National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Firewall Services Module (FWSM) Version 3.1 (3.17) for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers

Report Number: **CCEVS-VR-07-0027**
Dated: **March 5, 2007**
Version: **1.0**

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

Ken Dill
Alicia Squires
Maria Musa
.

Validation Personnel:

Robin Medlock, Mitre
John Nilles, The Aerospace Corporation

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Firewall Services Module (FWSM). 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 FWSM was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and evaluation work was completed during February 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 2.2 Part 2 and Part 3 conformant, including all Information Technology Security Evaluation Final Interpretations from January 2004 through March 25, 2004, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 4 have been met. In addition, the evaluation team confirmed that the TOE uses CCEVS precedent PD-0113, to satisfy SFR FAU_STG.1, and includes all security requirements from the U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000 [FWPP] (as modified under PD-0115) with the exception of AVA_VLA.3.

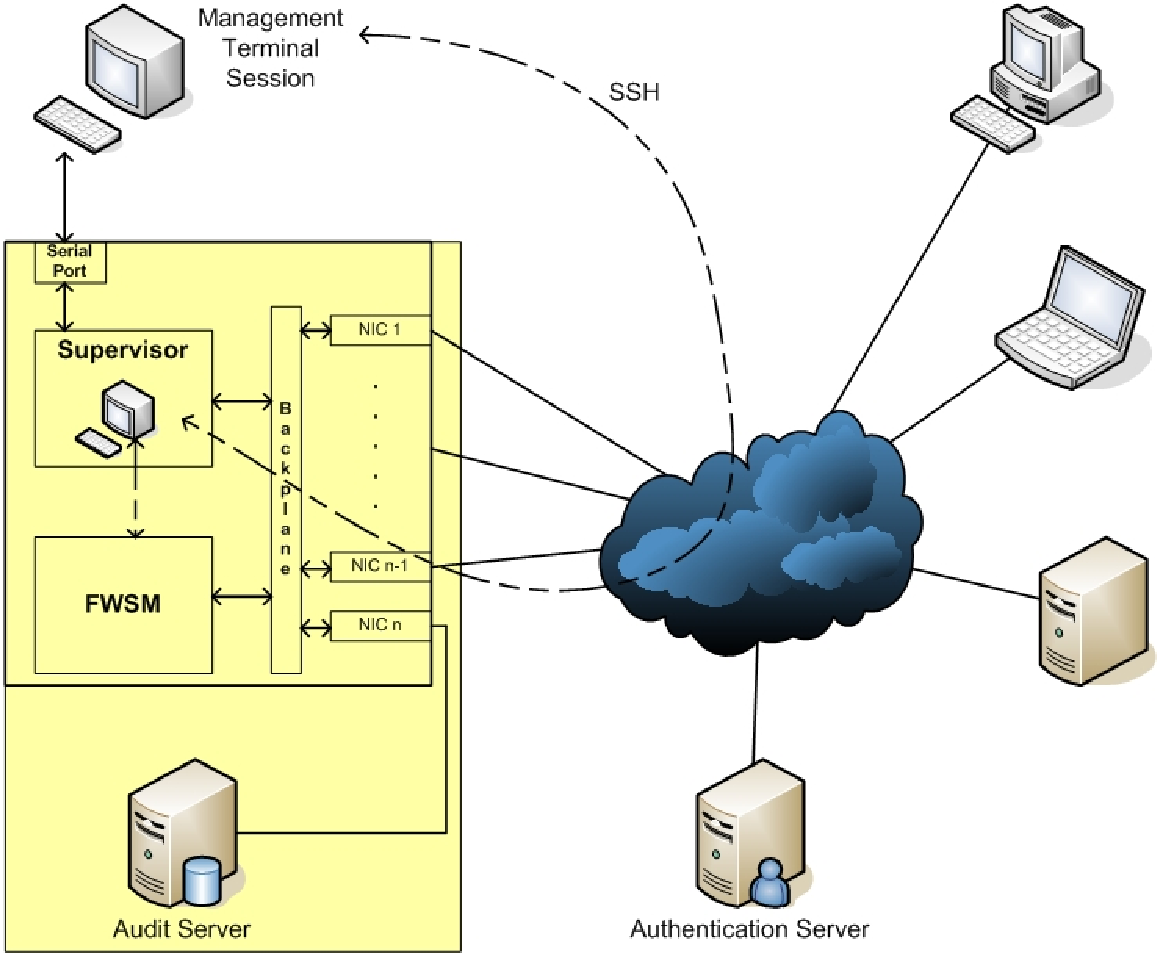
The Cisco FWSM is a firewall module that controls the flow of Internet Protocol (IP) traffic (datagrams) between network interfaces. Figure 1 illustrates the TOE and its environment. The TOE configuration consists of a Cisco FWSM that controls the flow of IP traffic between logical network interfaces over a single physical network connection. When installed inside a Cisco Catalyst 6500 Series Switch or Cisco 7600 Internet Router, the FWSM allows any port on the device to operate as a firewall port. The TOE configuration also includes a Windows 2000 or Windows XP server for the purpose of storing the audit data generated by the TOE, and an optional serial console connection and single-use TACACS+ or RADIUS authentication server for the administration of authentication of remote sessions are part of the environment. The following figure shows the FWSM in the context of a switch/router and example internet connections.
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 4 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.

