UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P152

Cisco Secure PIX Firewall

Version 5.2(3)

running on PIX 515, 520 and 525

Issue 1.0

February 2001

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

ARRANGEMENT ON THE
MUTUAL RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.*

*Mutual recognition applies to EAL4 but not to ALC_FLR.1 (basic flaw remediation).

Trademarks:

The following trademarks are acknowledged:

Cisco and PIX are registered trademarks of Cisco Systems Inc.
Ethernet is a registered trademark of Xerox Corporation.
Intel and Pentium are registered trademarks of the Intel Corporation.
Microsoft and Windows NT are registered trademarks of Microsoft Corporation.
Sun is a trademark of Sun Microsystems, Inc.

All other products or services mentioned herein are trademarks of their respective owners.

CERTIFICATION STATEMENT

Cisco Secure PIX Firewall Version 5.2(3) is a stateful packet filtering firewall that controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's authorised user. Traffic flow is also controlled by the use of other information, such as the direction (incoming or outgoing) of the IP packet on any given firewall network interface. The product was evaluated in a multi-homed configuration, mediating between up to 3 networks and having a network address on each.

Cisco Secure PIX Firewall Version 5.2(3) has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4, augmented with ALC_FLR.1, for the specified Common Criteria Part 2 conformant functionality, extended by a bespoke audit generation component (FAU_AUD.1), in the specified environment when running on the PIX 515, 520 and 525 hardware platforms as specified in Annex A.

Originator	**M D Brown** Certifier
Approval	**J C Longley** Deputy Technical Manager of the Certification Body
Authorisation	**Dr K Thacker** Senior Executive UK IT Security Evaluation and Certification Scheme
Date authorised	28 February 2001

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
ARP	Address Resolution Protocol
BIOS	Basic Input/Output System
CC	Common Criteria
CCI	Console Command Interface
CCO	Cisco Connection Online
CEM	Common Evaluation Methodology
CLEF	Commercial Evaluation Facility
CMS	Certificate Maintenance Scheme
DDTS	Distributed Defect Tracking System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarised Zone
DNS	Domain Name Server
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPC	Inter-Process Communication
IPSec	IP Security Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NT	New Technology
PCI	Protocol Control Information
PFSS	PIX Firewall Syslog Server
POP3	Post Office Protocol 3
RAM	Random Access Memory
RIP	Routing Information Protocol
ROM	Read Only Memory
RSH	Remote SHell
SFR	Security Functional Requirement
SIP	Session Initiation Protocol
SMTP	Simple Message Transfer Protocol
SNMP	Simple Network Management Protocol
SoF	Strength of Function
SPM	Security Policy Model
SQLNET	Structured Query Language NETworking
SSL	Secure Socket Layer
SUNRPC	Sun Remote Procedure Call
TCP	Transfer Control Protocol
TELNET	TELecommunications NETworking Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
UDP	User Datagram Protocol
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Security Target for Cisco Secure PIX Firewall 515, 520, 525,
Cisco Systems Inc,
ST, Version 1.6, January 2001.

b. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 4.0, February 2000.

c. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

d. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

e. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

f. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

g. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
Version 1.0, CEM-099/045, August 1999.

h. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation,
Common Criteria Evaluation Methodology Editorial Board,
Version 0.95 (Draft), CEM-2000/0040, June 2000.

i. Evaluation Technical Report, Common Criteria EAL4 Augmented Evaluation of Cisco Secure PIX Firewall, 515, 520 and 525, Version 5.2(3),
Syntegra CLEF,
LFS/T309/ETR, Issue 1.0, January 2001.

j. Supplement to LFS/T309 Evaluation Technical Report,
Syntegra CLEF,
LFS/T309/ETR/SUPP1, February 2001.

k. TOE Security Policy Model for Cisco Secure PIX Firewall 515, 520 and 525 Version 5.2(3),
Cisco Systems Inc,
SPM, Version 1.5, January 2001.

l. Certified Installation and Configuration for the Cisco Secure PIX Firewall 515, 520 and 525 Version 5.2(3),
Cisco Systems Inc,
78-12499-01.

m. Installation Guide for the Cisco Secure PIX Firewall Version 5.2,
Cisco Systems Inc,
78-11180-01.

n. Configuration Guide for the Cisco Secure PIX Firewall Version 5.2,
Cisco Systems Inc,
78-11201-01.

o. System Log Messages for the Cisco Secure PIX Firewall Version 5.2,
Cisco Systems Inc,
OL-0607-10.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) evaluation of Cisco Secure PIX Firewall Version 5.2(3) to the Sponsor, Cisco Systems Inc, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

- Cisco Secure PIX Firewall Version 5.2(3)

The product is also described in this report as the Target of Evaluation (TOE). The Developer was Cisco Systems Inc.

4. Cisco Secure PIX Firewall Version 5.2(3) is a stateful packet filtering firewall that controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's authorised user. This header information includes source and destination host (IP) addresses, source and destination port numbers and the Transport Service Application Protocol held within the data field of the IP packet.

5. For connection-oriented transport services, the firewall either permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. In addition to IP header information, the Cisco Secure PIX Firewall uses other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface.

6. For connectionless IP services, UDP and ICMP, the firewall either permits or denies connections on the basis of the interface at which the packet arrives, and the rules and the results of the match.

7. The product supports several connection topologies. No distinction is made between external and internal networks, although the evaluated configuration includes 3 networks, with at least one internal and one external network. The additional network interface provides for either an internal network connection (eg a DeMilitarised Zone (DMZ)) or an external network connection. The product provides a single point of defence and was evaluated in a multi-homed configuration, mediating between up to 3 networks and having a network address on each.

8. The Cisco Secure PIX Firewall software includes the Cisco proprietary operating system, Finesse, which is integrated in the TOE to provide the supporting environment under which the trusted servers of the TOE execute. The TOE software "image" is pre-installed in flash ROM on a purpose-built hardware platform. No configuration of the embedded operating system is required by the consumer to obtain a secure product. A summary of the configuration aspects is provided under "Installation and Guidance".

9. Further identification of the evaluated TOE, including the platforms on which it was evaluated, follows below under "TOE Scope".

10. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

11. An overview of the TOE's security architecture can be found in Annex B.

TOE Scope

12. Cisco Secure PIX Firewall Version 5.2(3), which includes the operating system, was evaluated running on the PIX 515, 520 and 525 hardware platforms as specified in Annex A. These platforms utilise a single Intel Pentium, Pentium II and Pentium III processor respectively.

13. Each PIX platform incorporates 3 network interface cards. The initial configuration of each platform is identical (ie the network security policy is to DENY everything). The TOE's physical boundary includes the PIX hardware and network interface cards. A fuller discussion of the consideration given to hardware platforms is detailed below under "Platform Issues".

14. The connection protocols through the TOE that are within the scope of the evaluation are Ethernet, ARP, DNS, Echo, Finger, IP, ICMP, TCP, UDP, FTP, HTTP, POP3, TELNET and SMTP. Any other type of connection through the TOE (eg H.323, SQLNET, SIP, RSH and SUNRPC) is outside the scope of the evaluation.

