

National Information Assurance Partnership



**Common Criteria Evaluation and Validation Scheme
Validation Report**

Cisco Intrusion Prevention System (IPS) v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS4260); Cisco AIP-SSM-10 and AIP-SSM-20; NM-CIDS, IDSM-2))

Report Number: CCEVS-VR-07-0032
Dated: May 31, 2007
Version: 6.0

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

National Security Agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95124-1706
USA

Evaluation Personnel:
Arca Common Criteria Testing Laboratory

Abdul Qayyum
Alicia Squires
Ken Dill

Validation Personnel:
Dr. Patrick W. Mallett, The MITRE Corporation
Jandria Alexander, The Aerospace Corporation

Table of Contents

1	Executive Summary	1
2	Identification	2
3	Security Policy	4
3.1	Roles	4
3.2	Identification and Authentication	4
3.3	Security Management	4
3.4	Audit	5
3.5	Network Traffic Analysis	5
3.6	Self-protection	5
4	Assumptions	5
5	Architectural Information	6
6	Documentation	7
7	IT Product Testing.....	8
7.1	Developer Testing	8
7.2	Evaluation Team Independent Testing	9
8	Evaluated Configuration.....	11
9	Results of the Evaluation	13
10	Validator Comments	14
11	Security Target.....	14
12	List of Acronyms	15
13	Bibliography	17
14	Interpretations	18
14.1	International Interpretations	18
14.2	NIAP Interpretations.....	18
14.3	Interpretations Validation	18

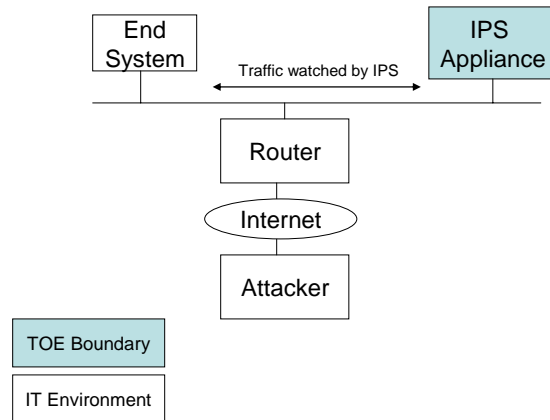
1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco IPS Version 6.0. 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 Cisco IPS Version 6.0 was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed during April 2007. The information in this report is largely derived from the Security Target (ST), written by Cisco Systems, Inc. and the Evaluation Technical Report (ETR) and associated Evaluation Team Test Report, both written by Arca CCTL. The evaluation team determined the product to be CC version 2.3 Part 2 extended and Part 3 augmented with ALC_FLR.1., and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 2 have been met. In addition, the evaluation team confirmed that the TOE uses CCEVS precedents PD-0061: Security Targets for a Software TOE that runs on Multiple Platforms, PD-0062: What Must Be Tested for an ST Running On Multiple Platforms?, PD-0097: Compliance with IDS System PP Export Requirements, PD-106: Situations Where AGD_USR May Be Vacuously Satisfied, PD-0107: IDSSPP v1.4: FPT_STM.1 Must Be Met by the TOE, PD-0108: FTP_ITC.1.3 Specifies The Functions For Which A Trusted Channel Is Provided, PD-0116: IDSSPP v1.4: Compliance with the Selective Audit Requirement, PD-0118: Assumptions in the IDS PP v1.4, and includes all security requirements from the U.S. Department of Defense Intrusion Detection System System Protection Profile, Version 1.6, dated April 4, 2006.

The Cisco IPS Version 6.0 consists of hardware and software used to provide an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) solution that is designed to identify, classify, and stop malicious traffic before they affect network continuity. Figure 1 illustrates the TOE and its environment. The TOE includes the Cisco IPS Version 6.0 Hardware and Software (shown by the IPS in the diagram).

