National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Cisco Security Agent 4.5.1.655

Report Number: CCEVS-VR-07-0020

Dated: 26 February 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

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

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

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the Cisco Security Agent 4.5.1.655 at EAL 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 12 December 2006. 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 2.1, 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.

CSA is a software-based intrusion detection and intrusion prevention application comprised of two essential components: the Management Center that installs on designated Windows systems and the Agent that installs on server and desktop Windows systems across the network. The security functionality associated with server and desktop(host) agents are identical, and this document refers to both types generically as Agents. The Management Center enables single-point administration of the Agents that are installed on desktops and servers throughout the network. The TOE consists of certain specific components of the software installed on the MC and software on the agents. The TOE includes a single MC and one or more [1] Agents. Functioning under specific policies to be defined by the needs of the deploying organization, the Management Center and Agent(s) work in parallel to defend against the proliferation of attempted intrusions and attack scenarios across networks and systems.

The TOE relies upon the underlying hardware and operating systems of the Management Center and Agent platforms and additional supporting software that is not included within the scope of this evaluation. Further details of the TOE architecture and the TOE boundary are described in Section 6 Architecture Information.

Significant portions of the text in this document has been taken from the vendor Security Target and the evaluation team reports.

2 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

[1] Vendor claims to support of up to 100,000 Agents, but that capability was not covered by the evaluation.

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 Cisco Security Agent 4.5.1	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco Security Agent 4.5.1.655
Protection Profile	N/A
Security Target	Cisco Security Agent Version 4.5.1 Security Target,, Document EDCS-507896, date April 4, 2007
Evaluation Technical Report	Evaluation Technical Report for the Cisco Security Agent(CSA) 4.5.1, Document No. F2-0307-003, Dated April 26, 2007
Conformance Result	Part 2 conformant and EAL2 Part 3 conformant
Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on June 16, 2004
Version of CEM	CEM Version 2.1 and all applicable NIAP and International Interpretations effective on February 2, 2005
Sponsor	Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134
Developer	Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134
Evaluator(s)	**COACT Incorporated** Diann Vechery Dawn Adams Brian Pleffner Christa Lanzisera Anthony Busciglio
Validator(s)	**NIAP CCEVS** Dr. Jerome Myers Tom Murphy Dustin Myers

2.1 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-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0426 – Content of PP Claims Rationale
I-0427 – Identification of Standards

International Interpretations

None

3 Security Policy

The TOE is a software-based intrusion detection and intrusion prevention application. The primary security policies that it offers are support for user data protection, logging and review of events, and centralized management.

3.1 User Data Protection

The TOE provides data protection by enhancing the underlying platforms access control on files, process memory space, and the Windows Registry. The TOE enforces an administratively defined Program Access Control Policy that determines whether applications can execute. Additionally, when the TOE Agent detects certain types of potentially malicious activity, the Agent will intercept the offending process and prompt the End User for guidance. These features provide protection against email-worms, keystroke logging, code injection, and buffer overflows.

Information flow to and from the machine through the network interface is also controlled by the TOE. This capability enables detection and/or protection from network scans, packet-sniffers, Syn-flood attacks, and malformed packet attacks.

When an Agent is installed, it registers with the Management Center. At this time, the security policy is given to the Agent. Also, the Agent polls the Management Center at configurable intervals for policy updates.

3.2 Security Audit Policy

The TOE generates records of Program Access Control Policy enforcement, malicious activity, and system management events that are then logged by the Agent into secured disk space on the Agent host. These event records are also sent to the Management Center.

3.3 Security Management

The TOE provides features for central administration of the TOE. Access to the MC is provided by the IT Environment through a Web interface.. The IT Environment ensures that only properly

identified and authenticated administrators can access the MC. Within the TOE portion of the MC, the Agents can be logically assembled into groups, to which security policies can be attached. The Web server and Web application are part of the Management Center installation. These configurations are then deployed to the Agents via secure HTTP.

