Natek Network Access Control (NAC)

V 5.4.2

Security Target

Release Date: 28.08.2014

Version 1.13

AUTHOR:

NATEK BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK YAZILIM TİCARET SANAYİ ANONİM ŞİRKETİ

Revision History

Version No	Reason for Change	Release Date	Prepared By	Approved By
1.0	First Draft	19.08.2013	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.1	SFR's Update	29.08.2013	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.2	Initial Draft (Before Release)	02.10.2013	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.3	Initial Version (Kick-off Meeting)	13.11.2013	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.4	"Survey Report 1"Update (GR_1)	26.11.2013	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.5	"Survey Report 2"Update (GR_2)	06.12.2013	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.6	"Survey Report 3"Update (GR_3)	16.12.2013	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.7	"Survey Report 4"Update (GR_4)	18.12.2013	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.8	"Survey Report 4"Update (GR_9)	26.02.2014	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.9	"Survey Report 5"Update (GR_10 and GR_11)	06.05.2014	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.10	NAC Version Update v.5.4.0	21.05.2014	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.11	NAC Version Update v.5.4.2	21.08.2014	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.12	"Survey Report 25"Update (GR_25)	28.08.2014	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL
1.13	Final Version	28.08.2014	Ahmet Sedat KAYA & Ertuğrul BALABAN	Necati ERTUĞRUL

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Guest computers, mobile devices, computers using out of date antivirus software creates important security risks for enterprises.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. Natek Network Access Control (NAC) is the solution to protect network from unauthorized access.

This Security Target is for evaluation of Natek Network Access Control (NAC) 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:	NATEK Network Access Control (NAC) Security Target
Version:	1.13
Publication Date:	28.08.2014
ST Author:	Natek Bilişim Bilgisayar, Eğitim, Danışmanlık, Yazılım Ticaret Sanayi Anonim Şirketi.
Assurance Level:	The ST is EAL 3 conformant.

1.2. TOE Reference

TOE Identification:	Natek Network Access Control (NAC)
Version:	5.4.2
Publication Date:	28.08.2014
Vendor:	Natek Corporation
Assurance Level:	The TOE is EAL 3 conformant.

1.3. TOE Overview

The TOE Description summarizes the usage and major security features. It also provides a context for the TOE Evaluation by identifying the TOE type, describing the product and defining the specific evaluated configuration.

The Target of Evaluation (TOE) is the Natek Network Access Control (NAC) Version 5.4.2 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. Natek NAC controls the device compliance to the company policy and authenticates this device. Compliance policies are defined by the company and introduced to Natek NAC 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. The TOE is a software-only product and consists of the Network Access Control (NAC) software components: NAC GUI, NAC Server, NAC Detector and NAC HotSpot GUI.

1.3.1. TOE Type

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

1.3.2. 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. Natek NAC has 4 main modules; NAC GUI, NAC Server (includes NAC Health Check, NAC Scanner), NAC Detector and NAC HotSpot GUI.

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

O/S:	Windows 7 or higher, preferably Windows Server 2008 64-bit, or higher
CPU:	Intel Pentium Core 2 Duo 2.4 GHz, or faster
RAM:	At least 2GB, preferably 4GB
Connectivity:	TCP/IP network interfaces
Disk space for TOE:	At least 1 GB
Disk space for logs:	Subject to Log details

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

O/S:	Windows 7 or higher, preferably Windows Server 2008 64-bit, or higher
CPU:	Intel Pentium Core 2 Duo 2.4 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 NAC Detector host computer are:

O/S:	Windows 7 or higher, preferably Windows Server 2008 64-bit, or higher
CPU:	Intel Pentium Core 2 Duo 2.4 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 NAC HotSpot GUI host computer are:

O/S:	Linux Distributions (Ubuntu, Redhat, Paradus, preferred Debian)
CPU:	Intel Pentium Core 2 Duo 2,4 GHz, or faster
RAM:	At least 512 MB, preferably 1GB
Connectivity:	TCP/IP network interfaces
Disk space for TOE:	At least 2,5 GB
Disk space for logs:	Subject to Log details

1.3.3. 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. In addition to this:

For NAC GUI;

• The operational environment must include 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 authorized administrators of the TOE as a medium of communication with the TOE's web GUI.

• The operational environment must include .NET Framework 4.0 and IIS 7.0 or higher

• The operational environment must include the database MSSQL 2008 or higher

• The operational environment must include either Windows 2008 or Windows 2012

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.

For NAC Server;

• The operational environment must include. NET Framework 4.0

• The operational environment must include the database MSSQL 2008 or higher

• The operational environment must include either Windows 2008 or Windows 2012

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.

For NAC Detector;

• The operational environment must include. NET Framework 4.0

• The operational environment must include the database MSSQL 2008 or higher

• The operational environment must include either Windows 2008 or Windows 2012

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.

For NAC HotSpot;

• The operational environment must include 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 authorized administrators of the TOE as a medium of communication with the TOE's web GUI.

• The operational environment must include. minimum Java 1.7, PHP and Apache Web Server Package

• The operational environment must include the database MSSQL 2008 or higher

• The operational environment must include Linux distributions (Ubuntu, Pardus, and preferred Debian 7.0)

• The operational environment must include below software packages;

Snort – Intrusion Detection Prevention

ULogD – Logs

Squid – Web Traffic Logs

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.

