National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme
Validation Report

Cisco PIX Security Appliances 515, 515E, 525, 535 and Adaptive Security Appliances 5510, 5520 and 5540, Version 7.0(6)

Report Number: **CCEVS-VR-07-0017**
Dated: **March 9, 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
Alicia Squires
Ken Dill
Maria Musa
.

Validation Personnel:
Robin Medlock, The MITRE Corporation
John Nilles, The Aerospace Corporation

Table of Contents

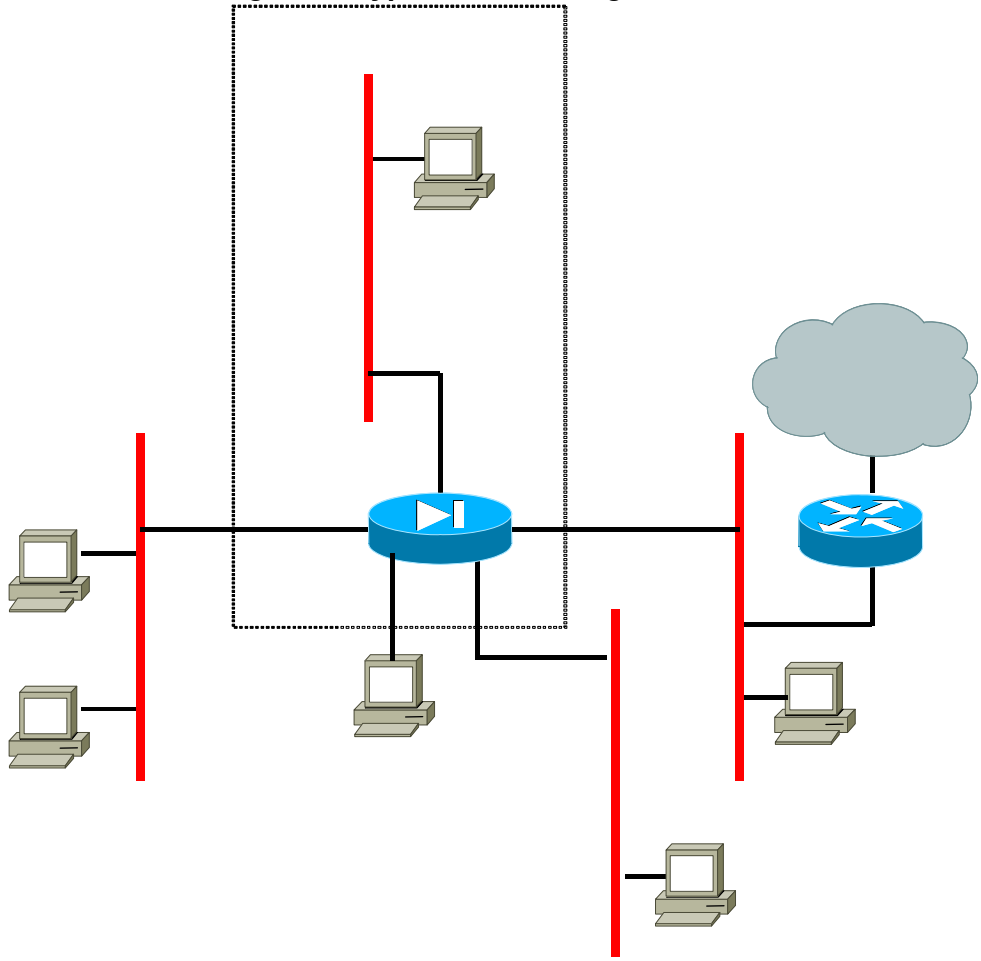
1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco PIX Security Appliance and Adaptive Security Appliance (ASA). 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 PIX and ASA was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and 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 applies 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 PIX and ASA are firewall appliances that control the flow of Internet Protocol (IP) traffic (datagrams) between network interfaces. Figure 1 illustrates the TOE and its environment. The TOE includes the Cisco PIX or ASA (shown by the Firewall in the diagram), Trusted Network for the audit server (DMZ1 in the diagram), and PIX Firewall Syslog Server (PFSS) (Audit Server 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 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.

