Certification Report

EAL 2+ Evaluation of Trustwave Network Access Control Software v3.4.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-129-CR
Version: 1.0
Date: November 12, 2009
Pagination: i to iii, 1 to 13

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is DOMUS IT Security Lab located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated the November 12, 2009, and the security target identified in Section 4 of this report.

The certification report, Certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria Portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarked or registered trademarks:

- Trustwave, the Trustwave logo, Trustwave NAC, Management Operations Console, and Advanced Compliance Server are trademarks or registered trademarks of Trustwave in the U.S. and other countries.

TABLE OF CONTENTS

Executive Summary

Trustwave Network Access Control Software v3.4.0 (hereafter referred to as Trustwave NAC), from Trustwave, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

The Trustwave NAC solution enables network administrators to control which devices gain admission to the network and what network services they may invoke. Sensors are connected to the network segments that are controlled, and monitor all the network traffic to detect any policy violations configured by administrators. As devices attempt to gain access to the network, Trustwave NAC immediately identifies the device and can run a policy check to determine if the device complies with the security policies in the network segment that it is attempting to join. When performing policy checks on managed devices, Trustwave NAC can perform monitoring of network traffic to identify attributes of the device, and/or a deep scan via a Java applet downloaded.

Network monitoring determines the device type, whether it is known or unknown, network function (e.g. IP telephony device, wireless device), and what services are currently running – such as instant messaging, file transfer protocol services, or peer-to-peer networking. Deep scans obtain more detailed information about the device configuration such as anti-virus version, signature update levels, OS patch levels, and the absence or presence of spyware and firewall software. Devices can be re-checked throughout their lifecycle on the network. After admission, Trustwave NAC monitors all network traffic, detects exceptions to the administrator-configured behavioral policy, and re-evaluates the network access permitted to the managed devices as new information about them is learned.

DOMUS IT Security Laboratory is the Common Criteria Evaluation Facility (CCEF) that conducted the evaluation. This evaluation was completed on October 30, 2009 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Trustwave NAC, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 2 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.* The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Trustwave NAC evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is Trustwave Network Access Control Software v3.4.0 (hereafter referred to as Trustwave NAC), from Trustwave.

2 TOE Description

The Trustwave NAC solution enables network administrators to control which devices gain admission to the network and what network services they may invoke. Sensors are connected to the network segments that are controlled, and monitor all the network traffic to detect any policy violations configured by administrators. As devices attempt to gain access to the network, Trustwave NAC immediately identifies the device and can run a policy check to determine if the device complies with the security policies in the network segment that it is attempting to join. When performing policy checks on managed devices, Trustwave NAC can perform monitoring of network traffic to identify attributes of the device, and/or a deep scan via a Java applet downloaded.

Network monitoring determines the device type, whether it is known or unknown, network function (e.g. IP telephony device, wireless device), and what services are currently running – such as instant messaging, file transfer protocol services, or peer-to-peer networking. Deep scans obtain more detailed information about the device configuration such as anti-virus version, signature update levels, OS patch levels, and the absence or presence of spyware and firewall software. Devices can be re-checked throughout their lifecycle on the network. After admission, Trustwave NAC monitors all network traffic, detects exceptions to the administrator-configured behavioral policy, and re-evaluates the network access permitted to the managed devices as new information about them is learned.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Trustwave NAC is identified in Section 6 of the Security Target (ST).

4 Security Target

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

Title: Trustwave Network Access Control (NAC) Software v3.4.0 Security Target
Version: 2.4
Date: 19 October 2009

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*.

Trustwave NAC is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - IDS_SDC.1 - System Data Collection
    - IDS_ANL.1 - Analyser Analysis
    - IDS_RCT.1 - Analyser React
    - IDS_RDR.1 - Restricted Data Review
    - IDS_STG.1 - Guarantee of System Data Availability
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 2 augmented*, with all the security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

Trustwave NAC implements an Access Zone Service Restriction policy to control network access; details of this security policy can be found in Sections 5, 6 & 7 of the ST.