15. Software and hardware features beyond the scope of the TOE Security Functions (TSF) and therefore unevaluated were:

- Cut-Through Proxies
- Failover
- Network Address Translation (NAT)
- RIP
- Remote Management
- SNMP
- DHCP Server and TFTP Configuration Server
- Virtual Private Networks (software- and hardware-based IPSec encryption)
- Boothelper Installation
- Accepting updates to TOE data structures (eg routing tables) from an authorised host
- AAA server to provide Identification and Authentication of both authorised users and communication sessions set-up through the TOE.

16. The TOE interacts with a Windows NT Server 4.0 machine for the purpose of storing the audit data generated by the TOE (ie to provide protected audit trail storage) and of providing audit review facilities. The requirements for the component of the IT environment providing this functionality are identified in the Security Target [a] as follows:

Operating System	Software and Hardware Requirements
Windows NT Server Version 4.0	Intel Pentium II-based PC running the Microsoft Windows NT Server 4.0 operating system with Service Pack 4.

Requirements of the machine storing audit data generated by the TOE

17. The functionality provided by the above machine for the storage and review of the audit data generated by the TOE is beyond the scope of the evaluation.

18. The TOE has been evaluated using configurations of either 2 or 3 of the pre-installed network interface cards configured for operation. In the minimum configuration, the TOE is connected to one internal network and one external network. The installation of additional network interface cards (beyond the 3 pre-installed cards), additional RAM, the DC voltage option and the PIX Firewall Syslog Server (PFSS) are outside the scope of the evaluation.

19. Consumer registration and acquisition of the activation key from the Cisco Connection Online (CCO), together with verification of the activation key pre-installed in the delivered TOE, was within the scope of the evaluation. However, the DES-based functionality that was used to generate the activation key and the SSL functionality that was used to transfer the activation key between the CCO website and the consumer was excluded from the evaluation. The consumer acquisition of new build releases and patches to the product via the same CCO website, together with the consideration of potential vulnerabilities related to website downloads (eg spoofing the CCO website), were also excluded.

20. Aspects such as performance and reliability are beyond the scope of the evaluation.

Protection Profile Conformance

21. The Security Target [a] did not claim conformance to any Protection Profile.

Assurance Requirement

22. CC Part 3 [f] describes the scale of assurance given by predefined Evaluation Assurance Levels (EALs) on the scale EAL1 to EAL7 (where EAL0 represents no assurance). An overview of CC is given in CC Part 1 [d]. The assurance requirement for the TOE, as defined in the Security Target [a], was EAL4 augmented with ALC_FLR.1 (basic flaw remediation).

Strength of Function Claims

23. The minimum Strength of Function (SoF) was SoF-Medium. There were no IT Security Functions that had an associated SoF claim.

24. Although the TOE is designed to operate with an AAA server to provide Identification and Authentication of local and remote authorised users and of communication sessions set-up through the TOE, this functionality was outside the scope of the evaluation. Therefore, the SoF claims did not extend to the authentication mechanism.

Security Policy

25. The TOE security policies are detailed in the Security Policy Model (SPM) [k] and summarised under "Security Policy Model". There are no Organisational Security Policies or rules with which the TOE must comply.

Security Functionality Claims

26. The Security Target [a] specifies the TOE's security objectives, the threats that these objectives counter and the Security Functional Requirements (SFRs) and IT Security Functions that elaborate these objectives. All are fully specified in the Security Target.

27. All but one of the SFRs are drawn from CC Part 2 [e], the use of this standard facilitating comparison with other evaluated products. The exception was FAU_AUD.1, which is a bespoke security functional component based on the CC Part 2 component FAU_GEN.1. It was found necessary to include FAU_AUD.1, rather than FAU_GEN.1, as the requirements imposed by FAU_GEN.1 were not appropriate for the TOE. FAU_AUD.1 requires generation of audit events for all attempted connections, both successful and unsuccessful.

28. Security functionality claims are made for the following IT Security Functions:

- Security Management Function, allowing changes to the information flow policy
- Information Control Flow Function, allowing interface rules to be set
- Audit Function, providing flexibility in audit event generation
- Protection Function, ensuring that TSP enforcement functions are invoked
- Clock Function, providing date and time information for reliable time stamps

Evaluation Conduct

29. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 [b, c]. The Scheme has established a Certification Body which is jointly managed by the Communications-Electronics Security Group and the Department of Trade and Industry on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Mutual Recognition Arrangement and the evaluation was conducted in accordance with the terms of this Arrangement.

30. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [f] and the Common Evaluation Methodology (CEM) [g]. In addition, the ALC_FLR.1 component was evaluated in accordance with the latest guidance detailed in a draft CEM Supplement [h].

31. The Certification Body monitored the evaluation which was carried out by the Syntegra Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the Evaluation Technical Report (ETR) [i] to the Certification Body in January 2001. Following the CLEF response [j] to a request for further information, the Certification Body produced this Certification Report.

Certification Result

32. For the certification result see the “Evaluation Outcome” chapter.

General Points

33. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

34. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body’s view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the products and whether such patches have been evaluated and certified.

35. The issue of a Certification Report is not an endorsement of a product.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

36. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [i] under the CC Part 3 [f] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with the subsequent assurance maintenance and re-evaluation of the TOE.

Security Policy Model

37. The Evaluators confirmed that the security behaviour of the TOE was clearly articulated by the rules and characteristics of the SPM [k]. The policies modeled in the SPM were as follows:

- Security Management Policy
- Audit Security Policy
- Information Flow Control Security Policies
- Protection Security Policy
- Clock Security Policy

38. The Evaluators were satisfied that all security policies represented by the SFRs claimed in the Security Target [a] were modeled and complete.

Delivery

39. Information on the TOE delivery is provided to the customer on the CCO website and in the Certified Installation and Configuration document [l]. These sources of information provide guidance for tracking the shipment, ensuring that the evaluated versions of the TOE constituent components have been supplied and that the security of the TOE has not been compromised during delivery, together with guidance for the use of the TOE within its evaluated configuration.

40. The following measures provide security for the TOE delivery:

a. The Cisco Release Operations Group installs the TOE image on to the PIX hardware at the Cisco production site. A 56-bit DES activation key, derived from the PIX hardware serial number and the TOE image, is also written to the hardware and is then stored on a Cisco database on the CCO website.

b. The PIX hardware is then packaged in a sealed box and stored in a Cisco secure warehouse until shipping.

c. The sealed box that contains the PIX hardware is labeled with the Cisco company name and logo.

d. The sealed box details the PIX hardware and software contained inside and the Cisco Customer reference number, which the customer is able to confirm.

e. The accompanying licence pack contains the product documentation and welcome letter.

f. When an order is received, the TOE (in the sealed box) and accompanying licence pack are distributed according to availability, using the recorded delivery service of a shipping company trusted by Cisco, direct to the customer. The identity of the shipping company is detailed on the CCO website to enable checking by the customer .

g. To verify the authenticity of the product received, the customer is instructed on the CCO website and in the Certified Installation and Configuration document [l] to check for tampering in the secure packaging, then to login to the CCO website to register the product and to verify the activation key stored in their instance of the TOE. To obtain the activation key, the customer registers the product using the PIX hardware serial number. Once registered, the Cisco server looks up the customer's hardware serial number and emails the associated 56-bit activation key number to the customer.

h. The customer then starts up the TOE as instructed in [l, m] and uses the `show version` command to verify that the activation key number pre-installed in the TOE and that received from the CCO website are identical.