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	Cisco PIX Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540 Version 7.0(6), 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(3).
Security Target	Security Target for Cisco PIX Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540 Version 7.0(6)

Item	Identifier
Evaluation Technical Report	• ASE (Security Target Evaluation): ASE Evaluation Technical Report for PIX Security Appliances 515, 515E, 525, 535 and Adaptive Security Appliances 5510, 5520 and 5540, Version 7.0(6), document Version 1.2, released February 5, 2007. • ACM (Configuration Management Evaluation): ACM_CAP.4; ACM_AUT.1; ACM_SCP.2 Evaluation Technical Report for PIX Security Appliances 515, 515E, 525, 535 and Adaptive Security Appliances 5510, 5520 and 5540, Version 7.0(6), document Version 1.2, released February 5, 2007. • ALC (Life Cycle Evaluation): ALC_DVS.1; ALC_TAT.1; ALC_LCD.1 Evaluation Technical Report for PIX Security Appliances 515, 515E, 525, 535 and Adaptive Security Appliances 5510, 5520 and 5540, Version 7.0(6), document version 1.3, released February 5, 2007. • ADO (Delivery and Installation Evaluation): ADO_DEL.2; ADO_IGS.1 Evaluation Technical Report for Cisco, document Version 1.2, released February 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 PIX Security Appliances 515, 515E, 525, 535 and Adaptive Security Appliances 5510, 5520 and 5540, Version 7.0(6), document Version 1.2 released February 5, 2007. • AGD (Administrative and User Guidance Evaluation): AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for PIX Security Appliances 515, 515E, 525, 535 and Adaptive Security Appliances 5510, 5520 and 5540, Version 7.0(6), document Version 1.2, released February 5, 2007. • 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 PIX Security Appliances 515, 515E, 525, 535 and Adaptive Security Appliances 5510, 5520 and 5540, Version 7.0(6), document Version 1.1, released February 5, 2007. • AVA Vulnerability Assessment Evaluation): AVA_MSU.2; AVA_VLA.2; AVA_SOF.1 Evaluation Technical Report for PIX Security Appliances 515, 515E, 525, 535 and Adaptive Security Appliances 5510, 5520 and 5540, Version 7.0(6), document Version 1.2, released February 5, 2007.
Conformance Result	CC Part 2 and CC Part 3 conformant, EAL 4
Applicable interpretations and precedents	▪ PD 0113: Use of Third-party Security Mechanisms in TOE Evaluations. ▪ ▪ I-0463: Platform Inclusion In A TOE With FPT_SEP
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

Item	Identifier
	Sterling, VA 20166
CCEVS Validator(s)	Robin Medlock The MITRE Corporation 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 directly connected terminal. In addition, the TSF supports the use of an external authentication server to provide single-use identity authentication for administrative users authenticating 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 using a directly-connected terminal device, 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,
- Privilege level of user role,
- 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 two administrator roles: authorized firewall administrator and authorized audit administrator. Only authorized firewall 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 administrators be successfully identified and authenticated prior to performing commands restricted to the authorized firewall administrator role. 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 appliance;
- 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;

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 data to the PIX Firewall Syslog Server (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 terminals connected directly to the firewall and a single-use authentication mechanism for user terminals connected through network interfaces. 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 appliance memory is restricted to functions implemented by the TOE's PIX/ASA software, which is the only software that executes on PIX and ASA appliances.

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

4 Assumptions

4.1 Physical Security Assumption

- A.PHYSEC: The TOE is physically secure.
- A.PROTECTPF: The PFSS is to be connected to the firewall such that the network interface of the PFSS is only accessible by the TSF. This may be achieved by either directly connecting the PFSS to the firewall, or indirectly over the trusted network. This protection of the PFSS network interface is required by PD-0113.

