National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

McAfee IntruShield Intrusion Detection System

Report Number: **CCEVS-VR-04-0072**
Dated: **31 August 2004**
Version: **1.1**

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

Jeffrey C. Gilliatt
Christopher Durham
Richard Murphy
Mitretek Systems,
Falls Church, Virginia

Common Criteria Testing Laboratory

SAIC Common Criteria Testing Laboratory
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the McAfee Incorporated IntruShield Product Family. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the McAfee Incorporated IntruShield Product Family was performed by the SAIC Common Criteria Testing Laboratory in the United States and was completed during July 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by SAIC. The evaluation team determined the product to be Part 2 conformant and Part 3 conformant, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 3 have been met.

The McAfee IntruShield Product Family is a network Intrusion Detection System (IDS) that provides real-time network intrusion detection and prevention. The TOE consists of the following components:

- One or more McAfee IntruShield Sensors:
    - IntruShield 1200 appliance, Rev. 2 or earlier
    - IntruShield 2600 appliance, Rev. 2 or earlier
    - IntruShield 4000 appliance, Rev. 2 or earlier
- IntruShield Security Management System (ISM) Version 1.8.3.5
- Update Server Version 04.06.07.01

The sensor components are dedicated systems that monitor network traffic on a designated network segment. They process traffic using signature information downloaded from the ISM (which obtains this information from the Update Server.) The ISM receives event and alert information from the sensors and provides a web-based user interface for display of event data and alerts, configuration of sensors, and updates of sensor information.

The sensors perform statefull inspection of network packets in order to detect and prevent intrusions, misuse, denial of service attacks, and distributed denial of service attacks. The three sensor products differ only in their bandwidth capacity and deployment strategies and provide the same security functions.

The following figure provides a high-level representation of the TOE.

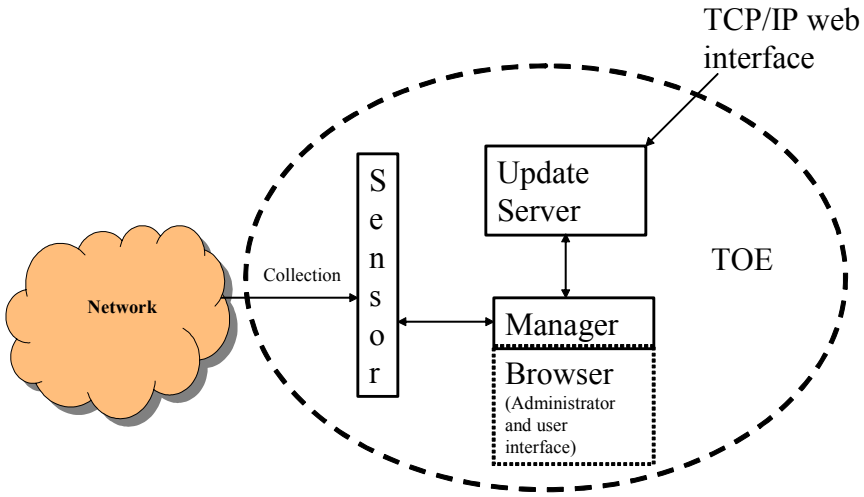

Figure 1 – High-Level TOE Representation

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 3 evaluation. Therefore the validation team concludes that the SAIC CCTL findings are accurate, and the conclusions justified.

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 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 desiring 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's 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 Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	McAfee Incorporated IntruShield Intrusion Detection System
Security Target	*IntruShield Product Family Intrusion Detection System Security Target*, August 25, 2004
Evaluation Technical Report	*Evaluation Technical Report for IntruShield Product Family;* August 30, 2004.
Conformance Result	CC Part 2 conformant, CC Part 3 conformant, EAL 3
Sponsor	McAfee Incorporated 3965 Freedom Circle Santa Clara, CA 95054
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, Maryland 21046
CCEVS Validator(s)	Jeffrey C. Gilliatt Christopher Durham Richard Murphy Mitretek Systems, Inc. 3150 Fairview Park South Falls Church, VA 22042-4519

3 Security Policy

The TOE implements an intrusion detection and prevention Security Policy by the use of stateful inspection of network traffic on designated network segments. The TOE implements an IDS policy as specified in the Security Target. These specify requirements for data collection, analysis, event response, and review of captured event information.

4 Assumptions

4.1 Personnel Assumptions

- There will be one or more competent System Managers assigned to manage the TOE and the security of the information maintained by the TOE.
- The system administrators are not careless, willfully negligent, or hostile. The administrators are assumed to follow guidance, and do not attempt to attack or subvert the TOE and its policy.
- Only authorized users are able to access the TOE.

