National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Cisco Intrusion Detection System Sensor Appliance IDS-4200 series Version 4.1(3)

Report Number: CCEVS-VR-04-0062

Dated: 28 May 2004

Version: 1.0

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

Jandria Alexander

John Nilles

The Aerospace Corporation

Columbia, Maryland

William Jones

National Security Agency

Linthicum, Maryland

Common Criteria Testing Laboratory

Cable and Wireless

Sterling, Virginia

Table of Contents

1 EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Cisco Systems, Inc. Appliance 4200 series Version 4.1(3) intrusion detection system. The evaluation was performed by the Cable and Wireless (C&W) Common Criteria Testing Laboratory. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by C&W and submitted to the validators. The evaluation determined that the product conforms to the Common Criteria Version 2.1, Part 2 extended and Part 3.

The Cisco IDS v4.1(3) is a stand-alone product consisting of a combination of hardware and software. The Event Viewer and the IDS Management Center for IDS Sensors (IDS MC) are not included in the TOE.

The Cisco IDS v4.1(3) as configured in the installation and start-up guidance documents comprises the TOE. The TOE is a network-based Intrusion Detection System capable of monitoring traffic. The TOE analyzes both the header and content of each packet. It analyzes single packets or a complete flow for attacks while maintaining flow state, allowing for the detection of multi-packet attacks. The TOE uses a rule-based expert system to interrogate the packet information to determine the type of attack.

Data collection and analysis is performed on a single dedicated hardware platform. In response to an attack, the TOE has several options that include generating an alarm, logging the alarm event, and killing TCP sessions. The validation team observed 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's observations support the conclusion that the product satisfies the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validation team concludes that the findings of the evaluation team are accurate, and the conclusions justified.

The TOE evaluation did not include assessments of the cryptographic functions provided by the Secure Web Server and the Secure Shell components.

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 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 Protection Profile to which the product is conformant (if applicable);
- 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	Cisco Intrusion Detection System Sensor Appliance IDS-4200 series Version 4.1(3)
Protection Profile	Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002.
Security Target	Cisco Intrusion Detection System v4.1(3) Security Target, Version 2.4, May 25, 2004
Evaluation Technical Report	Cisco Systems, Inc. Cisco Intrusion Detection System v4.1(3) Evaluation Technical Report, Version 1.5, May 24, 2004
Conformance Result	Part 2 extended, Part 3 conformant, EAL2
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Evaluators	Cable & Wireless
Validators	The Aerospace Corporation The National Security Agency

3 SECURITY POLICY

The Cisco Intrusion Detection System v4.1(3) does not implement a security policy in the traditional sense of enforcing a set of access control rules. The TOE collects, stores and manages all IDS System records.

The Security Objectives for the TOE as outlined in the IDS System PP require that:

- The TOE must protect itself from unauthorized modifications and access to its functions and data.
- The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
- The TOE must allow authorized users to access only appropriate TOE functions and data.
- The TOE must include a set of functions that allow effective management of its functions and data.
- The TOE must respond appropriately to analytical conclusions.
- The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
- The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
- The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
- The TOE must appropriately handle potential audit and System data storage overflows.
- The TOE must record audit records for data accesses and use of the System functions.
- The TOE must ensure the integrity of all audit and System data.
- When any IDS component or the TOE makes its data available to another IDS component, the TOE will ensure the confidentiality of the System data.

3.1 Roles

The product supports three roles: the Administrator role, an Operator role and a Viewer role.

- **Administrator** – Full access to the TOE. This role is able to manage the users of the TOE and to view/modify the configuration of the TOE and the logs. This role corresponds to the "authorized administrator" role that is called out in the FMT_SMR.1 requirement in each of the IDS system PP.

- **Operator** – Read Access to the TOE with limited management abilities. This role is able to view all logs and configuration information and may configure signatures, assign virtual sensor configurations to an interface, configured the list of managed routers and his/her own password.

- **Viewer** – Read-only access to the TOE. This role is able to view the logs and configuration of the TOE, but is not permitted to modify any information other than his/her own password.

Each authorized user of the TOE is assigned to one and only one role. A user account cannot be created without an associated role; if no role is specified when the user is created then the default role of viewer is assigned. Administrators are permitted to change their role or the roles of other users.

The TOE also contains an additional role of "service", however, the security characteristic of this role was not examined and its use is prohibited in the evaluated configuration.

3.2 Security Management

The TOE provides security management functionality necessary to manage TOE and IDS data. This includes the ability to query TOE data, enable/disable signatures, set and clear logs, and setting the clock.

4 ASSUMPTIONS

4.1 Usage Assumptions

The evaluation made the following assumptions concerning product usage.

- The TOE has access to all the IT system data and resources 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.

4.2 Physical Assumptions

The evaluation made the following environmental assumptions:

- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4.3 Personnel Assumptions

The evaluation made the following personnel assumptions:

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.

5 ARCHITECTURAL INFORMATION

The TOE consists of the following logical components:

- Sensor Application,
- Network Access Control,

- Secure Web Server,
- Authentication Application,
- Secure Shell (SSH),
- Command Line Interface (CLI),
- Event Store,
- Linux 7.3 OS (operating system) and hardware; and,
- Update Client.

Together the subsystems provide security functionality for audit generation, selection, review and protection; identification and authentication; management of security functions; protection of TOE security functions; and, Intrusion Detection System data collection, analysis, review, reaction and protection. The TOE evaluation did not include assessments of the cryptographic functions provided by the Secure Web Server and the Secure Shell components.

Sensor Application

The Sensor Application monitors network packets from the target IT network. The application parses data for analysis and compares the parsed data against signatures of known attacks.

Network Access Controller

The Network Access Controller provides analyzer react functionality. The Cisco IDS v4.1(3) can be configured to react to intrusions by sending a command to a component external to the TOE. When an intrusion is detected, the Network Access Controller sends a command to an external component such as a Cisco router, Cisco switch, or PIX firewall which is then instructed to block traffic from the alleged source address of the intrusion.

Secure Web Server

The Secure Web Server provides a TLS encrypted interface between the client web browsers and the system. Requests arrive as HTML encapsulated by the TLS connection. These requests are parsed and formatted as control transactions to be passed to the appropriate component within the system. Responses are converted into HTML and returned to the web browser.

Authentication Application

The Authentication application is responsible for associating usernames with groups. It receives requests and processes responses in the form of Control Transactions. It is dynamically linked with the Pluggable Authentication Module (PAM) library, which is part of the Linux OS, and depending on the service requested by the user to authenticate to the system, will interface with the appropriate module, which will authenticate the user.

Secure Shell

Secure Shell (SSH) provides confidentiality and integrity over an unsecured network. The sshd (daemon process for SSH) listens for connections from clients.

Command Line Interface

The Command Line Interface (CLI) allows an authorized user to issue commands on the system and receive data from the system. This data is sent over an SSH encrypted session (except in the case of console connection, in which it is sent in clear text). The CLI presents the user with a restricted command set. User commands are parsed and formatted as control transactions to be passed to the appropriate component within the system. After a user has been authenticated the CLI is responsible for enforcing that the user is only able to issue commands at his/her privilege level (i.e., group).

Event Store

The Event Store is comprised of the event store file and a shared object. It stores audit and system events. The shared object, called IDAPI, ensures that all events written to the event store conform to the IDIOM specification and is dynamically linked to all components required to write to and read from the event store file.

Operating System and Hardware

The OS and hardware are responsible for generating reliable time stamps. The OS also provides support for portions of the authentication process. The OS aids in authentication in two ways. When a user authenticates with a username and password this information is passed to PAM for authentication. Authentication data is stored in the etc/shadow file. In addition, PAM is responsible for authentication failure handling and account lockout. PAM is only called for authentication failure handling and account lockout. In addition when a user authenticates via the console the login program is called, which authenticates the user using PAM in the same manner as sshd. Reliable timestamps are generated by the system Clock.

Update Client

The update client uses an outbound connection only. It is used to retrieve attack signatures and software patches from Cisco. An administrator must manually configure the Cisco IDS v4.1(3) to connect to a specified Cisco server to receive updates. In the evaluated configuration, only protocols that can ensure confidentiality and integrity of data can be used (i.e., HTTPS, and SCP).

6 DOCUMENTATION

Following is a table of the evaluation evidence used to support this evaluation:

Evidence

Category	Title(s)
Security Target	Cisco Systems, Inc. Cisco Intrusion Detection System v4.1(3) Security Target v2.4, May 25, 2004
Configuration Management	Cisco Intrusion Detection System v4.1(3) Configuration Management Version 0.6
Delivery and Operation:	Cisco Intrusion Detection System v4.1(3) – Delivery

Category	Title(s)
	documentation Version 0.4
	Release Notes for the Cisco Intrusion Detection System Version 4.1, 4029_03, April 22, 2004
	Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1, 78-15597-01
	Cisco Intrusion Detection System Command Reference Version 4.1, 78-15599-01
	Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1, 78-15598-01 (excluding Chapter 6, IDS Event Viewer Introduction)
Design Documentation:	Cisco Intrusion Detection System v4.1(3) – Functional Specification Version 1.2
	Cisco Intrusion Detection System v4.1(3) – High-Level Design Version 0.6
	Cisco Systems, Inc. Cisco Intrusion Detection System v4.1(3) Correspondence Document Version 0.4
Guidance Documentation:	Release Notes for the Cisco Intrusion Detection System Version 4.1, 4029_02, April 22, 2004
	Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1, 78-15597-01
	Cisco Intrusion Detection System Command Reference Version 4.1, 78-15599-01
	Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1, 78-15598-01 (excluding Chapter 6, IDS Event Viewer Introduction)
	Cisco Intrusion Detection System v4.1(3) readme.txt file
Test Documentation:	Cisco Systems, Inc. Cisco Intrusion Detection System v4.1(3) Testing and Evidence of Coverage, Version 1.1
	Cisco Systems, Inc. Cisco Intrusion Detection System v4.1(3) Testing and Evidence of Coverage, Version 1.1
	4.1(1)Sx System Level Detailed Test Plan, Procedures and Results
	4.1(2)Sx Test Plan, Procedures and Results
	4.1(3)Sx Test Plan, Procedures and Results
Vulnerability and Assessment Documentation:	Cisco Systems, Inc. Cisco Intrusion Detection System v4.1(3) Strength of Function Analysis Version: 0.4
	Cisco Systems, Inc. Cisco Intrusion Detection System v4.1(3) Vulnerability Analysis, Version 1.2

Category	Title(s)
	Security Technologies Assessment Team Security Evaluation for CIDS 4.0 Sensor, Version 1.0
	Cisco Systems, Inc. Cisco Intrusion Detection System v4.1(3) Security Target v2.4, May 25, 2004

7 IT PRODUCT TESTING

7.1 Vendor Testing

At EAL2 testing must demonstrate correspondence between the tests and the functional specification. However complete testing is not required; "coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the TSF have been tested."[1]

The vendor testing included tests for each security function as listed:

- Security Audit (FAU)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of the TOE Security Functions (FPT)
- IDS Component Requirements (IDS)

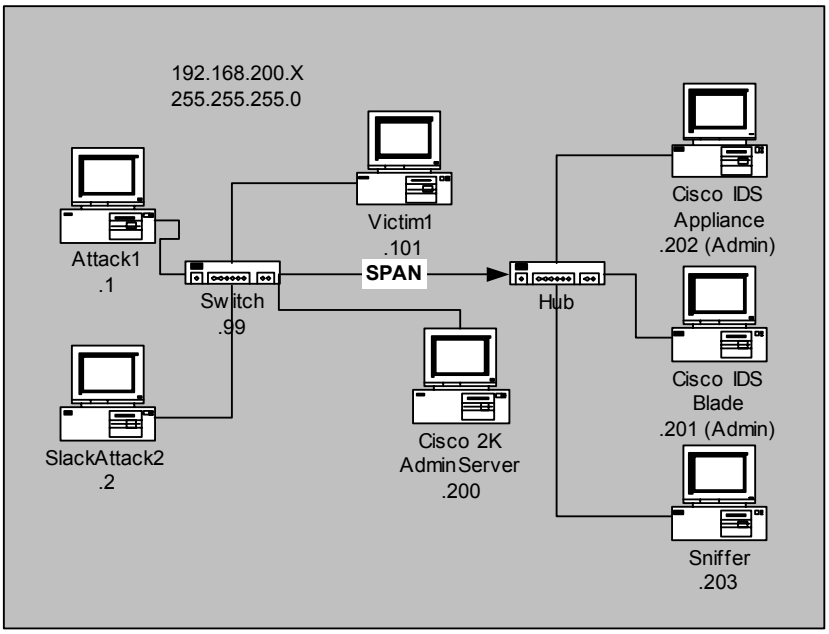
In addition the vendor test suite included extensive IDS signature verification tests.

7.2 Evaluator Testing

The evaluation team performed the TOE installation, as specified in the Installation, Generation and Startup documentation, functional, independent and vulnerability testing on the following configuration. The test configuration is depicted in Figure 1 below.

[1] CEM, V1.0, paragraph 6.8.2.2 (application note for EAL2:ATE_COV.1)

Figure 1 CCTL Testing Configuration



Evaluator testing covered the following areas:

- Collection and detection of intrusion attacks
- TSF Self protection at system interfaces;
- Audit pre-selection, and storage;
- Management roles enforcement;
- Password rule enforcement and Strength of Function testing.