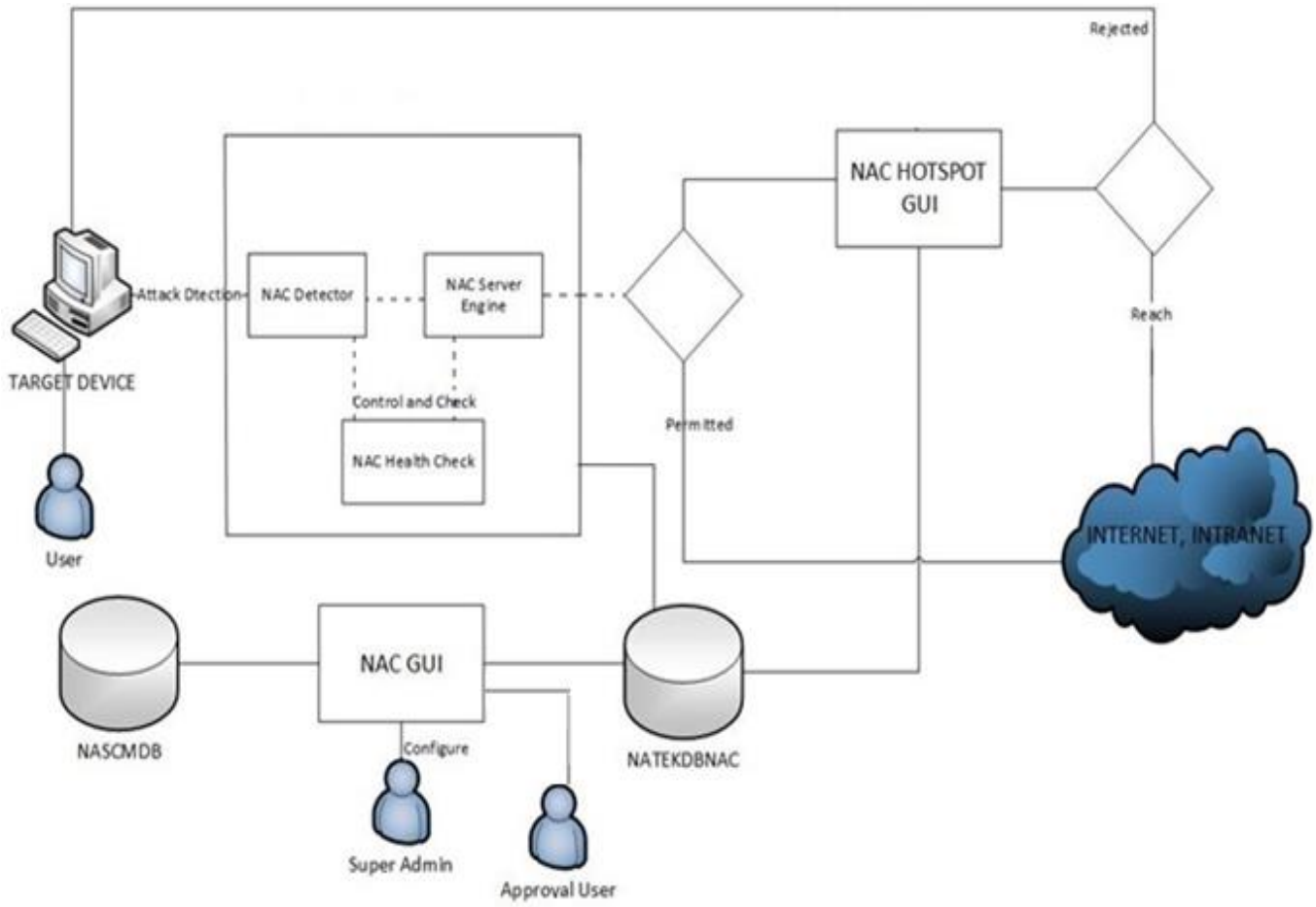
1.4. TOE Description

This section provides the detailed information and description of TOE included physical and Logical boundaries of the system.

Natek NAC operates based on two scenarios. First scenario controls network traffic by using ARP packets. In this scenario ARP Poisoning is applied to target devices so as to change the default gateway MAC Address of the Target Device. The second scenario controls network access of devices by changing switch settings for which the device is connected. The VLAN of the switch port can be changed or the port can be disabled. In addition, global ACL'S can also be applied to network devices to prevent the unauthorized access of target devices.

According to Scenarios below, Super Admin decides which scenario is suitable and applicable for the company according to company needs and infrastructure. After that, Super Admin applies the selected scenario on NAC GUI and make configuration.