Figure 1: Typical TOE Configuration



The validation team monitored the activities of the evaluation team, 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 Common Evaluation Methodology (CEM) work unit verdicts), 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 2 evaluation. Therefore the validation team concludes that the Arca CCTL findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a National Security Agency (NSA) 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) or candidate CCTLs using the 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 and candidate 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 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	IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS4240, IDS4215, IPS4260); Cisco AIP-SSM-10 and AIP-SSM-20; NM-CIDS, IDSM-2
Security Target	Cisco Intrusion Prevention System (IPS) Version 6.0

Item	Identifier
Evaluation Technical Report	<ul style="list-style-type: none"> • ASE (Security Target Evaluation): ASE Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 6.0, released May 31, 2007. • ACM_CAP.2 & ALC_FLR.1 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 5.0, released April 30, 2007.. • ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 5.0, released April 30, 2007. • ADV_FSP.1; ADV_HLD.1; ADV_RCR.1 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 6.0, released May 31, 2007. • AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 5.0, released April 30, 2007. • ATE_COV.1; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 6.0, released May 31, 2007. • AVA_VLA.1; AVA_SOF.1 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 5.0, released April 30, 2007.
Conformance Result	CC Part 2 conformant and CC Part 3 augmented with ALC_FLR.1, EAL 2
Applicable interpretations and precedents	<ul style="list-style-type: none"> ▪ PD-0061: Security Targets for a Software TOE that runs on Multiple Platforms, ▪ PD-0062: What Must Be Tested for an ST Running On Multiple Platforms?, ▪ PD-0097: Compliance with IDS System PP Export Requirements, ▪ PD-106: Situations Where AGD_USR May Be Vacuously Satisfied, ▪ PD-0107: IDSSPP v1.4: FPT_STM.1 Must Be Met by the TOE, ▪ PD-0108: FTP_ITC.1.3 Specifies The Functions For Which A Trusted Channel Is Provided, ▪ PD-0116: IDSSPP v1.4: Compliance with the Selective Audit Requirement, ▪ PD-0118: Assumptions in the IDS PP v1.4

Item	Identifier
Sponsor	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95124-1706
Common Criteria Testing Lab (CCTL)	SAVVIS Communications Arca Common Criteria Testing Laboratory NVLAP Lab Code 200429 45901 Nokes Boulevard Sterling, VA 20166
CCEVS Validator(s)	Patrick Mallet Mitre 7515 Colshire Drive McLean, VA 22102 Jandria Alexander The Aerospace Corporation 8840 Stanford Boulevard, Suite 4400 Columbia, MD 21045-5852

3 Security Policy

3.1 Roles

The TOE maintains two administrator roles: authorized system administrator and authorized administrator. Only authorized system administrators have the authority and permission to execute security management actions on the TOE. The authorized administrator is authorized to view all the TOE data.

3.2 Identification and Authentication

The TOE Identification and Authentication function requires users to provide credentials to the TOE in order to successfully be recognized as an authorized user. The user identifies and authenticates themselves through both the command line interface (CLI) and the Web interface using SSH and SSL/TLS respectively. Note that through the CLI interface, the user can also authenticate via RSA authentication. In the case of the physical console interface the user is directly allowed to provide a username and password to the TOE. The TOE maintains and stores user identity, authentication data, and authorizations in the underlying operating system.

3.3 Security Management

The TOE's security management functions provides security capabilities that guarantees all authorized users are required to identify and authenticate to the TOE before any administrative actions can be performed. Thus, an authorized user is one who has been successfully identified and authenticated by the TOE. The TOE provides administrator support functionality that enables a human user to manage and configure the TOE. The TOE manages roles for authorized users to ensure restricted access to the security functions and data for the TOE. The TSF restricts management (query, add, modify, view/read) of the TOE management data to authorized system administrators and only allow query and view/read capability to authorized administrators.