In addition, Trustwave NAC implements policies pertaining to security audit, identification and authentication, and security management. Further details on these security policies may be found in Sections 5, 6 & 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Trustwave NAC should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Managed devices will process received Address Resolution Protocol messages as specified in RFC826.

- The Administrator will install and configure the TOE according to the administrator guidance.
- There will be a network that supports communication between distributed components of the TOE. This network functions properly.
- Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.

7.3 Clarification of Scope

Trustwave NAC was designed and intended for use in a structured corporate environment. It cannot prevent authorized administrators from carelessly configuring the TOE such that the TOE security or the security of IT systems monitored by the TOE is compromised.

Trustwave NAC provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone.

While its user guidance documents do provide adequate advice for securing its operational environment, it is primarily the product administrator's responsibility to ensure that the networks and the systems which the Trustwave NAC is connected to or installed on are protected adequately.

Consumers of Trustwave NAC should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of Trustwave NAC.

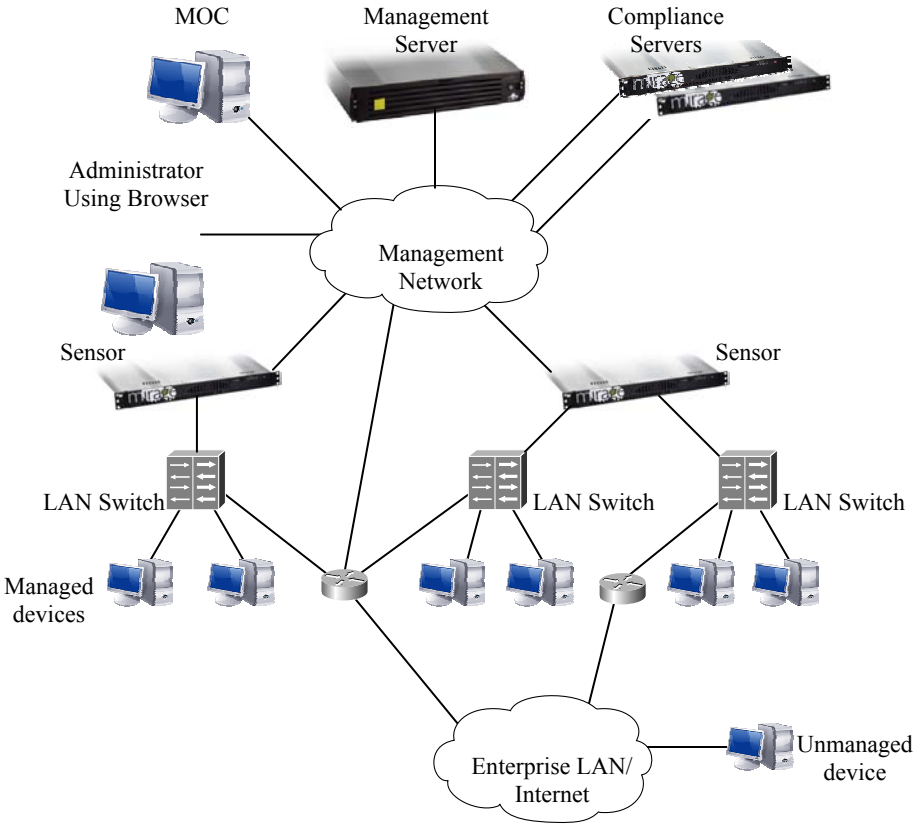
8 Architectural Information

The TOE is the software for the Trustwave NAC product, which consists of the following components distributed throughout the enterprise network:

1. *Management Operations Center (MOC)* – Software executing on a Windows PC that provides the user interface for the NAC. MOC communicates with the Management Server. A single MOC is used to control and monitor the NAC infrastructure.