Installation and Guidance Documentation

41. Procedures for the installation and startup of the TOE are described in the Certified Installation and Configuration document [l]. This document refers out to the Installation Guide [m] and Configuration Guide [n], indicating the relevant sections for information on:

a. the security parameters to be entered during the secure installation and startup of the TOE (changing the installation-specific security characteristics of entities under the control of the TSF); and

b. the exceptions and problems that may arise from the use of the console commands during installation and startup.

42. The Installation Guide [m] provides descriptions of the procedures for the secure installation, generation and startup of the TOE. It discusses the following relevant topics:

- Requirements and Safety Information
- Installation Overview and Installing PIX Firewall 515, 520, 525 models
- Installing the PIX Firewall Syslog Server

43. Secure operation of the Cisco Secure PIX Firewall by an administrator is fully described in the Configuration Guide [n], System Log Messages guide [o] and the Certified Installation and Configuration document [l]. There is no end-user documentation as there are no end-users of the TOE.

44. The Configuration Guide [n] includes details of the firewall commands, including the method used to invoke the command (via the Command Console Interface (CCI)) and the

command parameters that can be set, together with examples. The guide also details the large number of security parameters that are under the control of the administrator. The System Log Messages guide [o] contains a listing of all those events relevant to TOE administration that are logged by the System Logger Agent. The guide is structured into sections for groups of error messages.

45. The Certified Installation and Configuration document [l] ensures that the TOE will be maintained in the evaluated configuration and that it will be administrated in a secure manner.

Strength of Function

46. The SoF claim for the TOE was as given above under "Strength of Function Claims". Based on their examination of all the evaluation deliverables, the Evaluators confirmed that there were no probabilistic or permutational mechanisms in the TOE.

Vulnerability Analysis

47. The Developer's vulnerability analysis described all known vulnerabilities identified in the Cisco website (ie at http://www.cisco.com/warp/public/770/52.html), which had been used as the public domain source of vulnerability information relating to the TOE. This website included feedback from consumers of the product. The analysis included a fix (ie a patch) to resolve each vulnerability identified and each patch had been included within the TOE software image. The Evaluators confirmed that there were no vulnerabilities within the scope of the evaluation that were addressed by operating constraints. They also confirmed that the following website vulnerabilities were identified as not applicable to the intended environment, as they affected functionality that was outside the scope of evaluation:

- Kerberos Client Authentication Failure, dated 1 January 2000
- Cisco PIX Firewall Manager File Exposure, dated 2 September 1998
- PIX Private Link Key Processing and Cryptography Issues, dated 16 June 1998

48. The Evaluators' vulnerability analysis considered public domain sources on 6 different recognised websites, but found no vulnerabilities beyond those detailed on the Cisco website. The Evaluators' analysis also considered the evaluation deliverables for potential vulnerabilities. The Evaluators confirmed that the Developer's vulnerability analysis was consistent with the Security Target [a] and the countermeasures detailed in the Certified Installation and Configuration document [l]. This analysis resulted in the identification of 14 penetration tests.

Testing

49. The correspondence between the tests specified in the Developer's test documentation and the IT Security Functions specified in the Functional Specification, and between the tests and the High Level Design, was complete and accurate in terms of the coverage of the Security Functions and High Level Design. Although the Evaluators identified some additional tests in the test documentation that were not identified in the Developer's mappings, the Evaluators were nevertheless satisfied that the tests were suitable to demonstrate the expected behaviour of the Security Functions. For each command used in a test, the Developer tested for correct operation,

error conditions, incorrect entry of the command, incorrect parameters (where appropriate) and parameters out of range (where appropriate).

50. The test documentation included the Test Plan and Analysis document, which detailed the test descriptions/procedures (including the pre-requisites, test order dependencies and expected results), the mapping of Security Functions to test cases, the mapping of High Level Design to test cases, the mapping of interfaces to test cases, the test environments, the test tools and the actual test results. The test results included the results of regression testing and all test results were found to be consistent with the expected results. The Evaluators noted that the test environment, including the PFSS configuration, was consistent with the security environment requirements and assumptions stated in the Security Target [a].

51. The Developer's testing was performed using a largely automated test suite, comprising both fully automated tests and manual tests, the latter prompting for external stimuli before return of control to the test suite. The test suite recorded the test results. All IT Security Functions and the TSF Interface were exercised during the testing and were addressed under the following test categories:

- Initialisation
- Basic network operation
- Console command interface
- Accounting and auditing
- Network application access control

52. The Developer tested all commands identified in the Functional Specification, except `exit` (from unprivileged mode), `pager`, `name`, `show tech-support`, `hostname`, `names`, `show traffic` and `help`. These were included in the independent tests performed by the Evaluators. The Evaluators concluded that, although the testing performed by the Developer was not exhaustive and focussed on using only 2 of the 3 network interface cards available, it provided completeness in terms of testing all of the Security Functions identified in the Functional Specification.

53. The Evaluators used the same test facilities (but several different IP addresses) as the Developer to perform independent testing as follows:

a. Prior to the start of each test on the PIX 515, 520 or 525 platform, the TOE configuration was set to a known, initial state by reloading a set of configuration parameters (eg default routes and IP addresses) from a specified, saved configuration file.

b. All but one of the 15 TOE-specific developer tests was repeated on the PIX 515 to validate the Developer's security functional testing. (The omitted test was excluded as it demonstrated the same accounting ability as one of the other repeated tests, but with different target output devices (ie the console and PFSS).) The sample included tests of all Security Functions and all developer tests that involved the use of test tools and scripts.

c. An additional test subset was devised and performed on the PIX 515 that:

i. exercised other attributes of security functionality specified in the Functional Specification that were not completely covered by the testing performed by the Developer, as documented in the Test Plan and Analysis, ie usage of commands available at the CCI;

ii. exercised most Security Functions specified in the Functional Specification, augmenting and supplementing the developer tests to more rigorously test and vary the testing approach of the Security Functions where possible;

iii. exercised the TOE using all 3 network interface cards configured for operation;

iv. focussed on the information flow control Security Functions, as these are the most complex and significant Security Functions of the TOE;

v. concentrated on "incorrect" Security Function parameters, as the developer tests were mainly positive testing of security functionality; and

vi. enabled all required TOE configuration changes to be performed at the CCI.

d. The test subset included only 13 independent functional tests due to the thoroughness of the Developer's tests.

