National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

McAfee VirusScan 8.5i and ePolicy Orchestrator 3.6.1

Report Number: CCEVS-VR-07-0047

Dated: 22 June 2007

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Jerome F. Myers
David M. Dignan

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

1 Identification 5
1.1 Applicable Interpretations 6
2 Security Policy 7
2.1 Audit 7
2.2 Management 7
2.3 Cryptographic Operations 7
2.4 Protection of the TOE 7
2.5 Security Function Strength of Function Claim 7
2.6 Protection Profile Claim 8
3 Assumptions 8
3.1 Physical Assumptions 8
3.2 IT Environment Assumptions 8
3.3 Personnel Assumptions 8
3.4 Threats 8
4 Clarification of Scope 9
5 Architecture Information 10
5.1 Evaluated Configuration 10
5.2 Functionality Excluded from the Evaluation 12
6 Product Delivery 12
7 IT Product Testing 13
7.1 Evaluator Functional Test Environment 13
7.2 Functional Test Results 15
7.3 Evaluator Independent Testing 15
7.4 Evaluator Penetration Tests 15
7.5 Test Results 16
8 RESULTS OF THE EVALUATION 16
10. VALIDATOR COMMENTS 16
11. Security Target 17
12. List of Acronyms 17
13. Bibliography 18

List of Figures

Figure 1 - TOE Components 10
Figure 2 - Test Configuration/Setup 13

List of Tables

Table 1 - Evaluation Identifier 6
Table 2 - Evaluated Configuration 10
Table 3 - Test Configuration 13

EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the McAfee VirusScan 8.5i and ePolicy Orchestrator 3.6.1 at EAL2 augmented with ALC_FLR.2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 24 May 2007. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.2, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) EAL2 augmented with ALC_FLR.2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the McAfee VirusScan and ePolicy Orchestrator that consists of a set of software components executed on Windows platforms. The TOE is comprised of two parts: the McAfee VirusScan agent and the ePolicy Orchestrator. McAfee VirusScan and ePolicy Orchestrator collectively is a Virus Scanning tool and management tool intended for use in networked environments. The database and underlying hardware and software are not part of the evaluation.

McAfee VirusScan Enterprise v8.5i (VSE) is an anti-virus end-point solution that detects and cleans virus-infected files before they enter the corporate network**.** McAfee ePolicy Orchestrator v3.6 (ePO) provides management capabilities to VSE, although a VSE client agent also runs on the ePO server to help it protect itself. VSE and ePO provide a high degree of user configurability to customize the management of viruses and virus-infected files. Together, VSE and ePO comprise the TOE.

The VirusScan Agent (hereafter referred to as Agent) is a software package designed to protect enterprise networks from viruses, worms, Trojans, as well as unwanted code and programs. VSE can be configured to scan local and network drives, as well as Microsoft Outlook and Lotus Notes email messages and attachments. It is possible to configure VSE to respond to infections and malicious code that it finds by identifying the intrusive files, removing them, and reporting on them.

In addition to the Agent, the TOE includes ePolicy Orchestrator (ePO) version 3.6.1. ePO distributes and manages agents that reside on client systems. By using ePO you can manage a large enterprise network. A centralized but distributed architecture allows the Agent software to be centrally managed and yet decrease network traffic required to manage clients. ePO provides the management interface and functionality for the administrators of the TOE. It also provides centralized audit collection and review functionality.

1 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifier

Evaluation Identifiers for McAfee VirusScan and ePolicy Orchestrator system	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	McAfee VirusScan 8.5i and ePolicy Orchestrator 3.6.1
Protection Profile	*U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness, v1.1*, April 4, 2006
Security Target	VirusScan Enterprise v 8.5i, ePolicy Orchestrator Security v3.6 Target, revision 6, dated June, 2007
Evaluation Technical Report	Evaluation Technical Report for McAfee VirusScan 8.5i and ePolicy Orchestrator 3.6.1
Conformance Result	Part 2 conformant and EAL2 augmented with ALC_FLR.2 Part 3 conformant
Version of CC	CC Version 2.2 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on May 6, 2006
Version of CEM	CEM Version 2.2 and all applicable NIAP and International Interpretations effective on May 5, 2006
Sponsor	McAfee Inc.
Developer	McAfee Inc.
Evaluator(s)	**COACT Incorporated** Brian Pleffner, Anthony Busciglio, Christa Lanzisera, Ryan Kane, Nicholas Rojewski, Brooks Leitch
Validator(s)	**NIAP CCEVS,** Jerome F. Myers, David M. Dignan