Figure 1: Typical TOE Configuration



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	Firewall Services Module (FWSM) Version 3.1 (3.17) for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers, including Windows PC in its evaluated configuration as specified by the Windows 2000 Security Target, Version 2.0, 18 October 2002 or Microsoft Windows 2003/XP Security Target, Version 1.0, 28 September 2005, and PIX Firewall Syslog Server version 5.1(4).
Security Target	Security Target for Cisco Firewall Services Module (FWSM)
Evaluation Technical Report	• ASE (Security Target Evaluation): ASE Evaluation Technical Report for Firewall Services Module (FWSM) Version 3.1 (3.17) for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers, document Version 0.4, released March 5, 2007. • ACM (Configuration Management Evaluation): ACM_CAP.4; ACM_AUT.1; ACM_SCP.2 Evaluation Technical Report for Firewall Services Module (FWSM) Version 3.1 (3.17) for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers, document Version 0.4, released March 5, 2007. • ALC (Life Cycle Evaluation): ALC_DVS.1; ALC_TAT.1; ALC_LCD.1 Evaluation Technical Report for Firewall Services Module (FWSM) Version 3.1 (3.17) for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers, document version 0.3, released March 5, 2007. • ADO (Delivery and Installation Evaluation): ADO_DEL.2; ADO_IGS.1 Evaluation Technical Report for Cisco Firewall Services Module (FWSM) Version 3.1 (3.17) for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers, document Version 0.4, released March 5, 2007. • ADV (Development Evaluation): ADV_FSP.2; ADV_HLD.2; ADV_LLD.1; ADV_IMP.1; ADV_RCR.1; ADV_SPM.1 Evaluation Technical Report for Firewall Services Module (FWSM) Version 3.1 (3.17) for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers, document Version 0.3 released March 5, 2007. • AGD (Administrative and User Guidance Evaluation): AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for Firewall Services Module (FWSM) Version 3.1 (3.17) for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers, document Version 0.3, released March 5, 2007.