3.4 Audit

The TOE's Audit security function supports audit record generation, storage, and review. The TOE maintains time to generate a reliable timestamp which is applied to each audit event record. Note that the Module TOE must receive an initial time from its host IT environment via a trusted channel to set its internal clock. Audit capabilities of the TOE include selective audit review by authorized users, audit storage, and protection of audit records from unauthorized deletion..

3.5 Network Traffic Analysis

The TOE monitors network traffic from the target IT network. The TOE collects and stores information about all events that are indicative of inappropriate activity. Received data is parsed for analysis and compared against known attacks. The TOE utilizes advance methods for the inspection and analysis of traffic to include event correlation, risk rating calculation, and threat identification (e.g., protocol analysis, pattern recognition, anomaly detection). Based on the analytical result, the TOE has several options for reaction (depending on the interface mode) that include generating an alarm, logging the alarm event, dropping or modifying packets, sending a command to a Cisco router, switch, or firewall to block traffic specific offending network traffic, or killing TCP sessions.

3.6 Self-protection

The protection mechanisms employed by the TOE ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. More specifically, once a user has been authenticated via the CLI or Web interface, the Identification and Authentication is used to query and return the user's role. The role is used to determine what functionality is presented to the user. For the Module TOE, the host IT environment administrator can access the TOE to change the time and halt the execution of the module. Because the host IT environment is considered to be a trusted IT entity and the interface established to change the time and halt the module is via a trusted channel, the security domain for the Module TOE is still considered protected from interference and tampering. No other means, other than described above, are provided for the user to interact with the TOE.

The Self-protection function is responsible for providing an execution domain that is protected from interference and tampering by unauthorized users. The TOE is a hardware device that executes all of its processes internally. It is accessible only via the defined interfaces and only authorized users and the host IT environment for the Module TOEs are able to modify the functionality of the TOE. The sensor interface enforces domain separation in that any data sent to this interface (which is presumed untrusted) is logically separated from all other TOE data. It is never executed but rather is parsed for analysis. Traffic flowing through the TOE is subject to the policies as defined by the authorized users. At all physical interfaces, the TOE intercedes to ensure domain separation. Traffic can only come into the TOE via three physical interfaces: the Serial Port (which is used only during initial setup and configuration of the TOE), the command and control interface (access to which is controlled by a username and a password), or the sensor interface (where the traffic is monitored and analyzed by the TOE but no actions can be executed). Traffic and/or unauthorized users cannot bypass the identification and authentication mechanisms, preventing interference and tampering by untrusted subjects and thereby maintaining a domain for its own execution.

4 Assumptions

The specific conditions listed in Table 2 are assumed to exist in the TOE's IT environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE. They are classified as to whether they apply to personnel security, physical security, or to the IT environment.

Table 2: TOE Assumptions

Name	Assumption	Area
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions	IT Environment
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.	IT Environment
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.	IT Environment
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	Physical
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	Physical
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	Personnel
A.NOEVIL	The authorized administrators are not careless, willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.	Personnel
A.NOTRST	The TOE can only be accessed by authorized users.	IT Environment

5 Architectural Information

The TOE consists of following physical devices:

- One of the following Cisco IPS v6.0 appliances or modules:
 - Appliances: IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260);
 - Modules: AIP-SSm-10, AIP-SSM-20; NM-CIDS; IDSM-2
 - Software: IPS Version 6.0

6 Documentation

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

Table 3: Evaluation Evidence

Assurance Requirement	Title(s)
ACM_CAP.2	Cisco Intrusion Prevention System (IPS) Version 6.0 Configuration Management and Flaw Remediation Documentation, Version 6.0
ALC_FLR.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Configuration Management and Flaw Remediation Documentation, Version 6.0
ADO_DEL.1	Cisco Intrusion Prevention System (IPS) Version 6, Delivery Documentation, Version 1.0, March 8, 2006
ADO_IGS.1	Cisco Intrusion Prevention System (IPS) Version 6.0, Installation, Generation, and Start-Up Documentation, Version 5.0
ADO_IGS.1	Release Notes for Cisco Intrusion Prevention System 6.0
ADO_IGS.1	Installing and Using Cisco Intrusion Prevention System Device Manager 6.0
ADV_FSP.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Functional Specification, Version 7.0
ADV_HLD.1	Cisco Intrusion Prevention System (IPS) Version 6.0 High Level Design, Version 6.0
ADV_RCR.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Representation Correspondence, Version 6.0
AGD_ADM.1	Cisco Intrusion Prevention System (IPS) Version 6.0, Administrator Guide, Version 6.0
AGD_ADM.1	Command Reference for Cisco Intrusion Prevention System 6.0
AGD_ADM.1	Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0
AGD_ADM.1	Release Notes for Cisco Intrusion Prevention System 6.0
AGD_ADM.1	Installing and Using Cisco Intrusion Prevention System Device Manager 6.0
AGD_USR.1	As all users of the TOE are Administrative in nature. No user guidance is provided for this product as there are no non-administrative users (PD-0106). This work unit is vacuously satisfied.
ATE_COV.1	Cisco Intrusion Prevention System (IPS) Version 6.0, Test Coverage, Version 5.0
ATE_FUN.1	Cisco Intrusion Prevention System (IPS) Version 6.0, Test Coverage, Version 5.0
ATE_FUN.1	Nubra_CLI_Enhancements_Detailed_Test_Plan.doc (EDCS-490612)
ATE_FUN.1	Nubra_Regression_Authentication_Test_Plan.doc (EDCS-486899)
ATE_FUN.1	Nubra_Regression_Event_Actions.doc (EDCS- 487525)
ATE_FUN.1	Nubra_Regression_IDS2_IOS_Interoperability_Test_Plan.doc (EDCS-477942)
ATE_FUN.1	Nubra_Regression_Signature_Engines_Test_Plan.doc (EDCS-476853)
ATE_FUN.1	Nubra_Regression_SSM_F1_Interoperability_Test_Plan.doc (EDCS-477946)
ATE_FUN.1	Nubra_Regression_Time_Setting_Test_Plan.doc (EDCS-486895)

Assurance Requirement	Title(s)
ATE_FUN.1	EDCS_476853_Results.xls
ATE_FUN.1	EDCS_477942_Results.xls
ATE_FUN.1	EDCS_477946_Results.xls
ATE_FUN.1	EDCS_486895_Results.xls
ATE_FUN.1	EDCS_486899_Results.xls
ATE_FUN.1	EDCS_487525_Results.xls
ATE_FUN.1	EDCS_490612_Results.xls
ATE_IND.1	<i>Cisco_IPS_v6_EAL2_CCTL_Team_Test_Plan_v5.0.doc</i>
AVA_SOF.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Strength of Function, Version 5.0
AVA_VLA.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Vulnerability Analysis, Version 6.0
ASE	Cisco Intrusion Prevent System (IPS) Version 6.0, Security Target, Version 7.0

The following is the list of other non-proprietary evaluation evidence provided by the sponsor:

- Cisco Intrusion Prevention System (IPS) Version 6.0, Installation, Generation, and Start-Up Documentation, Version 5.0
- Release Notes for Cisco Intrusion Prevention System 6.0
- Installing and Using Cisco Intrusion Prevention System Device Manager 6.0
- Cisco Intrusion Prevention System (IPS) Version 6.0, Administrator Guide, Version 6.0
- Command Reference for Cisco Intrusion Prevention System 6.0
- Cisco Intrusion Prevent System (IPS) Version 6.0, Security Target, Version 7.0

7 IT Product Testing

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

7.1 Developer Testing

The developer performed a testing and coverage analysis, which examined a subset of SFRs and developed one or more Cisco test cases that verified the function or command requirement. These tests were documented in the EAL2 Detailed Test Plan. The scope of the developer tests included all TOE Security Functions. The developer also tested all of the models that are part of the evaluation.

The developer performed a testing and coverage analysis, which examined a subset of SFRs and developed one or more Cisco test cases that verified the function or command requirement. These tests were documented in the EAL2 Detailed Test Plan. The scope of the developer tests included all TOE Security Functions. The developer also tested all of the models that are part of the evaluation. The evaluation team determined that the developer's test methodology met the coverage requirements and that the actual test results matched the expected results.

The developer testing addresses the following security functionality claimed by the TOE: audit generation and recording, Identification and authentication mechanism, ability of the

administrators to carry out management functions, functionality of the sensor to collect, analyze and react to network traffic systems data, set time, halt execution and TOE Self protection

There are 24 different test sets performed by the developers and each tested different TSFIs and SFRs (or a subset of SFRs). The test sets contained one to many individual test cases. The test case steps are performed using either CLI commands or the IDM GUI.

The CLI or IDM execute the function as defined in the SFR being tested. A part of the test case the steps were included to verify that the function was executed as expected. These validation steps may have included checking the audit log or obtaining a screen capture, the actual validation information depended on the SFR in question.

For example, if the wrong user credentials were provided to login to the TOE, in addition to an audit log entry generated and logged, the actual result was the screen informing the user that the TOE had denied access.

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.

This was done by completing analysis and the associated mapping documents to verify the correctness of the test case to TSFI/SFR mapping provided by the vendor. A Subset of the vendor tests were re-run confirming that the results generated matched the actual results provided by developer. In addition to this the evaluation team performed it's own independent testing to provide additional verification of a sample of the functions tested by the developer. Additionally the team picked functions either not tested or not directly tested in the vendor test sets.

The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests and penetration tests. The evaluation team reran a subset of the developer's test suite that tested five of the five TSF, and 18 of the 31 SFRs. The TSF tested during testing included audit generation and recording (FAU_GEN.1, FPT_STM.1, IDS_RDR.1), Identification and authentication mechanism (FIA_UID.1, FIA_UAU.1, FIA_ATD.1), ability of the administrators to carry out management functions (FMT_MTD.1, FMT_SMR.1, FMT_MOF.1, FMT_SMF.1), functionality of the sensor to collect, analyze and react to network traffic systems data (IDS_SDC.1, IDS_ANL.1, IDS_RCT.1), set time (FPT_STM.1) and halt execution (FTP_ITC.1(2)) TOE Self protection (FCS_COP.1(1), FCS_COP.1(2), FCS_CKM.1, FCS_CKM.4).

The evaluation team also performed a penetration flaw hypothesis analysis of the product to prepare for a penetration testing effort. The analysis examined each SFR to determine whether it was possible that the evaluated configuration could be susceptible to a vulnerability. The specific penetration tests executed include the following:

- Use a port scanner to check for open ports on the TOE (IPS 4240 and IDSM-2)
- Checked that TOE does not allow any non-encrypted communication (HTTP and Telnet) to the TOE Management interfaces (IDM and CLI)
- Checked that the TOE hide/mask all use of password by any means (IDM, CLI, Console) and that the actual password cannot be seen though eavesdropping

- Checked that the TOE does not allow access to any of its Management Interfaces (IDM, CLI, Console) without proper I&A performed and successfully completed first

The evaluation team constructed and ran each of the identified tests. The results of the penetration test execution verified that none of the hypothesized flaws was exploitable.

8 Evaluated Configuration

The evaluated configuration of the TOE includes four representations. **Error! Reference source not found.**2 below shows an actual picture of the physical TOE representations. On the left side of the picture is the Cisco IPS 4200 Series appliance, representative of all appliance models covered in this ST. The appliance is a self contained unit which provides all TOE functionality for the Appliance TOE. The Cisco NM-CIDS and Cisco IDSM-2 shown in the picture are the plug-in modules sitting atop the router appliance and switch appliance respectively. The plug-in modules each provide all TOE functionality for the Module TOE. Though the Cisco AIP SSM is not pictured, it is similar to the Cisco NM-CIDS and the Cisco IDSM-2 in that the AIP SSM is a plug in module for the ASA appliance and provides all TOE functionality for the Module TOE. The specific module and appliance models for the TOE are listed below in **Error! Reference source not found.**. These models only differ in hardware configuration and throughput and do not affect how the security functions specified in the ST are met.