1.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0405 – American English Is An Acceptable Refinement
I-0426 – Content of PP Claims Rationale

I-0427 – Identification of Standards

International Interpretations

None

2 Security Policy

The TOE is the McAfee VirusScan and ePolicy Orchestrator that consists of a set of software components executed on Windows platforms. The TOE is comprised of two parts: the McAfee VirusScan agent and the ePolicy Orchestrator. McAfee VirusScan and ePolicy Orchestrator collectively is a Virus Scanning tool and management tool intended for use in networked environments.

2.1 Audit

The OnAccess Scan Log provides auditing of scan operations and event logs for virus events that can be reviewed from the workstation. The events are also transmitted and logged on the ePO server and are kept in separate log files.

2.2 Management

Enables the Central Administrator to centrally manage virus scan settings on workstations, configure and manage the actions the virus scan component takes when detection of an infection occurs, and manage the audit logs.

2.3 Cryptographic Operations

VirusScan anti-virus packages are encrypted using a key pair that uses the Digital Signature Algorithm (DSA) and is then encrypted using 168 bit key 3DES and pushed to the workstation.

2.4 Protection of the TOE

The TOE provides for self protection and ensures that of functions within the TOE's scope of control (TSC). The TOE protects itself from tampering and interference from untrusted subjects at the TSFI's of the TOE. The TOE also relies on the underlying software and hardware to assist in protecting security functions from tampering and interference.

2.5 Security Function Strength of Function Claim

The claimed strength of function is SOF-basic. The rationale for choosing SOF-basic was to be consistent with the Basic Robustness guidelines. SOF-basic is appropriate for the intended use of the TOE in environments with threat agents with low attack potential.

2.6 Protection Profile Claim

This Security Target claims conformance to the U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness, v1.1, April 4, 2006.

3 Assumptions

The specific conditions listed in the following subsections are assumed to be met by the environment and operating conditions of the system. The assumptions are ordered into three groups. They are personnel assumptions, physical assumptions, and IT environment assumptions.

A) Personnel assumptions describe characteristics of personnel who are relevant to the system.

B) Physical environment assumptions describe characteristics of the non-IT environment that the system is deployed in.

C) IT environment assumptions describe the technology environment within which the TOE is operating.

3.1 Physical Assumptions

The results of the evaluation rely upon the following assumptions regarding the physical environment.

A.PHYSICAL	It is assumed that the appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

3.2 IT Environment Assumptions

The results of the evaluation rely upon the following assumptions regarding the IT Environment.

A. SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
A. SECURE_UPDATES	Administrators will implement secure mechanisms for receiving and validating updated signature files from the Anti-Virus vendors, and for distributing the updates to the central management systems.

3.3 Personnel Assumptions

The results of the evaluation rely upon the following assumptions regarding personnel relevant to the system.

A. AUDIT_BACKUP	Administrators will back up audit files and monitor disk usage to ensure audit information is not lost.
A. NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrative guidance.

3.4 Threats

The following threats are addressed by the TOE.

Threats Addressed by the TOE

The TOE addresses the following threats:

T.ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.AUDIT_ COMPROMISE	A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being discovered thereby causing potential security vulnerabilities.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to scan files or process administrator requests.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted)
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNIDENTIFIED_ACTIONS	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.
T.VIRUS	A malicious agent may attempt to introduce a virus onto a workstation via network traffic or removable media to compromise data on that workstation, or use that workstation to attack additional systems.