Item	Identifier
	• ATE (Functional Testing, Testing Coverage, Testing Depth and Independent Testing Evaluation): ATE_COV.2; ATE_DPT.1, ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Firewall Services Module (FWSM) Version 3.1 (3.17) for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers, document Version 0.3, released March 5, 2007. • AVA Vulnerability Assessment Evaluation): AVA_MSU.2; AVA_VLA.2; AVA_SOF.1 Evaluation Technical Report for Firewall Services Module (FWSM) Version 3.1 (3.17) for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers, document Version 0.3, released March 5, 2007.
Conformance Result	CC Part 2 and CC Part 3 conformant, EAL 4 Augmented with ALC_FLR.1
Applicable interpretations and precedents	▪ PD 0113: Use of Third-party Security Mechanisms in TOE Evaluations.
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)	Robin Medlock Mitre 7515 Colshire Drive McLean, VA 22102 John Nilles The Aerospace Corporation 8840 Stanford Boulevard Suite 4400 Columbia, MD 21045-5852

3 Security Policy

3.1 Identification and Authentication

The TOE requires each user to identify itself and provide authentication information before performing any other TSF-mediated action for the user. The TSF implements a password based user authentication mechanism that is used by administrative users that login via a console session to the firewall. In addition, the TSF supports the use of an external authentication server to provide single-use identity authentication for administrative users authenticating to the supervisor card (IOS) or remotely via an ssh (v2) protected network connection and for authentication of application traffic (e.g., telnet or FTP sessions) transiting through the firewall.

3.1.1 Password Based Authentication

When authenticating via a console session to the firewall, the TOE authenticates the user upon entry of the user's identity and password, relying on the following attributes, which are maintained for each user:

- User identity,
- Password,
- User's authorized administrator role association,
- Number of failed logins, and
- Lockout status.

In the event that a user fails to authenticate more than an authorized administrator-defined, non-zero number of times, the TOE locks out the user's account until an authorized administrator takes the appropriate action to allow the locked-out user to again authenticate to the TOE successfully.

3.1.2 External Authentication

When authenticating using a remotely connected terminal device, the TOE forwards the user's identity and authentication information to an external authentication server to provide authentication of the user's identity.

3.2 Roles

The TOE maintains three administrator roles: authorized firewall administrator, authorized supervisor administrator, authorized audit administrator. Only authorized firewall and supervisor administrators have the authority and permission to execute security management actions on the TOE. The authorized audit administrator is authorized to perform all privileged and administrative actions on the audit trail, which resides on the PFSS server.

3.3 Security Management

The TSF requires that authorized firewall and supervisor administrators be successfully identified and authenticated prior to performing commands restricted to the authorized firewall and supervisor administrator roles. The TSF restricts management of the following TOE management data to authorized firewall administrators:

- Enabling and disabling TOE operation;
- Enabling and disabling single-use authentication functions;
- Enabling, disabling, and managing audit trail management, including backup and restore of audit trail data on the module;
- Enabling, disabling, and managing backup and restore for TSF data and information flow rules; and

- Enabling, disabling, and managing communication of authorized external IT entities with the TOE.
- Creation, modification, and deletion of information flow rules;
- Overriding default object or information attribute values;
- Creation, modification, and deletion of user attributes;
- Setting system time;
- Setting the limit on authentication failures;

The TSF restricts management of the following TOE management data to authorized supervisor administrators:

- Enabling and disabling TOE operation;
- Enabling and disabling single-use authentication functions;
- Enabling, disabling, and managing audit trail management, including backup and restore of audit trail data on the supervisor;
- Enabling, disabling, and managing backup and restore for TSF data; and
- Enabling, disabling, and managing communication of authorized external IT entities with the TOE.
- Creation, modification, and deletion of user attributes;
- Setting system time;
- Setting the limit on authentication failures;

3.4 Security Audit

The TOE maintains an audit trail that records the date, time, subject identity, and outcome of each of the following events:

- Startup and shutdown of audit functions;
- Success and failure of all cryptographic operations;
- All decisions on information flow requests;
- User lockout (exceeding the configured number of failed logins) and restoration from lockout;
- Authentication decisions and use of the user identification mechanism;
- User attribute modifications, including user role assignments;
- Time changes; and
- Use of all audit management functions.

