives for the Operational Environment are addressed below:

- ✓ **OE.ADMINISTRATOR AUTHENTICATION-OE.ADMAUT:** The TOE environment will be able to identify and authenticate Root User prior to allowing access to TOE administrative functions and data.
- ✓ **OE.ADMINISTRATOR TRAINING-OE.ADMTRA:** Root User will be trained to appropriately install, configure and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.
- ✓ **OE.COMMUNICATION-OE.COMM:** communication will be protected between the TOE and system outside the TOE boundary from disclosure.
- ✓ **OE.ENVIRONMENT SECURITY-OE.ENVSEC:** The company has responsibility for the TOE will ensure that those parts of TOE should be running in a secure and protected environment.
- ✓ **OE.GUIDANCE-OE.GUIDAN:** The TOE will be delivered, installed, administrated and operated in a manner that maintains security and correctness.
- ✓ **OE.TIMESTAMP-OE.TSP:** The IT environment provides reliable time stamps which show the accurate dates and times of audit logs
- ✓ **OE.TRUSTED PERSON-OE.PERTRST:** Root User, >scopNET Admin, coders, designers and also service personnel will be trusted persons and they will not generate any threat for the TOE.

4.3. Security Objectives Rationale

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

Assumption & Threats / Objectives	T.ACC_AUD	T.DOS	T.FUL_AUD	T.DATALOSS/MODIFY	T.INFLUX	T.MASQ	T.MEDIAT	T.NOAUTH	T.UNSECCONF	A.ACCDATA	A.NOEVIL	A.EDUCUSER	A.PYHPROT	A.SECENV	A.TRUST	OSP.SECURE TRANSFER
O.ACCOUN	✓					✓		✓								
O.ADMIN	✓							✓	✓							
O.AUDREC	✓					✓		✓								
O.DATASTOR		✓	✓		✓											
O.IDAUTH						✓		✓								
O.MEDIAT		✓			✓		✓									
O.RESACC		✓	✓	✓		✓	✓	✓	✓							
O.SECFUN				✓		✓		✓	✓							
OE.ADMTRA											✓	✓				
OE.ADMAUT				✓					✓			✓	✓			
OE.COMM													✓	✓		✓
OE.GUIDAN										✓		✓				
OE.ENVSEC													✓	✓		
OE.PERTRST											✓	✓			✓	
OE.TSP	✓									✓						

4.3.1. Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.ACC_AUD	This threat is completely countered by; • **O.ACCOUN** which ensures user accountability for information flows through the TOE and for Root User's use of security functions related to audit. • **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. • **O.AUDREC** which ensures the TOE provides a means to record a readable audit trail of security-related events, and a means to search the audit trail based on relevant attributes. • **OE.TSP** ensures that the IT environment provides reliable time stamps. Time stamp value shows the accurate dates and times of audit logs.
T.DOS	This threat is countered by; • **O.RESACC** which must control access to resources based on the identity of users. The TSF must allow Root User to specify which resources may be accessed by which users. • **O.MEDIAT** which ensures the TOE mediates the flow of all information from users on an external network to resources on an internal network. • **O.DATASTOR** which ensures the TOE will provide user and audit data storage including user account passwords and audit timestamp value in a secure manner. When it will be out of memory, the audit data will be deleted or stored or transferred to a suitable data storage according to the Root User's decision.
T.FUL_AUD	This threat is completely countered by; • **O.RESACC** which must control access to resources based on the identity of users. The TSF must allow Root User to specify which resources may be accessed by which users. • **O.DATASTOR** which ensures the TOE will provide user and audit data storage including user account passwords and audit timestamp value in a secure manner. When it will be out of memory, the audit data will be deleted or stored or transferred to a suitable data storage according to the Root User's decision.

T.DATALOSS/MODIFY	This threat is completely countered by; • **O.RESACC** which must control access to resources based on the identity of users. The TSF must allow Root User to specify which resources may be accessed by which users. • **OE.ADMAUT** which ensures the identification and authentication for Root User prior to allowing access to TOE administrative functions and data. • **O.SECFUN** which ensures the TOE provides functionality that enables Root User to use the TOE Security Functions and also ensures that only Root User is able to access such functionality.
T.INFLUX	This threat is countered by; • **O.MEDIAT** which mediates the flow of information from users on an external network to resources on an internal network, and will ensure that residual information from a previous information flow is protected and not transmitted in any way. • **O.DATASTOR** which ensures the TOE will provide user and audit data storage including user account passwords and audit timestamp value in a secure manner. When it will be out of memory, the audit data will be deleted or stored or transferred to a suitable data storage according to the Root User’s decision.
T.MASQ	This threat is completely countered by; • **O.IDAUTH** which ensures the unique identification and authenticates the claimed identity of all users before granting a user access to TOE functions. • **O.RESACC** which must control access to resources based on the identity of users. The TSF must allow Root User to specify which resources may be accessed by which users. • **O.ACCOUN** which ensures user accountability for information flows through the TOE and for Root User’s use of security functions related to audit. • **O.AUDREC** which ensures the TOE provides a means to record a readable audit trail of security-related events, and a means to search the audit trail based on relevant attributes. • **O.SECFUN** which ensures the TOE provides functionality that enables Root User to use the TOE Security Functions and also ensures that only Root User is able to access such functionality.

