**National Information Assurance Partnership**


TM

# Common Criteria Evaluation and Validation Scheme
# Validation Report

## Cisco IOS Firewall Versions 12.3(14)T and 12.4(4)T

**Report Number:** **CCEVS-VR-06-0050**
**Dated:** **November 27, 2006**
**Version:** **3.0**

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:
Kenneth Eggers, Orion Security Solutions
John Nilles, The Aerospace Corporation

# Table of Contents

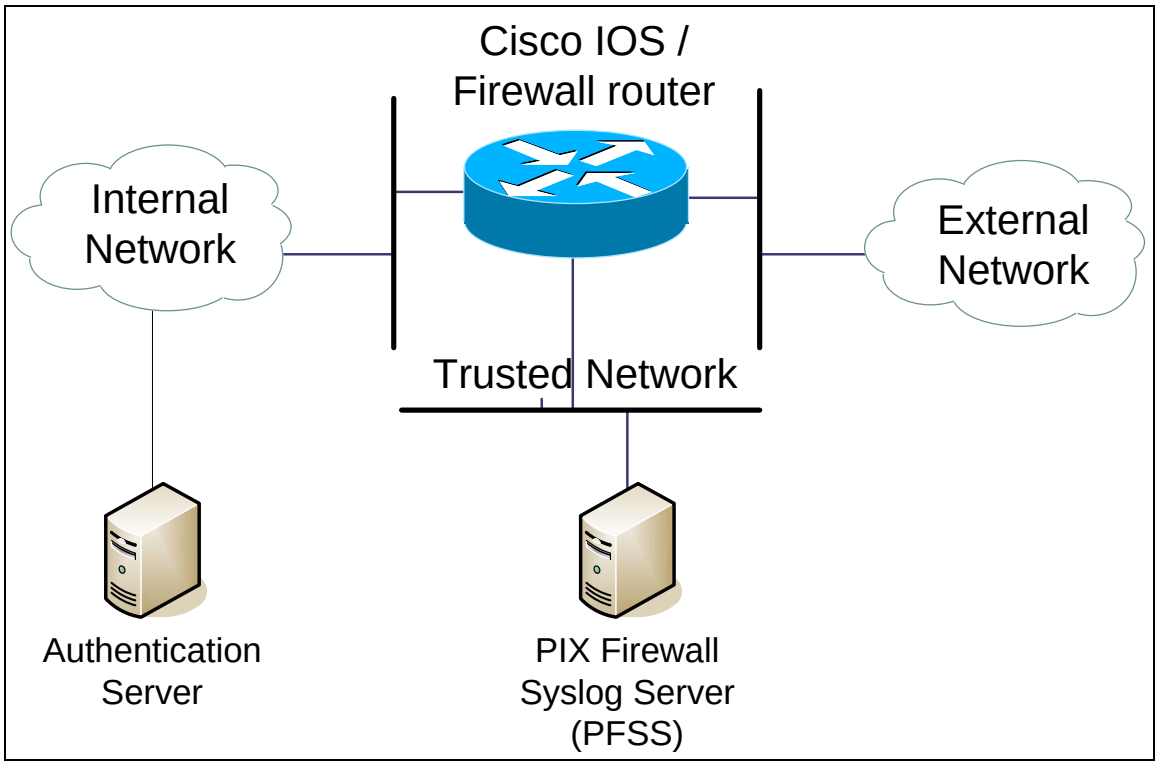
# 1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco IOS Firewall. 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 IOS Firewall was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed during October 2006. 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 September 30, 2004, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.1 have been met. In addition, the evaluation team confirmed that the TOE uses CCEVS precedent PD-0113, to satisfy SFR FAU_STG.1.

The Cisco IOS Firewall is the firewall functionality that operates within a specific group of Cisco routers running the Cisco Internetwork Operating System (IOS). Figure 1 illustrates the TOE and its environment. The TOE includes the Cisco IOS Firewall Router, Trusted Network, and PIX Firewall Syslog Server (PFSS). The evaluated configuration is specified in Section 8, Evaluated Configuration.