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 two physical devices:

- One of the following Cisco security appliances:
  - PIX 515, 515E, 525, 535, or,
  - ASA-5510, ASA-5520, or ASA-5540

  configured with the Cisco Secure PIX Firewall 'image' version 7.0(6), and
- PIX Firewall Syslog Server (PFSS) software version 5.1(3) (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 Cisco Adaptive Security Appliance, Version 7.0(6) (ADM/IGS)	February 2007
Functional Specification for Cisco PIX Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540 Version 7.0 (FSP)	version 1.7, 4 February 2007.
TOE Security Policy Model for Cisco PIX Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540 (SPM)	version 1.3, September 2006
High Level Design for Cisco Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540 Version 7.0 (HLD)	version 1.5, 20 December 2006
Low Level Design for Cisco Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540 Version 7.0(6) (LLD),	version 0-6, December 2006
Configuration Management, Lifecycle and Delivery Procedures for Cisco PIX Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540 Version 7.0 (CMP)	version 1.3, February 2007
Development Security for Cisco Secure PIX Firewall, Cisco adaptive Security Appliances and Cisco Systems Firewall Services Module (FWSM) (DEV)	version 1.1, 16 August 2005
Development Security for Cisco Secure PIX Firewall, Cisco adaptive Security Appliances and Cisco Systems Firewall Services Module (FWSM) (ATE)	version 2.0, 16 January 2007
Misuse Analysis for Cisco Secure PIX Firewall 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520, and 5540 Version 7.0 (MSU)	version 1.1, 12 May 2006
Strength of Function Analysis for Cisco Secure PIX Firewall 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520, and 5540 Version 7.0 (SOF)	version 1.0, 29 June 2005
Vulnerability Analysis for Cisco Secure PIX 515, 515E, 525 & 535, ASA 5510, 5520, 5540 Version 7.0(6) (VUL)	version 0-4, January 2007
Representation Correspondence for Cisco PIX Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540 Version 7.0 (RCR)	version 1.3, 20 December 2006

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

- Cisco PIX Security Appliance Release Notes
- Cisco ASA 5500 Series Release Notes
- Cisco PIX 515E Security Appliance Quick Start Guide
- Cisco ASA 5500 Quick Start Guide
- Cisco PIX Security Appliance Hardware Installation Guide
- Cisco ASA 5500 Hardware Installation Guide
- Cisco PIX Security Appliance Regulatory Compliance and Safety Information
- Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series
- Cisco Security Appliance Command Line Configuration Guide
- Cisco Security Appliance Command Reference
- Cisco Security Appliance System Log Messages
- 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 PIX Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540, Version 0.14, 7 December 2006
- PIX Firewall Syslog Server Release Notes for Version 5.1(3)

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).

Table 4, PIX and ASA Devices, identifies the individual appliances that can compose the evaluated product. The developer performed an analysis of hardware equivalency that showed that each of the devices executes the same 7.0(6) software image and that the only differences are amount of RAM, processor speed, on-board network interface cards. 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: PIX and ASA Devices

Model	CPU	DRAM	NICS (Default)
ASA 5510 adaptive security appliance	1.6 GHz Celeron	256 MB	3-10/100, 1-10/100 OOB
ASA 5520 adaptive security appliance	2.0 GHz Celeron	512 MB	4-10/100/1000, 1-10/100 OOB
ASA 5540 adaptive security appliance	2.0 GHz Pentium 4	1024 MB	4-10/100/1000, 1-10/100 OOB
PIX 515	200 MHz MMX	32 MB	2-10/100
PIX 515E	433 MHz Celeron	64 MB or 128 MB	2-10/100
PIX 525	600 MHz Pentium III	128 MB or 256 MB	2-10/100
PIX 535	1 GHz Pentium III	512 MB or 1GB	2-10/100

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 five of the six TSF, and 26 of the 30 SFRs.

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 determine whether the PFSS (Windows 2000 or XP) platform can interfere with the firewall, and performed full port scans and vulnerability scans to and through the network interfaces of the firewall.
- Confirm that messages are temporarily stored locally as well as sent off the firewall to the PFSS box. Ensure that administrator executed events while the TOE is unable to establish a connection with the syslog server are logged in the buffer, and determine whether they make it to the PFSS once logging is restored.
- Test the different administrative privilege levels and granting command access to the different levels.
- Search for publicly known buffer overflows that result in command execution or bypassing the TSF.
- Use a port scanner to check for open ports on the firewall unmanaged by a rule.

