National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5

Report Number: CCEVS-VR-VID10421-2011
Version 1.0
Dated: 17 October 2011

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

Department of Defense
National Security Agency
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul A. Bicknell
Sunil J. Trivedi

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

Executive Summary 5
1 Identification 6
1.1 Applicable Interpretations 7
2 TOE Description 8
2.1 McAfee VirusScan Enterprise 8
2.2 McAfee ePolicy Orchestrator 9
2.3 McAfee Agent 9
3 Assumptions 10
4 Threats 11
5 Clarification of Scope 13
6 Security Functions 14
7 Architecture Information 15
8 Product Delivery and Documentation 18
9 IT Product Testing 19
9.1 Evaluator Functional Test Environment 19
9.2 Functional Test Results 20
9.3 Evaluator Independent Testing 20
9.4 Evaluator Penetration Tests 20
9.5 Test Results 21
10 Results of the Evaluation 22
11 Validator Comments 23
12 Security Target 24
13 List of Acronyms 25
14 Bibliography 26

List of Figures

Figure 1 - TOE Boundary 15
Figure 2 - Test Configuration/Setup 19

List of Tables

Table 1 - Evaluation Identifier 6
Table 2 - IT Environment Requirements for VSE and Agent 15

Table 3 - IT Environment for ePO 17
Table 4 - Test Configuration Overview 19

Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the McAfee VirusScan Enterprise 8.8 (VSE) and ePolicy Orchestrator 4.5 (ePO) at EAL2. 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 17 October 2011. 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 3.1, Revision 2, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5.

McAfee VirusScan Enterprise 8.8 (VSE) and ePolicy Orchestrator 4.5 (ePO) is a software package designed to protect Microsoft Windows-based desktop and server computers 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 entities, removing them, and reporting on them.
The management capabilities for VSE are provided by ePO. ePO manages McAfee Agents and VSE software that reside on client systems. By using ePO you can manage a large enterprise network from a centralized system. ePO also provides scheduling capabilities to distribute updated VSE security policies and maintains audit files.

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

McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5
Protection Profile	U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments, version 1.2, dated 25 July 2007
Security Target	McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator Security Target, version 1.3.
Evaluation Technical Report	McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5 Evaluation Technical Report, Document No. F2-1011-001, Dated 6 October 2011.
Conformance Result	Part 2 extended and EAL2 Part 3 conformant
Version of CC	CC Version 3.1 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on December 17, 2008.
Version of CEM	CEM Version 3.1 and all applicable NIAP and International Interpretations effective on December 17, 2008.
Sponsor	McAfee, Inc. 2821 Mission College Blvd.

McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5	
	Santa Clara, CA 95054
Developer	McAfee, Inc. 2821 Mission College Blvd. Santa Clara, CA 95054
Evaluator(s)	**COACT Incorporated** Greg Beaver Dave Cornwell Jonathan Alexander
Validator(s)	**NIAP CCEVS** Paul A. Bicknell Sunil J. Trivedi

1.1 Applicable Interpretations

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

NIAP Interpretations

FAU_GEN.1-NIAP-0347	Audit Data Generation
FAU_GEN.2-NIAP-0410	User Identity Association
FAU_STG.NIAP-0414-NIAP-0429	Site-Configurable Prevention of Audit Loss

International Interpretations

None

2 TOE Description

The TOE consists of the following three main components:

A) McAfee VirusScan Enterprise 8.8 – The VSE software provides protection from viruses, worms, Trojans, as well as unwanted code and programs

B) McAfee ePolicy Orchestrator 4.5 - ePO distributes and manages agents that reside on client systems. By using ePO you can manage a large enterprise network. ePO provides the management interface and functionality for the administrators of the TOE. It also provides centralized audit collection and review functionality.

C) McAfee Agent 4.5 – The McAfee Agent is a vehicle of information and enforcement between the ePO server and each managed system. It provides common communication functionality between ePO and all of McAfee's product-specific software (such as VSE).

McAfee VirusScan Enterprise 8.8 (VSE) and ePolicy Orchestrator 4.5 (ePO) is a software package designed to protect Microsoft Windows-based desktop and server computers 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 entities, removing them, and reporting on them.
The management capabilities for VSE are provided by ePO. ePO manages McAfee Agents and VSE software that reside on client systems. By using ePO you can manage a large enterprise network from a centralized system. ePO also provides scheduling capabilities to distribute updated VSE security policies and maintains audit files.