54. The Evaluators performed the 14 penetration tests that had been identified during the evaluation on the PIX 515. These penetration tests were devised to confirm the non-exploitability of potential vulnerabilities that had been noted during the course of the evaluation. The tests were categorised under the headings of Reboot, Flood, Connection State, Spoof, Scan, ACK Spoof and Bypass. They included port flood, port scanning, ACK spoofing and TELNET flood tests using the following 4 tools:

- Divine Intervention – Plague, Version 3.0
- Krate Port Flooder, downloaded 28/11/00
- Sniffer Pro, Version 1.5.02
- AA Tools, Version 4.0c

55. Test coverage on the PIX 520 and 525 hardware platforms was as outlined below under "Platform Issues".

Platform Issues

56. The Developer repeated all security functional tests on each TOE platform (each including 3 network interface cards, but with only 2 cards in use) to demonstrate secure operation of the TOE on the PIX 515, 520 and 525 hardware platforms, including tests for all types of connection protocol. These tests used the Functional Test Configuration as detailed in Annex A. The Evaluators confirmed that all of the test results were identical and consistent with the expected results.

57. The Evaluators repeated their sample of 14 developer tests on the PIX 515 platform using an equivalent Functional Test Configuration as detailed in Annex A. No significant differences were found from the Developer's tests. To confirm consistency of results across the PIX platforms, the Evaluators repeated 3 of these 14 developer tests on either the PIX 520 or PIX 525 platforms and another 3 of these tests on all 3 PIX platforms. Therefore, the Evaluators:

- repeated 20% of the total developer tests performed, across all 3 PIX platforms
- repeated 40% of the developer tests on 2 of the PIX platforms
- repeated 93% of the developer tests on at least one PIX platform

58. The Evaluators performed their 13 independent functional tests on the PIX 515 using the same Functional Test Configuration with all 3 network interface cards in use. To confirm consistency of results across the PIX platforms, in particular for the information flow controls, the Evaluators repeated 3 of these 13 tests on either the PIX 520 or PIX 525 platforms and another 3 of these tests on all 3 PIX platforms.

59. The Evaluators performed their 14 penetration tests on the PIX 515 using the Penetration Test Configurations detailed in Annex A. To confirm consistency of results across the PIX platforms, the Evaluators repeated 8 of these 14 tests on either the PIX 520 or PIX 525 platforms and another one of these tests on all 3 PIX platforms.

60. The Evaluators found that the test results were consistent with the expected results and that the test results were consistent across all the platforms tested. No discrepancies were found for any of the tests repeated on multiple platforms.

61. The TOE has no firmware components other than the flash memory that holds the TOE image. There were no firmware dependencies affecting the evaluation.

62. The Evaluators confirmed that no security functionality traced to the hardware. However, the hardware was relied upon to provide general supporting protection mechanisms and the real time clock.

Assurance Maintenance and Re-evaluation Issues

63. With respect to the ALC_FLR.1 augmentation, the Evaluators confirmed that the flaw remediation procedures documentation was satisfactory. The procedures dealt with Bug Reports and Customer Reported Issues, including all those related to TOE security. Details of all the security flaws are maintained using the Distributed Defect Tracking System (DDTS), which tracks the corrective action and status for each product defect. Existing customers are notified of each security flaw and associated fix and the method for obtaining an updated product release by a variety of methods (although product release and patch downloads are outside the scope of the evaluation):

- TOE users are informed of information relating to a security flaw either via the monthly electronic newsletter distributed to all registered customers (ie CCO Users) or by visiting the CCO website, hosted at http://www.cisco.com.

- Information relating to flaws raised by security advisories are detailed at http://www.cisco.com/warp/public/770/52.html. This is updated with fixes and workarounds as soon as they are identified by the DDTS process.

- Information relating to a product release, patch or updated guidance can be found at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix. This will include any guidance to the User required to mitigate a security flaw or to implement the patch to a security flaw.

- The website entry http://www.cisco.com/cgi-bin/tablebuild.pl/pix provides links to all released versions of the product available to the User. The User must be a registered CCO User to access these downloads. The User is able to access patches to counter security flaws from this site.

64. Consumers should note that the EAL4 augmentation with assurance component ALC_FLR.1 was expressly included as the Sponsor intends to maintain the assurance established under an assurance maintenance scheme. Consumers should also note that continued assurance in the TOE, and any related patches, may be provided under the UK Certificate Maintenance Scheme (CMS) as briefly described in UKSP 01 [b], but this is yet to be confirmed. If the Sponsor decides to proceed with this approach, details of the most recent product build or patch covered by CMS would be provided on the UK Scheme website. Details of all updated product builds and patches covered by CMS would also be provided on the CCO website. The consumer download of updated builds and patches from the CCO website is currently outside the scope of the evaluation.

(This page is intentionally left blank)

III. EVALUATION OUTCOME

Certification Result

65. After due consideration of the ETR [i], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Cisco Secure PIX Firewall Version 5.2(3) meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4, augmented with ALC_FLR.1, for the specified Common Criteria Part 2 conformant functionality, extended by FAU_AUD.1, in the specified environment when running on the PIX 515, 520 and 525 hardware platforms as specified in Annex A.

Recommendations

66. Prospective consumers of Cisco Secure PIX Firewall Version 5.2(3) should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should only be used in accordance with the environmental considerations specified in the Security Target.

67. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under “TOE Scope” and “Evaluation Findings”.

68. The TOE should only be configured and used in accordance with the supporting guidance documentation as listed in Annex A and as briefly summarised under “Installation and Guidance Documentation”.

69. Potential consumers and administrators of the product should note the following general points with regard to the firewall:

a. a network security policy should be defined prior to any attempted installation or implementation of the firewall;

b. only the approved administrators should have physical access to the firewall, the firewall console and the PFSS; and

c. the network connections to the firewall should be controlled to prevent any firewall bypass connection from being installed.

70. Potential consumers of the TOE should ensure that the security functionality and assurance of the AAA server for the authentication of administrators and of FTP and TELNET connections, where required, is adequate for their needs.

71. Potential consumers of the TOE should also ensure that the PFSS (ie the separate Windows NT 4.0 machine allocated to the storage and review of audit data generated by the TOE) has adequate assurance to meet their needs.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of :

    - Cisco Secure PIX Firewall Version 5.2(3)

2. The Cisco Secure PIX Firewall software "image" (Version 5.2.3) is pre-installed during manufacture on the PIX platforms.

3. The supporting guidance documents are:

    - Certified Installation and Configuration for the Cisco Secure PIX Firewall 515, 520 and 525 Version 5.2(3), 78-12499-01 [l]

    - Installation Guide for the Cisco Secure PIX Firewall Version 5.2, 78-11180-01 [m]

    - Configuration Guide for the Cisco Secure PIX Firewall Version 5.2, 78-11201-01 [n]

    - System Log Messages for the Cisco Secure PIX Firewall Version 5.2, OL-0607-10 [o]

4. Further discussion of the supporting guidance material is given above under "Installation and Guidance Documentation".

TOE Configuration

5. The TOE can be configured for operation with either 2 or 3 network interface cards for internal and external networks. In both cases, at least one internal and one external network card are configured.