4 Clarification of Scope

The TOE is the McAfee VirusScan and ePolicy Orchestrator that consists of a set of software components executed on Windows platforms. The TOE is comprised of two parts: the McAfee VirusScan agent and the ePolicy Orchestrator. The following capabilities are not part of the evaluation: of the McAfee VirusScan and ePolicy Orchestrator for its advertised usage in updating the TOE source code, Scriptscan feature that scans JavaScript and VBScript scripts, ability to identify spyware, ability to protect against buffer overflows, and the ability to scan email.

The ability to update the TOE scanning engine and the ability to update signature files are two separate update operations. Updating the engine is not permitted in the evaluated configuration. The TOE does not by default update signature files and the administrator must set up the signature file update either manually update or periodically check for updates.

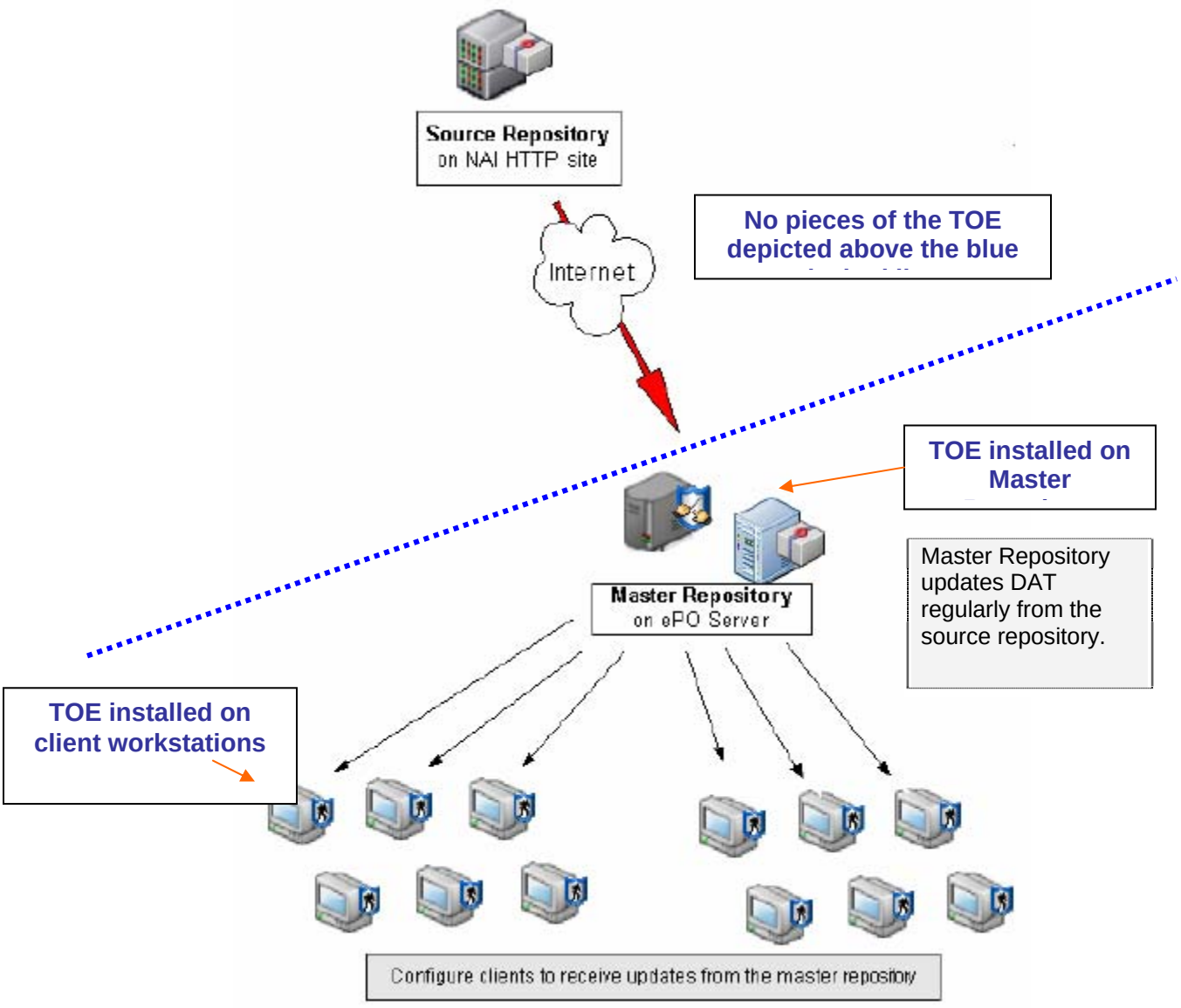
The database and underlying hardware and operating systems are not part of the TOE evaluation and the TOE relies upon their correct functionality to protect the TOE.