Scenario 1

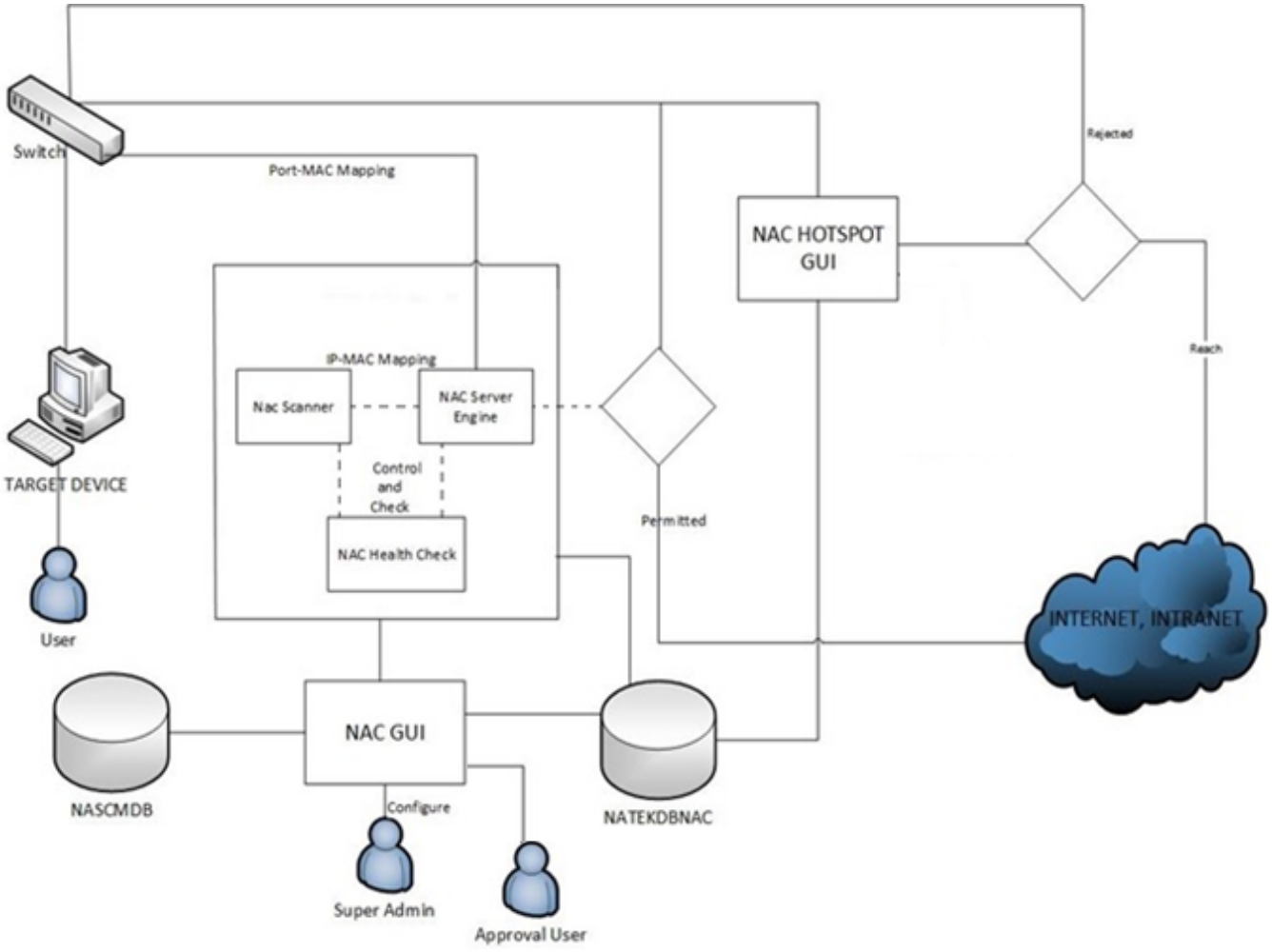


Natek NAC components (NAC GUI, NAC Server, NAC Detector, NAC HotSpot GUI) connect with each other using with Natekdbnac Database. The steps of operation are as follows:

1) Target Device enters the network.
2) ARP request is sent by Target Device to find neighbor devices.
3) NAC Detector intercepts ARP request, SSDP and DHCP packages.
4) NAC Detector records the device in the central MSSQL Database for classification.
5) The NAC Server identifies and classifies the device with the following methods:
    a. WMI; Inventory information is collected. Any WMI data can be collected, get hard disk space, username informations.
    b. Remote Registry; Inventory information is collected. Any key value can be enumerated.
    c. RPC; Calling the Procedure on Target Device, computer name is collected for classification.
    d. SNMP; Get inventory information from Device, MIB-2 Inventory Information is collected.
    e. NMAP; Mac Vendor, OS Guessing and Open Port Information is collected.
    f. Active Directory; Computer name is collected for classification.
    g. In case of company request (company decide whether to install Agent or not), Natek Agent Component installs to the target devices. Inventory information is collected. Any WMI data and registry key data can also be collected.
6) If classification is successful i.e. , NAC Server gets any information from Target Device using above methods, inventory is collected for the device. If device is compliant to the policy, target device reaches a limited network. Limitation is done according to device properties and company compliance policy (inventory policy).
7) Otherwise, if the classification fails or incompliance to inventory policy is detected, NAC Server sets the attack status of related record of target device to ON (1).
8) NAC Detector makes attack to devices whose attack status is ON (1) with ARP Poisoning. ARP Poisoning is used to change the default gateway MAC Address of the attacked device (Block the network access of the device). The attacked device is redirected to NATEK Hotspot GUI. The ARP Poisoning packet contains an ARP Reply packet with the IP address of the default gateway and MAC address of NAC Hotspot.

9) NAC Detector prevents Target Device to reach network. It also redirects the device to the NAC HotSpot Components.
10) NAC HotSpot GUI (Graphical User Interface) authorizes the Target Device via a Captive Portal. (Sample authorization types are; Guests, Corporate Employee)
11) NAC HotSpot GUI also provides a warning message for the reason of incompliance. It also provides all related records and registration process.
12) All registration records are validated with one of the approval with SMS, approval via mail, manager permission, and super admin approval methods.
13) Target Device reaches the network with restrictions after validation is performed on NAC HotSpot GUI.

Scenario 2



Natek NAC components (NAC GUI, NAC Server, NAC Detector, NAC HotSpot GUI) connect with each other using with Natekdbnac Database.