4.2 Physical Assumptions

- The TOE hardware and software are protected from unauthorized physical modifications.

- The TOE is located within a controlled access facility which will prevent unauthorized physical access.

4.3 IT Environment Assumptions

.

- The TOE has access to all the IT System data that it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE is appropriately scalable to the IT System the TOE monitors.
- The Windows 2000 operating system, which is a part of the environment, shall provide reliable time stamps for the TOE.

5 Architectural Information

The components of the IntruShield IDS TOE are the Collection Subsystem, the ISM Subsystem, and the Update Server Subsystem. These subsystems are depicted in Figure 2 and are summarized in the text below.

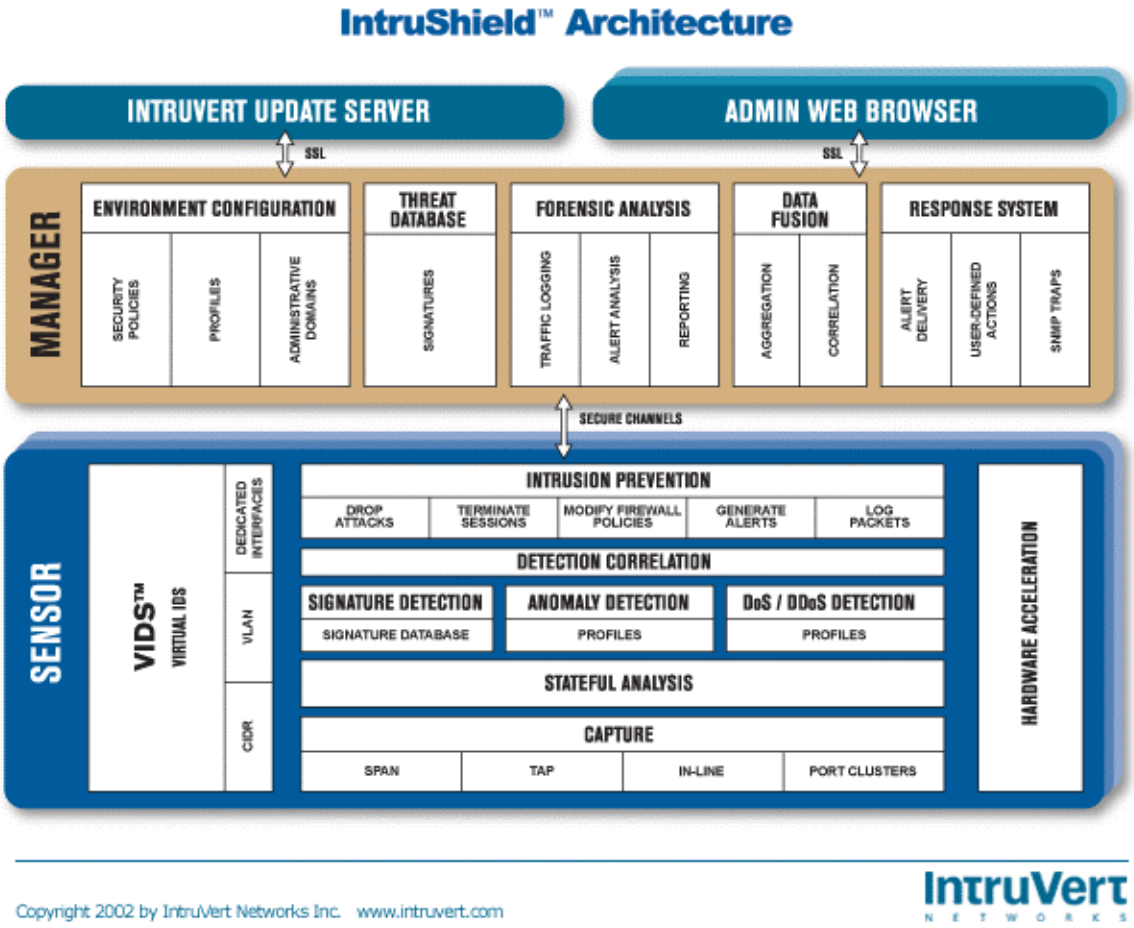

Figure 2: McAfee IntruShield Architecture

a) Collection Subsystem: The Collection Subsystem is provided by the IntruShield Sensor appliance. The primary function of the IntruShield sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The sensor examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The sensor examines packets according to user-configured *policies*, or rule sets, which determine what attacks to watch for, and how to react with countermeasures if an attack is detected. If an attack is detected, the sensor raises an *alert* to describe the event, and responds according to its configured policy. Sensors can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and

even dropping packets entirely before they reach their target. A sensor may be connected to multiple network segments in multiple operating modes.