The TOE also contains the Database Capacity Monitor Extension 1.0. This component is used to monitor the storage capacity of the database used by the TOE and can warn the administrator when that database has reached a specified size.

Communication between the distributed components of the TOE is protected from disclosure and modification by cryptographic functionality provided by the operational environment.

The main TOE components are further described in the following sections:

2.1 McAfee VirusScan Enterprise

The VSE software is installed on client machines. The VSE software provides protection from viruses, worms, Trojans, as well as unwanted code and programs. Scanning occurs when files are either read from, or written to the computer the TOE client agent is installed on. Identification of a virus, worm, or Trojan is referred to as an "infection." When an infection occurs, the TOE takes certain actions depending on what has been configured. There are Primary and Secondary actions that the TOE takes when an infection occurs. The primary actions that the TOE takes when an infection occurs:

- Cleaning of files automatically (after quarantining the original)
- Denying access to infected files

- Move infected files to a quarantine folder in email scanning. For stored files, the file is quarantined off-host before being deleted

Secondary actions are actions that the TOE takes if the Primary action fails. Secondary actions that the TOE takes on discovery of an infection include:

- Move infected files to a quarantine folder
- Denying access to infected files (quarantine)
- Delete infected files automatically

When a virus is detected (e.g. an infection occurs) the On-Access Scan Messages box pops up and remains on the screen until the user session ends, or until the alert is acknowledged.

2.2 McAfee ePolicy Orchestrator

The ePO application is installed on a dedicated centralized server. ePO distributes and manages agents that reside on client systems. By using ePO you can manage a large enterprise network. ePO provides the management interface and functionality for the administrators of the TOE. It also provides centralized audit collection and review functionality.

The ePO requires a database but the DBMS is not part of the TOE.

Using ePO, an alert indicating a virus can be configured to display on the screen of the Central Administrator's console if a session is active (the Virus Alert List Box). The alert identifies the system where the infection has occurred, the name of the virus, and the action taken by the TOE.

2.3 McAfee Agent

The McAfee Agent is installed on client machines. The McAfee Agent is a vehicle of information and enforcement between the ePO server and each managed system. It provides common communication functionality between ePO and all of McAfee's product-specific software (such as VSE).

3 Assumptions

The assumptions listed below are assumed to be met by the environment and operating conditions of 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.

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.

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.

4 Threats

The threats identified in the following table sections are addressed by the TOE and/or Operating Environment. The following threats are addressed by the TOE and IT environment, respectively.

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 cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.

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 may result in incorrect TOE behavior being undiscovered 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
The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.

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.

5 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 extended in this case).
- As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- TOE uses cryptographic operation only for assuring integrity of VirusScan anti-virus packages with a SHA-1 hash value distributed to the client workstations. TOE depends on IT environment for providing secure communication between distributed components. The cryptography used in this product was not analyzed or tested to conform to cryptographic standards during this evaluation.

6 Security Functions

The TOE's Security Functions are:

A) **Audit –** The OnAccess Scan Log provides audit viewing capabilities on the client for that system. Audit information is concurrently generated for transmission to the ePO management databases. Audit logs for all clients can be reviewed from the ePO console.

B) **Cryptographic Operation** – VirusScan anti-virus packages are distributed to the workstation with a SHA-1 hash value used to verify the integrity of the package.

C) **Management** – ePO 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.

D) **Virus Scanning and Alerts** – VSE provides the following functionality related to virus scanning and alerts:

1. Access Protection - This function protects ports, files, the registry and processes resident in memory from intrusions by restricting access to them. You can create rules to block either inbound or outbound ports, and by doing so, restrict access to files and residual data allocated in memory. If an outbreak occurs, the administrator can restrict access to the infected areas to prevent further infection until new signature files are released.

2. Email Scanning - This function provides scanning of messages and databases in order to identify viruses, worms, and Trojans for the purpose of removing them and reporting on them.

3. Automatic Updates – Allows signature (DAT) files to be updated automatically per the configured schedule.

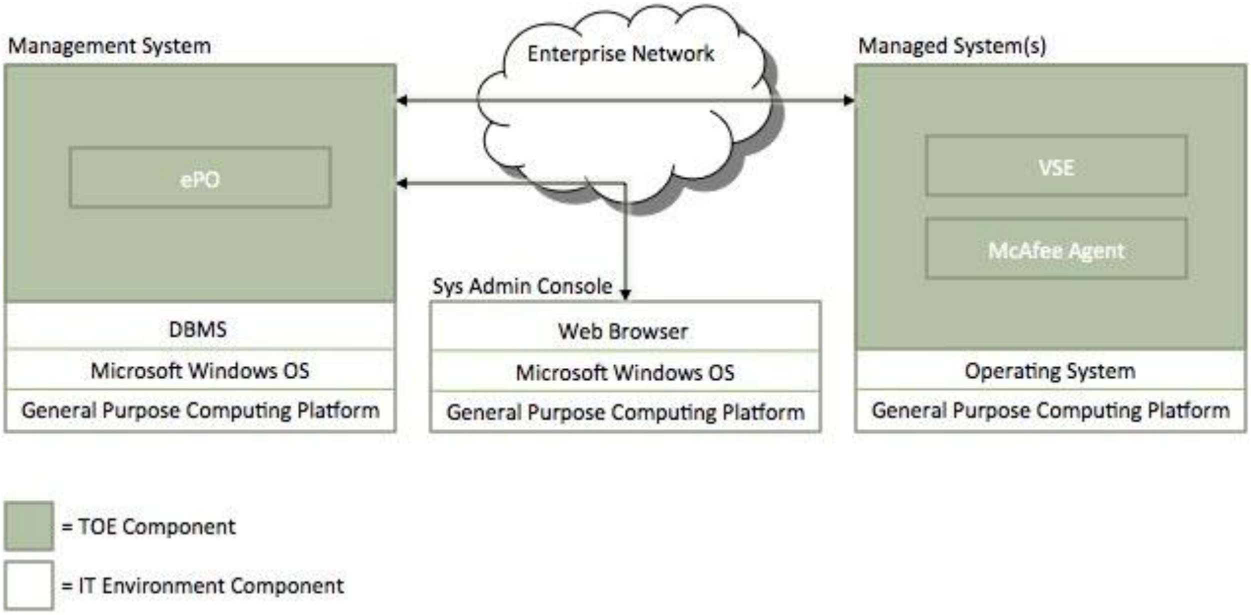
7 Architecture Information

The components of the TOE are installed on general-purpose computers. The McAfee VirusScan Enterprise and McAfee ePolicy Orchestrator are installed on two separate PCs connected via a network. The McAfee Agent is installed on the same PC as the McAfee VirusScan Enterprise. The physical boundary of the TOE is/are the software applications themselves and the APIs that they expose.

The logical boundary of the TOE is the application software that corresponds to version 8.8 of the McAfee VirusScan Enterprise, v4.5 of the McAfee ePolicy Orchestrator and v4.5 of the McAfee Agent.

See Figure 1 below.

Figure 1 - TOE Boundary



The IT environment of the TOE for McAfee VirusScan Enterprise 8.8 and McAfee Agent 4.5 includes the following:

Table 2 - IT Environment Requirements for VSE and Agent

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium or Celeron processor running at a minimum of 166 MHz or Pentium II processor running at a minimum of 350 MHz
Memory	128MB RAM (minimum) for a Pentium or Celeron processor running at 166 MHz and 256MB RAM (minimum) for a Pentium II processor running at 350 MHz
Free Disk Space	240 MB

COMPONENT	MINIMUM REQUIREMENTS
Browser	Microsoft Internet Explorer version 6.0 or later
Operating System	**Server Operating Systems:** Microsoft Windows 2000 Server with SP4 Microsoft Windows 2000 Advanced Server with SP4 Microsoft Windows 2000 Datacenter Server with SP4 Microsoft Windows Server 2003 Standard (32-bit and 64-bit) with SP1 or SP2 Microsoft Windows Server 2003 Enterprise (32-bit and 64-bit) with SP1 or SP2 Microsoft Windows Server 2003 Web Edition (32-bit and 64-bit) with SP1 or SP2 Microsoft Windows Server 2003 R2 (32-bit and 64-bit) Standard, Enterprise, Web Edition Microsoft Windows Server 2003 R2 Datacenter Edition (32-bit and 64-bit) Microsoft Windows Storage Server 2003 Microsoft Windows Server 2008 (32-bit and 64-bit) Microsoft Windows Server 2008 Datacenter (32-bit and 64-bit) Microsoft Windows Server 2008 Datacenter (32-bit and 64-bit) Microsoft Windows Server Core 2008 (32-bit and 64-bit) Microsoft Windows 7 Home Premium, Professional, and Ultimate (32 and 64 bit) **Workstation Operating Systems:** Microsoft Windows 2000 Professional with SP4 Microsoft Windows XP Home with SP1, SP2, or SP3 Microsoft Windows XP Professional with SP1, SP2, or SP3 Microsoft Windows XP Tablet PC Edition with SP3 Microsoft Windows Vista Home Basic Microsoft Windows Vista Home Premium Microsoft Windows Vista Business Microsoft Windows Vista Enterprise Microsoft Windows Vista Ultimate Microsoft Windows 7 Home Premium, Professional, and Ultimate (32 and 64 bit)
Additional Software	Microsoft Windows Installer (MSI) version 3.1 or later
Network Card	Ethernet, 10Mb or higher

The IT environment of the TOE for McAfee ePolicy Orchestrator includes the following:

Table 3 - IT Environment for ePO

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium III-class or higher; 1GHz or higher
Memory	1 GB RAM
Free Disk Space	1 GB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2003 Enterprise with Service Pack 2 or later Windows Server 2003 Standard with Service Pack 2 or later Windows Server 2003 Web with Service Pack 2 or later Windows Server 2003 R2 Enterprise with Service Pack 2 or later Windows Server 2003 R2 Standard with Service Pack 2 or later Windows Server 2008 Enterprise Windows Server 2008 Standard
DBMS	SQL Server 2005 SQL 2005 Express SQL 2008 SQL 2008 Express
Additional Software	MSXML 6.0 Internet Explorer 7 or 8, or Firefox 3.0 .NET Framework 2.0 Microsoft Visual C++ Redistributable Microsoft Visual C++ Redistributable - x86 9.0.21022 MDAC 2.8 Microsoft updates MSI 3.1 RSA Crypto-C ME 2.0 RSA Crypto-J 4.0
Network Card	Ethernet, 100Mb or higher
Disk Partition Formats	NTFS
Domain Controllers	The system must have a trust relationship with the Primary Domain Controller (PDC) on the network

8 Product Delivery and Documentation

Customers obtain the TOE via a website that permits them to select the version to download. A Grant Code is provided to the customers that restricts access to relevant downloads. The customer performs specific steps to download VSE, ePO, and the Database Capacity Monitor Extension, as well as the TOE documentation. HTTPS is used for all downloads.

The following documentation is downloaded from the product download site:

A) McAfee ePolicy Orchestrator 4.5 Product Guide

B) McAfee ePolicy Orchestrator 4.5 Installation Guide

C) McAfee VirusScan Enterprise 8.8 Software Product Guide

D) McAfee VirusScan Enterprise 8.8 Software Installation Guide

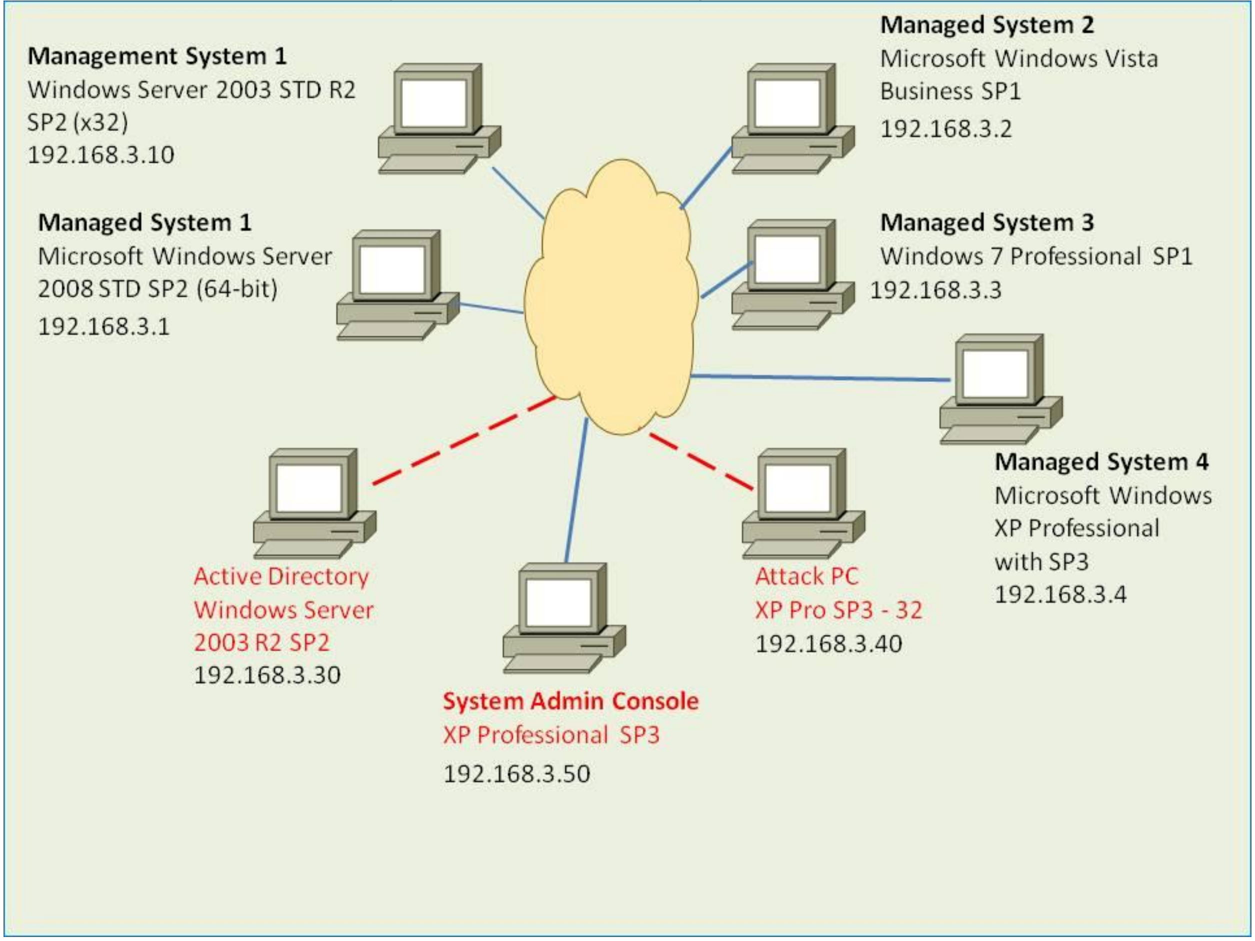
9 IT Product Testing

Testing was completed on September 3, 2011 at the COACT CCTL in Columbia, Maryland. COACT employees performed the tests.

9.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of the following test bed configuration.

Figure 2 - Test Configuration/Setup



An overview of the purpose of each of these systems is provided in the following table.

Table 4 - Test Configuration Overview

System	Purpose
Management System 1	System on which the ePO management system is installed.
Managed System 1	The managed host with Microsoft Windows Server

System	Purpose
	2008 (64-bit) installed.
Managed System 2	The managed host with Microsoft Windows Vista Business installed.
Managed System 3	The managed host with Windows 7 Professional installed.
Managed System 4	The managed host with Microsoft Windows XP Professional SP3
Active Directory	Computer to provide the Active Directory and DNS Server services.
Attack PC	Computer from which the penetration tests will be launched against the TOE.
System Admin Console	Computer from which the ePO is managed through the Web browser.

9.2 Functional Test Results

The evaluator repeated all of the developer functional tests. All of the developer's functional tests passed.

9.3 Evaluator Independent Testing

The tests chosen for independent testing allowed the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests was to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allowed for a finer level of granularity of testing compared to the developer's testing, or provided additional testing of functions that were not exhaustively tested by the developer. The tests allowed specific functions and functionality to be tested. The tests reflected knowledge of the TOE gained from performing other work units in the evaluation. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

9.4 Evaluator Penetration Tests

The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE. The evaluator searched the Internet for potential vulnerabilities in the TOE (McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5). Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerability. These searches led to the identification of 7 potential vulnerabilities in the TOE. A suite of penetration tests were created to investigate these potential vulnerabilities.

9.5 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.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the McAfee, Inc. VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5 TOE meets the security requirements contained in the Security Target.

The criteria against which the McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The COACT, Inc. Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5 TOE is EAL2 augmented with ALC_FLR.2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed on 17 October 2011.

11 Validator Comments

The Validators were satisfied with the evaluation team’s evaluation and testing efforts. The validators did not identify any gaps or missing information. The CCTL was well prepared, and the material was complete and correct.

12 Security Target

Security Target McAfee VirusScan Enterprise 8.8 and ePolicy Orchestrator 4.5, Document Version 1.3, July 6, 2011.

13 List of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CM	Configuration Management
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
GB	Giga-Byte
GUI	Graphical User Interface
I&A	Identification and Authentication
IT	Information Technology
MB	Mega-Byte
NIAP	National Information Assurance Partnership
OS	Operating System
OSP	Organizational Security Policy
PC	Personal Computer
PP	Protection Profile
RAM	Random Access Memory
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSFI	TOE Security Function Interface

14 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 3.1, Revision 3, dated July 2009
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 3.1, Revision 3, dated July 2009
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 3.1, Revision 3, dated July 2009
- Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, dated July 2009
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000