The Management Center also provides the capability to generate reports based upon the event logs collected from the Agents.

3.4 Protection Profile Claim

This Security Target does not claim conformance to any registered Protection Profile.

4 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.

A complete listing of the assumptions is provided in the Security Target. The follow is only a summary of the most significant assumptions:

4.1 Personnel Assumptions

A.NOEVILADMIN	The Administrator is non-hostile and follows all administrator guidance when using the TOE.
A.NOEVILUSERS	Authorized users of Agent hosts (End Users) are non-hostile and do not attempt to attack or subvert the CSA system and its policy.
A.PLATFORM_A	The Administrator will install and configure the platforms protected by the Agents in conformance with Table 1.
A.PLATFORM_MC	The Administrator will install and configure the platform used to host the Management Center in conformance with Table 1.
A.INSTALL	The Administrator will install and configure the hardware, operating systems, and software required to support the TOE in conformance with the CSA installation guides.

4.2 Physical Assumptions

A.ENVIRON_A	The Agent will be located in an environment that provides physical security.

A.ENVIRON_MC	The Management Center will be located in an environment that provides physical, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware.

4.3 IT Environment Assumptions

None.

4.4 Threats

The following threats are addressed by the TOE and IT environment, respectively.

4.4.1 Threats Addressed by the TOE

The TOE addresses the threats discussed below. The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

T.KEYLOG	A malicious program may be executed on a system protected by the TOE that attempts to monitor all keystrokes entered by an End User to gain password information or other sensitive data.
T.PORTSCAN	An attacker may send network traffic that is received on a system protected by the TOE that attempts to scan ports as a means to gather information about or identify weaknesses in systems protected by the TOE.
T.SYNFLOOD	An attacker may send network traffic that is received on a system protected by the TOE that attempts to SYN-flood a server system protected by the TOE. When a TCP/IP connection request is received from a return address that is not in use, a useless, half-open connection will persist for a period of time. Having too many of these connections will prevent legitimate connections from being established.
T.MALPACK	An attacker may send network traffic that is received on a system protected by the TOE that attempts to exercise a bug in the operating system's network implementation. This type of attack can cause the system to crash.
T.OVERFLOW	A program may be executing on a system protected by the TOE that reads data from the network which causes an overflow of memory buffers. If this happens the network data may contain and execute arbitrary code with full privilege on the system.
T. WORM	A malicious email attachment may execute on a system protected by the TOE that attempts to send itself to other networked systems. The malicious execution may also modify Windows Registry keys, write its own script files or modify existing files on the system protected by the TOE.
T.TROJAN	A malicious program may be executed on a system protected by the TOE that attempts to inject malicious code into the memory space of another process.

T.PWDTHEFT	A malicious program may be executed on a system protected by the TOE that attempts to access a restricted area of the Windows Registry that contains the hashes of system passwords.
T.COVERT	A malicious program may be executed on a system protected by the TOE that attempts to send data covertly over the network utilizing unsolicited ICMP response packets.
T.REGACC	A malicious program may attempt to gain unauthorized access to the Windows Registry and disclose or corrupt sensitive information stored there.
T.FILEACC	A malicious program may attempt to gain unauthorized access to the file system and disclose or corrupt sensitive information stored in files.
T.NETACC	A malicious program may attempt to gain unauthorized access to network functions such as sending information, creating server sockets to receive information, setting the network interface to promiscuous mode, or sending ICMP packets for the purpose of subverting a host protected by the TOE.
T.COMACC	A malicious program may attempt to gain unauthorized access to Component Object Model components in order to use their functions to carry out some part of an attack for the purpose of subverting a host protected by the TOE.
T.BYPASS	A malicious subject on a platform protected by the TOE may access the TSF or TSF data without invoking the TSF.