In this method the configuration on corporate network devices is changed to prevent unauthorized access:

1) Target Device enters the network.
2) NAC Server Engine connects to the corporate network switches using Telnet, SSH or SNMP.
3) NAC Server Engine retrieves the MAC (Media Access Control) address table and port information of corporate network switches. This information is stored centrally to detect which device is connected to which port of network switch.
4) NAC Server detects the MAC Address - IP Address of Target Device from DHCP logs or through network scanning. NAC Scanner component performs network scanning.
5) The NAC Server identifies and classifies the device with the methods mentioned above; (WMI, Remote Registry, RPC, SNMP, NMAP, Active Directory, NATEK Agent)
6) If classification is successful i.e., NAC Server gets the related information from using above methods, inventory is collected for the device. If device is compliant to the policy, target device reaches the limited network.
7) Otherwise, if the classification fails or incompliance to inventory policy is detected NAC Server sets the attack status of related record of target device to ON (1).
8) NAC Server makes Switch Attack to Target Device using following methods according to Switch properties;

   Port Shut (Shut the Switch Port), VLAN Change (Change the VLAN Address to another VLAN) or Adding ACL (Add records to the Access Control List).

   IF VLAN of Port Is Changed
9) NAC Server redirect the Target Device's VLAN to a VLAN which NAC Host Spot GUI is the default gateway.
10) NAC HotSpot GUI authorizes the Target Device via Captive Portal. (Sample authorization types are; Guests, Corporate Employee, Company Employee)
11) NAC HotSpot GUI also provides a warning message for the reason of incompliance. It also provides all related records and registration process.
12) All registration records are validated with different procedures. (Approval with SMS, approval via mail, Manager Permission ...etc.)

13) Target Device reaches the network with restrictions after validation is performed on NAC HotSpot GUI.

In other cases the target device cannot access corporate network.

According to scenarios above, as a summary with the concept of the TOE, NAC and its components have the following functions;

- NAC Detector; detects the Target Device and uses ARP Poisoning to redirect the target device to the NAC HotSpot GUI.
- NAC Server Engine; 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.
- NAC Server detects the MAC Address - IP Address of Target Device from DHCP (Dynamic Host Configuration Protocol) logs or through network scanning.
- NAC Health Check; checks and controls the NAC Component's status (NAC Server Engine, NAC Detector and NAC Scanner), if one of them down, it is restarted. It also provides emergency status action to stop or start all system via NAC GUI.
- NAC HotSpot GUI defines the authorization procedures referred for the authorization of the Target Device and also provides access to the network with limitations.
- NAC GUI Component; provides Management and Configuration functions of the all NAC System. (Network and Attack Configurations, Logs, Reports)
- NASCMDB and Natekdbnac Databases;
    - NASCMDB stores user's information for controlling access to GUI.
    - Natekdbnac stores target device information, logs, reports and configuration information about NAC System. Other NAC Components also use Natekdbnac and all add, delete and update operations are stored in it.

1.4.1. Physical Boundary

The TOE composed of multiple software modules that run as complete IT products 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). For a graphical representation of the scope and the points of interaction between the various components of the TOE also refer to the Scenario 1 and Scenario 2 Figures.

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.

Security Functions	DESCRIPTION
Security Audit	The TOE generates audit records for security events. Only the admin role is allowed to view the audit trail.
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. Administrator can configure the TOE, manage users and audit among other routine Maintenance activities.

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. The data can be viewed only by administrators.

1.4.2.2. User Data Protection

The information below which are identified in TOE scope, is protected against access by unauthorized users. This information is used by Natek NAC components.

- User Information (Super Admin or other user)
- Authorization and Authentication Information (Roles, Menu, Ticket etc...)
- Configuration and Configuration Items Information (Network and Credentials etc…)
- System Logs (GUI, functions and database etc…)
- Device and Inventory Information (Scanned Device, OS, Installed Applications etc…)
- Network resources

1.4.2.3. 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.

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, the password will be encapsulated by system automatically using SHA-1 when saved into the database (NASCMDB).

Authorization for the User (Target Device User) is done on NAC Hot Spot GUI. NAC Hot Spot GUI wants related information from user (name, surname, phone number, mail address and department). According to user information, NAC Hot Spot GUI redirects these information to the Approval User. Approval User evaluates the requests and decides on the access of the limited network. According to corporation configuration, request type can be sent differently (via mail or sms and decision of the Super Admin).

NAC GUI is SSL support provided by the operational environment for secure authentication. SSL is a network protocol primarily used to secure the transmission of data between 2 remote locations; essentially providing protection for intercept when data packets are flowing “on the wire”.

1.4.2.4. Security Management

TOE provides Security Management functions like configuration of TOE; manage the users, audit, maintenance activities etc… In the Security Management activities of the TOE uses the list below;

- Users and passwords
- Roles, Tickets, Menus
- Authentication and Authorization Mechanism
- Audit Logs

The TOE allows for the management of sessions (NAC GUI) connection. Authorized administrators are granted the ability to set the idle timeout threshold after which an authorized user would be automatically logged out of his active session. Idle timeout is defined as a period of inactivity from the user on database (Default value is an hour).

1.5. Document Conventions

The notation formatting and conventions used in this Security Target are consistent with those used in Version 3.1 Revision 4 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, FDP_ACC.1(A)

1.6. Document Terminology

The table below defines the acronyms used in this Security Target document of Natek NAC.

ABBREVIATION	MEANING
ACL	Access Control List
ARP	Address Resolution Protocol
CC	Common Criteria
DAU	Data Authentication
DHCP	Dynamic Host Configuration Protocol
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 (September 2012) 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 4 (September 2012). 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 4, September 2012.