6. The following initial product configuration was used for the developer and evaluator tests:

    a. TOE configuration as defined in the installation and configuration guidance documentation [l-n], including identification of network interfaces and their security levels, creation of default routes and configuration of the PFSS;

    b. 3 network interface cards: 1 internal network, 1 external network and 1 DMZ. (The DMZ was configured for use in the evaluator-specified tests, but not for the developer-specified tests);

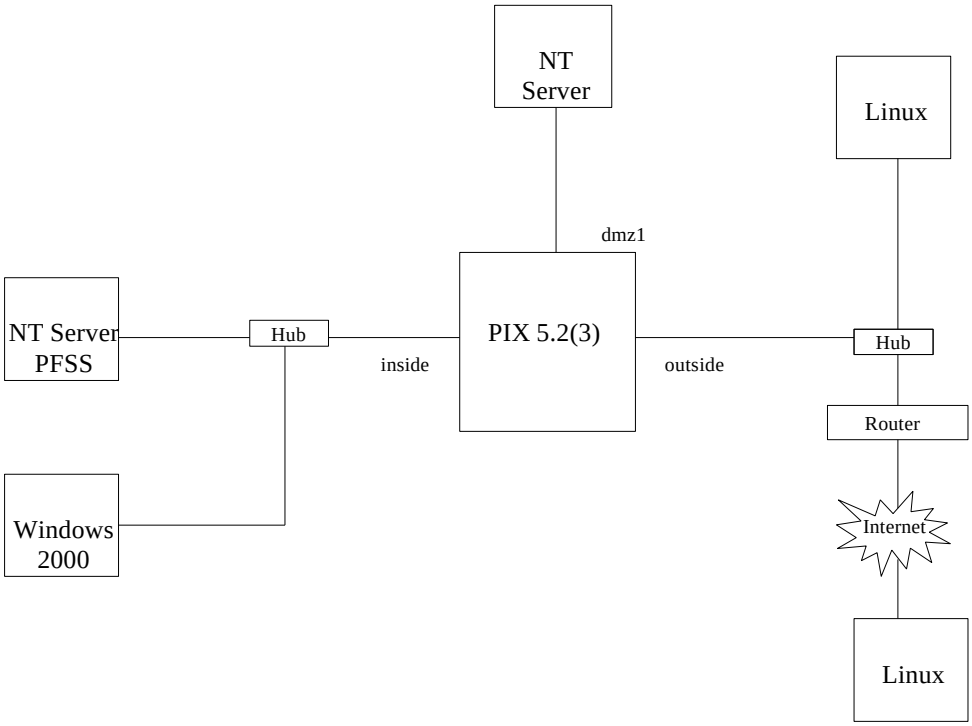
    c. connections permitted for Ethernet, ARP, DNS, Echo, Finger, IP, ICMP, TCP, UDP, FTP, HTTP (World Wide Web), POP3, TELNET and SMTP; and

    d. NAT disable option set.

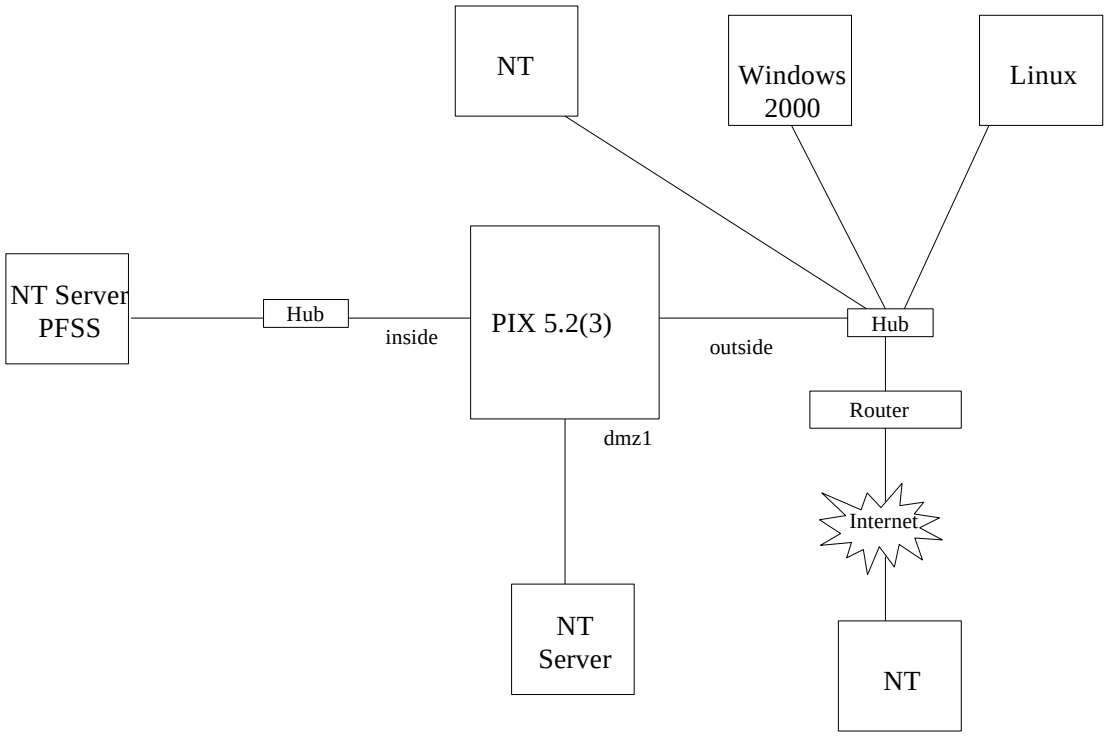
Environmental Configuration

7. The TOE was evaluated on the PIX 515, 520 and 525 hardware platforms specified below. These platforms incorporate single Intel Pentium, Pentium II and Pentium III processors respectively. The TOE includes device drivers to support the network interface cards.

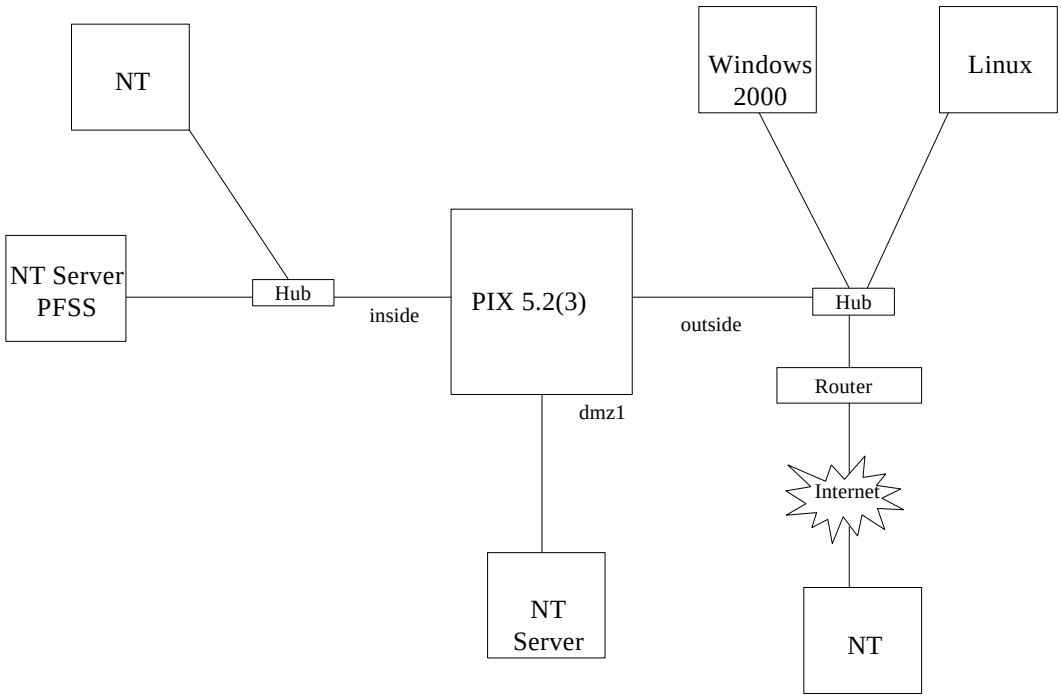
8. The following 4 diagrams illustrate the configuration of the test environments used for the functional and penetration tests that took place in the Cisco Systems Inc development premises.