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 PIX and ASA appliances identified in Table 2.

Figure 2: Cisco PIX/ASA testing environment

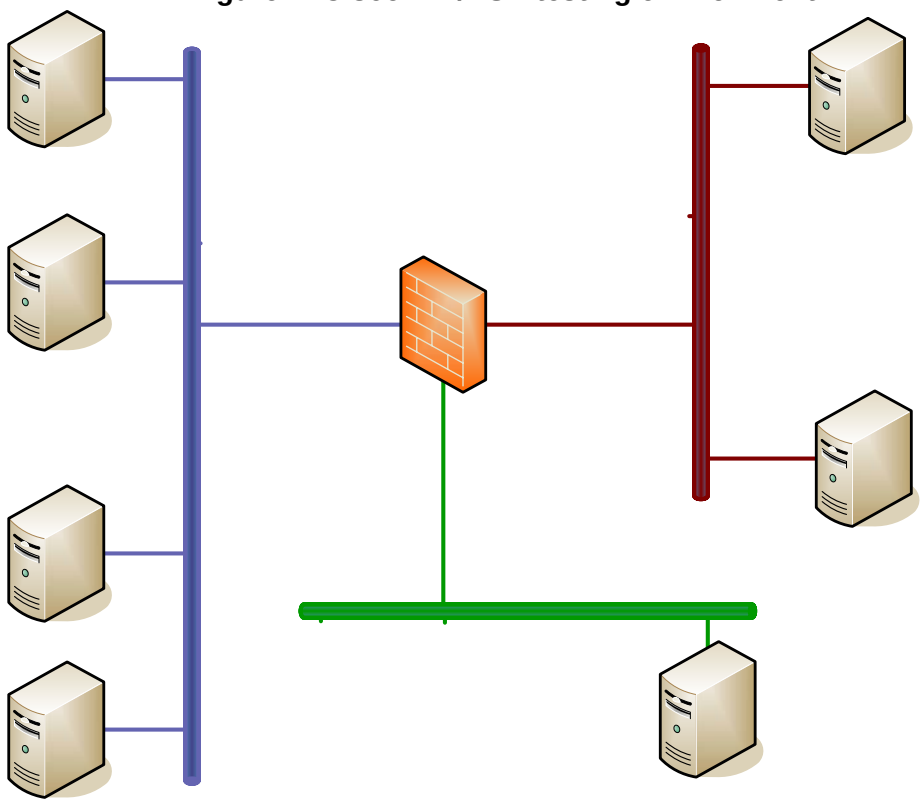


Table 3 - Hardware and Software Components

Component	Description
Cisco PIX 525	PIX running Cisco Secure PIX Firewall 'image' version 7.0(6)
Cisco ASA 5520	ASA running Cisco Secure PIX Firewall 'image' version 7.0(6)
PIX Firewall Syslog Server (PFSS)	PFSS software version 5.1(3) running on a Windows 2000 PC in its evaluated configuration as specified by the Windows 2000 Security Target, Version 2.0, 18 October 2002 (referred to as the PIX Firewall Syslog Server).

9 Validator Comments

None.

Internal Victim
x.243

10 Security Target

Security Target for Cisco PIX Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540, Version 1, March 2007.

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
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 PIX Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540, Version 0.16, 4 February 2007.

[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 PIX Security Appliances 515, 515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520 and 5540, Version 7.0(6) EAL4 Team Test Plan and Report Version 1.2.

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:

13.2 NIAP Interpretations

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

- Precedent Database (PD) 0113: Use of Third-party Security Mechanisms in TOE Evaluations.
- Interpetation I-0463: Platform Inclusion In A TOE With FPT_SEP

13.3 Interpretations Validation

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

- I-0463: Platform Inclusion In A TOE With FPT_SEP