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

Roles:

NAC GUI Roles

- Super Admin: Uses NAC GUI Module, defines new user, makes the configuration
- Approval User: Monitors the system monitor. In addition approve or reject the requests or view limited screens. (NAC Base User)

HOT Spot GUI Roles:

- User: request network access and accesses the network over HOT Spot GUI

Assets:

- Configuration and device data store in the Natekdbnac. These data are directly stored to the database.
- Audit data
- User information data such as role, ticket data related to GUI. This data is stored in the NASCMDB.
- 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 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 Natekdbnac, Audit data and User information data. 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.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.LOSS OF DATA-T.DATALOSS:** An attacker from the outside network may attempt to remove or destroy Configuration and device data store in the Natekdbnac.

- ✓ **T.MEDIATE-T.MEDIAT:** An attacker from the outside network person 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.

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 are no OSPs defined for this Security Target.

3.3. Assumptions

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

- ✓ **A.NO EVIL USER-A.NOEVIL:** Authorized administrator, who manage the TOE are non-hostile use, configure and maintain the TOE and follow all guidance.

- ✓ **A.EDUCATED USER-A.EDUCUSER:** Authorized administrator and end users are educated so as to use the Natek NAC system suitably and correctly.

- ✓ **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:** The designer, programmer (coder) and administrator who are responsible for creation of architecture, coding and administrative functions done by trusted persons.

- ✓ **A.TRANSFER SECURITY – A.TRANSSEC:** Operational environment will provide a secure channel so that credentials are protected between the NAC GUI user (super admin and approval user) and NAC GUI application server.

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.

- ✓ **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, with accurate dates and times 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.

- ✓ **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.RESOURCE ACCESS-O.RESACC:** The TOE will control access to resources based on the identity of users. The TSF must allow authorized administrators (Super Admin) to specify which resources may be accessed by which users.

- ✓ **O.SECURITY FUNCTIONS-O.SECFUN:** The TOE will provide functionality that enables an authorized administrator to use the TOE security functions and will ensure that only authorized administrator are 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 administrators prior to allowing access to TOE administrative functions and data.

- ✓ **OE.ADMINISTRATOR TRAINING-OE.ADMTRA:** Authorized administrators 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.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.GUIDAN-OE.GUIDAN:** The TOE will be delivered, installed, administrated and operated in a manner that maintains security.

- ✓ **OE.TRUSTED PERSON-OE.PERTRST:** Authorized administrators, coder, designer and also service personnel will be trusted person 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.FUL_AUD	T.DATALOSS	T.MEDIAT	T.NOAUTH	A.NOEVIL	A.EDUCUSER	A.PYHPROT	A.SECENV	A.TRUST	A.TRANSSEC
O.ACCOUN	✓										
O.ADMIN			✓								
O.AUDREC	✓										
O.IDAUTH					✓						
O.MEDIAT				✓							
O.RESACC		✓	✓	✓	✓						
O.SECFUN		✓									
OE.ADMTRA						✓					
OE.ADMAUT			✓				✓				
OE.GUIDAN							✓				
OE.ENVSEC								✓	✓		✓
OE.PERTRST							✓			✓	

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 administrator 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, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
T.FUL_AUD	This threat is completely countered by • O.SECFUN which ensures the TOE provides functionality that enables an administrator to use the TOE Security Functions and also ensures that only administrator are able to access such functionality. Admin also examines the log and takes the necessary actions. • O.RESACC which must control access to resources based on the identity of users. The TSF must allow authorized administrators to specify which resources may be accessed by which users.
T.DATALOSS	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 authorized administrators to specify which resources may be accessed by which users. • OE.ADMAUTH which ensures the identification and authentication for administrators prior to allowing access to TOE administrative functions and data
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 authorized administrators 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 authorized administrators to specify which resources may be accessed by which users.

4.3.2. Rationale for Security Objectives of the TOE

OBJECTIVES	RATIONALE
O.ACCOUN	This security objective is necessary to counter the threat: T.ACC_AUD because it requires that users are accountable for information flows as well as management function.
O.ADMIN	This security objective is necessary to counter the threat: T.DATALOSS which contains an unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
O.AUDREC	This security objective is necessary to counter the threat: T.ACC_AUD by requiring a readable audit trail and a means to search the information contained in the audit trail.
O.IDAUTH	This security objective is necessary to counter the threat: T.NOAUTH because it requires that user be uniquely identified before accessing the TOE.
O.MEDIAT	This security objective is necessary to counter the threats: T.MEDIAT which has to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE.
O.RESACC	This security objective is necessary to counter the threats: T.FUL_AUD, T.DATALOSS, T.MEDIAT and T.NOAUTH which consists of unauthorized access to data and resources.
O.SECFUN	This security objective is necessary to counter the threat: T.FUL_AUD by requiring that the TOE provides functionality that ensures that only authorized users have access to the TOE security functions.
OE.ADMAUT	This security objective is necessary to counter the threat: T.DATALOSS requires that all administrators be identified and authenticated prior to being given access to TOE administrative functions and data. This prevents unauthorized users from removing or destroying data collected and produced by the TOE. A.EDUCUSER which ensures the authorized administrator and end users are educated so as to use the Natek NAC system suitably and correctly.
OE.ADMTRA	This non-IT security objective is necessary to counter the assumption: support the assumption A.NEOVIL because it ensures that authorized administrators, receives the proper training in the correct configuration, installation and usage of the TOE.
OE.ENVSEC	This non-IT security objective is necessary for the providing environment security of the product that the TOE ensure that it is protected and it has secure environment which also provides secure channel for administrator authentication procedure. (A.SECENV, A.TRANSSEC and A.PYHPROT)

OE.GUIDAN	This non-IT security objective is necessary to counter the assumption: A.EDUCUSER which ensures that it is delivered, installed, administrated and operated in a secure manner and usage.
OE.PERTRST	This non-IT security objective provides reliability about personality related with the TOE security. All personnel are faithful, trained and not permit offensive attack about product. (A.TRUST and A.EDUCUSER)

5. Extended Components Definition

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

5.1. Extended TOE Security Functional Components

There is no Extended TOE Security Functional Components Definition in the Security Target.