**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 joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) 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 IOS Firewall Versions 12.3(14)T and 12.4(4)T, including Windows PC in its evaluated configuration as specified by the Windows 2000 Security Target, Version 2.0, 18 October 2002, and PIX Firewall Syslog Server version 5.1(3). |
| Security Target | Security Target for Cisco IOS Firewall Version 1.0 |
| Evaluation Technical Report | • ACM_AUT.1, ACM_CAP.4, ACM_SCP.2 Evaluation Technical Report for Cisco IOS Firewall Versions 12.3(14)T and 12.4(4)T, Version: 1.4, 27 August 2006<br>• ADO_DEL.2; ADO_IGS.1 Evaluation Technical Report for Cisco IOS Firewall Versions 12.3(14)T and 12.4(4)T, Version 1.3, 27 November 2006 |

| Item | Identifier |
|---|---|
| | • AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for IOS Firewall Versions 12.3 (14)T and 12.4(4)T, Version 1.4, 27 November 2006<br>• ALC_DVS.1, ALC_LCD.1, ALC_TAT.1 Evaluation Technical Report for Cisco IOS Firewall Versions 12.3(14)T and 12.4(4)T, Version 1.5, 27 November 2006<br>• ASE Evaluation Technical Report for IOS Firewall Versions 12.3(14)T and 12.4(4)T, Version 1.2, 19 September 2006<br>• AVA_MSU.1; AVA_SOF.1; AVA_VLA.2 Evaluation Technical Report for IOS Firewall Versions 12.3(14)T and 12.4(4)T, Version 1.5, 27 November 2006<br>• ADV - ADV_FSP.2; ADV_HLD.2; ADV_RCR.1; ADV_LLD.1; ADV_IMP.1; ADV_SPM.1 Evaluation Technical Report for IOS Firewall Versions 12.3(14)T and 12.4(4)T, Version 1.3 28 August 2006<br>• ATE - ATE_COV.2; ATE_DPT.1 ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for IOS /Firewall Versions 12.3(14)T and 12.4(4)T, Version 1.2, 25 August 2006 |
| 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.<br>▪ PD 0115: Third Party Authentication is permitted by the ALFWPP-MR<br>▪ I-0463: Platform Inclusion In A TOE With FPT_SEP |
| Sponsor | Cisco Systems Inc.<br>170 West Tasman Drive<br>San Jose, CA 95124-1706 |
| Common Criteria Testing Lab (CCTL) | SAVVIS Communications<br>Arca Common Criteria Testing Laboratory<br>NVLAP Lab Code 200429<br>45901 Nokes Boulevard<br>Sterling, VA 20166 |
| CCEVS Validator(s) | Kenneth W. Eggers<br>Orion Security Solutions, Inc.<br>4115 Earl Lee Cove<br>Williamsburg, VA 23188-8026<br><br>John Nilles<br>The Aerospace Corporation<br>8840 Stanford Boulevard<br>Suite 4400<br>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 log 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 in-band network connection. TOE support for authentication of application message traffic (e.g., telnet or FTP messages) transiting through the router was not included in the evaluation.

### 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 authentication information to an external authentication server to provide authentication of the user's identity.

## 3.2 Roles

The TOE maintains three administrator roles: privileged administrator, semi-privileged administrator, and audit administrator. Only privileged administrators have the authority and permission to execute security management actions on the TOE. The 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 authenticated administrators explicitly enter the "enable" command and password prior to performing commands restricted to the privileged administrator role. The TSF restricts management of the following TOE management data to privileged administrators:

- 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;
- 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 router;
- 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.

## 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;
- User attribute modifications, including user role assignments;
- User login and logout attempts;
- User lockout (exceeding the configured number of failed logins) and restoration from lockout;
- All decisions on information flow requests;
- Success and failure of all cryptographic operations;
- 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.

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 operating system to provide protection of the stored audit records. Purpose-built 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 TOE-enabled router. The policy ACLs and rules can include:

- presumed source and destination IP addresses,
- protocol identifiers,
- 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. 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.

### 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 router 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 authenticated privileged 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 router memory is restricted to functions implemented by the TOE's IOS software, which is the only software that executes on TOE-enabled routers.

Internally, the TOE distinguishes and separates information flows through the router 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.

## 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.REMACC: Authorized administrator may access the TOE remotely from the internal and external networks.
- A.PROTECTIF: The PFSS is to be connected to the IOS\Firewall enabled router 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 router, or indirectly over the trusted network. This protection of the PFSS network interface is required by PD-0113.

# 5 Architectural Information

The TOE consists of two physical devices:

- One of the following Cisco routers:
  - Model c871, c876, c877, or c878,
  - Model c1811 or c1812, or
  - Model c1801, c1802, or c1803,

  configured with the IOS operating system and firewall software version 12.4(4)T; or
  - Model c1841,
  - Model c2801, c2851, c2821, or c2811,
  - Model c3845 or c3825, or
  - Model 7206VXR, 7204VXR, or CISCO7301

  configured with the IOS operating system and firewall software version 12.3(14)T, and
- PIX Firewall Syslog Server (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).