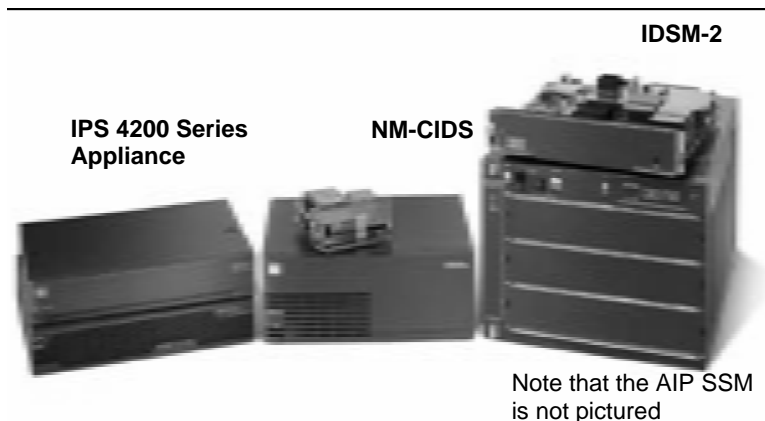


Figure 2 TOE Implementations

Table 4: TOE Appliances and Modules

Model Name	Part Number
Appliances	
IDS-4215	IDS-4215-4FE-K9
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9
IPS-4240	IPS-4240-K9
IPS-4255	IPS-4255-K9
IPS-4260	IPS-4260-K9
Modules	
AIP-SSM-10	ASA-SSM-AIP-10-K9
AIP-SSM-20	ASA-SSM-AIP-20-K9
IDSM-2	WS-SVC-IDSM2-K9
NM-CIDS	NM-CIDS-K9

The evaluation team determined that the developer’s test methodology met the coverage requirements and that the actual test results matched the expected results.

The evaluated configuration was tested in the configuration identified in Figure 3, below. The evaluation results are valid for all configurations of Cisco IPS v6.0 (appliance and modules) identified in Table 4.

Figure 3: Cisco IPS v6.0 testing environment

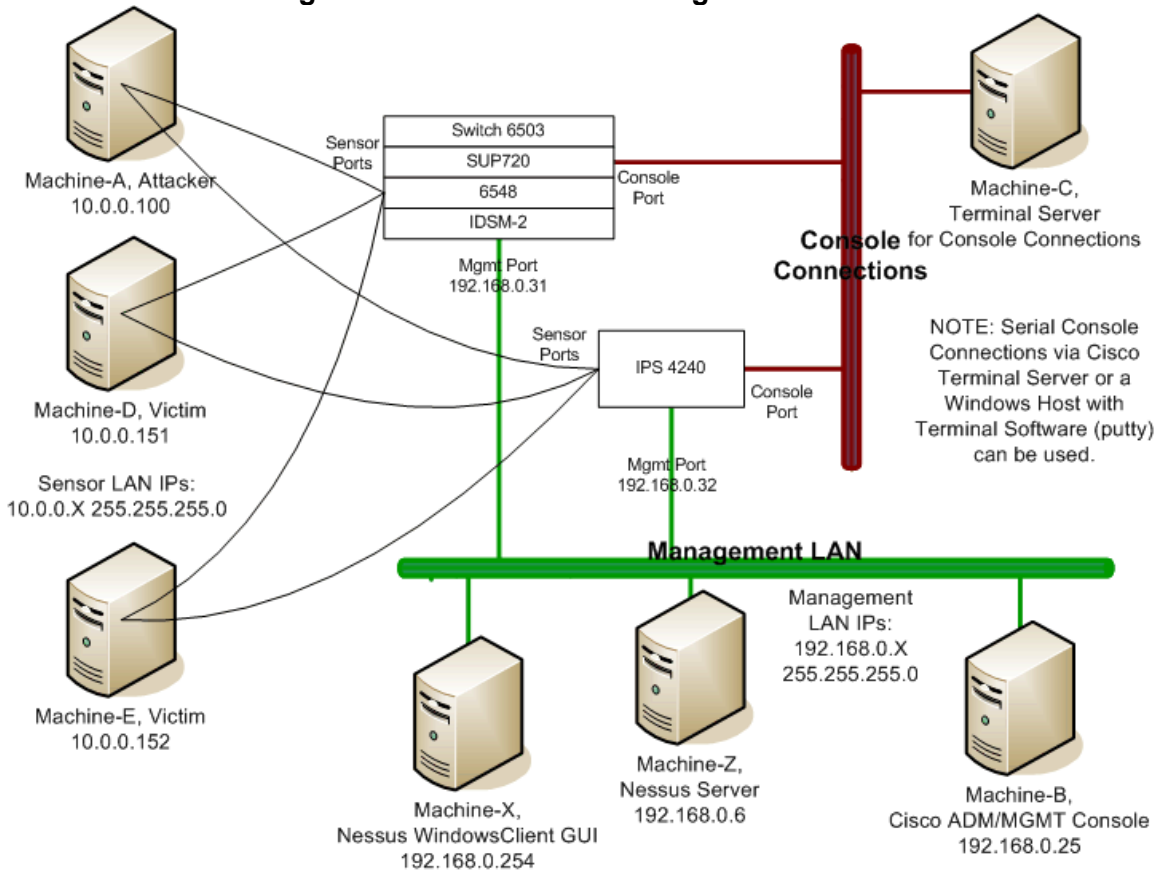


Table 4 - Hardware and Software Components

Component	Description
TOE: Cisco IPS v6.0 IDSM-2 Module (WS-SVC-IDSM2-K9) IT Environment: Cisco Switch 6503 with SUP720 module	Module TOE IDSM-2 running IPS software 6.0 with the IT Environment Cisco Switch 6503 with SUP720 and 6548 modules, SUP720 running 12.2(18)SXF5
TOE: Cisco IPS 4240	Appliance TOE IPS 4240 running IPS software 6.0

9 Results of the Evaluation

The evaluation was conducted based on the Common Criteria (CC), Version 2.3, and the Common Evaluation Methodology (CEM), Version 2.3. The evaluation confirmed that the CISCO IPS v6.0 product is compliant with the Common Criteria Version 2.3 functional requirements (Part 2) and assurance requirements (Part 3) for EAL2.

The details of the evaluation are recorded in the CCTL's Evaluation Technical Reports (ETRs), which consist of the following documents.

- *ASE (Security Target Evaluation): ASE Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 6.0, released May 31, 2007.*
- *ACM_CAP.2 & ALC_FLR.1 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 6.0, released May 31, 2007.*
- *ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 5.0, released April 30, 2007.*
- *ADV_FSP.1; ADV_HLD.1; ADV_RCR.1 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 6.0, released May 31, 2007.*
- *AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 6.0, released May 31, 2007.*
- *ATE_COV.1; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 6.0, released May 31, 2007.*
- *AVA_VLA.1; AVA_SOF.1 Evaluation Technical Report for Cisco IPS v6.0 (IDS 4200 Series Sensors v6.0 (IPS 4255, IDS 4250, IPS 4240, IDS 4215, IPS 4260); Cisco AIP-SSm-10 and Cisco AIP-SSM-20; NM-CIDS; IDSM-2)), document version 6.0, released May 31, 2007.*

The Validator followed the procedures outlined in the CCEVS Scheme Publication #3, *Guidance to Validators of IT Security Evaluations*. The Validator observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology and the CCEVS. The Validator therefore concludes that the evaluation team's results are correct and complete.