5.2. Extended TOE Security Assurance Components

There is no Extended TOE Security Assurance Components Definition in the Security Target.

5.3. Rationale for Extended Security Functional Components

There is no extended Security Functional Components and Security Assurance Components that have been defined for this Security Target.

6. Security Requirements

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

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	SELECT	ASSIGN	REFINE	ITERATE
Security Audit	FAU_GEN.1	Audit data generation	✓	✓		
	FAU_SAR.1	Audit review		✓		
User Data Protection	FDP_ACC.1(A)	Subset access control		✓		
	FDP_ACC.1(B)	Subset access control		✓		
	FDP_ACF.1(A)	Security attribute based access control		✓		
	FDP_ACF.1(B)	Simple Security Attributes		✓		
Identification and Authentication	FIA_ATD.1	User Attribute Definition		✓		
	FIA_UAU.2	User Authentication before any action				
	FIA_UID.2	User Identification before any action				
	FIA_USB.1	User Subject Binding		✓		
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		✓		
TOE Access	FTA_SSL.3	TSF Initiated termination		✓		

SFR	**Dependency**	**Applied**
FAU_GEN.1	FPT_STM.1 Reliable Time Stamp	TOE Environment provides timestamp for the TOE's use.
FAU_SAR.1	FAU_GEN.1 Audit data generation	YES
FDP_ACC.1(A)	FDP_ACF.1 Security attribute based access control	YES FDP_ACF.1(A) is included
FDP_ACC.1(B)	FDP_ACF.1 Security attribute based access control	YES FDP_ACF.1(B) is included
FDP_ACF.1(A)	FDP_ACC.1 Subset Access Control FMT_MSA.3 Static Attribute Initialization	YES FDP_ACC.1(A) and FMT_MSA.3(A) are included
FDP_ACF.1(B)	FDP_ACC.1 Subset Access Control FMT_MSA.3 Static Attribute Initialization	YES FDP_ACC.1(B) and FMT_MSA.3(B) are included
FIA_ATD.1	No dependencies	-
FIA_UAU.2	FIA_UID.1 Timing of identification.	YES FIA_UID.2 hierarchical to FIA_UID.1 is included
FIA_UID.2	No dependencies	-
FIA_USB.1	FIA_ATD.1 User attributes definition.	YES FIA_ATD.1 is included

FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.	YES FMT_SMR.1 and FMT_SMF.1 are included
FMT_MSA.1(A)	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.	YES FDP_ACC.1, FMT_SMR.1 and FMT_SMF.1 are included
FMT_MSA.1(B)	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.	YES FDP_ACC.1, FMT_SMR.1 and FMT_SMF.1 are included
FMT_MSA.3(A)	FMT_MSA.1 Management of Security Attributes FMT_SMR.1 Security roles	YES FMT_MSA.1 and FMT_SMR.1 are included
FMT_MSA.3(B)	FMT_MSA.1 Management of Security Attributes, FMT_SMR.1 Security roles	YES FMT_MSA.1 and FMT_SMR.1 are included
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1 Timing of identification	YES FIA_UID.2 hierarchical to FIA_UID.1 is included
FTA_SSL.3	No dependencies	-

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, database events and Exceptions]

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 PP/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 [Super admin] with the capability to read [all recorded audit information] from the audit records.

6.1.2. Class User Data Protection (FDP)

6.1.2.1. FDP_ACC.1(A) Subset Access Control

Description: Subset access control, requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE

Hierarchical to: No other components.

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

FDP_ACC.1.1.(A) The TSF shall enforce the [Natek Access Control SFP] on

[Subjects: end user systems (target devices) attempting to access network resources,

Objects: specifies network resources,

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

6.1.2.2 FDP_ACC.1(B) Subset Access Control

Description: Subset access control, requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE

Hierarchical to: No other components.

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

FDP_ACC.1.1(B) The TSF shall enforce the [Administrative Access Control SFP] on

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

Objects: user interface items, policies, NAC authentication and authorzation configurations,

Operations: all interactions between the subjects and objects identified above].

6.1.2.3 FDP_ACF.1(A) Access Control Functions

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(A) Subset Access Control, FMT_MSA.3 Static Attribute Initialization

FDP_ACF.1.1(A) The TSF shall enforce the [Natek Access control SFP] to objects based on the following: [Subject attribute: Authorization status as determined by the TOE, IP Address; Object attributes: 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, etc.))].

FDP_ACF.1.2(A) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [if the end systems(target device) has been authorized by the TOE according to defined rules, allocate the appropriate network resources otherwise deny network access.]

FDP_ACF.1.3(A) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [if Administrator enters the record in White List about the end systems(target device), allocate the appropriate network resources].