5 Architecture Information

The TOE consists of two software applications that execute on two different hardware platforms. These two software applications provide, audit, management, cryptographic operations, and protection of the TOE. The TOE is divided into two primary components, the ePolicy Orchestrator and VirusScan Agent.

Figure 1 - TOE Components

1. Physical Boundary



5.1 Evaluated Configuration

Table 2 - Evaluated Configuration

Component	Version	Quantity
McAfee ePolicy Orchestrator	3.6.1	1
McAfee VirusScan	8.5i	1 or more

The following table summarizes the minimum hardware and software requirements for each of the TOE components.
Server operating system configuration options (outside the scope of the TOE) for the VSE server are listed in the following table:

Operating System Options for VSE Server

Environment Operating Systems Options for VSE Server	
Operating System (one of the listed versions is required)	Windows NT Server 4.0 with Service Pack 6 or 6a
	Windows Server 2003 Standard Edition
	Windows Server 2003 Enterprise Edition
	Windows 2000 Server with Service Pack 3 or 4

Client workstation operating system configuration options are listed in the following table:
Operating System Options for VSE Client

Environment Operating Systems Options for VSE Client System	
Operating System (one of the listed versions is required)	Windows 2000 Professional with Service Pack 3 or 4
	Windows XP Home and Professional with Service Pack 1, RC2
	Windows XP Tablet PC

Other requirements for both server and client workstations include adequate disk space and are listed in Table 3. Disk Space Requirements for VSE

Disk Space Requirements for VSE
38Mb for a complete installation of all the program's features and components
22Mb used during the installation process that is then freed up when the installation is complete.
40Mb if you are using a management tool to deploy VirusScan. This space is normally freed when installation has completed depending on the management tool you are using.

The ePO server requires a dedicated computer with an Intel Pentium II-class (or higher) processor of at least 500MHz.
Other hardware and network components and configuration requirements for the ePO server (outside the scope of the TOE) are listed in the table below.
Hardware and Network Components Required for ePO Server

Hardware and Network Environment Requirements	
Memory	512mb RAM, 1GB recommended
Monitor	1024 x 768; 256 color, VGA monitor
NIC	Network Interface Card with 100mb capacity
File system	NTFS partition
IP Address	Static IP Address
Free Disk Space	250 MB minimum for a first time installation, 650 MB minimum for an upgrade; 2Gb recommended

The ePO server also requires a database that is not part of the TOE. If managing more than 5,000 clients, the database server should be a dedicated server with a dedicated network connection. If the database server uses the same computer (hardware) as the ePO server, two-thirds of the memory should be use for the database, e.g. if the server has 1GB RAM, then 660MB should be used as fixed memory for the SQL Server 2000. The database is part of the TOE environment.
Software and operating system components (outside the scope of the TOE) that are required for the ePO server are listed in table below..
Software Components and Requirements for the ePO Server

Software Components and Requirements of the Environment	
Operating System (one of the listed versions is required)	Windows 2000 Advanced Server with Service Pack 2
	Windows 2000 Server
	Windows 2003 Enterprise
	Windows 2003 Standard
	Windows 2003 Web
Database (one of the following is required)	Microsoft SQL Server 2000 Standard with SP 3
	Microsoft SQL Server 2000 Enterprise with SP 3
	Microsoft SQL Server 7 Standard with SP 3 or 4
	Microsoft SQL Server 7 Enterprise with SP 3 or 4
Browser	Microsoft Internet Explorer v6.0
Domain Controller	The server must have a trust relationship with the Primary Domain Controller (PDC) on the network.