The TSF restricts management of the following TOE management data to audit administrators:

- Enabling, disabling, and managing audit trail management, including backup and restore of audit trail data on the PFSS Server.
- Creation, modification, and deletion of user attributes;
- Setting system time;
- Setting the limit on authentication failures;

TCP syslog is used to transmit syslog data from the FWSM module to the PIX Firewall Syslog Server (PFSS), and UDP syslog is used to transmit syslog data from the Supervisor to the PFSS. The PFSS stores audit data to the local hard disk, using the Windows 2000 or XP operating system (CC-evaluated versions) to provide protection of the stored audit records. Cisco software included with the PFSS can be used to view, search, and sort the audit logs.

3.5 Information Flow Control

The TOE performs packet filtering by applying an information flow security policy, in the form of access control lists (ACLs) and stateful inspection, to the specific interfaces of the firewall. The policy ACLs and rules can include:

- user identity
- presumed source and destination IP addresses,
- protocol identifiers,
- security-relevant service command
- interface identifiers, and
- source or destination User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) port numbers.

The TOE permits a packet arriving through one external information technology (IT) system interface to be transmitted out through another external IT system interface if each of the ACLs and rules for the interfaces is satisfied and if the human user initiating the information flow authenticates successfully (ftp and telnet traffic). Packets that do not satisfy any of these rules are logged and discarded by the TOE.

The TOE also rejects packets arriving on an external IT system interface where the presumed address associated with the packet is associated with an external IT system interface different from the one on which it arrived, effectively blocking traffic from known spoofed addresses, broadcasts, and loopbacks. In addition, protocol filtering proxies are used to deny access or service requests that do not conform to their associated published protocol.

3.6 Protection of the TSF

The TOE protects itself from external access by untrusted subjects by implementing a password-based authentication mechanism for user console connections to the firewall and a single-use authentication mechanism for all other authentication. In addition, in the evaluated configuration, the TOE provides network filtering on all network ports.

The TOE implements trusted administrator accounts and permits only authorized administrators to configure the TOE. The TOE does not support non-administrative user accounts.

The TOE implements purpose-built operating system software that does not provide the capability to load and execute additional software. All access to firewall memory is restricted to functions implemented by the TOE’s FWSM software and IOS, which are the only software that executes on FWSM blades and supervisor cards.

Internally, the TOE distinguishes and separates information flows through the appliance based on the presumed address of source and destination subjects, identification of the transport layer protocol, arriving and departing TOE interface, and network service. The privileged administrator can use these subject and information security attributes to construct access control lists that further limit information flows through the TOE. The TOE also uses the identified subject and information attributes to maintain control and separation among multiple information flows and accounts for all packets traversing the firewall in relation to the associated information stream. Therefore no residual information relating to other packets will be reused on that stream.

The TOE provides two distinct and separate communications channels: a network traffic channel and an Ethernet Out-of-Band channel (EOBC). The network traffic channel is used for traffic traversing the switch and firewall. The EOBC is used for communication between the switch supervisor and the other blades in the switch chassis (including the firewall). These two communications channels are physically separate.

4 Assumptions

4.1 Physical Security Assumption

- A.PHYSEC: The TOE is physically secure.

4.2 Personnel Security Assumption

- A.NOEVIL: Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

4.3 IT Environment Assumptions

- A.MODEXP: The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
- A.GENPUR: There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- A.PUBLIC: The TOE does not host public data.
- A.SINGEN: Information cannot flow among the internal and external networks unless it passes through the TOE.
- A.DIRECT: Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
- A.NOREMO: Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
- A.REMACC: Authorized administrator may access the TOE remotely from the internal and external networks.