T.MEDIAT	This threat is completely countered by; • **O.MEDIAT** which ensures the TOE mediates the flow of all information from users on an external network to resources on an internal network. • **O.RESACC** which ensures the control of access to resources based on the identity of users and allows Root User to specify which resources may be accessed by which users.
T.NOAUTH	This threat is completely countered by; • **O.IDAUTH** which ensures the unique identification and authenticates the claimed identity of all users before granting a user access to TOE functions. • **O.RESACC** which must control access to resources based on the identity of users. The TSF must allow Root User to specify which resources may be accessed by which users. • **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. • **O.ACCOUN** which ensures user accountability for information flows through the TOE and for Root User's use of security functions related to audit. • **O.AUDREC** which ensures the TOE provides a means to record a readable audit trail of security-related events, and a means to search the audit trail based on relevant attributes. • **O.SECFUN** which ensures the TOE provides functionality that enables Root User to use the TOE Security Functions and also ensures that only Root User is able to access such functionality.
T.UNSECCONF	This threat is completely countered by; • **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. • **O.RESACC** which must control access to resources based on the identity of users. The TSF must allow Root User to specify which resources may be accessed by which users. • **OE.ADMAUT** which ensures the identification and authentication for Root User prior to allowing access to TOE administrative functions and data. • **O.SECFUN** which ensures the TOE provides functionality that enables Root User to use the TOE Security Functions and also ensures that only Root User is able to access such functionality.

4.3.2. Rationale for Assumptions of the TOE

ASSUMPTION	RATIONALE
A.ACCDATA	This assumption is completely countered by; • **OE.GUIDAN** provides The TOE to be delivered, installed, administrated and operated in a manner that maintains security and correctness. • **OE.TSP** ensures that the IT environment provides reliable time stamps. Time stamp value, which shows the accurate dates and times of audit logs.
A.NOEVIL	This assumption is completely countered by; • **OE.ADMTRA** which ensures the identification and authentication for Root User prior to allowing access to TOE administrative functions and data. • **OE.PERTRST** which provides Root User, >scopNET Admin, coder, designer and also service personnel to be trusted person and they will not generate any threat for the TOE.
A.EDUCUSER	This assumption is completely countered by; • **OE.ADMAUT** which ensures the identification and authentication for Root User prior to allowing access to TOE administrative functions and data • **OE.GUIDAN** provides The TOE to be delivered, installed, administrated and operated in a manner that maintains security and correctness. • **OE.PERTRST** which provides Root User, >scopNET Admin, coder, designer and also service personnel to be trusted person and they will not generate any threat for the TOE. • **OE.ADMTRA** which ensures the identification and authentication for Root User prior to allowing access to TOE administrative functions and data.
A.PYHPROT	This assumption is completely countered by; • **OE.ENVSEC** provides to ensure that those parts of TOE should be running in a secure and protected environment. • **OE.COMM** which protects the communication between the TOE and system outside the TOE boundary from disclosure. • **OE.ADMAUT** which ensures the identification and authentication for Root User prior to allowing access to TOE administrative functions and data

A.SECENV	This assumption is completely countered by; • **OE.ENVSEC** provides to ensure that those parts of TOE should be running in a secure and protected environment. • **OE.COMM** which protects the communication between the TOE and system outside the TOE boundary from disclosure.
A.TRUST	This assumption is completely countered by; • **OE.PERTRST** which provides Root User, >scopNET Admin, coder, designer and also service personnel to be trusted person and they will not generate any threat for the TOE.

4.3.3. Rationale for Organizational Security Policy of the TOE

OBJECTIVES	RATIONALE
OSP.SECURE TRANSFER	This organizational security policy is countered by; • **OE.COMM** which protects the communication between the TOE and system outside the TOE boundary from disclosure.

5. Extended Components Definition

No extended components are defined.

6. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE.

6.1. Security Functional Requirements

This section specifies the SFRs for the TOE and also organizes the SFRs by CC Class.

CLASS	CLASS FAMILY	DESCRIPTION
Security Audit	**FAU_GEN.1**	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support	**FCS_COP.1(A)**	Cryptographic operation – Password Protection
	FCS_COP.1(B)	Cryptographic operation – Hash Operation
	FCS_COP.1(C)	Cryptographic operation – User Password Hashing
User Data Protection	**FDP_IFC.2**	Complete information flow control
	FDP_ACC.2	Complete access control
	FDP_IFF.1	Simple Security Attributes
	FDP_ACF.1	Simple Security Attributes

Identification and Authentication	**FIA_UAU.2**	User Authentication before any action
	FIA_UAU.5	Multiple Authentication Mechanisms
	FIA_UID.2	User Identification before any action
	FIA_SOS.1	Verification of Secrets
Security Management	**FMT_MOF.1**	Management of Security Functions Behavior
	FMT_MSA.1(A)	Management of security attributes
	FMT_MSA.1(B)	Management of security attributes
	FMT_MSA.3(A)	Static attribute initialization
	FMT_MSA.3(B)	Static attribute initialization
	FMT_SMF.1	Specifications of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	**FPT_FLS.1**	Failure with preservation of secure state
Resource Utilisation	**FRU_FLT.1**	Degraded fault tolerance
TOE Access	**FTA_SSL.3**	TSF Initiated termination
	FTA_SSL.4	User Initiated termination
Trusted Path/Channels	**FTP_TRP.1**	Trusted path

6.1.1. Class Security Audit (FAU)

6.1.1.1. FAU_GEN.1 – Audit Data Generation

Description: Audit Data Generation defines the level of auditable events and specifies the list of data that shall be recorded in each record.

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable Time Stamp

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

a) Start-up and Shutdown of the audit Functions
b) All auditable events for the [*not specified*] level of audit; and
c) [User access: login/logout and user activity logs,
Database events: create, modify and delete operations of database logs, user rights, user authorization, user roles, tickets,
Exceptions: list of errors for helping developers to fix]

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

a) Date and time of 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 ST, [event message according to event type].