2. *Management Server* – The Management Server is an appliance that provides the centralized control, monitoring, and data collection functions for the set of Sensors and Compliance Servers in a deployment. A single Management Server is used for the NAC infrastructure.
3. *Sensors* – The Sensor appliances are connected to one or more LAN segments and control network access for devices connected to the LAN segments. These devices discover managed devices and enforce the network access control policies. A single sensor may service multiple LAN segments. As many sensors are deployed as are required to connect to all the monitored segments.
4. *Compliance Servers* – The Compliance Server appliances perform the deep scans of managed devices. A Java application is dynamically downloaded to these managed devices when a scan is required. Sufficient compliance servers are installed to handle the number of managed devices in the deployment. These systems may be centralized or distributed.

A typical deployment for these components is shown in the following diagram.

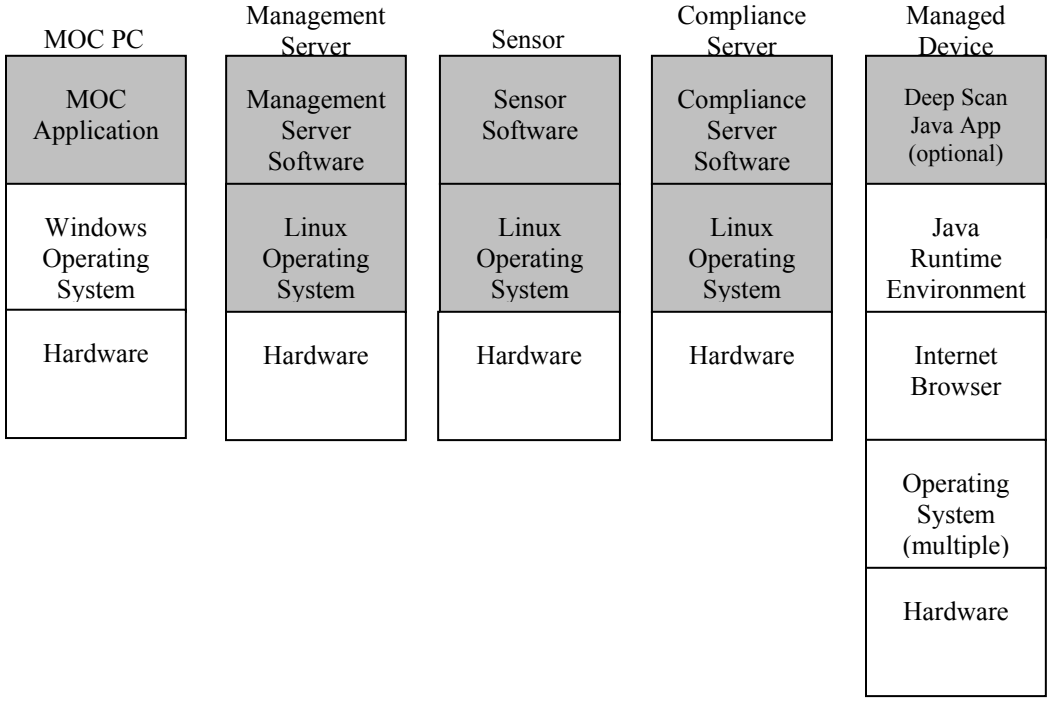


The TOE subsystems correspond to the TOE software components listed above, as follows:

1. MOC PC Software.

2. Management Server Software (Application and Operating System are a single subsystem).
3. Sensor Software (Application and Operating System are a single subsystem).
4. Compliance Server Software (Application and Operating System are a single subsystem).
5. Deep Scan Java Application Software.

The physical boundary of the TOE is all the software executing on the appliances, including the operating system, along with the MOC application and the Java application used to perform deep scans on managed devices, as depicted in the following diagram (shaded items are within the TOE boundary).



9 Evaluated Configuration

The evaluated configuration for Trustwave NAC comprises:

The evaluated configuration consists of the following TOE components, executing on systems complying with the minimum hardware and software requirements specified for each component[2]:

1. One instance of the MOC executing on a PC dedicated to this purpose.
2. One instance of the Management Server.
3. One or more instances of the Compliance Server.
4. One or more instances of the Sensor.