5 Architectural Information

The TOE consists of the following:

- Firewall Services Module (FWSM) Version 3.1 (3.17) installed on one of the following Cisco switches:
    - 7600 Series chassis (7603, 7606, 7609, 7613) with Supervisor Engine 720, or,
    - Catalyst 6500 series (6503, 6506, 6509-NEB, 6509, 6513) with Cisco Catalyst 6500 Series Supervisor Engine 2 with Multilayer Switch Feature Card 2 (MSFC2) or Cisco Catalyst 6500 Series Supervisor Engine 720

  configured with the Cisco IOS Software Release 12.2(18)SXF5, and

- PIX Firewall Syslog Server (PFSS) software version 5.1(4) (referred to as the PIX Firewall Syslog Server) running on a:
    - Windows 2000 PC in its evaluated configuration as specified by the Windows 2000 Security Target, Version 2.0, 18 October 2002, or.
    - Windows XP PC in its evaluated configuration as specified by the Windows 2003/XP Security Target, Version 1.0, 28 September 2005.

6 Documentation

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

Table 2: Evaluation Evidence

Document Title	Version & Date
Installation and Configuration for Common Criteria EAL4+ Evaluated Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module Version 3.1(3.17) (ADM/IGS)	March 2007
Functional Specification for Firewall Services Module (FWSM) (FSP)	version 1.5, 27 February 2007.
TOE Security Policy Model for Cisco Firewall Services Module (FWSM) (SPM)	November 2006 Version: 1.2
High Level Design for Firewall Services Module (FWSM) (HLD)	27 February 2007, Version: 1.4
Low Level Design for Firewall Services Module (FWSM) (LLD),	February 2007 Version: 0-7
Configuration Management, Lifecycle and Delivery Procedures for Cisco Firewall Services Module Version 3.1 (CMP)	March 2007, Version 1.4
Development Security for Cisco PIX Security Appliances, Cisco Adaptive Security Appliances and Cisco Firewall Services Module, Reference PIXASA70FWSM31-EAL4-DEV-v1-1 (DEV)	version 1.1, 16 August 2005
Cisco Firewall Services Module (FWSM) EAL4 Detailed Test Plan (ATE)	version 1-3, March 5, 2007
Misuse Analysis for Cisco Firewall Services Module (FWSM) (MSU)	21 December 2006, Version: 1.1
Strength of Function Analysis for Cisco Firewall Services Module (FWSM) (SOF)	5 March 2007 Version: 1-2
Vulnerability Analysis for FWSM Version 3.1(3.17) (VUL)	February 2007, version 0-5
Representation Correspondence for Firewall Services Module (FWSM) (RCR)	27 February 2007 Version: 1.3

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

- Release Notes for the Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module, Software Release 3.1
- Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module from Release 2.x to Release 3.1
- Regulatory Compliance and Safety Information for the Catalyst 6500 Series and Cisco 7600 series Switches
-
- Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 3.1
- Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference, 3.1
- Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages, 3.1
- Windows 2000 Security Target, Version 2.0, dated 18 October 2002
- Windows 2003/XP Security Target, Version 1.0, 28 September 2005
- Security Target for Cisco Firewall Services Module (FWSM), Version 0.10, 5 March 2007
- PIX Firewall Syslog Server Release Notes for Version 5.1(4)

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 each SFR and developed one or more Cisco test cases that verify the function or command requirement. These tests were documented in the EAL4 Detailed Test Plan. The scope of the developer tests included all TOE Security Functions.

The developer testing addresses the following security functionality claimed by the TOE: acls, ssh communications, user lockout, logging, syslog connections, tracking of attributes for administrators, ability of administrators to carry out management functions, residual information testing, and traffic-filtering requirements (including protocol-specific inspection).

There's only one hardware model available for purchase for the FWSM, WS-SVC-FWM-1-K9. Likewise, there is one model of Supervisor Engine 2 available for customer purchase, but there are three models of Supervisor Engine 720 available. Table 4, Feature comparison for Sup720 models, identifies the differences between the three Sup720 modules. None of these differences were found to affect the security functionality of the TOE as claimed by the FSP. The developer selected one representative device to execute testing upon, configured it according to the evaluated configuration, and built a test environment to facilitate testing.