6.1.1.2. FAU_SAR.1 – Audit Review

Description: Audit review, provides the capability to read information from the audit records.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_SAR.1.1 The TSF shall provide [Root User] with the capability to read [all recorded audit information] from the audit records.

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

6.1.1.3. FAU_SAR.2 – Restricted Audit Review

Description: Restricted audit review, requires that there are no other users except those that have been identified in FAU_SAR.1 Audit review that can read the information.

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit Review

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

6.1.1.4. FAU_SAR.3 – Selectable Audit Review

Description: Selectable audit review, requires audit review tools to select the audit data to be reviewed based on criteria.

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [sorting and filtering] of audit data based on [active block network device ports, detector-based blocking, active events, captive portal logs, computer/user logs, engine logs, network devices, GUI logs, IP address, MAC address, Host Name, Name, Rule Name, Date & Time].

6.1.1.5. FAU_STG.1 – Protected Audit Trail Storage

Description: Protected audit trail requirements are placed on the audit trail. It will be protected from unauthorised deletion and/or modification.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

6.1.1.6. FAU_STG.4 – Prevention of Audit Data Loss

Description: Prevention of audit data loss, specifies actions in case the audit trail is full.

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [*ignore audit records*] and [informs Root user] if the audit trail is full.

Application note 1: The audit data will be deleted or transferred to an appropriate data storage according to Root User’s decision as explained in >scopNET Administration Guide.

6.1.2. Class Cryptographic Support (FCS)

6.1.2.1. FCS_COP.1(A) Cryptographic Operation –Password Protection

Description: Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(A) The TSF shall perform [SNMP and requester account password encryption/decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [256 bit] that meet the following: [FIPS 140-2 and Annex A, NIST FIPS 197].

6.1.2.2. FCS_COP.1(B) Cryptographic Operation – Hash Operation

Description: Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(B) The TSF shall perform [timestamp value of audit log hashing] in accordance with a specified cryptographic algorithm [MD5] and cryptographic key sizes [128 bit] that meet the following: [RFC 6151].

6.1.2.3. FCS_COP.1(C) Cryptographic Operation – User Password Hashing

Description: Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(C) The TSF shall perform [Root User, >scopNET Admin and >scopNET Read Only User account password hashing] in accordance with a specified cryptographic algorithm [SHA-256] and cryptographic key sizes [256 bit] that meet the following: [(FIPS) PUB 180-4].

6.1.3. Class User Data Protection (FDP)

6.1.3.1. FDP_ACC.2 Complete Access Control

Description: Complete access control, requires that each identified access control SFP cover all operations on subjects and objects covered by that SFP. It further requires that all objects and operations protected by the TSF are covered by at least one identified access control SFP.

Hierarchical to: FDP_ACC.1 Subset access control.

Dependencies: FDP_ACF.1 Security attribute-based access control

FDP_ACC.2.1 The TSF shall enforce the [Administrative Access Control SFP] on

[Subjects: Root User, >scopNET Admin and >scopNET Read Only Users attempting to establish and interactive session with the TOE,

Objects: user interface items, policies, >scopNET authentication and authorization configurations] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.1.3.2. FDP_ACF.1 Security Attribute Based Access Control

Description: Security attribute-based access control Security attribute-based access control allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorize or deny access to an object based upon security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset Access Control, FMT_MSA.3 Static Attribute Initialization

FDP_ACF.1.1 The TSF shall enforce the [Administrative access control SFP] to objects based on the following:
[Subjects: Root User, >scopNET Admin and >scopNET Read Only Users attempting to establish and interactive session with the TOE,
Subject attribute:

1.User Role,

2.User ID,

3.User Permission

Objects: user interface items, policies, >scopNET authentication and authorization configurations
Object attributes: none].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[1. If the subject request access to an object and subject has permission the object, then access is granted,

2. If none of the above rules apply, access is denied].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [IP Address].

6.1.3.3. FDP_IFC.2 – Complete Information Flow Control

Description: Complete information flow control, requires that each identified information flow control SFP cover all operations on subjects and information covered by that SFP. It further requires that all information flows and operations controlled by the TSF are covered by at least one identified information flow control SFP.

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies : FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [MAY Cyber Access Control SFP] on [Subjects: requesters attempting to access network resources, and information: MAC Address, IP Address, Network Services and Resources, Protocol, Enumerate Target Device Information(Domain Information, Process Information, Antivirus Information and other gathering information using this methods (WMI, Remote Registry, RPC, SNMP, NMAP, Active Directory))] and all operations that cause that information to flow to and from subjects covered by the SFP**.**

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.1.3.4. FDP_IFF.1 – Simple Security Attributes

Description: Simple security attributes, requires security attributes on information, and on subjects that cause that information to flow and on subjects that act as recipients of that information. It specifies the rules that must be enforced by the function and describes how security attributes are derived by the function.

Hierarchical to: No other components

Dependencies : FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [MAY Cyber Access Control SFP] based on the following types of subject and information security attributes: [Subjects: requesters attempting to access network resources

Information controlled: MAC Address, IP Address, Network Services and Resources, Protocol, Enumerate Target Device Information (Domain Information, Process Information, Antivirus Information and other gathering information using these methods (WMI, Remote Registry, RPC, SNMP, NMAP, Active Directory))

Security attributes: authorization type (corporate employee, guest, company employee)].

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

[a) if the requester has been authorized as “corporate employee” by the TOE according to defined firewall rules, allocate the appropriate network resources, both internet and intranet access.

b) if the requester has been authorized as “guest” by the TOE according to defined firewall rules, by default allocate only internet access,

c) if the requester has been authorized as “company employee” by the TOE according to defined firewall rules, allocate access rights upon request,

d) if the requester has not been authorized according to defined firewall rules, deny network access].

FDP_IFF.1.3 The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [if Root User enters the record in White List about requester, allocate the appropriate network resources].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [if Root User enters the record in Black List about the requester, deny network access].

6.1.4. Class Identification and Authentication (FIA)

6.1.4.1. FIA_UAU.2 – User Authentication Before any Action

Description: User authentication before any action, requires that users are authenticated before any other action will be allowed by the TSF.

Hierarchical to: FIA_UAU.1 Timing of authentication.

Dependencies: FIA_UID.1 Timing of identification.

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

6.1.4.2. FIA_UAU.5 – Multiple Authentication Mechanisms

Description: Multiple authentication mechanisms, requires that different authentication mechanisms be provided and used to authenticate user identities for specific events.

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

[a) Authentication for LDAP users

b) Authentication for Captive Portal User] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the

[a) LDAP users are authenticated in the TOE by username and password

b) Captive Portal user is authenticated in the TOE by username, password and captcha].

6.1.4.3. FIA_UID.2 – User Identification Before any Action

Description: User identification before any action, requires that users identify themselves before any other action will be allowed by the TSF.

Hierarchical to: FIA_UID.1 Timing of authentication.

Dependencies: No dependencies.

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.

6.1.4.4. FIA_SOS.1 - Verification of Secrets

Description: Verification of secrets, requires the TSF to verify that secrets meet defined quality metrics.

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[a) Should be at least 6 characters long,

b) Should contain at least 1 non-alphanumeric character]

6.1.5. Class Security Management (FMT)

6.1.5.1. FMT_MOF.1 – Management of Security Functions Behaviour

Description: Management of security functions behavior allows the authorized users (roles) to manage the behavior of functions in the TSF that use rules or have specified conditions that may be manageable.

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behavior of, disable and enable*] the functions [Authorization configuration, attack rule configuration] to [Root User].

Application note 1: Root User change the configuration about attack rules. For example, Root User decide that start attacks if the target devices (not in the domain, antivirus software not updated, running malicious process etc.)

6.1.5.2. FMT_MSA.1(A) – Management of Security Attribute

Description: Management of security attributes allows authorized users (roles) to manage the specified security attributes.

Hierarchical to: No other components.

Dependencies: **[**FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions.

FMT_MSA.1.1(A) The TSF shall enforce the [MAY Cyber Access Control SFP] to restrict the ability to *[query, modify, delete]* the security attributes [Subject IP address, Object MAC Address, Object IP Address, Network Services and Resources, Protocol, Enumerate Target Device Information, authorization type (corporate employee, guest, company employee)] to [Root User].

6.1.5.3. FMT_MSA.1(B) – Management of Security Attribute

Description: Management of security attributes allows authorized users (roles) to manage the specified security attributes.

Hierarchical to: No other components.

Dependencies: **[**FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions.

FMT_MSA.1.1(B) The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to *[query, modify, delete]* the security attributes [user role, user ID, Permissions] to [Root User].

6.1.5.4. FMT_MSA.3(A) – Static Attribute Initialization

Description: Static attribute initialization ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of Security Attributes, FMT_SMR.1 Security roles

FMT_MSA.3.1(A) The TSF shall enforce the [MAY Cyber Access Control SFP] to provide *[restrictive]* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(A) The TSF shall allow the [Root User] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.5. FMT_MSA.3(B) – Static Attribute Initialization

Description: Static attribute initialization ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of Security Attributes, FMT_SMR.1 Security roles

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 [Root User] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.6. FMT_SMF.1 – Specification of Management Functions

Description: Specification of Management Functions requires that the TSF provide specific management functions.

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [monitor system and service status, enable and disable External IT entities from communicating to the TOE, configure authorization rules, configure attack rules and access requests, deny access based on IP Address, enter record in White List/Black List].

6.1.5.7. FMT_SMR.1 – Security Roles

Description: Security roles specify the roles with respect to security that the TSF recognizes.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [Root User, >scopNET Admin, >scopNET Read Only User and requester].

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

6.1.6. Class Protection of the TSF (FPT)

6.1.6.1. FPT_FLS.1 - Failure with Preservation of Secure State

Description: TOE will always enforce its SFRs in the event of identified categories of failures in the TSF.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [If >scopNET Server or >scopNET Detector is down unexpectedly].

6.1.7. Class Resource Utilisation (FRU)

6.1.7.1. FRU_FLT.1 - Degraded Fault Tolerance

Description: TOE will maintain correct operation even in the event of failures.

Hierarchical to: No other components.

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1.1 The TSF shall ensure the operation of [interchangeability of >scopNET Server and >scopNET Detector] when the following failures occur: [if >scopNET Server or >scopNET Detector is not reachable].

6.1.8. Class TOE Access (FTA)

6.1.8.1. FTA_SSL.3 TSF Initiated Termination

Description: TSF-initiated termination, provides requirements for the TSF to terminate the session after a specified period of user inactivity.

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after [1 hour].

6.1.8.2. FTA_SSL.4 User Initiated Termination

Description: User-initiated termination, provides capabilities for the user to terminate the user's own interactive sessions.

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.1.9. Trusted Path/Channels (FTP)

6.1.9.1. FTP_TRP.1 – Trusted Path

Description: Trusted path, requires that a trusted path between the TSF and a user be provided for a set of events. The user and/or the TSF may have the ability to initiate the trusted path.

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification*].