b) Manager Subsystem: The ISM is the Manager Subsystem. The ISM server is a dedicated Windows 2000 platform running the ISM software. The ISM is also referred to as The Manager. There are two versions of the ISM system, which differ only in the number of sensors supported. Functionally, the products are otherwise identical. The Security Target uses the term "ISM" to describe either version. The ISM provides a web-based user interface for managing and configuring the IntruShield Sensors. Components of the ISM include:
    a. Network Console is the first screen displayed after the user logs on to the system. The Network Console displays system health—i.e., whether all components of the system are functioning properly, the number of unacknowledged alerts in the system and the configuration options available to the current user. Options available within the Network Console are determined by the current user's assigned role(s).
    b. System Health Viewer displays the status of the ISM, database, and any deployed sensors; including all system faults.
    c. System Configuration Tool provides all system configuration options, and facilitates the configuration of sensors, administrative domains, users, roles, attack policies and responses, user-created signatures, and system reports. Access to various activities, such as user management, system configuration, or policy management is based on the current user's role(s) and privileges.
    d. Alert Viewer displays detected security events that violate your configured security policies. The Alert Viewer provides powerful drill-down capabilities to enable you to see all the details on a particular alert, including its type, source and destination addresses,

The ISM operates on a dedicated Windows 2000 workstation using a MySQL database for event storage.

c) Update Server: The Update Server is a McAfee Incorporated -owned and -operated file server that updates the signature files of IntruShield sensors in customer installations. McAfee Incorporated uses the Update Server to securely provide fully automated, real-time signature updates without requiring any manual intervention. According to a user-configured schedule or via a manual process, the ISM polls the McAfee Incorporated Update Server, and compares the file on the Update Server with what is already available in the ISM server to determine what it needs to download. Once it has received the update, the ISM then determines what signatures need to be pushed out to sensors based on the policy applied to the sensor.

    The TOE uses the Update Server to securely provide fully automated, real-time signature updates without requiring any manual intervention according to a user-configured schedule or via a manual process. The ISM polls the Update Server, and compares the file on the Update Server with what is already available in the ISM server to determine what it needs to download. Once it has received the update, the ISM then determines what signatures need to be pushed out to sensors

based on the policy applied to the sensor. For example, a policy defined for a Windows environment will receive only updated signatures that apply to that environment.

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

Design documentation:
IntruShield Functional Specification Document (ADV_FSP.4), Version 5.0, June 22, 2004
IntruShield High-Level Design Document (ADV_HLD.5), Revision 5, May 25, 2004
IntruShield Informal Correspondence Document, Version 7.0, July 7, 2004

Guidance documentation:
IntruShield IDS System Release Notes Release 1.8
IntruShield IDS System Manager Administrator's Guide Version 1.8, Revision 3, 06-2004
IntruShield IDS System Getting Started Guide Version 1.8, revision 2, 06-2004
IntruShield IDS System Manager Installation Guide, Version 1.8, rev 3 07-2004
IntruShield IDS System Sensor Installation and Configuration Guide Version 1.8, 09-2003

Configuration Management:
IntruShield IDS System Configuration Management Document, Revision 11, Release Date 7/2/2004

Lifecycle Support:
Assurance Life Cycle Support Document (ALC) Version 3.0, 03/23/04

Delivery and Operation documentation:
NAI Intruvert Order, Delivery, and Billing, Version 13.0, 6/23/04
Director Reseller Direct Processing, Version2, 12 September 2003
Manufacturing Flow Process and Test Plan, rev 5.0, 2/10/04
IntruShield Update Server Delivery Procedure (ADO) Document, Version 1, 3/18/04
IntruShield IDS System Getting Started Guide Version 1.8, revision 2, 06-2004
IntruShield IDS System Manager Administrator's Guide Version 1.8, Revision 3, 06-2004
IntruShield IDS System Manager Installation Guide, Version 1.8, rev 3 07-2004
IntruShield IDS System Sensor Installation and Configuration Guide, Version 1.8, 09-2003
IntruShield IDS System Release Notes, Version 1.8

Test documentation:
IntruShield IDS System Test (ATE) Document, Version 7.0
ATE Test Results version 4.0, 06/23/2004

