Certification Report

EAL 3 Evaluation of

NATEK BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK YAZILIM TİC. SAN. A.Ş.

NATEK NAC (Network Access Control)
Version 5.4.2

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	***03.09.2014***
Version of Report	***1.0***
Author	***Kerem KEMANECİ***
Technical Responsible	***Mustafa YILMAZ***
Approved	***Mariye Umay AKKAYA***
Date Approved	***03.09.2014***
Certification Report Number	***21.0.01/14-024***
Sponsor and Developer	***NATEK BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK YAZILIM TİC. SAN. A.Ş***
Evaluation Lab	***TÜBİTAK BİLGEM OKTEM***
TOE	***NATEK NAC (Network Access Control) Version 5.4.2***
Pages	***24***

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
0.1	***25.08.2014***	***All***	***Initial***
1.0	***03.09.2014***	***All***	***Final***

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4 This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the STCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL) under CCCS' supervision. CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by TÜBİTAK BİLGEM OKTEM, which is a public/commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for NAC (Network Access Control) Version 5.4.2 whose evaluation was completed on 29.08.2014 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no ST v1.13 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the STCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

Evaluated IT Product Name: *NATEK NAC (Network Access Control) Version 5.4.2*
Developer: *NATEK BİLİŞİM A.Ş.*
Name of CCTL: *TÜBİTAK BİLGEM OKTEM*
Assurance Package: *EAL 3*
Completion Date of Evaluation: *29.08.2014*

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.

1.1 Major Security Features:

- 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.

1.2 Threats

The threats identified in this section are addressed by the TOE.

T.ACCOUNT AUDIT: 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: 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: An attacker from the outside network may attempt to remove or destroy Configuration and device data store in the Natekdbnac.

T.MEDIATE: 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: 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.

1.3 Organizational Security Policies

The TOE does not include any Organizational Security Policy.

1.4 Configuration Required by the TOE

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.

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.

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

For detailed configuration requirements for the TOE see section ***2.7 Evaluated Configuration*** in this report.

1.5 Summary of Evaluation;

ASSURANCE CLASS	**CCTL's Verdict**	**CCCS's Decision**
ASE – Security Target	PASS	POSITIVE
ALC – Life Cycle	PASS	POSITIVE
AGD - Guidance	PASS	POSITIVE
ADV - Development	PASS	POSITIVE
ATE - Tests	PASS	POSITIVE
AVA – Vulnerability Analysis	PASS	POSITIVE
RESULT	**PASS**	**POSITIVE**

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	***TR-21.0.01/TSE-CCCS-022***
TOE Name and Version	***NATEK NAC (Network Access Control) Version 5.4.2***
Security Target Title	***NAC- ST Version 1.13***
Security Target Version	***1.13***
Security Target Date	***28.08.2014***
Assurance Level	***EAL 3***
Criteria	• *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012* • *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012* • *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 4, September 2012*
Methodology	• *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012, Version 3.1, Revision 4*
Protection Profile Conformance	***None***
Common Criteria Conformance	• *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012* • *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 4, September 2012*
Sponsor and Developer	***NATEK BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK YAZILIM TİC. SAN. A.Ş.***
Evaluation Facility	***TÜBİTAK BİLGEM OKTEM***
Certification Scheme	***Turkish Standards Institution Common Criteria Certification Scheme***

2.2 Security Policy

The TOE does not include any Organizational Security Policy.

2.3 Assumptions and Clarification of Scope

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. The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used. The consumers who plan to use the product should consider the assumptions below.

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

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

A.PHYSICAL ACCESS AND PROTECTION: 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: 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: The designer, programmer (coder) and administrator who are responsible for creation of architecture, coding and administrative functions done by trusted persons.

A.TRANSFER SECURITY: 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.