FTP_TRP.1.2 The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*initial user authentication*].

6.2. Security Functional Requirements Dependencies

This section specifies the dependencies of SFRs for the TOE.

SFR	Dependency	Applied
FAU_GEN.1	FPT_STM.1	*FAU_GEN.1 Audit data generation requires that FPT_STM.1 Reliable Time Stamp is included as a component. However, the TOE is not capable of providing this Functionality. This functionality will be provided by a TOE Environment. Hence, FPT_STM.1 Reliable Time Stamp is not included.*
FAU_SAR.1	FAU_GEN.1	*FAU_GEN.1 Audit data generation is included.*
FAU_SAR.2	FAU_SAR.1	*FAU_SAR.1 Audit review is included.*
FAU_SAR.3	FAU_SAR.1	*FAU_SAR.1 Audit review is included.*
FAU_STG.1	FAU_GEN.1	*FAU_GEN.1 Audit data generation is included.*
FAU_STG.4	FAU_STG.1	*FAU_STG.1 Protected audit trail storage is included.*
FCS_COP.1(A)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	*FCS_CKM.1Cryptographic key generation is not included since cryptographic keys are kept embedded in code, key generation or key import is not required.* *FCS_CKM.4 Cryptographic key destruction is not included because passwords are being encapsulated by the hash algorithm thus, keys are not being destructed.*
FCS_COP.1(B)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	*FCS_CKM.1Cryptographic key generation is not included because hash algorithms don't require cryptographic keys.* *FCS_CKM.4 Cryptographic key destruction is not included because passwords are being encapsulated by the hash algorithm thus, keys are not being destructed.*

FCS_COP.1(C)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	*FCS_CKM.1Cryptographic key generation is not included because hash algorithms don’t require cryptographic keys.* *FCS_CKM.4 Cryptographic key destruction is not included because passwords are being encapsulated by the hash algorithm thus, keys are not being destructed.*
FDP_ACC.2	FDP_ACF.1	*FDP_ACF.1 Security attribute-based access control is included.*
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	*FDP_ACC.2 Complete Access Control which is hierarchical to FDP_ACC.1 Subset Access Control and FMT_MSA.3(B) Static Attribute Initialization are included.*
FDP_IFC.2	FDP_IFF.1	*FDP_IFF.1 Simple security attributes is included.*
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	*FDP_IFC.2 Complete Information Flow which is hierarchical to FDP_IFC.1 Subset information flow control and FMT_MSA.3(A) Static Attribute Initialization are included.*
FIA_UAU.2	FIA_UID.1	*FIA_UID.2 User identification before any action, which is hierarchical to FIA_UID.1 Timing of identification is included.*
FIA_UAU.5	No dependencies	**-**
FIA_UID.2	No dependencies	**-**
FIA_SOS.1	No dependencies	**-**
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	*FMT_SMR.1 Security roles and FMT_SMF.1 Specification of Management Functions are included.*

FMT_MSA.1(A)	[FDP_ACC.1] or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	*FDP_ACC.2 Complete access control which is hierarchical to FDP_ACC.1 Subset Access Control, FMT_SMR.1 Security roles and FMT_SMF.1 Specification of Management Functions are included.*
FMT_MSA.1(B)	[FDP_ACC.1] or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	*FDP_ACC.2 Complete access control which is hierarchical to FDP_ACC.1 Subset Access Control, FMT_SMR.1 Security roles and FMT_SMF.1 Specification of Management Functions are included.*
FMT_MSA.3(A)	FMT_MSA.1 FMT_SMR.1	*FMT_MSA.1 Management of Security Attributes and FMT_SMR.1 Security roles are included.*
FMT_MSA.3(B)	FMT_MSA.1 FMT_SMR.1	*FMT_MSA.1 Management of Security Attributes and FMT_SMR.1 Security roles are included.*
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1	*FIA_UID.2 User identification before any action which is hierarchical to FIA_UID.1 Timing of identification is included.*
FPT_FLS.1	No dependencies	-
FRU_FLT.1	FPT_FLS.1	*FPT_FLS.1 Failure with preservation of secure state is included.*
FTA_SSL.3	No dependencies	**-**
FTA_SSL.4	No dependencies	**-**
FTP_TRP.1	No dependencies	-

6.3. Security Assurance Requirements

EAL3 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation, and an architectural description of the design of the TOE, to understand the security behavior.

The assurance security Requirements for the Security Target are taken from Part 3 of the CC v.3.1 Revision 5 (April 2017). These assurance requirements compose an Evaluation Assurance Level 3 (EAL 3). The assurance components are summarized in the following table:

ASSURANCE CLASS	ASSURANCE COMPONENTS	DESCRIPTION
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural Design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorization Control
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended component definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specifications
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

6.4. Security Functional Requirements Rationale

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

Objective SFR	O.ACCOUN	O.ADMIN	O.AUDREC	O.DATASTOR	O.IDAUTH	O.MEDIAT	O.RESACC	O.SECFUN
FAU_GEN.1	✓		✓					
FAU_SAR.1	✓		✓					
FAU_SAR.2	✓		✓					
FAU_SAR.3			✓					
FAU_STG.1	✓		✓	✓			✓	
FAU_STG.4			✓	✓			✓	
FCS_COP.1(A)				✓				
FCS_COP.1(B)				✓				
FCS_COP.1(C)				✓				
FDP_IFC.2	✓	✓				✓	✓	
FDP_ACC.2	✓	✓				✓	✓	
FDP_IFF.1	✓	✓				✓	✓	
FDP_ACF.1	✓	✓				✓	✓	
FIA_UAU.2	✓				✓		✓	
FIA_UAU.5	✓				✓		✓	
FIA_UID.2	✓				✓		✓	
FIA_SOS.1					✓			
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	✓	✓					✓	✓
FPT_FLS.1						✓		
FRU_FLT.1						✓		
FTA_SSL.3								✓
FTA_SSL.4								✓
FTP_TRP.1	✓							