FDP_ACF.1.4(A) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [if Administrator enters the record in Black List about the end systems(target device), deny network access].

6.1.2.4 FDP_ACF.1(B) Access Control Functions

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(B) Subset Access Control, FMT_MSA.3 Static Attribute Initialization

FDP_ACF.1.1(B) The TSF shall enforce the [Administrative access control SFP] to objects based on the following:
[Subject attribute:

1.User Role,
2.User ID,
3.User's Permissions.

Object attributes:

1. Permissions assigned objects,
2.Absence of permissions assigned to objects.].

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

[If the subject is the TOE Administrator, then access is granted,

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

FDP_ACF.1.4(B) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [no additional rules].

6.1.3. Class Identification and Authentication (FIA)

6.1.3.1. FIA_ATD.1 – User Attribute Definition

Description: User attribute definition, allows user security attributes for each user to be maintained individually.

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [Authorization status as determined by the TOE, User role, User ID, IP Address].

6.1.3.2. 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.

6.1.3.3. 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.

6.1.3.4. FIA_USB.1 – User Subject Binding

Description: User-subject binding, requires the specification of any rules governing the association between user attributes and the subject attributes into which they are mapped.

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attributes definition.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [Authorization status as determined by the TOE, User role, User ID, IP Address].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [None].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [None].

6.1.4. Class Security Management (FMT)

6.1.4.1. 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 [the super admin].

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

6.1.4.2. 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 [Natek 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] to [the super admin].

6.1.4.3. 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, user permission, Permissons assigned objects, Absence of permissions assigned to objects] to [the super admin].

6.1.4.4. 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 [Natek access control SFP] to provide *[permissive]* default values for security attributes that are used to enforce the SFP.

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

6.1.4.5. 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 [super admin] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.6. 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: [System and Service Start-up and Shutdown, Create, Delete, Modify and View security attribute values, enable and disable External IT entities from communicating to the TOE, review of audit trail, configure authorization rules, configure attack rules and access requests].

6.1.4.7. 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 [Super Admin and Approval User (Base User)].

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

6.1.5. Class TOE Access

6.1.5.1. 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 [a logout or a specified time interval of user inactivity set by an authorized administrator. The default session timeout value is 1 hour].

6.2. 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 4 September 2012. 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

6.3. 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.IDAUTH	O.MEDIAT	O.RESACC	O.SECFUN
FAU_GEN.1	✓		✓				
FAU_SAR.1	✓		✓				
FDP_ACC.1(A)		✓				✓	
FDP_ACC.1(B)		✓				✓	
FDP_ACF.1(A)						✓	
FDP_ACF.1(B)		✓				✓	
FIA_ATD.1				✓		✓	
FIA_UAU.2				✓		✓	
FIA_UID.2	✓			✓		✓	
FIA_USB.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						✓	✓
FTA_SSL.3							✓

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.
FDP_ACC.1(A)	This requirement defines subjects, objects and operations controlled by the Natek Access Control Policy. This component traces back to and aids in meeting the following objectives: O.ADMIN and O.RESACC.
FDP_ACC.1(B)	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 and O.RESACC.
FDP_ACF.1(A)	The requirement meets the objective by defining the subject and object attributes, and the rules by which subjects can operate on objects under the Natek Access Control SFP. This component traces back to and aids in meeting the following objectives: O.RESACC.
FDP_ACF.1(B)	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 allow authorized administrators (Super Admin) to specify which resources may be accessed by which users. This component traces back to and aids in meeting the following objectives: O.ADMIN
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH This component also identifies control access to resources based on the subject attribute of users. This component traces back to and aids in meeting the following objectives: O.RESACC

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 control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: O.RESACC
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 control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: O.RESACC
FIA_USB.1	This component consists of success and failure of binding of user security attributes to a subject (e.g. success and failure to create a subject). 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
FMT_MOF.1	This component was 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
FMT_MSA.1(A)	This component restricts the ability to modify, delete, or query object and subject security attributes for the Natek Access Control SFP to super admin. It also assists in effective management and such as aids in meeting O.SECFUN and O.MEDIAT. 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
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 super admin. It also assists in effective management, and such as aids in meeting O.SECFUN and O.MEDIAT. 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
FMT_MSA.3(A)	This component ensures that the TOE provides a default permissive value for security attributes, yet allows a super admin to override the default values. This component traces back to and aids in meeting the following objectives: O.MEDIAT and 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

FMT_MSA.3(B)	This component ensures that the TOE provides a default restrictive value for security attributes, yet allows a super admin to override the default values. This component traces back to and aids in meeting the following objectives: O.MEDIAT and 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
FMT_SMF.1	This component was chosen to consolidate all TOE management, administration and security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN
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 an authorized administrator. 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
FTA_SSL.3	This component ensures that TOE terminates interactive session after specified time interval of user inactivity set by an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN

6.4. Security Assurance Requirements Evidence

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

ASSURANCE REQUIREMENTS	EVIDENCE
ADV_ARC.1 Security architecture description	Security and Design Architecture: Natek Network Access Control NAC v 5.4.2
ADV_FSP.3 Functional specification with complete summary	Functional Specification: Natek Network Access Control NAC v 5.4.2
ADV_TDS.2 Architectural Design	Security and Design Architecture: Natek Network Access Control NAC v 5.4.2
AGD_OPE.1 Operational user guidance	Operational User Guide: Natek Network Access Control NAC v 5.4.2
AGD_PRE.1 Preparative procedures	Installation and Delivery: Natek Network Access Control NAC v 5.4.2
ALC_CMC.3 Authorization Control	Configuration Management: Natek Network Access Control NAC v 5.4.2
ALC_CMS.3 Implementation Representation CM coverage	Configuration Management: Natek Network Access Control NAC v 5.4.2
ALC_DEL.1 Delivery procedures	Installation and Delivery: Natek Network Access Control NAC v 5.4.2
ALC_DVS.1Identification of Security Measures	Development Environment Security: Natek Network Access Control NAC v 5.4.2
ALC_LCD.1 Developer defined life-Cycle model	Software Life-Cycle: Natek Network Access Control NAC v 5.4.2
ATE_COV.2 Analysis of coverage	Testing Plan and Analysis: Natek Network Access Control NAC v 5.4.2
ATE_DPT.1 Testing: Basic Design	Testing Plan and Analysis: Natek Network Access Control NAC v 5.4.2
ATE_FUN.1 Functional testing	Testing Plan and Analysis: Natek Network Access Control NAC v 5.4.2

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
- User Data Protection
- Identification and Authentication
- Security Management

7.1.1. Security Audit

The TOE generates a set of audit logs. These logs are stored on the database and administrator can also view them to a local machine.

The TOE generates Local Logs for the following list of events:

- All user of user identification and authentication mechanism, which includes the user identities provided to the TOE in each related log;
- All user database interactions logs like Create, Update, Delete Operations;
- All system Exception logs within any failure

The logs are only accessible through the Web-Based Administrative interface, which only authorized operators can access. When logs are saved from the TOE, they are transferred to the PC connected to the Web-Based Administrative interface.

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

- FAU_GEN.1: The TOE generates all the audit events identified in this requirement. Within each event is the information listed above which addresses all required details. The log which is generated by this security function also includes Time Stamp value.
- FAU_SAR.1: TOE provides ability to review logs.

7.1.2. 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.

The TOE provides authorized administrators with the ability to configure network access policies and rules using the Natek NAC GUI. The GUI provides for the creation of rules that define actions the TOE is to take based on a set of conditions. The conditions and actions provide either the allowed access to network resource or not. The specific network resources to which a user or personnel is given access is determined by the administrator when the policy is configured. Therefore, Natek NAC System determines which network resources are permitted for access by an end-user attempting to connect to the network that has been authorized by the TOE. (Access Control SFP)

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

The families in this class are organized into two groups for Natek Network Access Control and protection of user data is provided by these security functions.

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

- FDP_ACC.1(A): This component ensures that the access control policies are enforced on all operations among subjects and objects in the Natek Access Control SFP.
- FDP_ACC.1(B): This component ensures that the access control policies are enforced on all operations among subjects and objects in the Administrative Access Control SFP.
- FDP_ACF.1(A): This component ensures that permissions and privileges can be granted to specific subjects and objects for different accesses according to Natek Access Control SFP.
- FDP_ACF.1(B): This component ensures that permissions and privileges can be granted to specific subjects and objects for different accesses according to Administrative Access Control SFP.

7.1.3. Identification and Authentication

The TOE performs identification and authentication of all users and administrators accessing the TOE. The TOE has the ability to authenticated users locally using a password or can integrate with a remote authentication server. Users enter a username and password, which is validated by the TOE against the user information stored by the database. If the authentication succeeds, the user receives a session token that is used for identification of subsequent requests during that session.

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

- FIA_ATD.1: For each registered user, the TOE stores the following information:
    - User Identity
    - User Name
    - User Roles
    - Password
- FIA_UAU.2: The TOE requires a valid password associated with a username before providing access to the TOE.
- FIA_UID.2: The TOE requires a username during the identification and authentication Process. 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.
- FIA_USB.1: The TOE associates a username with a subject acting on the user's behalf upon successful identification and authentication of the administrator use.

7.1.4. Security Management

The TOE provides security management functions via browser interface. The Administrator logs on to the TOE from a protected network and performs all management functions through the browser interface. The administrator has the ability to control all aspects of the TOE configuration including:

- User Management
- Audit Management
- System and Service Start-up and Shutdown

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

- FMT_MOF.1: This component restrict the ability to determine the behavior of, disable and enable Authorization configuration, attack rule configuration functions to super admin.
- FMT_MSA.1(A): This component restricts the ability to modify, delete or query the subject and object security attributes for the Natek Access Control SFP to the super admin role
- FMT_MSA.1(B): This component restricts the ability to modify, delete or query the subject and object security attributes for the Administrative Access Control SFP to the super admin role
- FMT_MSA.3(A): TOE provides permissive default values for security attributes specified in FDP_ACF.1(A)
- FMT_MSA.3(B): TOE provides restrictive default values for security attributes specified in FDP_ACF.1(B)
- FMT_SMF.1: The TOE supports the following security management functions:
    - System and Service Start-up and Shutdown
    - Create, Delete, Modify and View user attribute values, which include a user's identity, association and authentication credentials.
    - Enable and Disable External IT entities from communicating to the TOE.
    - Review the Audit Records
    - Configure authorization rules
    - Configure attack rules

- FMT_SMR.1: The TOE supports the roles super admin, limited administrator role user and approval user.
    - The super admin role can perform all management functionalities. The administrator dynamically sets up user roles and access rules associated with the roles.
    - The limited administrator role user has only the Diagnostic Access.
    - Approval User evaluates the requests (via mail or sms) and decides on the access of the limited network.
- FTA_SSL.3: TOE terminates interactive session after specified time interval of user inactivity set by an authorized administrator. Default value is 1 hour.