10 Validator Comments

The Validator's observations support the evaluation team's conclusion that the CISCO IPS v6.0 product meets the claims stated in the Security Target.

.

11 Security Target

Cisco Intrusion Prevent System (IPS) Version 6.0, Security Target, Version 7.0

12 List of Acronyms

Table 55 presents the acronyms and abbreviations are used in this Security Target:

Table 5: Acronyms and Abbreviations

Acronyms / Abbreviations	Definition
ACL	Access Control List
AIP	Advanced Inspection and Prevention
ASA	Adaptive Security Appliance
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCIMB	Common Criteria Implementation Board
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
CMS	Certificate Management System
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FSP	Functional Specification
HLD	High Level Design
HMAC	Hashed Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ID	Identifier
IDS	Intrusion Detection System
IDSM-2	Intrusion Detection System Services Module
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
MAC	Message Authentication Code
NAC	Network Access Control
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NIAP	National Information Assurance Partnership
NM-CIDS	Cisco Network Module IDS
NSA	National Security Agency
NTP	Network Time Protocol
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PP	Protection Profile
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement

Acronyms / Abbreviations	Definition
SFR	Security Functional Requirement
SOF	Strength of Function
SPAN	Switched Port Analyzer
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transfer Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VACL	VLAN Access Control Lists
VLAN	Virtual Local Area Network
VR	Validation Report
XML	Extensible Markup Language

13 Bibliography

The following documents referenced during preparation of the validation report.

- [1] Common Methodology for Information Technology Security Evaluation. ISO/IEC18045. August 2005 version 2.3 CCMB-2005-08-004.
- [2] Common Criteria for Information Technology Security Evaluation, Parts 1-3, August 2005 version 2.3
- [3] CCIMB Interpretations
- [4] [CCIMB CC and CEM Interpretations Database](#)
- [5] Common Criteria Evaluation and Validation Scheme (CCEVS) for IT Security, Scheme Publications 1-6, v 2.0
- [6] [CCEVS Precedents Database](#)
- [7] [CCEVS CC and CEM Public Interpretations Database](#)
- [8] ISO/IEC 17025 General Requirements for the competence of testing and calibration laboratories, First Edition (1999, 12-15)
- [9] National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) Handbook 2001 Edition 150 Procedures and General Requirements
- [10] National Institute for Standards and Technology (NIST) Handbook 150: Requirements Analysis. 1994 Edition and 2001 Edition.
- [11] NIST NVLAP Handbook 150 IT Security Testing Handbook
- [12] Cisco Intrusion Prevent System (IPS) Version 6.0, Security Target, Version 7.0
- [13] *Cisco_IPS_v6_EAL2_CCTL_Team_Test_Plan_v5.0.doc*

14 Interpretations

14.1 International Interpretations

Official start date of the evaluation was March 24, 2006. The evaluation team performed an analysis of the international interpretations and applied those that were applicable and had impact to the TOE evaluation as the CEM work units were applied.

The following international interpretations were applied for this evaluation:

None, as all Common Criteria International Interpretations were incorporated in Version 2.3.

14.2 NIAP Interpretations

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

Table 6: Applicable Precedents

Precedent	Date
PD-0061: Security Targets for a Software TOE that runs on Multiple Platforms	2002-08-13
PD-0062: What Must Be Tested for an ST Running On Multiple Platforms?	2002-08-13
PD-0097: Compliance with IDS System PP Export Requirements	2003-08-19
PD-0106: Situations Where AGD_USR May Be Vacuously Satisfied	2004-04-20
PD-0107: IDSSPP v1.4: FPT_STM.1 Must Be Met by the TOE	2004-07-19
PD-0108: FTP_ITC.1.3 Specifies The Functions For Which A Trusted Channel Is Provided	2004-07-19
PD-0116: IDSSPP v1.4: Compliance with the Selective Audit Requirement	2005-02-04
PD-0118: Assumptions in the IDS PP v1.4	2005-05-23

14.3 Interpretations Validation

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