SFR	RATIONALE
FAU_GEN.1	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: **O.AUDREC** and **O.ACCOUN**.
FAU_SAR.1	This requirement provides the ability to review logs. This component traces back to and aids in meeting the following objectives: **O.AUDREC** and **O.ACCOUN**.
FAU_SAR.2	This requirement provides the restricted audit review, requires that there are no other users except those that have been identified in **FAU_SAR.1**. Audit review that can read the information and aids in meeting the following objectives: **O.ACCOUN** and **O.AUDREC**.
FAU_SAR.3	This requirement allows audit review tools to select the audit data to be reviewed based on criteria. This component traces back to and aids in meeting the following objective: **O.AUDREC**.
FAU_STG.1	This requirement is placed on the audit trail. It will be protected from unauthorised deletion and/or modification. Unauthorised modifications to the stored audit records in the audit trail are preventented. This component traces back to and aids in meeting the following objectives: **O.AUDREC**, **O.ACCOUN**, **O.DATASTOR** and **O.RESACC**.
FAU_STG.4	This requirement specifies actions in case the audit trail is full and prevents the audit data loss. Root User is informed and according to Root User's decision the audit data will be deleted or transferred to a suitable data storage if the audit trail is full. This component traces back to and aids in meeting the following objectives: **O.AUDREC**, **O.DATASTOR** and **O.RESACC**.
FCS_COP.1(A)	This component requires the encryption operation which can be based on an assigned standard. This cryptographic support item is used for SNMP and requester account password protection in >scopNET System. This component traces back to and aids in meeting the following objective **O.DATASTOR**.

FCS_COP.1(B)	This component requires the hash operation which can be based on an assigned standard. This cryptographic support item is used for timestamp value of audit log protection in >scopNET System. This component traces back to and aids in meeting the following objective **O.DATASTOR**.
FCS_COP.1(C)	This component requires the hash operation which can be based on an assigned standard. This cryptographic support item is used for Root User, >scopNET Admin and >scopNET Read Only User account password protection in >scopNET System. This component traces back to and aids in meeting the following objective **O.DATASTOR**.
FDP_IFC.2	This requirement defines the information flow control policies are enforced on all operations among subjects and objects by the MAY Cyber Access Control Policy. This component traces back to and aids in meeting the following objectives: **O.ADMIN**, **O.RESACC**, **O.ACCOUN** and **O.MEDIAT**.
FDP_ACC.2	This requirement defines subjects, objects and operations controlled by the Administrative Access Control Policy. This component traces back to and aids in meeting the following objectives: **O.ADMIN**, **O.RESACC**, **O.ACCOUN** and **O.MEDIAT**.
FDP_IFF.1	The requirement meets the objective by defining the subject attributes on information and on subjects that cause that information to flow and on subjects that act as recipients of that information and the rules under the MAY Cyber Access Control SFP. This component traces back to and aids in meeting the following objectives: **O.ADMIN**, **O.MEDIAT**, **O.ACCOUN** and **O.RESACC**.
FDP_ACF.1	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. This component traces back to and aids in meeting the following objectives: **O.RESACC**. This component also identifies control access to resources based on the subject attributes of users. The TSF must Root User to specify which resources may be accessed by which users. This component traces back to and aids in meeting the following objectives: **O.ADMIN**, **O.ACCOUN** and **O.MEDIAT**.
FIA_UAU.2	This component requires successful authentication of a role before having access to the TSF and such aids in meeting **O.IDAUTH**. This component also identifies controlled access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC** and **O.ACCOUN**.

FIA_UAU.5	This component requires that different authentication mechanisms to be provided and used to authenticate user identities for specific events. This component traces back to and aids in meeting the following objective: **O.IDAUTH**, **O.RESACC** and **O.ACCOUN**.
FIA_UID.2	This component requires successful identification of a role before having access to the TSF and such aids in meeting **O.IDAUTH** and **O.ACCOUN** This component also identifies controlled access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**.
FIA_SOS.1	This component requires the TSF to verify that secrets meet defined quality metrics. This component traces back to and aids in meeting the following objective: **O.IDAUTH**.
FMT_MOF.1	This component has been chosen to determine all TOE management, administration and security functions behaviour. This component traces back to and aids in meeting the following objectives: **O.SECFUN**, **O.RESACC**, **O.ADMIN** and **O.ACCOUN**.
FMT_MSA.1(A)	This component restricts the ability to modify, delete, or query object and subject security attributes for the MAY Cyber Access Control SFP to Root User. It also assists in effective management and such as aids in meeting **O.SECFUN**. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**, **O.ACCOUN** and **O.ADMIN**.
FMT_MSA.1(B)	This component restricts the ability to modify, delete, or query object and subject security attributes for the Administrative Access Control SFP to Root User. It also assists in effective management, and such as aids in meeting **O.SECFUN**. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**, **O.ACCOUN** and **O.ADMIN**.

FMT_MSA.3(A)	This component ensures that the TOE provides a default restrictive value for security attributes yet allows a Root User to override the default values. This component traces back to and aids in meeting the following objective: **O.SECFUN**. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**, **O.ADMIN** and **O.ACCOUN**.
FMT_MSA.3(B)	This component ensures that the TOE provides a default restrictive value for security attributes yet allows a Root User to override the default values. This component traces back to and aids in meeting the following objective: **O.SECFUN**. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**, **O.ADMIN** and **O.ACCOUN**.
FMT_SMF.1	This component has been chosen to consolidate all TOE management, administration and security functions. This component traces back to and aids in meeting the following objectives: **O.SECFUN**, **O.ADMIN** and **O.ACCOUN**.
FMT_SMR.1	This component ensures that roles are available to allow for varying levels of administration capabilities and restricts access to perform TSF relevant functionality depending on the role assigned to a user. This component traces back to and aids in meeting the following objectives: **O.SECFUN**. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**, **O.ADMIN** and **O.ACCOUN**.
FPT_FLS.1	This requirement outlines that the system remains in a secure state after a failure. >scopNET Health Check controls the status of >scopNET Detector and >scopNET Server, if one of them is down it is restarted. >scopNET Health Check also provides emergency status action to stop or start all system via >scopNET GUI. This component traces back to and aids in meeting the following objective: **O.MEDIAT**.

FRU_FLT.1	This component ensures the availability of capabilities even in case of a failure. This component also supports the requirement which outlines that the system remains in a secure state after a failure. This component traces back to and aids in meeting the following objective: **O.MEDIAT**.
FTA_SSL.3	This component ensures that TOE terminates interactive session after 1 hour. This component traces back to and aids in meeting the following objectives: **O.SECFUN**.
FTA_SSL.4	This component ensures that TOE provides capabilities for the user to terminate his/her own interactive sessions. This component traces back to and aids in meeting the following objectives: **O.SECFUN**.
FTP_TRP.1	This component is required for trusted path, which requires a trusted path between the TSF and a user be provided for a set of events. This component traces back to and aids in meeting the following objective: **O.ACCOUN**.

6.5. Security Assurance Requirements Rationale

The general level of assurance for the TOE consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market. Besides, TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL3 from part 3 of the Common Criteria. Therefore EAL 3 was chosen to provide a moderate level of assurance that is consistent with good commercial practices.

7. TOE Summary Specifications

This section presents the Security Functions implemented by the TOE.

7.1. TOE Security Functions

The Security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilisation
- TOE Access
- Trusted Path/Channels

7.1.1. Security Audit

The TOE generates a set of audit logs. All recorded audit information can be viewed by Root User with the ability to apply sorting and filtering of audit data based on active block network device ports, detector-based blocking, active events, captive portal logs, computer/user logs, engine logs, network devices, GUI logs, IP Address, MAC Address, Host Name, name, Rule Name, date and time. Recorded audit information is prevented and protected against unauthorized modifications, deletion or audit data loss. If the audit trail is full, the TSF ignores audit records and the Root User is informed and according to Root User’s decision the audit data will be deleted or transferred to a suitable data storage.

The TOE generates logs for the following list of events:

- Start-up and Shutdown of the audit Functions
- User access: login/logout and user activity logs
- Database events: create, modify and delete operations of database logs, user rights, user authorization, user roles, tickets
- Exceptions: list of errors for helping developers to fix

Generated logs should include Time Stamp value. Time Stamp value is hashed with MD5 algorithm and kept in a separate colon of the database table.

The Security Audit functions are designed to satisfy the following security functional requirements:

- **FAU_GEN.1** - Audit Data Generation
- **FAU_SAR.1** - Audit Review
- **FAU_SAR.2** - Restricted Audit Review
- **FAU_SAR.3** - Selectable Audit Review
- **FAU_STG.1** - Protected Audit Trail Storage
- **FAU_STG.4** - Prevention of Audit Data Loss

7.1.2. Cryptographic Support

In >scopNET System, SNMP and requester account passwords are encrypted by system automatically using AES_256 algorithm that meets the criteria defined in FIPS 140-2 and Annex A, NIST FIPS 197 when saved into the database. Moreover, timestamp value of audit logs in TOE is hashed using MD5 algorithm with 128-bit cryptographic key sizes that meets the criteria defined in RFC 6151 when saved into the database. Passwords of Root User, >scopNET Admin and >scopNET Read Only User are hashed using SHA-256 algorithm with 256-bit cryptographic key sizes that meets the criteria defined in (FIPS) PUB 180-4 when saved into the database.

The Cryptographic Support functions are designed to satisfy the following security functional requirement

- **FCS_COP.1(A)** – Cryptographic Operation – Password Protection
- **FCS_COP.1(B)** – Cryptographic Operation – Hash Operation.
- **FCS_COP.1(C)** – Cryptographic Operation – User Password Hashing

7.1.3. User Data Protection

User data protection defines how users of the TOE, and user related data for connecting to the network, are allowed to perform operations on objects and reach limited network.

For complete access control, TOE enforces Administrative Access Control SFP on Root User, >scopNET Admin and >scopNET Read Only User attempting to establish an interactive session with the TOE and user interface items, policies, >scopNET authentication and authorization configurations based on user role, user ID and user permission.

For complete information flow control, TOE enforces MAY Cyber Access Control SFP on requesters attempting to access network resources, and information based on authorization type (corporate employee, guest, company employee), using the methods like WMI, Remote Registry, RPC, SNMP, NMAP, Active Directory;

- MAC Address,
- IP Address,
- Network Services and Resources,
- Protocol,
- Enumerate target device information
  - Domain Information
  - Process Information
  - Antivirus Information

If the requester has been authorized as "corporate employee" by the TOE according to defined firewall rules, allocates the appropriate network resources, both internet and intranet access. If the requester has been authorized as "guest" by the TOE according to defined firewall rules, by default allocate only internet access. If the requester has been authorized as "company employee" by the TOE according to defined firewall rules, allocate access rights upon request. If the requester has not been authorized according to defined firewall rules, deny network access.

Additionally, Root User can allocate appropriate network resources with the requester by entering a record in White List. Root User can also deny network access of the requester by entering a record in Black List.

The User Data Protection functions are designed to satisfy the following security functional requirements:

- **FDP_ACC.2** – Complete Access Control
- **FDP_ACF.1** – Security Attribute Based Access Control
- **FDP_IFC.2** – Complete Information Flow Control
- **FDP_IFF.1** – Simple Security Attributes

7.1.4. Identification and Authentication

The TOE performs the identification and authentication of all users accessing the TOE. The TOE requires a valid password associated with a username before providing access to the TOE. The username is entered, then a password. If the password is valid, the user will be associated with a role and set of privileges based on the username. Also, TOE provides multiple authentication and identification mechanisms to authenticate user identities for specific events. LDAP can be used as an external database for user authentication. When a user attempts to log in to the >scopNET, the user name and password are checked against the user name and password that are stored in the LDAP server, that will not only identify a specific user to the system but also define the level of access permitted to that particular user account.

Authentication for the requester is done on >scopNET Captive Portal GUI & Engine, and the user is authenticated in the TOE by username, password and captcha. A mechanism is provided by the TOE to verify the rules for user authentication that forces users to have a strong password policy, which should be at least 6 characters long and should contain at least 1 non-alphanumeric character.

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

- **FIA_UAU.2** – User Authentication Before Any Action
- **FIA_UAU.5** – Multiple Authentication Mechanisms
- **FIA_UID.2** – User Identification Before Any Action
- **FIA_SOS.1** – Verification of Secrets

7.1.5. Security Management

The TOE maintains three security roles by default; Root User, >scopNET Admin and >scopNET Read Only User for the management and monitoring of TOE.

- Root User; uses >scopNET GUI Module, defines new user, makes the configuration, has access for each and every menu and action in >scopNET GUI.
- >scopNET Admin; has a read only access to each menu in >scopNET GUI. In addition is allowed to discard host, add network device and credential.
- >scopNET Read Only User; has access to each menu (except settings) but is not allowed to execute any operation. Only monitors the system.

In addition to this there is “requester” role when >scopNET Captive Portal GUI & Engine is in question which is the target device that requests network access and accesses the network over Captive Portal GUI & Engine. There are three kinds of authorization type for a requester;

- Guest: has only internet access and he/she cannot access any internal network resource.
- Corporate Employee: has both internet and intranet access.
- Company Employee: is a custom created authorization type and his/her access rights are allocated upon request.

The TOE is capable of performing the management functions such as monitor system and service status, enable and disable External IT entities from communicating to the TOE, configure authorization rules, configure attack rules and access requests, deny access based on IP Address, enter record in White List/Black List.

The TOE restricts the ability to configure authorization rules, attack rules to Root User. Root User change the configuration about attack rules. For example, Root User decide that start attacks if the target device is not in the domain, antivirus software is not updated, is running malicious process etc.

The TOE enforces the MAY Cyber Access Control SFP to restrict the ability to query, modify and delete the following security attributes to Root User;

- Subject and Object IP addresses,
- Object MAC address,
- Network Services and Resources,
- Protocol,
- Enumerate Target Device Information
- Authorization type (corporate employee, guest, company employee)

The TOE enforces Administrative Access Control SFP to restrict the ability to query, modify and delete the following security attributes to Root User;

- User Role
- User ID
- Permissions Assigned Objects
- Absence of Permissions Assigned to Objects

Both MAY Cyber Access Control SFP and Administrative Access Control SFP provides restrictive default values for security attributes that are used to enforce these SFPs.

Additionally, TOE allows the Root User to specify alternative initial values to override the default values when an object or information is created.

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

- **FMT_MOF.1** – Management of Security Functions Behaviour
- **FMT_MSA.1(A)** – Management of Security Attribute
- **FMT_MSA.1(B)** – Management of Security Attribute
- **FMT_MSA.3(A)** – Static Attribute Initialization
- **FMT_MSA.3(B)** – Static Attribute Initialization
- **FMT_SMF.1** – Specification of Management Functions
- **FMT_SMR.1** – Security Roles

7.1.6. Protection of the TSF

The TOE preserves its secure state if >scopNET Server or >scopNET Detector is down unexpectedly.

The Protection of the TSF function is designed to satisfy the following security functional requirement:

- **FPT_FLS.1** – Failure with Preservation of Secure State

7.1.7. Resource Utilisation

The TOE is able to continue its operation if either >scopNET Server or >scopNET Detector is not reachable. For this purpose, the TOE ensures the interchangeability of >scopNET Server and >scopNET Detector.

The Resource Utilisation function is designed to satisfy the following security functional requirement:

- **FRU_FLT.1** – Degraded Fault Tolerance

7.1.8. TOE Access

After the logout or a specified time interval of user inactivity, TOE terminates interactive session. The session timeout value is by default 1 (one) hour and set by Root User.

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

- **FTA_SSL.3** – TSF Initiated Termination
- **FTA_SSL.4** – User Initiated Termination

7.1.9. Trusted Path/Channels

TOE provides a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification. In >scopNET System, credentials are protected between the >scopNET users and >scopNET GUI application server. SSL (Secure Socket Layer), cryptographic protocols designed to provide communications security over a computer network, is used for communication between >scopNET Users and >scopNET GUI. It provides "HTTPS" connection.

The Trusted Path/Channels function is designed to satisfy the following security functional requirement:

- **FTP_TRP.1** – Trusted Path