In addition, the following configuration options must be specified to conform to the evaluated configuration:

1. Scanning is enabled at the domain level.
2. Restricted access is enabled at the domain level.
3. The only External Authorities configured are the Compliance Servers; these are automatically configured during installation.
4. All administrative accounts are configured at the top level domain.
5. All management of the TOE after installation is performed using the MOC. The Terminal User Interface (TUI) to the appliances is only used during installation. The configuration functionality available through the Management Server web server functionality is not used.
6. As part of its device visibility functionality, Trustwave provides network-based OS detection of all devices in a managed segment. In order to maintain the integrity of an implemented security policy, Trustwave recommends leveraging this functionality for the purposes of excluding Embedded OS devices from compliance scanning. Setting compliance-scanning exclusions based upon endpoint OS characteristics makes it much more difficult for malicious users to bypass the security policy. Please refer to Section 14 for further details.

10 Documentation

The Trustwave documents provided to the consumer are as follows:

1. *Trustwave NAC A-500 Hardware*
2. *Trustwave NAC Advanced Compliance Server Deployment and Branding*

[2] Refer to Section 1.5.3 of the Security Target for specific hardware and software requirements

3. *Trustwave NAC M-1/M-10 Hardware Guide*
4. *Management Operations Console User's Guide*
5. *Trustwave NAC X-[50, 100, 500, 1000] Hardware Guide*
6. *Trustwave NAC X-2500 Hardware Guide*
7. *Trustwave NAC Hardware Guide*
8. *Trustwave Network Access Control (NAC) Version 3.4.0 Installation Supplement*

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Trustwave NAC, including the following areas:

Development: The evaluators analyzed the Trustwave NAC functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Trustwave NAC security architectural description and determined that the initialization process was secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance Documents: The evaluators examined the Trustwave NAC preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Trustwave NAC configuration management system and associated documentation was performed. The evaluators found that the Trustwave NAC configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Trustwave NAC during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Trustwave for Trustwave NAC. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Trustwave NAC. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Trustwave NAC potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the Trustwave NAC in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[3].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of DOMUS IT Security Lab test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data;

c. Audit: The objective of these tests is to ensure that event logging requirements have been met;

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

d. Identification and Authentication: The objective of these tests is to ensure that access to the TOE is restricted to authorized administrators only; and

e. Network Access Control: The objective of this test goal is to ensure that configured policies for devices using the managed segments are enforced.

12.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Port and Vulnerability Scanning; and
- Masquerading and Substitution Attacks;

The independent penetration testing did not uncover any exploitable vulnerability in the anticipated operating environment.

12.4 Conduct of Testing

Trustwave NAC was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Developer's location in Austin, Texas. The Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Trustwave NAC behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The evaluator re-iterates the following developer guidance regarding scan bypass noted in the evaluated configuration of the security target:

Bypassing the compliance scan is often necessary for network devices such as printers, HVAC controllers, badge readers, security cameras and network infrastructure devices, such as routers and switches. While configuring exclusions for these devices is a normal part of

any NAC deployment, basing the exclusions on either the MAC or IP Address of the device poses risks, since malicious users may attempt to hijack the excluded device's address for the purposes of avoiding the compliance scan. As part of its device visibility functionality, Trustwave provides network-based OS detection of all devices in a managed segment. In order to maintain the integrity of an implemented security policy, Trustwave recommends leveraging this functionality for the purposes of excluding Embedded OS devices from compliance scanning. Setting compliance-scanning exclusions based upon endpoint OS characteristics makes it much more difficult for malicious users to bypass the security policy.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LAN	Local Area Network
MAC	Media Access Control
MOC	Management Operations Center
NAC	Network Access Control
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TUI	Terminal User Interface
TOE	Target of Evaluation
TSF	TOE Security Functionality

16 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

c. CEM version e.g. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

d. Trustwave Network Access Control Software v3.4.0 Security Target, v2.4, 19 October 2009

e. Trustwave Network Access Control Software v3.4.0 ETR, v0.6, 20 October 2009