4.4.2 Threats Addressed by the Operating Environment

The TOE relies upon the IT Environment to protect the server platform on which the TOE resides. The associated threats that are addressed by the IT Environment Requirements are:

TE.TAMPER	A malicious subject may gain unauthorized access to TSF data.
TE.INTRCPT_A	A malicious subject may intercept or modify unencrypted network traffic between the Management Center and the Agent for the purpose of subverting the TOE or a host protected by the TOE.
TE.INTRCPT_MC	A malicious subject may intercept or modify unencrypted network traffic between the Management Center and the Administrator's HTML browser for the purpose of subverting the TOE or a host protected by the TOE.
TE.UNAUTH	An attacker may attempt to assume the identity of the Administrator in order to modify the TOE configuration.

5 Clarification of Scope

The TOE consists of a set of components from a software product. The TOE relies upon properties of the underlying hardware, operating systems, and databases to provide support to

some of its security functions. Each of these items is considered to be part of the IT Environment and is hence not covered by this evaluation. Portions of the IT Environment (Web Server for MC and Cisco Works VPN/Security Management System(VMS) are installed as part of the TOE installation.

The evaluated configuration includes the Management Center executing on a Windows platform (with VMS) and Agents executing on Windows hosts. The vendor provides Server Agents for Solaris and Linux, but those product are not covered by this evaluation.

6 Architecture Information

6.1 Overview

CSA consists of a single Management Center (MC) for CSA and between one and 100,000 Agents. Both Host Agents and Server Agents are supported. The security functionality associated with them is identical, and this document refers to both types generically as Agents. The Management Center enables single-point administration of the Agents that are installed on desktops and servers throughout the network.

6.1.1 Management Center

The CSA Management Center and an Agent, as represented in Figure 1, represent the TOE. The Report Generator, GUI Page Generator, Configuration Manager, and Global Events Manager are the only components of the MC that are included within the scope of the TOE evaluation. CiscoWorks VPN/Security Management System (VMS) provides support infrastructure to the Management Center for CSA. It provides Identification & Authentication (I&A) functionality when administrators connect to the system, and performs session locking and re-authentication.

TOE includes those components of the MC that push security policies to the agents and coordinate the events it receives back from the agents. The mechanisms that are required to perform those tasks are described here as part of the CSA MC architecture.