Table 4: Feature comparison for Sup720 models

#	Feature	WS-SUP720	WS-SUP720-3B	WS-SUP720-3BXL
1	ACE counters	No	Yes	Yes
2	Port security	Yes	Yes	Yes
3	IEEE 802.1x and 802.1x extensions	Yes	Yes	Yes
4	VLAN and router ACLs and Port ACLs	Yes	Yes	Yes
5	Security ACL entries	32K	32 K	32K
6	Reflexive ACLs	128K	128 K	256K
7	uRPF check in hardware	Up to 6 paths	Up to 6 paths	Up to 6 paths
8	CPU rate limiters (DoS protection)	10 special case rate limiters plus Control Plane Policing	10 special case rate limiters plus Control Plane Policing	10 special case rate limiters plus Control Plane Policing
9	Private VLANs	Yes	Yes	Yes
10	# of Interfaces with unique ACLs	512	4000	4000
11	MAC ACLs on IP	No	Yes	Yes
12	Transmission Control Protocol (TCP) intercept hardware acceleration	Yes	Yes	Yes

The developer used an existing test suite to test the PFSS component of the product.

The evaluation team determined that the developer's test methodology met the coverage and depth requirements and that the actual test results matched the 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. The evaluation team also ensured that all subsystem interfaces were tested by the developer.

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 all of the six TSF, and all 3 configurable components of the TOE.

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 line by line 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 firewall unmanaged by a rule using Nessus..
- Test the different privilege levels and granting command access to the different levels.
- Use a port scanner to test whether the PFSS server is accessible across the firewall.
- Evaluate the EOBC interface for exposure to traffic capturing.
- Explore the switch control protocol for vulnerabilities.
- Determine whether mis-configuration of the TOE would allow traffic to pass through IOS from one VLAN to another without FWSM inspection.
- Test potential abuse privilege levels using the “autocommand” command.
- Test potential misuse of the “kron” command to run commands as another user.

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 was tested in the configuration identified in Figure 2, below. The evaluation results are valid for all configurations of FWSM and its host switches identified in Section 5 of this Validation Report.