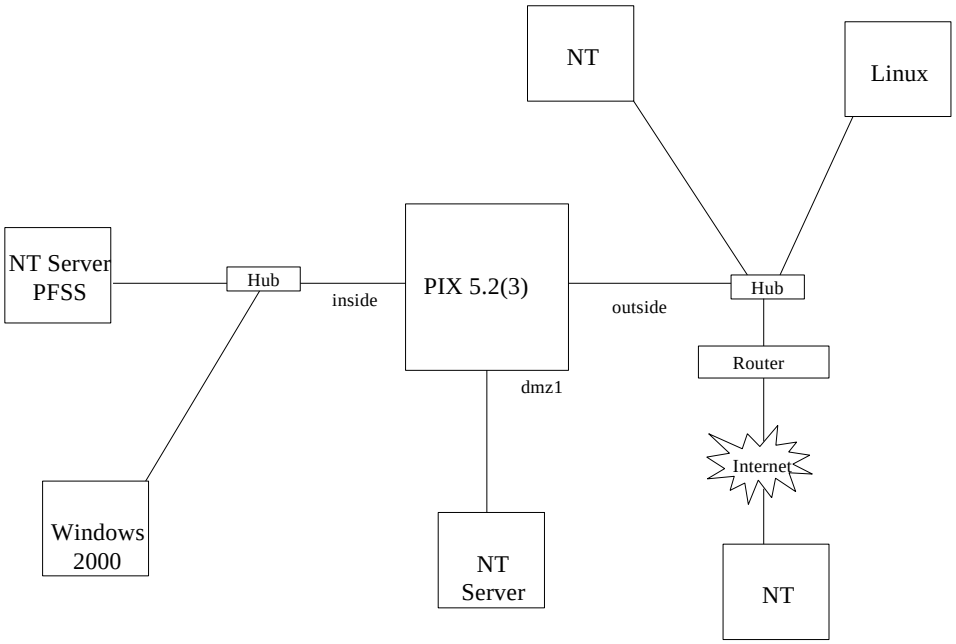
Functional Test Configuration



Penetration Test Configuration 1



Penetration Test Configuration 2



Penetration Test Configuration 3

9. The TOE in each of these test configurations was running on the PIX 515, 520 or 525 hardware platform as appropriate to the specific test.

10. The test environment included unique IP addresses for all firewalls, workstations, servers, hubs and routers in the internal and external networks of the test configurations. (The target firewall platform required 3 unique IP addresses.) All test equipment was connected to the internal and external networks via Ethernet using 10BaseT network connections (RJ45 connectors).

11. The Functional Test Configuration enabled all developer and evaluator tests related to connection protocols, different network configurations (ie 2 or 3 network interface cards operational) and the PFSS to be performed. Most of the penetration tests were run on Penetration Test Configuration 1. Several supporting penetration tests were run on Performance Test Configurations 2 and 3. Penetration Test Configuration 2 was used for the TELNET port attacks and Penetration Test Configuration 3 was used for testing the SMTP commands during shutdown.

12. The specifications of the TOE platforms are detailed below. In addition to these platforms, the test environment required the use of a variety of workstations and servers on the internal network, external network and DMZ. These machines were used to test the functionality of the TOE and to launch various penetration attacks. Although these test machines are not within the scope of the TOE, their specifications are detailed below for completeness.

13. The specification of the PIX 515 platform was as follows:

- 200MHz Intel Pentium single processor
- Flash 32k BIOS
- 64MB RAM
- 3 Intel Fast Ethernet 82559 network interface cards

14. The specification of the PIX 520 platform was as follows:

- 349MHz Intel Pentium II single processor
- 4.3 embedded and 4.0 Firewall BIOS
- 32MB RAM
- 1.44MB 3.5" Floppy Drive
- 3 Intel Fast Ethernet 82559 network interface cards

15. The specification of the PIX 525 platform was as follows:

- 600MHz Intel Pentium III single processor
- 4.3 embedded and 4.0 Firewall BIOS
- 128MB RAM
- 3 Intel Fast Ethernet 82559 network interface cards

16. The specification of the Linux workstations was as follows:

- HP Vectra XA, with RedHat Linux Release 6.1
- Family 5x86 Pentium
- Phoenix 4.05.6 BIOS
- Quantum FB ST 2.5A 2.5GB hard drive
- 64MB RAM
- Intel Pro/100b PCI adapter network interface card

17. The specification of the NT workstations was as follows:

- HP Vectra XA, with Windows NT Workstation 4.0 & Service Pack 4
- Family 5x86 Pentium
- Phoenix 4.05.6 BIOS
- Quantum FB ST 2.5A 2.5GB hard drive
- 64MB RAM
- Intel Pro/100b PCI adapter network interface card

18. The specification of the Windows 2000 workstation was as follows:

- HP Vectra XA, with Windows 2000
- Family 5x86 Pentium
- Phoenix 4.05.6 BIOS
- Quantum FB ST 2.5A 2.5GB hard drive
- 64MB RAM

- Intel Pro/100b PCI adapter network interface card

19. The specification of the PIX Firewall Syslog Server was as follows:

- Cisco In-house, with Windows NT Server 4.0 & Service Pack 4
- Family 6x86 Pentium II
- AM 1.00.06 CS1 BIOS
- Quantum FB ST 2.1A 2.1GB hard drive
- 128MB RAM
- Intel 82557 10/100 PCI adapter network interface card

20. The specification of the DMZ server was as follows:

- HP Vectra VL, with Windows NT Server 4.0 & Service Pack 6
- Family 5x86 Pentium
- Phoenix 4.05u BIOS
- Quantum FB ST 2.5A 2.5GB hard drive
- 128MB RAM
- Intel 82557 10/100 PCI adapter network interface card

21. The specification of the other network hardware was as follows:

- External hub: Cisco Fast Hub 100 series
- Internal hub: Cisco Micro Hub 10/100
- External router: Cisco 7000 Series Router

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report.

Major Architectural Features

Trusted Components and Privilege

2. The Cisco Secure PIX Firewall product consists of a set of servers executing in the environment of the Finesse operating system kernel. These operating system and server subsystems provide the network services that are executed on the firewall on behalf of an internal network machine. All subsystems are security enforcing. (For further details of these subsystems, see next subsection.)