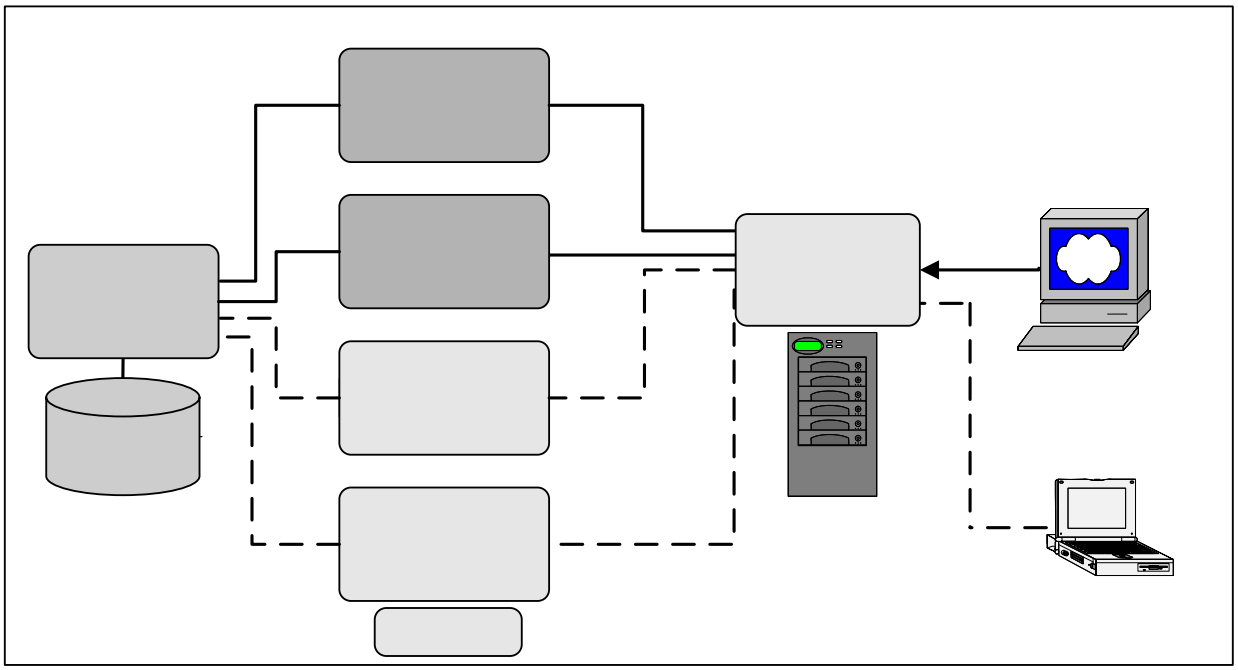

Figure 1: Management Center Architecture

The web browser, shown on the right in Figure 1, represents any web browser on any system across an enterprise from which administrators can securely access the CSA MC web-based interface. Communications between the web browser and the web server occur over SSL, allowing administrators to securely access the database of rule configurations from any location.

The web server provides the means of communication between the web browser and all other CSA MC system components. The web server displays reporting information, configuration version data, and event logging data. The reports are generated by the TOE and displayed by the IT Environment.

It is through the web server that the agents installed on systems across an enterprise can exchange data with the CSA MC configuration manager and the global event manager. When agents poll in to CSA MC for rule set updates, it is the configuration manager that pulls the rules from the database and distributes them to the particular agents for which they are intended. Agents also send events to the global event manager which stores this information in the central SQL server database.

The SQL server database is the central repository for configuration data (host agents, groups, file rules, network rules, registry rules, etc.) created by the administrator and for the system event information provided by the agents. It is in this database that rules and information on system groupings are stored when the administrator generates rules and policies through the web-based interface. When reports are requested by the

administrator, the report generator component gathers rule and event data kept in the database and produces reports using this information.
All information (rule configurations, event logs, etc.) passed between CSA MC and the agents distributed across your enterprise is encrypted providing a secure communication channel for the exchange of data.

The TSF data of the Management Center are the Agent registrations, Agent grouping and policy configurations, the event logs, and a public/private-key certificate. These assets are stored in the database shown in Figure 1. The database infrastructure (binaries and raw data) is protected by the Agent on this host. Access to use the database is also restricted by the Agent to only the Management Center application. The binaries and configuration files for the Management Center are also valuable assets of the TOE. These binaries and configuration files are located within the CSA install directory and are protected by the Agent on this host.

The sensitive capabilities of the Management Center are the ability to publish Agent security policies and the ability to generate reports. These capabilities are only configurable from within the Web-based administration tool. Administration sessions are authenticated and use secure HTTP. The Web server's infrastructure (binaries and published resources) is protected by the Agent on this host. Access to administer the Web server is also restricted to only the Management Center application.

6.1.2 Agent Components

Figure 2 illustrates the security architecture of an Agent host in the TOE configuration. The dark shaded areas represent the TOE portion of the Agent host architecture. Figure 2 shows the agent in terms of its system components, displaying where those components operate in relation to general system functions. For example, the interceptors shown in the diagram install and work at the kernel level.