# 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 IOS Firewall (ADM) | version 1-0, October 2006 |
| Functional Specification for Cisco IOS Firewall (FSP) | version A.20, 28 July 2006. |
| TOE Security Policy Model for Cisco IOS Firewall (SPM) | version A.13, 24 August 2005 |
| High Level Design for Cisco IOS Firewall (HLD) | version A.14, 30 June 2006 |
| Low Level Design for Cisco IOS /Firewall (LLD), | version 1-5, 28 June 2006 |
| Cisco's Configuration Management Plan and Delivery Procedures (CMP) | version 0-8, 7 August 2006 |
| Cisco IOS Firewall Specific Configuration Items List and Delivery Procedures (CL) | version 0-9, 30 June 2006 |
| Development Security for Cisco IOS (DEVSEC) | version 0-3, September 2005 |
| IOSFirewall-EAL4-COV-DPT spreadsheet (ATE) | version 0-11, June 2006 |
| Misuse Analysis for Cisco IOS Firewall (MSU) | version 0-3, August 2005 |
| Vulnerability Analysis/Strength of Function Analysis for Cisco IOS Firewall (VLA-SOF), | version 0-8, April 2006 |

| Document Title | Version & Date |
|---|---|
| Representational Correspondence Demonstration for Cisco IOS Firewall (RCR) | version A.10, 30 June 2006 |

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

- Cisco IOS Configuration Fundamentals and Network Management Configuration Guide
- Cisco IOS Configuration Fundamentals Command Reference
- Cisco IOS Security Configuration Guide (12.3)
- Cisco IOS Security Command Reference
- Cisco IOS IP Configuration Guide
- Cisco IOS IP and IP Routing Command Reference
- Cisco IOS Software System Error Messages
- Release Notes for Cisco IOS Release 12.3(x)
- Caveats for Cisco IOS Release 12.3
- Hardware Installation Guides for each router platform (Table 4)
- Regulatory Compliance and Safety Information specific to each router platform (Table 2)
- RSA SecurID Ready Implementation Guide
- Windows 2000 Security Target, Version 2.0, dated 18 October 2002
- Security Target for Cisco IOS/Firewall, Version 1.0, dated October 2006
- PIX Firewall Syslog Server Release Notes for Version 6.0(1)

# 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 identified one or more existing IOS test case documents that includes test cases that verify the function or command requirement. Where tests did not exist for SFRs or functions, additional test procedures were created and documented in an evaluation-specific Adjunct Test Procedure document. The scope of the developer tests included all TOE Security Functions.

Cisco performs regression testing on major IOS releases, including "T" releases, on a weekly basis according to a schedule. The goal of regression testing is to find defects in the product prior to release. Cisco product developers write tests for their products and they are scripted for repeatability. They are then turned over to Cisco's Automated Regression Facility group, who runs them regularly on new releases of the product. 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.

Table 4, Router Model Families, identifies the individual router models that can host the evaluated product. The developer performed an analysis of hardware equivalency that showed that each router model in a model family is equivalent to the other routers in the same family with respect to testing. The developer selected one representative router from each router family, configured it according to the evaluated configuration, and built a test environment to facilitate testing each of the routers.

**Table 4: Router Model Families**

| Model Family | Models | IOS Version |
|---|---|---|
| 8xx | c871, c876, c877 ,c878 | 12.4(4)T |
| 18xx | c1841, c2801 | 12.3(14)T |

| | | |
|---|---|---|
| 18xx | c1811, c1812 | 12.4(4)T |
| | c1801, c1802, c1803 | 12.4(4)T |
| 28xx | c2851, c2821, c2811 | 12.3(14)T |
| 38xx | c3845, c3825 | 12.3(14)T |
| 72xx, 73xx | 7206VXR, 7204VXR, CISCO7301 | 12.3(14)T |

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 each of the 26 SFRs. The CCTL met with Cisco test developers to determine how a sample of these tests exercised the SFRs. The evaluation team was satisfied with the results of this walk through.

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) platform can interfere with the router, and initiate connection attempts to port 80 and 443 on the router.
- Confirm that messages are held in a buffer on the router in case they need to be resent. The ST states that only the events from a 9-minute period can be lost.
- Test the different privilege levels and granting command access to the different levels.
- Search for buffer overflows that result in command execution or bypassing the TSF.
- Use a port scanner to check for open ports on the router unmanaged by a rule.

In working with the validation team, the following two additional penetration tests were constructed:

- Layer 2 (VLAN tagging) testing against the IOS Firewall enabled routers – Configure the firewall between two VLAN-enabled, trunked, switched ports (on

same VLAN) and test whether those packets pass through the same CEF engine as other received traffic.