3. The Finesse operating system subsystem is an integral part of the TOE and performs the following functions:

- Enables the administrator to configure the system real time clock
- Ensures that residual memory is cleared before reallocation
- Maintains the clock used by the Logger Agent
- Verifies the stack on each context switch to prevent stack overflow
- Provides device control
- Provides process management (including context switching)
- Provides memory management

4. Cisco Secure PIX Firewall has only one class of user who is the administrator. The administrator is trusted to manage the TOE, either locally or remotely, but remote management is outside the scope of the evaluation. Users of the network service connections through the firewall have limited rights and privileges and cannot log on to the firewall.

5. Aspects such as user identification and authentication and the storage of audit records are outside the scope of the evaluation.

External Interfaces

6. The external interfaces that comprise the TSF Interface are as follows:

- The user interface between the CCI subsystem and the terminal server

- The network interface between the IP and ARP subsystem and the network interface card

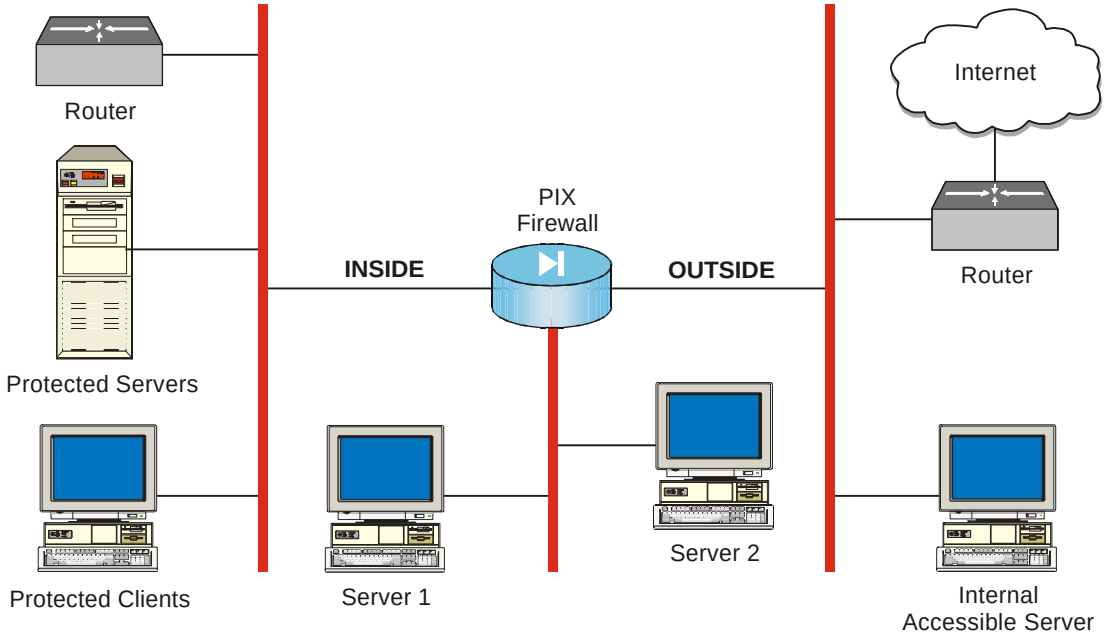
- The software/hardware interface between the Finesse subsystem and the underlying hardware

7. The CCI provides the method by which the administrator can configure the network services and directly accesses all subsystems of the TSF as described in the Configuration Guide [n]. The mechanism operates in 3 stages: unprivileged stage, privileged stage and config stage. To enter the privileged stage, the user enters a password, which changes the prompt from 'pixfirewall>' to 'pixfirewall#'. To enter the config stage, the user enters 'configure terminal' and the prompt changes to 'pixfirewall(config)#'. This mechanism helps protect changes being made to Security Functions by providing a warning to the user about the current stage. (The password mechanism is outside the scope of the evaluation.)

8. The network interface is required to enable the firewall to control traffic between an internal and external network. There are 3 physical network interface cards on the TOE. The interface to all hardware other than the network interfaces (eg the real time clock) is via the Finesse subsystem.

Design Subsystems

9. The Cisco Secure PIX Firewall controls the flow of IP traffic between network interfaces in the context illustrated below. The Cisco Secure PIX Firewall is a purpose built hardware device that uses a single Intel Pentium, Pentium II or Pentium III processor and runs the Cisco Secure PIX Firewall (Version 5.2.3) "image" .



Context for the Cisco Secure PIX Firewall

10. The physical scope of the TOE is:

- Hardware - PIX 515 (Pentium I), PIX 520 (Pentium II) or PIX 525 (Pentium III)
- Software - Cisco Secure PIX Firewall "image" (Version 5.2.3)

11. The TOE interacts with an NT Server 4.0 machine (running Service Pack 4) for the purpose of storing the audit data generated by the TOE.

12. The software code in the Cisco Secure PIX Firewall can be divided into 2 classes, operating system (Finesse) and trusted servers (Console Command Interface, IP and ARP, ICMP, TCP, Logger and Firewall). Finesse is the core kernel that provides the supporting environment under which the various trusted servers execute. The trusted servers are runtime instances of the software subsystems that provide services to other servers or to external events.

13. The purpose of each of these subsystems is identified in the table below:

Subsystem	Description
Finesse	Provides an executing environment, scheduling device management, inter-process communication and memory management.
Console Command Interface (CCI)	Provides a mediating interface agent between the TOE and the administrator.
IP & ARP Subsystem	Provides addressing, packet forwarding and packet delivery of the Internet Protocol over Ethernet.
ICMP Subsystem	Notifies IP of remote node errors such as remote host unreachable or communications failure due to link mtu and provides command interface for host discovery, ICMP (ping).
TCP Subsystem	Handles TCP packets that terminate at the TOE.
Logger Subsystem	Fans out auditing events to a console, remote Syslog Server and internal buffer.
Firewall Subsystem	Provides packet control and application level inspection. Handles all IP packets routed through the TOE

Purpose of TOE subsystems

Finesse

Executing Environment

14. Finesse provides a C runtime environment for program execution. Each instance of the program is a thread that includes a per-thread stack for variables of local scope, a virtual set of registers and a shared memory address pool. The use of a globally shared memory pool enables Finesse to avoid the high context switch penalty associated with a full flushing of the translation look-aside buffer on every context switch.

15. Finesse supports the execution of servers that are constructed with the Cisco Secure PIX Firewall image. No execution of external or third party programs is possible with Finesse. The

implication is that only trusted servers are executed. Therefore, there is no functional need for the operating system to protect itself from malicious programs.

Scheduling

16. Finesse employs a simple scheduler that has 4 priorities: critical, high, normal and low. Each lightweight process or thread selects an immutable priority and is scheduled to execute when no other higher-priority thread is ready to be executed.

Device Management

17. Finesse provides a standard framework (initialisation, registration and interfaces) for device management. Each device, except those supported directly by Finesse (such as CPU, memory, real time clock and interrupt controller), exports a device initialisation routine at startup, an initial entry point, an announcement or registration routine and a standard set of Input/Output interface functions.