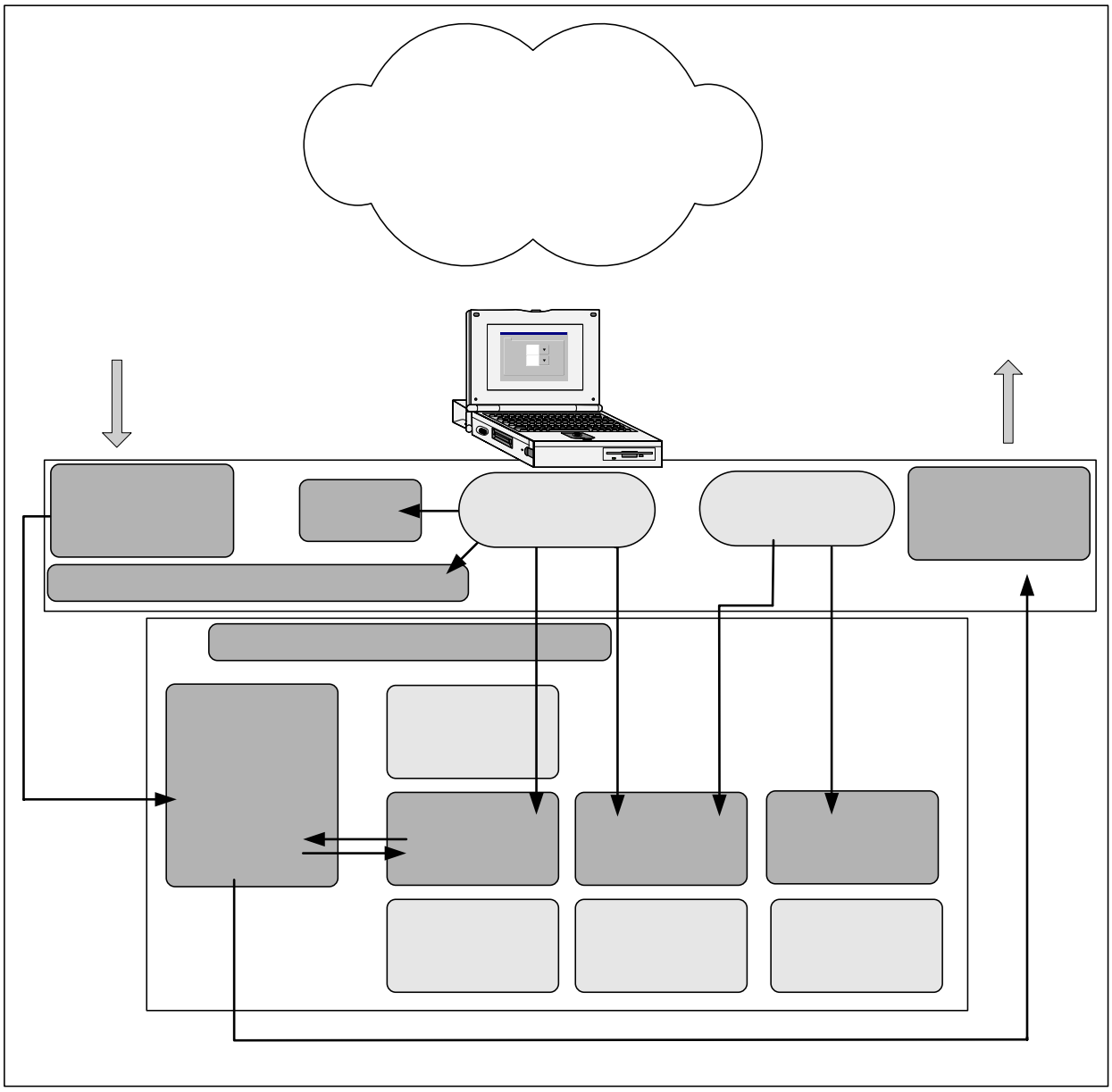

Figure 2: Cisco Security Agent Components (Windows)

Starting from the left side of the diagram, the agent **policy manager** receives the rules configured by the administrator from CSA MC. These rules are sent to the agent's **rule/event correlation** engine. If a rule set already exists there, these rules are updated or replaced with the newest rule set.