5.2 Functionality Excluded from the Evaluation

A) The ability to protect against buffer overflows
B) The ability to identify spyware
C) The Scriptscan feature that scans JavaScript and VBScript scripts
D) The ability to update the TOE (scan engine). Note that the ability to update the virus signatures is included in the evaluation.
E) The optional Alert Manager product
F) The ability to scan email

6 Product Delivery

The TOE delivery is via download from a secure FTP site operated by McAfee.

The download site has available the correct version of software clearly labeled:

McAfee VirusScan 8.5i
ePolicy Orchestrator 3.6.1

The download site also contains the following documents for download (all were part of the evaluation):

ePolicy Orchestrator (EPO) Deploy and manage security products and network systems version 3.6 Installation Guide revision 2.0
VirusScan® Enterprise Version 8.5i Product Guide version 1.0;

VirusScan® Enterprise Version 8.5i for use with ePolicy Orchestrator® 3.5 or later Configuration Guide revision 1.0
ePolicy Orchestrator Deploy and manage security products and network systems version 3.6 Product Guide revision 3.1.
readme.txt file for ePolicy Orchestrator (there is no readme file for VirusScan)
ePolicy Orchestrator version 3.6 Quick Reference Card
Troubleshooting with Log Files Guide ePolicy Orchestrator® version 3.6
ePolicy Orchestrator Walkthrough Guide
ePolicy Orchestrator Reporting Guide

There are no other documents that are available for download.

7 IT Product Testing

Testing was performed on May 7 through May 11 at the COACT Laboratory in Columbia, MD. Two COACT employees performed the tests.

7.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of a four test PCs, hub, two McAfee VirusScan Agents, and the ePolicy Orchestrator, and attack software.

Figure 2 - Test Configuration/Setup

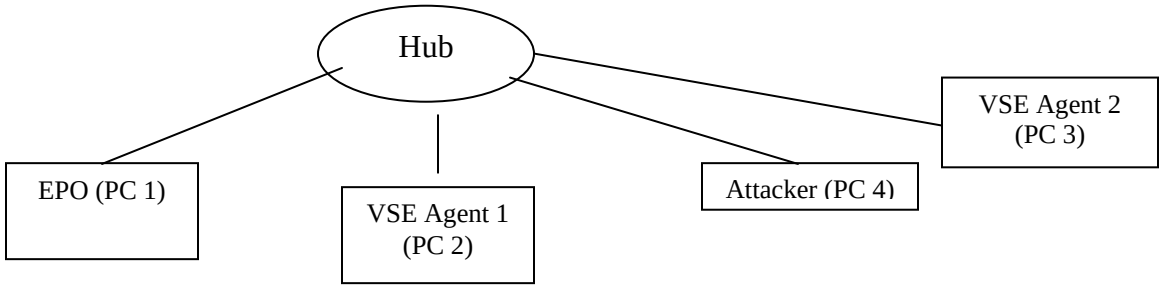


Table 3 - Test Configuration

Component	Description
ePO Server Computer	EPolicy Orchestrator 3.6.1 Pentium 4, 1.70 GHz 512 MB RAM Microsoft Windows 2000 Server Service Pack 4
Agent PC 1	VirusScan 8.5i agent Pentium 4, 1.70 GHz 384 MB RAM Microsoft Windows XP Professional Version 2002 Service Pack 2

	NmapGUI v.0.2 NeWT Security Scanner v.2.2.1 Wireshark v.99.4
Agent PC 2	VirusScan 8.5i agent Pentium 4, 3.20 GHz 2 GB RAM Microsoft Windows XP Professional Version 2002 Service Pack 2 NmapGUI v.0.2 NeWT Security Scanner v.2.2.1 Wireshark v.99.4
Attack PC	Pentium 4, 1.60 GHz 228 MB RAM Microsoft Windows 2000 Server Service Pack 4 NmapGUI v.0.2 The Dude v.2.0 Wireshark v.99.4 Tenable Nessus Security Scanner version 3.0.3 Tiger Suite v.4.5 Cain & Abel v.3.9
Hub	3Com 10Base-T Hub

7.2 Functional Test Results

The vendor chose not to use the original test suite from the development of the TOE. The vendor instead generated a customized test suite that focused on testing the specific security requirements in the Security Target. The evaluation team executed the entire developer test suite. All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the developer and CCTL proprietary report, McAfee VirusScan Functional Test Report F2-0607-002, dated 22 June 2007.