- Determine whether source-routed packets arriving at the firewall are dropped.

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 IOS operating system and Cisco IOS Firewall on Cisco routers identified in Table 2.

**Figure 2: Cisco IOS Firewall testing environment**

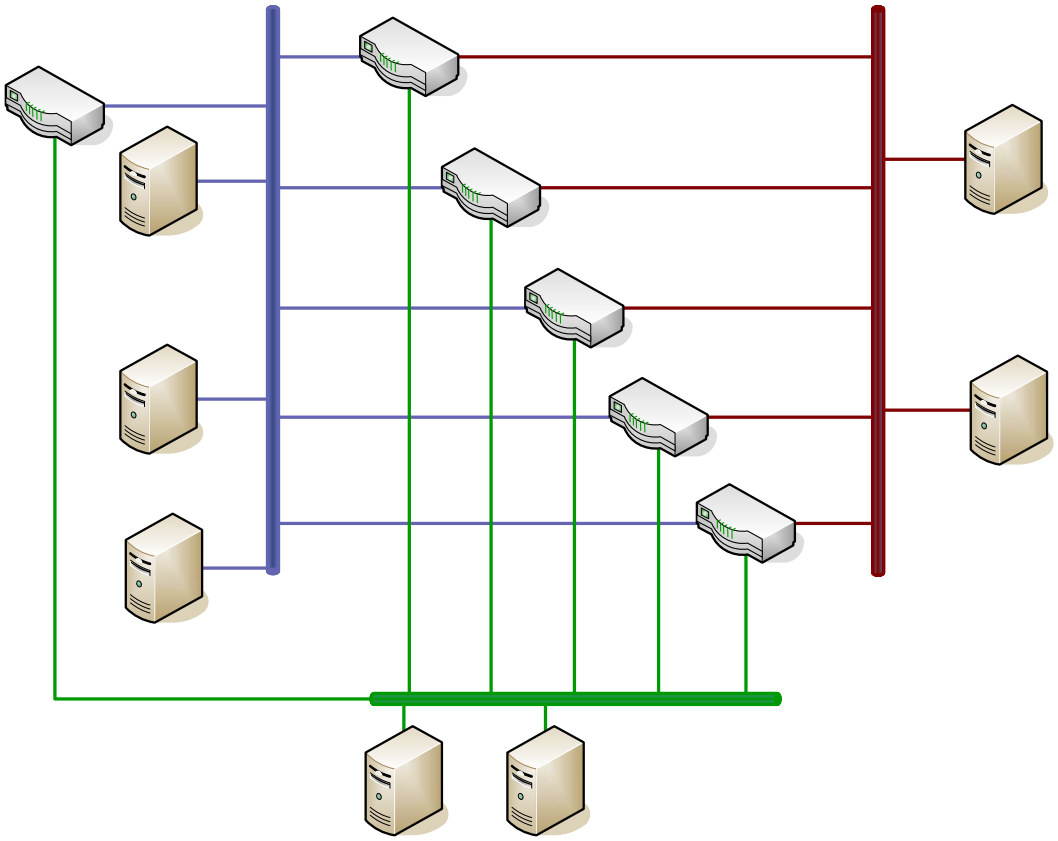


**Table 3 - Hardware and Software Components**

| Component | Description |
|---|---|
| Cisco Router Model c871, c876, c877, c878, c1811 c1812, c1801, c1802, or c1803 | Router configured with the Cisco IOS Firewall software version 12.4(4)T |
| Cisco Router Model c1841,Model c2801, c2851, c2821, c2811, c3845, c3825, 7206VXR, 7204VXR, or CISCO7301 | Router configured with the Cisco IOS Firewall software version 12.3(14)T |
| 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). |

port

port 5

WAN(4)

LAN 0

11 c871

x.50

port 2

port

# 9 Validator Comments

None.

# 10 Security Target

Security Target for Cisco IOS Firewall Version Versions 12.3(14)T and 12.4(4)T, Version 1-0, October 2006.

# 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 |
| **IOS** | Internetwork Operating System |
| **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 validation team used the following documents to prepare 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 IOS Firewall Versions 12.3(14)T and 12.4(4)T, Version 1-0, October 2006.

[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 IOS Firewall, Versions 12.3(14)T and 12.4(4)T EAL4 Team Test Plan and Report Version 1.6, 28 August 2006.

# 13 Interpretations

## 13.1 International Interpretations

Official start date of the evaluation was September 30, 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.

## 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