The **interceptors** do as their name indicates, they intercept key actions that are attempted on the system and check the action in question against the rule correlation engine to determine if a rule set allows or denies it. Based on the information the interceptors receive, they either allow the action to take place or they stop it cold. Actions are stopped based on certain criteria that are part of each rule and consequently each interceptor acts based on a component-targeted set of criteria.

For example, the **network application interceptor** controls which applications are allowed to communicate with the network, while the **network traffic interceptor** provides system hardening features such as SYN flood protection and port scan detection. The **file interceptor** controls which applications can read and/or write to specified system files and directories. The **registry interceptor** controls system behavior, preventing applications from writing to particular registry keys. All of these controls can be as broad or as granular as necessary.

As the interceptors are allowing or denying actions, they produce an event each time a rule set is triggered by a system action. These events are stored in the rule/event correlation engine which forwards them on to the **local event manager** and **global event manager**. Events are also stored in the NT event log or W2K event viewer on the agent system.

The sensitive assets of the Agent are the security policy, the events log, and the binaries of the Agent. The Agent always enforces a built-in self-protection policy as well as the explicit, downloaded policy. The built-in policy controls write access to all of the data files and binaries in the Agent install directory. This includes the events log, the security policy, and the binaries. The built-in policy also protects the DLLs and drivers that are in stored in appropriate directories of the operating system. This feature also protects write access to memory and disk space that is vital to Agent operation. The Agent on the Management Center host provides the same protection for the Management Center.

The sensitive capabilities of the Agent are the ability to receive security policies from the Management Center, the ability to send events to the Management Center, and the ability to enforce its security policy. The first two capabilities are communications between the Agents and the Management Center. These communications utilize the secure HTTP capability provided by the Web server to keep the data from being intercepted. In addition, policy enforcement is protected by the assumption that the operating system always invokes the TSF and provides dedicated process space for the TOE.

6.2 TOE Boundaries

The TOE consists of a set of software components of the MC and components of the Agents. The items listed in Table 2: TOE Components comprise the physical TOE. The TOE does not include any component that is not specified in this table. Specifically, the TOE does not include any hardware, any operating system which TOE operates upon, any Web server, any Database, any network, or any applications running on the Agent host. The table is broken down into components for each installation type: the Management Center and the Agent.

Table 2: TOE Components

Installation	Physical Component
Management Center	Report Generator Web Application GUI Page Generator Configuration Manager Global Event Manager
Agent	Rule/Event Correlation Engine AgentPolicy Manager Local Event Manager Buffer Overflow/COM Component Interceptor File Interceptor Registry Interceptor Network Application Interceptor Network Traffic Interceptor

The logical boundaries of the TOE include security features of the Agent and the secured interfaces to the Management Center. The logical boundary of the TOE consists is defined by the following security features:

User Data Protection
Security Auditing
Security Management

The basic properties of these features are already described in Section 3: Security Policy. Further details may be found in the Security Target.

6.3 IT Environment

The TOE requires the hardware and software listed in Table 3: Platform Requirements for IT Environment be provided for the IT Environment. Additional components of the IT environment (e.g. VMS) are included with during the TOE installation.

Table 3: Platform Requirements for IT Environment

Component	Description
Management Center Host	PC with 1GHz or faster processor CD-ROM drive 100Base-T or faster connection 1 GB RAM 9 GB available disk drive space 2 GB virtual memory Color monitor with video card capable of 16-bit color Windows 2000 Server or Advanced Server, Service Pack 4
Web Browser	Internet Explorer v. 6.0 with Service Pack 1 Supporting 128 bit encryption Cookies enabled, maximum medium setting for Internet Security JavaScript enabled.
Agent Host	Intel Pentium 200MHz or faster processor 128 MB system memory or greater 15 MB disk space or greater One Ethernet interface supporting TCP/IP Windows 2000 Professional, Server, or Advanced Server, Service Pack 0, 1, 2 or 3 -OR- Windows NT 4.0 Workstation, Server, or Enterprise Server, Service Pack 4 or higher -OR- Windows XP (Professional English 128 bit), Service Pack 0 or 1 -OR- Windows 2003