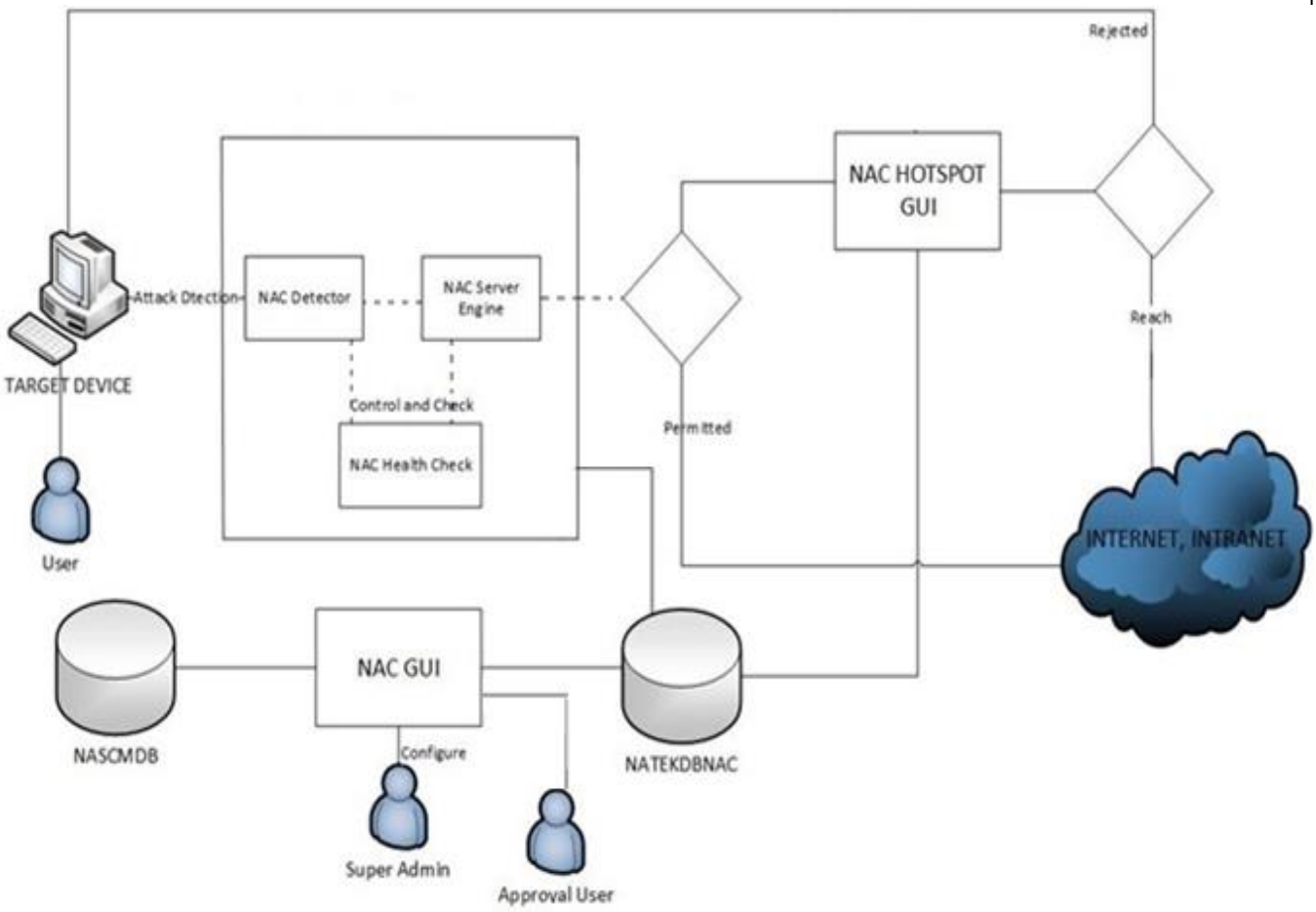
2.4 Architectural Information

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

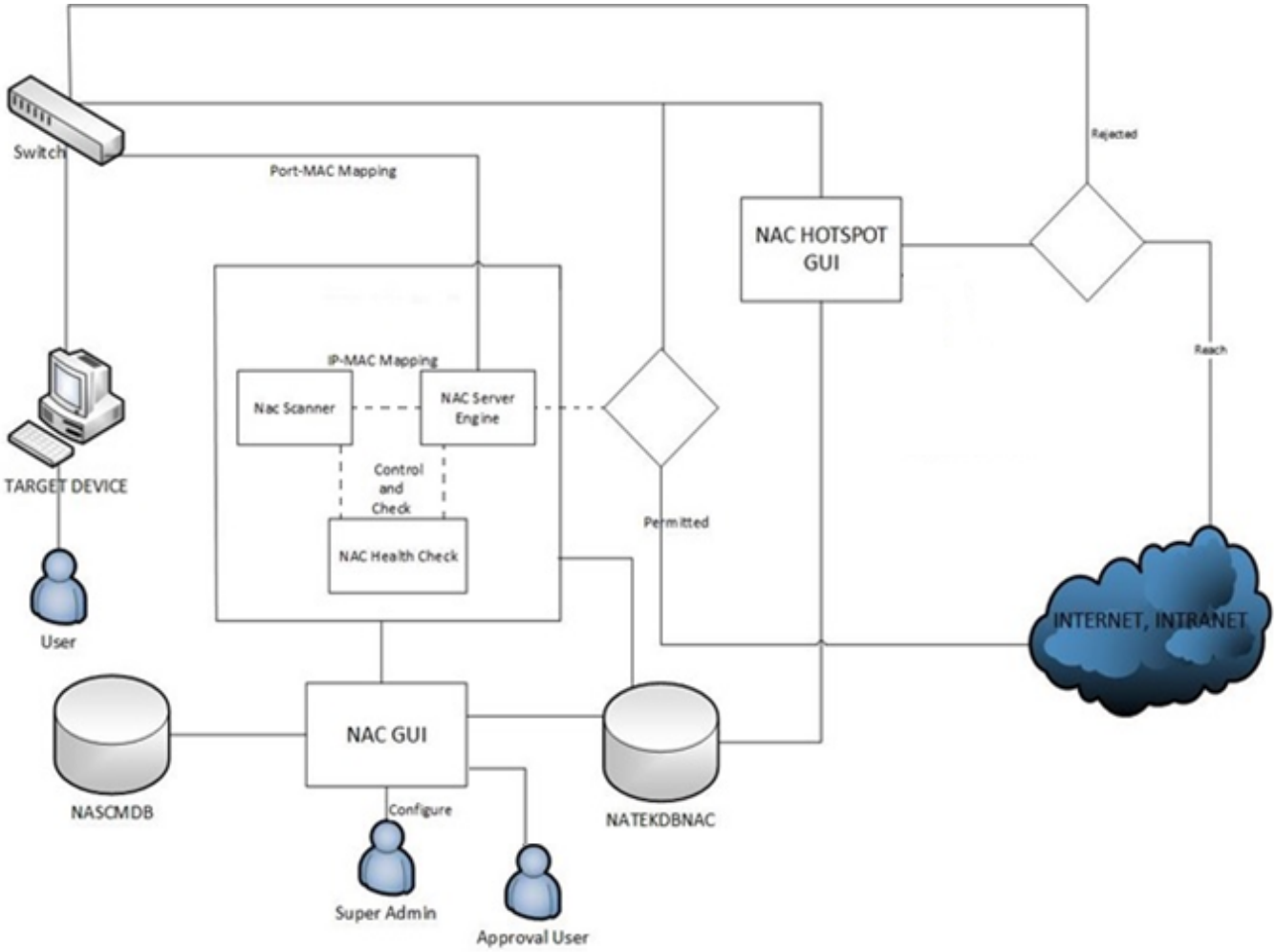
Portal. (Sample authorization types are; Guests, Corporate Employee)

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.

2.5 Documentation

Document list for customers:

- NAC-ST Version 1.13
- NAC -FONKSİYONEL ÖZELLİKLER_Versiyon 1.6
- NAC -MİMARİ TASARIM_Versiyon 1.7
- NAC -TEST KAPSAM ve DERİNLİK_Versiyon 1.5
- NAC- YÖNETİM KİTABI- KULLANICI KILAVUZU_Versiyon1.9
- NAC- YÖNETİM KİTABI- KURULUM KILAVUZU_Versiyon1.5
- NAC-KURULUM ve TESLİM Versiyon 1.4

2.6 IT Product Testing

Developer Tests:

The developer's testing strategy was to define test cases that specified complete coverage of all security functions defined in the ST. The test cases were written by the developers to exercise the security functionality of the TOE.

In all the developer submitted 69 tests those are divided to 4 groups of subsystems; NAC GUI, NAC Server, NAC Detector, NAC Hotspot GUI.

Evaluator Tests:

The evaluator ran a representative sample of the developer tests to show completeness of the test coverage. The sample included tests to exercise each security function and TSFI. The purpose of running this sample of the tests was to gain confidence in the developer's functional test results.

The evaluator reran 9 out of the 69 developer tests. All tests that were rerun by the evaluator passed.

Evaluator Defined Tests:

The evaluator's strategy in developing the evaluator-defined tests for the TOE was to supplement the developer's functional tests and the penetration tests.

The evaluator-defined tests were devised to augment the developer's functional tests in order to exercise functionality in greater depth than the developer tests provided. The Evaluator defined 17 independent tests in 4 groups , consisting of TOE Main Security Functions: Identification and Authentication, Security Management, Security Audit, User Data Protection.
All of those 17 evaluator defined independent tests were run by the evaluator passed.

Penetration Tests:

Totally 10 penetration tests were defined by the evaluator. All of the tests were run by the evaluator passed.

2.7 Evaluated Configuration

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.