7.3 Evaluator Independent Testing

The evaluation team performed an analysis of all of the developer tests to assess the level of developer testing corresponding to each of the TSFIs. The following tests were performed during independent functional testing:

1. To ensure the workstation user and Central administrator have the capability to read all records on a workstation.
2. Ensure the workstation user and Central administrator have only the capability to query and delete audit records on a workstation.
3. Ensure the workstation ignores auditable events if the workstation audit log is full.
4. Ensure the central management system ignores auditable events if the central management system audit log is full.

The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests. All tests were performed satisfactorily and the results were as expected. The TOE passed all tests.

7.4 Evaluator Penetration Tests

The evaluators examined the developer's vulnerability analysis. The developer concluded that there are currently no known obvious vulnerabilities with the TOE. The developer checked numerous public databases including http://www.cert.org, http://www.securityfocus.com, http://nvd.nist.gov/, http://www.osvdb.org/, and http://archives.neohapsis.com/ with some vulnerabilities that have been mitigated in previous versions of the TOE.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if any additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities.

As a result of the evaluator's examination of the developer's vulnerability analysis and the independent search for obvious TOE vulnerabilities, the evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the vulnerabilities. The scope of evaluator analysis and testing included potential obvious vulnerabilities in the IT Environment that would be introduced as a result of the presence of the TOE. The following Penetration tests were performed by the evaluator:

1. Attempt to overwhelm the management console with ICMP (ping), HTTP, and FTP requests and gain unauthorized access to the TOE.
2. Although trusted channels are provided by the IT Environment TOE may not use them when communicating between distributed TOE components.

3. It may be possible to disable the TOE or PC in which the components reside (IT Environment) by attacking the exposed connections with a Penetration Scanner.
4. Attempt to circumvent the TOE enforced Policies by changing the Client UI policy associated with an agent while the agent is open and in use.
5. Attempt to compromise the TOE by spoofing an authorized agent IP address.
6. The tester will attempt to cause unprotected inter-TOE communications by corrupting the .dll providing protection (accessed as an administrator).
7. Attempt to disrupt inter-TOE communications by corrupting the .dll that provides protection.
8. It may possible to gain unauthorized access to the database housing the TOE audit records by accessing the DB through in unconventional ways.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, COACT document F2-0607-003 McAfee VirusScan Penetration Test Report, dated 22 June 2007.

7.5 Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

8 RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 augmented with ALC_FLR.2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the COACT document F2-0607-001, for the Evaluation Technical Report for McAfee VirusScan 8.5i and ePolicy Orchestrator 3.6.1, Dated 16 June 2007 contains the verdicts of “PASS” for all the work units.

The evaluation determined that the product meets the requirements for EAL 2 augmented with ALC_FLR.2. The details of the evaluation are recorded in the, Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10. VALIDATOR COMMENTS

Prospective users of this application will find a helpful collection of information in the executive summary and clarification of scope portions of this report.

The Validators found that the evidence reviewed prior and during the Final Validation Oversight Review (VOR) supported the determination that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validators agree that the CCTL presented appropriate rationales to support the evaluation results presented in Evaluation Technical Report for the" McAfee VirusScan 8.5i and Epolicy Orchestrator 3.6.1. The Validators conclude that the evaluation and Pass result for the ST and TOE are complete and correct.

11. Security Target

The VirusScan Enterprise v 8.5i, ePolicy Orchestrator Security v3.6 Target, revision 5, dated June 6, 2007, is incorporated here by reference.

12. List of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
VSE	VirusScan Enterprise
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute for Standards Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VOR	Validation Oversight Review

13. Bibliography

The following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.2, dated January 2004
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000