7 Product Delivery

The TOE delivery includes a CD that contains the following documents that were included within the scope of the evaluation:

- Installing Management Center for Cisco Security Agents 4.5.1
- Release Notes for Management Center for Cisco Security Agents 4.5.1 Revision 1
- Using Management Center Security Agents 4.5.1
- Using Management Center for IDS Sensors 2.0

In addition, there are some documents delivered on the CD that were not covered by the evaluation. The user is cautioned that they should not rely upon the contents of those documents for information about using the product in the evaluated configuration. The specific documents not covered by the evaluation are:

- Release 3.5
- User Guide for Resource Manager Essentials Software Release 3.5 CiscoWorks
- Readme for Incremental Device
- Update (IDU) 12.0 on Resource
- Manager Essentials 3.5 (Windows)
- Using Monitoring Center for Security 2.0 For Windows and Solaris October 2004

This is all of the documentation that is delivered to the end-user with the evaluated product.

8 IT Product Testing

Functional and Penetration testing activities were completed at the end of November 2006. After appropriate analysis and test preparation, the actual testing was conducted during the period of November 27-29, 2006 at a vendor facility in Massachusetts. One evaluator from the CCTL performed the final testing.

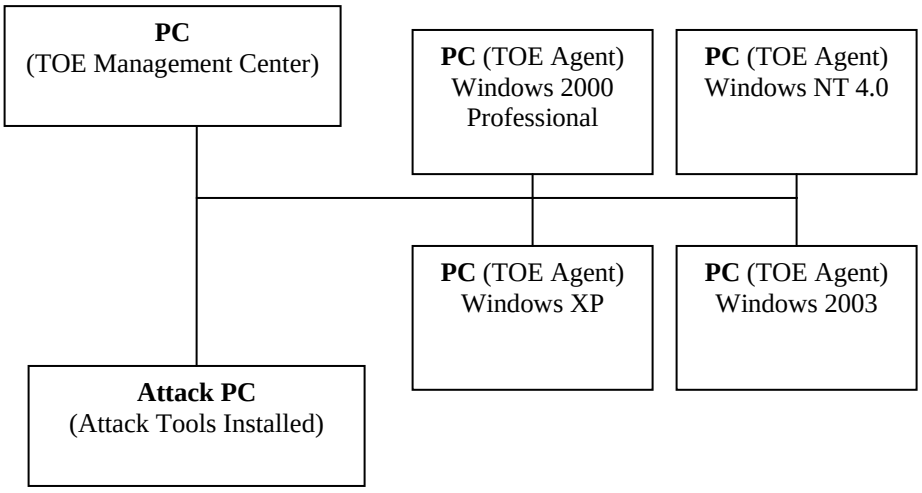

Figure 3: Test Configuration

8.1 Evaluator Functional Test Environment

The evaluation team analysis of the vendor functional testing resulted in a conclusion that the vendor had provided a comprehensive set of tests. There were no specific areas of functional testing that stood out as needing special emphasis during evaluation team testing. As a result, the evaluation team elected to repeat a subset of the vendor tests that exercised each of the claimed TOE SFRs, at least once. The evaluation team repeated a total of twelve of the forty-six tests from the vendor test suite.

Testing was performed on a test configuration consisting of six PCs connected through a Hub. Figure 3: Test Configuration illustrates the network configuration used for testing The one PC was configured as the MC and four of the other PCs were configured with the Agent package. Distinct hardware platforms were chosen to test the TOE on each of the different base platforms covered by the scope of the evaluation. One additional PC was used for penetration testing. The hardware and software configurations for the server and client for functional testing is detailed below in Table 4 : Test Bed Configuration Details.The table shows the actual hardware/software configuration the CCTL used to conduct the vendor tests and independent tests. Appropriate analysis was performed and evidence presented to ensure that the results from testing on this test configuration applied to all variant configurations of the evaluated TOE.