Vulnerability Assessment documentation:
IntruShield IDS System Release Notes Release 1.8
IntruShield IDS System Manager Administrator's Guide Version 1.8, Revision 3, 06-2004
IntruShield IDS System Getting Started Guide Version 1.8, revision 2, 06-2004
IntruShield IDS System Manager Installation Guide, Version 1.8, rev 3 07-2004
IntruShield IDS System Sensor Installation and Configuration Guide Version 1.8, 09-2003
IntruShield Vulnerability Assessment Document Version 4.0, 04/14/04
IntruShield Product Family Intrusion Detection System Security Target, v0.97, August 25. 2004

Security Target
IntruShield Product Family Intrusion Detection System Security Target, v0.97, August 25. 2004

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and the high level design and mapped each test to the security function tested. The scope of the developer tests included all TOE Security Functions: Security Audit, User Data Protection, Identification and Authentication, Security Management, Protection of TOE Security Functions, and Intrusion Detection System.

Test depth is addressed by analyzing the functions addressed in the high level design and associating test cases that cover the addressed functionalities. The high level design addressed the general functions of the TOE components. Each security function maps to the appropriate test suite, and the test rationale demonstrates why the test suites provide adequate test coverage of a given security function.

The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification and high level design. The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests and penetration tests.

Although the evaluation team performed a sample of the developer's test suite, the selected tests were representative of the TOE Security Functions.

8 Evaluated Configuration

The evaluated configuration consisted of the components identified in the table below.

Component	Description
IntruShield 1200, 2600, or 4000 appliance Rev. 2 or earlier	Network data collection sensor
IntruShield Security Manager System (ISM) Version 1.8.3.5	Software to manage and configure the Sensor subsystems
Update Server Version 04.06.07.01	Maintains signature updates for the Sensor subsystems

Table 2 - Hardware and Software Components

9 Validator Comments

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

10 Security Target

IntruShield Product Family Intrusion Detection System Security Target, August 25, 2004, Version 0.97.

11 Glossary

CC	Common Criteria
IDS	Intrusion Detection System
ISM	IntruShield Security Management
IT	Information Technology
NIAP	National Information Assurance Partnership
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

12 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, version 2.1, August 1999, Parts 1, 2, and 3

- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, version 0.6, 11 January 1997.

- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, version 1.0, August 1999.

- *IntruShield Product Family Intrusion Detection System Security Target* August 25, 2004.

- Evaluation Technical Report for the IntruShield Product Family, Version 0.2, August 30 2004.

- National and International Interpretations

The Evaluation Team determined that the following CCIMB Interpretations were applicable to this evaluation:

1. *RI # 3 – Unique Configuration of CIs - ACM*
2. *RI # 4 - ACM_SCP.*.1C requirements unclear - ACM*
3. *RI # 6 – Underlying Hardware and Firmware - ADV*
4. *RI # 8 – Augmented and Conformant Overlap - ASE*
5. *RI #16 – Delivery procedures may include confidentiality - ADO*
6. *RI #24 – Evidence is required of entire TOE - ADV*
7. *RI #25 – Level of detail required for hardware descriptions - ADV*
8. *RI #27 – Events and Actions – AGD*
9. *RI #31 – Vulnerabilities not in TOE not applicable – AVA*
10. *RI #32 – SOF analysis need not be in ST*
11. *RI #37 – CM applicable to TOE – ACM*
12. *RI #38 – CM requirement modified - ASE*
13. *RI #51 – ADO_IGS and AVA_VLA requirements modified - ASE*
14. *RI # 65 – FMT_SMR (new requirement) as a dependency of FMT_MOF – ASE, ADV*
15. *RI #84 – Separate objectives for TOE and environment - ASE*
16. *RI #116 – Indistinguishable work units for ADO_DEL – ADO*
17. *RI #141 – FAU_STG.2 modified – ASE, ADV*
18. *RI #202 – FAU_GEN.1 permits the selection of only one option – ASE, ADV*

The Evaluation Team determined that the following NIAP interpretations were applicable to this evaluation:

1. *I-0347 – Including Sensitive Information in Audit Records*
2. *I-0407 – Empty Selections Or Assignments*
3. *I-0410 – Auditing Of Subject Identity For Unsuccessful Logins*
4. *I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3*
5. *I-0422 – Clarification of "Audit Records"*
6. *I-0426 – Content of PP Claims Rationale*
7. *I-0427 – Identification of Standards*
8. *I-0429 – Selecting One Or More*

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.