Inter-Process Communication (IPC)

18. There are 3 IPC mechanisms in the Cisco Secure PIX Firewall: shared memory, standard device interface and block queue. Shared memory is the simplest mechanism and provides access to shared values. It is used mainly as communication between the CCI and the various software modules.

19. For general producer/consumer IPC, either the Cisco Secure PIX Firewall device management interface channel or a block queue is used. With the channel mechanism, a process implements a full device interface. Other processes that wish to communicate with the device can open the device to obtain a channel for IPC.

20. An alternative to exporting a device interface is a standard block queue interface. In the block queue interface, a standard queue and a sleep thread channel are created. Delivery to the block queue entails appending a message to the queue and waking up the associated waiting threads.

Memory Management

21. Finesse provides 3 types of runtime memory: automatic memory, dynamic memory and block memory:

- A stack that can be used as a scratch space for automatic memory
- 2 interfaces to dynamically allocate memory. The choice of interface is based on the frequency of utilisation. For long lived data objects, the standard ANSI C *malloc* and *free* functions are sufficient. For short lived data objects, the chunk interfaces are more efficient.
- Block memory is used for IP packet and network input/output

Console Command Interface

22. The CCI is composed of a single thread that accepts input from the user at the control console. The command is then parsed and relayed into the appropriate subsystems. It is then that the subsystem will act upon the command.

IP and ARP Subsystem

23. The IP and ARP subsystem provides addressing, packet forwarding and packet delivery of the Internet Protocol over Ethernet.

24. The IP and ARP subsystem is composed of IP devices or IP stacks and a single global routing table. The number of IP stacks corresponds to the number of datalink interfaces that exist in the TOE. One IP stack is instantiated per physical interface.

ICMP Subsystem

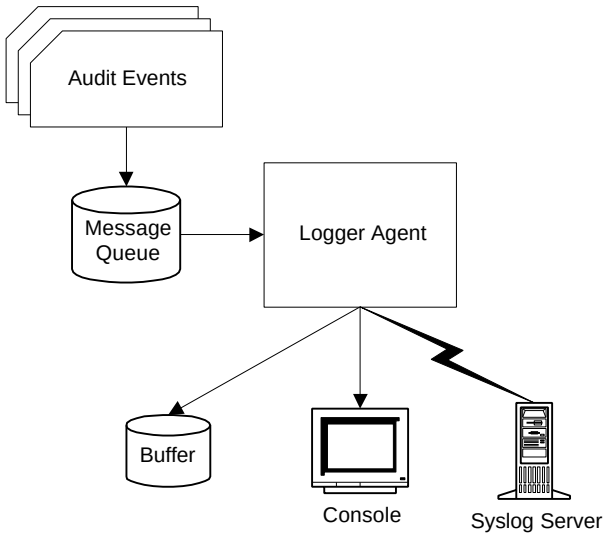
25. The ICMP subsystem implements the helper protocol to IP. The ICMP notifies IP of remote node errors such as remote host unreachable or communication failure due to link mtu. The ICMP also exports a command interface for host discovery (ping).

TCP Subsystem

26. The TCP subsystem handles TCP packets that terminate at the TOE.

Logger Subsystem

27. The Logger subsystem fans out auditing events to a console, remote Syslog Server and internal buffer, as illustrated below.



Logger Processing

28. The Logger subsystem is composed of a single functional interface, syslog, for the various systems to invoke and to deposit messages to the Logger Agent. The Logger Agent then fans out the messages to the console, remote Syslog Servers, or an internal buffer syslog monitor.

Firewall

29. The Firewall subsystem provides access control and application level inspection. The Firewall subsystem handles all IP packets that are routed through the TOE.

30. The Firewall Engine controls network sessions between 2 security zones. Each security zone is physically associated with the networks that are reachable, through to a network interface. Logically the security zone is represented by a security level associated with an interface. Networks that reside behind an interface with high security level are assumed to be more secure than networks that reside behind an interface with lower security level. At the policy level, the implication is that a session initiated from low security zone to a high secure zone is implicitly denied, while a session that is initiated from a high security level to a low security level is implicitly permitted.

31. The Firewall subsystem is composed of 3 databases: access control elements, application level inspection functions and application sessions. With stateful inspection, once a flow is established, data that belong to the flow will not need permission from the access-list to traverse the Cisco Secure PIX Firewall. The data, however, must pass the stateful inspection of the application inspection function.

32. Each flow is mapped loosely to an application communication. For TCP, the flow is defined to be the 4 tuples of source address, destination address, source port and destination port, that is initiated by a 3 way set-up handshake and is terminated with a 4 way close down sequence. For UDP, the flow is based on the same 4 tuple fields as in TCP, but with a timeout mechanism. For all other protocols, each flow degenerates to one packet.

Access Control Database (access-list)

33. The Access Control Database is the main database that controls what flows can be established through the TOE. The access-list is composed of elements that define wildcard selectors that are used to match the control data that initiated a flow. Definable selectors are IP source address, IP destination address, IP protocol and transport fields, such as TCP and UDP ports and ICMP types.

Application Level Inspection Functions (fixup)

34. The fixup database contains a static pre-defined set of application level inspection functions. These functions include FTP, HTTP and SMTP. (H.323, RSH, SQLNET and SIP are also supported, but are outside the scope of the evaluation.)

35. During initial flow set-up, a set of application level inspection functions is associated with the fixup function. The `fixup` command is used to specify the set of connection protocols and

associated ports for inspection by these functions. These connection protocols and ports are then inspected in a pre-established order for each datum that uses the flow.

Application Sessions (connection)

36. The connection database holds the states or contexts for all flows. The states are used by the protocol inspection function (stateful inspection) to verify the security attributes of data that use the connection. In addition to inspection, the states of the flow can also be used to prepare other flows that belong to the same application.

Network Address Translation

37. While NAT is not part of the Security Target, it is covered here for completeness since by default the Cisco Secure PIX Firewall assumed NAT is configured. To disable NAT, an access-list that matches all IP packets must be configured. The `nat 0 access-list` command is then used to bind the permit-all access-list to divert traffic away from NAT.

Environmental Dependencies

38. FTP and TELNET connections requiring an authentication mechanism to verify user identity rely on the AAA server, which is outside the scope of the TOE. The AAA server mediates all TELNET sessions destined for the firewall (ie those for Remote Management). For TELNET and FTP traffic flow connections routed through the TOE, the use of the AAA server depends on the TELNET and FTP server settings). Users of these connections have limited rights and privileges. Only TELNET connections related to Remote Management (which is beyond the scope of the TOE) can log on to the firewall. The administrator local login uses the same authentication mechanism to verify the administrator's access to the firewall.

39. Auditing events are recorded on the PFSS, which is outside the scope of the TOE. The PFSS is hosted on a separate machine that meets the software, hardware and security environment requirements specified in the Security Target [a]. This machine is relied upon to securely store (ie physically protect) the audit records so that only authorised access is provided to review these records.

(This page is intentionally left blank)