Table 4 : Test Bed Configuration Details

System	Hardware Minimum Required	Minimum Software Requirements
Agent PC 1	Intel Pentium 2.5GHz processor 1 GB RAM 20 GB disk space or greater One Ethernet interface supporting TCP/IP	Windows 2000
Agent PC 2	Intel Pentium 2.5GHz processor 1 GB RAM 20 GB disk space or greater One Ethernet interface supporting TCP/IP	Windows NT 4.0
Agent PC 3	Intel Pentium 2.5GHz processor 1 GB RAM 20 GB disk space or greater One Ethernet interface supporting TCP/IP	Windows XP
Agent PC 4	Intel Pentium 2.5GHz processor 1 GB RAM 20 GB disk space or greater One Ethernet interface supporting TCP/IP	Windows 2003
MC PC	Intel Pentium 2.5GHz processor 1 GB RAM 20 GB disk space or greater One Ethernet interface supporting TCP/IP	Windows 2000 Server or Advanced Server, Service Pack 4
Attack PC	Intel Pentium 2.5GHz processor 1 GB RAM	NeWT, version 2.0 NMap, version 4.0

System	Hardware Minimum Required	Minimum Software Requirements
	20 GB disk space or greater One Ethernet interface supporting TCP/IP	Ethereal, version 0.10.11

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, *Cisco Security Agent 4.5.1.655 Functional Test Report, dated March 9, 2007*.

8.2 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 conclusions that the evaluation team reached were that the vendor had provided a thorough suite of tests. The evaluators identified a total of five additional functional tests.. Those tests were chosen to exercise the claimed functionality in a slightly different manner than had already been tested by the vendor.

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.

8.3 Evaluator Penetration Tests

The evaluators examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. While verifying the information found in the developer's vulnerability assessment, the evaluators conducted a search to verify that no additional obvious vulnerabilities existed for the TOE.

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluators made an assessment of the rationales provided by the developer indicating that the vulnerability was non-exploitable in the intended environment of the TOE. Any possible vulnerability that required further evaluator analysis was identified as "suspect". The evaluators found that most of the vendor analysis was satisfactory and identified one "suspect" potential vulnerabilities that warranted further analysis. After performing a threat analysis on that potential vulnerability, the evaluators decided to conduct further testing of that vulnerabilities.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluators examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities. The evaluation team identified five additional vulnerabilities that warranted further testing.

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 evaluation team conducted total of six tests for potential vulnerabilities that supplemented the vendor tests.

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 F2-0307-002 *Cisco Security Agent 4.5.1.655 Penetration Test Report, dated April 26, 2007*.

8.4 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.

9 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 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 document *Evaluation Technical Report for the Cisco Security Agent 4.5.1.655, dated March 9, 2007* contains the verdicts of “PASS” for all the work units.

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

10. Validator Comments

This evaluation began prior to the CCEVS establishment of Scheme Policy 13 which restricts the types of TOEs that can be evaluated. Due to the fact that some software components that are provided with the TOE were not covered by this evaluation, this scope of the evaluation of this TOE would have had to have been broader to meet Policy 13. Potential users of this TOE may need to perform additional analysis of those component of the IT Environment to determine if the TOE is suitable for their applications.

All other validator comments are already captured in the Clarification of Scope section (page 10) of this report.

11. Security Target

The Security Target document, *Cisco Security Agent Version 4.5.1 Security Target, Document EDCS-507896, dated April 4, 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
CSA	Cisco Security Agent
C&A	Certification and Accreditation
EAL	Evaluation Assurance Level
IT	Information Technology
MC	Management Center
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
VMS	Cisco Works VPN/Security Management System

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 2.1, dated August 1999
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.1, dated August 1999

- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.1, dated August 1999
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.1, dated August 1999
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.1, dated August 1999
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000