Figure 2: Cisco FWSM testing environment

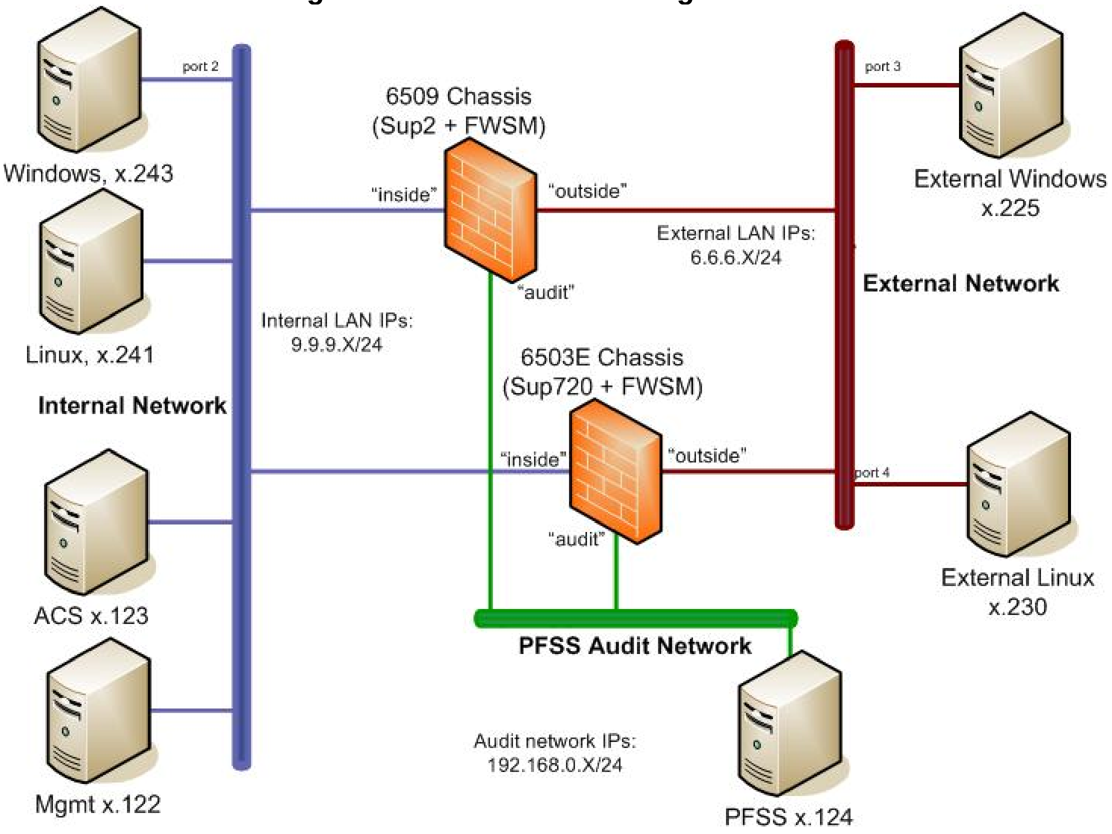


Table 3 - Hardware and Software Components

System Configuration Name	Hardware Platform	Software Platform	NICS
6509 Chassis	6509 Sup2 FWSM	IOS 12.2(18)SXF5 FWSM 3.1(3.17)	48-port 10/100 Ethernet module
6503E Chassis	6503E Supervisor 720 FWSM	IOS 12.2(18)SXF5 FWSM 3.1(3.17)	48-port 10/100 Ethernet module
Windows Management Machine	Compaq Proliant 1850R	Windows 2K Server	10/100
Windows PFSS Machine	Compaq Proliant 1850R	Windows 2K Server	10/100
Windows ACS Server	Compaq Proliant 1850R	Windows 2K Server	10/100
Windows Internal Victim	Compaq Proliant 1850R	Windows 2K Server	10/100

RedHat Internal Scanner	Compaq Proliant 1850R	Windows 2K Server	10/100
RedHat External Scanner	Compaq Proliant 1850R	Windows 2K Server	10/100
RedHat Esternal Sniffer	Compaq Proliant 1850R	Windows 2K Server	10/100

9 Validator Comments

At the conclusion of this evaluation, there are three Denial of Service (DOS) vulnerabilities in the product (FWSM 3.1(3.17)). These vulnerabilities are within the TOE but considered outside the scope of the evaluation because the Security Target does not include the threat of DOS.

These vulnerabilities have been patched in a later version of the product (FSWM 3.1(4)). The vendor has entered into assurance continuity and a maintenance release that patches these vulnerabilities will be posted.

10 Security Target

Security Target for Cisco Firewall Services Module (FWSM), Version 1.0, April 2007, text part number OL-12643-01.

11 List of Acronyms

ACL	Access Control List
API	Application Programming Interface
CC	Common Criteria
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
CLI	Command Line Interface
CMS	Certificate Management System
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
EOBC	Ethernet Out-of-Band Channel
ETR	Evaluation Technical Report
FW	Firewall
FIPS	Federal Information Processing Standard
ID	Identifier
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PC	Personal Computer
PD	Precedent Database
PFSS	PIX Firewall Syslog Server
RFC	Request for Comment
SAR	Security Functional Requirement
SFR	Security Assurance Requirement
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VR	Validation Report

12 Bibliography

The following documents referenced during preparation of the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated January 2004, Version 2.2.

[7] Security Target for Cisco Firewall Services Module (FWSM), Version 1.0, April 2007, text part number OL-12643-01.

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

[9] Cisco FWSM 3.1(3.17) EAL4 Team Test Plan and Report Version 1.3.

13 Interpretations

13.1 International Interpretations

Official start date of the evaluation was March 25, 2004. 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.

13.2 NIAP Interpretations and Precedents

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

- Precedent Database (PD) 0113: Use of Third-party Security Mechanisms in TOE Evaluations.

13.3 Interpretations Validation

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

- None.