8 EVALUATED CONFIGURATION

The evaluation configuration consists of Cisco Intrusion Detection System series 4200 appliance running version 4.1(3) software. The specific models in the Cisco IDS 4200 Series include:

1. IDS-4220-E (Pentium III 600MHz, 512MB RAM, SMC 10/100BASE-TX NIC)
2. IDS-4230-FE (Dual Pentium III 600MHz, 512MB RAM, SMC 10/100BASE-TX NIC)
3. IDS-4210-K9 (566MHz Celeron, 512MB RAM, SMC 10/100BASE-TX NIC)
4. IDS-4215-K9 (566MHz Celeron, 512MB RAM,10/100BASE-TX NIC)
5. IDS-4235-K9 (Pentium III 1.26GHz, 1GB RAM, 10/100/1000BASE-TX NIC)
6. IDS-4250-TX-K9 (Dual Pentium III 1.26GHz, 1GB RAM, 10/100/1000BASE-TX NIC)
7. IDS-4250-SX-K9 (Dual Pentium III 1.26GHz, 1GB RAM, 1000BASE-SX (Fiber) NIC)
8. IDS-4250-XL-K9 (Dual Pentium III 1.26GHz, 1GB RAM, Dual 1000BASE-SX (Fiber) NIC)

In addition, the series must be installed and operated as described in the "Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1", "Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1"and Release Notes for the Cisco Intrusion Detection System Version 4.1, 4029_03, April 22, 2004.

9 RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [5]; and all applicable National and International Interpretations in effect on 4 February 2002. The evaluation confirmed the product as being Part 2 extended and Part 3 EAL 2 compliant. The details of the evaluation are recorded in the Evaluation Technical Report, which is controlled by the Cable and Wireless CCTL. The evaluation determined the product to be **Part 2 extended conformant, Part 3 conformant,** and to meet the requirements of **EAL 2**. The product was evaluated and tested against the claims presented in the *Cisco Systems, Inc. Cisco Intrusion Detection System Sensor v4.1(3) Security Target v2.4*, dated May 25, 2004.

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

Evaluation of the Cisco Intrusion Detection System Sensor v4.1(3) Security Target (ST) (ASE)

The evaluation team applied each EAL 2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies; a statement of security requirements claimed to be met by the Cisco Intrusion Detection System Sensor product that are consistent with the Common Criteria; and product security function descriptions that support the requirements.

Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; in particular, that configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. Configuration Management (CM) systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking changes and by ensuring that all changes are authorized. The Evaluation Team identified and analyzed the CM process to ensure that its documented procedures were followed and the procedures were employed during the course of this evaluation. The evaluation team ensured that the following items were considered configuration items: TOE implementation, design documentation, test documentation, and user guidance.

Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to securely deliver, install, configure, and operationally use the TOE; and ensured that the security protection offered by the TOE was not compromised during these events.

Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF implements/employs the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team verified the adequacy of the administrator guidance in describing how to securely administer the TOE.

Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain obvious vulnerabilities that can be exploited in the evaluated configuration, based upon the developer strength of function analysis and the developer vulnerability analysis as well as the evaluation team's performance of penetration tests.

Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test further demonstrated the claims in the ST.

10 VALIDATOR COMMENTS AND RECOMMENDATIONS

The validator observations support the evaluation teams conclusion that the Cisco Intrusion Detection System Sensor v4.1(3) meets the claims stated in the Security Target. In particular, the product provides the functionality cited in the IDS System Protection Profile to which it claims conformance.

The TOE evaluation did not include assessments of the cryptographic functions provided by the Secure Web Server and the Secure Shell components.

The TOE also contains an additional role of "service", however, the security characteristic of this role was not examined and its use is prohibited in the evaluated configuration. The Event Viewer and the IDS Management Center for IDS Sensors (IDS MC) are not included in the TOE.

11 SECURITY TARGET

The ST, Cisco Intrusion Detection System Sensor v4.1(3) Security Target dated 25 May 2004 is included here by reference.

12 GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PAM	Pluggable Authentication Module
PP	Protection Profile
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation

TSF	TOE Security Function
TSFI	TOE Security Function Interface

13 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements; dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes; dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements; dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology; dated August 1999, version 1.0.

[7] Cisco Systems, Inc. Cisco Intrusion Detection System Sensor v4.1(3) Security Target v2.4, dated May 25, 2004.

[8] Cisco IDS EAL 2 Team Test Report Version 1.7, May 13, 2004, Cable and Wireless

[9] Evaluation Technical Report, for Cisco Intrusion Detection System Sensor v4.1(3), dated May 24, 2004 Ver.1.5; 24 May 2004, Cable and Wireless