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.

Super Admin decides which scenario is suitable and applicable for the company according to company needs and infrastructure. Super Admin applies the selected scenario on NAC GUI and make configuration. See section **2.4 Architectural Information** for details.

The minimum operating system (O/S) and hardware requirements for:

NAC GUI host computer;

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

NAC Server host computer;

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

NAC Detector host computer;

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

NAC HotSpot GUI host computer;

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

Required Configuration for the 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.

2.8 Results of the Evaluation

All evaluator actions are satisfied for the evaluation level of EAL 3 as defined by the

Common Criteria and the Common Methodology. The overall verdict for the evaluation is PASS. The results are supported by evidence in the ETR. There is no residual vulnerability for this product. TOE is resistant against to "BASIC LEVEL" attack potential attackers.

Assurance class	Assurance components	VERDICT
ADV: Development	ADV_ARC.1 Security architecture description	PASS
	ADV_FSP.3 Security enforcing functional specification	PASS
	ADV_TDS.2 Basic design	PASS
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	PASS
	AGD_PRE.1 Preparative procedures	PASS
ALC: Life cycle support	ALC_CMS.3 Parts of the TOE CM coverage	PASS
	ALC_DVS.1 Development Security	
	ALC_CMC.3 Use of a CM system	PASS
	ALC_DEL.1 Delivery procedures	PASS
	ALC_LCD.1 Lifecycle Definition	
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	PASS
	ASE_ECD.1 Extended components definition	PASS
	ASE_INT.1 ST Introduction	PASS
	ASE_OBJ.2 Security objectives	PASS
	ASE_REQ.2 Derived security requirements	PASS
	ASE_SPD.1 Security Problem Definition	PASS
	ASE_TSS.1 TOE summary specification	PASS
ATE: Tests	ATE_IND.2 Independent testing sample	PASS
	ATE_FUN.1 Functional testing	PASS
	ATE_COV.1 Evidence of coverage	PASS
	ATE_DPT.1 Depth	
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of NATEK NAC (Network Access Control) Version 5.4.2 product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The ST associated with this Certification Report is identified by the fallowing nomenclature:

Title: NAC-ST Version
Version: V1.13
Date: 28.08.2014

4 GLOSSARY

ADV	: Assurance of Development
AGD	: Assurance of Guidance Documents
ALC	: Assurance of Life Cycle
ASE	: Assurance of Security Target Evaluation
ATE	: Assurance of Tests Evaluation
AVA	: Assurance of Vulnerability Analysis
BİLGEM	: Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
CC	: Common Criteria (Ortak Kriterler)
CCCS	: Common Criteria Certification Scheme (TSE)
CCRA	: Common Criteria Recognition Arrangement
CCTL	: Common Criteria Test Laboratory (OKTEM)
CEM	:Common Evaluation Methodology
CMC	: Configuration Management Capability
CMS	: Configuration Management Scope
CSRF	: Cross-Site Request Forgery
DB	: Database
DEL	: Delivery
EAL	: Evaluation Assurance Level
GR	: Observation Report - Gözlem Raporu
GUI	: Graphical User Interface
HTML	: HyperText Markup Language
HTTP	: HyperText Transfer Protocol
OKTEM	: Ortak Kriterler Test Merkezi
OPE	: Opretaional User Guidance
OSP	: Organisational Security Policy
PP	: Protection Profile

PRE : Preperative Procedures
SAR : Security Assurance Requirements
SFR : Security Functional Requirements
SQL : Structured Query Language
ST : Security Target
STCD :Software Test and Certification Department
TOE : Target of Evaluation
TSF : TOE Secırity Functionality
TSFI : TSF Interface
URL : Uniform Request Locater
XSS : Cross-Site Scripting

5 BIBLIOGRAPHY

1. NAC-ST Version 1.13
2. NAC -FONKSİYONEL ÖZELLİKLER_Versiyon 1.6
3. NAC -MİMARİ TASARIM_Versiyon 1.7
4. NAC -TEST KAPSAM ve DERİNLİK_Versiyon 1.5
5. NAC- YÖNETİM KİTABI- KULLANICI KILAVUZU_Versiyon1.9
6. NAC- YÖNETİM KİTABI- KURULUM KILAVUZU_Versiyon1.5
7. NAC-KURULUM ve TESLİM Versiyon 1.4
8. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012
9. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012
10. Common Criteria for Information Technology Security Components,Version 3.1, Revision 4, September 2012
11. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012, Version 3.1, Revision 4
12. YTBD-01-01-TL-01 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 1.0

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections.