Security Target

for

Cisco Secure PIX

Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535

Version 6.2(2)

Reference: ST

November 2002

Version: 2.4

Europe:
Cisco Systems Ltd
10 New Square
Bedfont Lakes
Feltham
Middlesex TW14 8HA
United Kingdom

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

DOCUMENT AUTHORISATION

ENG-70839	Security Target for Cisco Secure PIX Firewall 515, 520 & 525 Version 5.2(3)
EDCS-214795	Security Target for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2)

Reference	**Version**	**Date**	**Description**
ST	1.0 DRAFT – a	22 October 1999	Draft issue for discussion with Cisco
ST	1.0 DRAFT – b	1 November 1999	Updated to reflect IT environment audit collection functionality
ST	1.0 DRAFT – c	14 December 1999	Updated following discussions with Cisco USA.
ST	1.0 DRAFT – d	26 January 2000	Updated following discussion with Certifier and Cisco.
ST	1.0 DRAFT –e	22 May 2000	Updated following comments raised in EORs
ST	1.0	3 July 2000	Updated following discussions with Cisco USA.
ST	1.1	11 August 2000	Updated following comments raised in EORs
ST	1.2	September 2000	Updated to include platform 525
ST	1.3	October 2000	Updated following discussions
ST	1.4	November 2000	Updated following discussions to remove Solaris.
ST	1.5	December 2000	Updated following discussions regarding testing platform.

ST	1.6 draft	June 2002	Initial draft to include remote management via telnet, NAT, increase supported hardware and software platforms
ST	1.7 draft	June 2002	Model references to include 501, 506, 506E, 515, 515E, 520, 525 and 535 Re-drawn the diagram to clearly show multiple interfaces Included references for maximum number of interfaces per model
ST	2.0	July 2002	Released for re-evaluation
ST	2.1 draft	July 2002	Incorporating comments from Cisco and CB
ST	2.1	July 2002	Released
ST	2.2	July 2002	Re-instated PIX model 520
ST	2.3	July 2002	Incorporating EOR1 and EOR2. More exact description of TOE. Include new Fixup protocols. Release to evaluator
ST	2.4	November 2002	Synchronise version with EDCS revision

CONTENTS

REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (aligned with ISO 15408).

GLOSSARY AND TERMS

AAA	Authentication, Authorisation and Accounting
ARP	Address Resolution Protocol
Authorised User	A user who may, in accordance with the TSP, perform an operation.
CC	Common Criteria
DHCP	Dynamical Host Control Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
H.323	a suite of protocols defined by the International Telecommunication Union (ITU) for multimedia conferences over LANs
Human User	Any person who interacts with the TOE
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IT	Information Technology
MAC	Media Access Control
NAT	Network Address Translation
NIC	Network Interface Card
OS	Operating System
PAT	Port Address Translation
POP	Post Office Protocol
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
RTSP	Real Time Streaming Protocol

SFP	Security Function Policy
SIP	Session Initiation Protocol
skinny	also known as Simple Client Control Protocol (SCCP)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SSH	Secure Shell
ST	Security Target
TACACS+	Terminal Access Controller Access Control System Plus.
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSAP	Transport Service Application Protocol
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user, that does not affect the operation of the TSF.
WWW	World Wide Web

1 Introduction to the Security Target

1.1 Security Target Identification

Title: Security Target for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).

Assurance Level: EAL4, augmented with ALC_FLR.1.

1.2 Security Target Overview

The Cisco Secure PIX Firewall is a stateful packet filtering firewall. A stateful packet filtering firewall 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 (TSAP) held within the data field of the IP packet. 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, Cisco Secure PIX firewalls use other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface.

1.3 CC Conformance Claim

This TOE has been developed to include components as defined in the Common Criteria version 2.1 [CC] part 2 extended by a bespoke audit generation component. The TOE has been developed to conform to the EAL4 assurance level, augmented with ALC_FLR.1 as identified in part 3 of [CC].

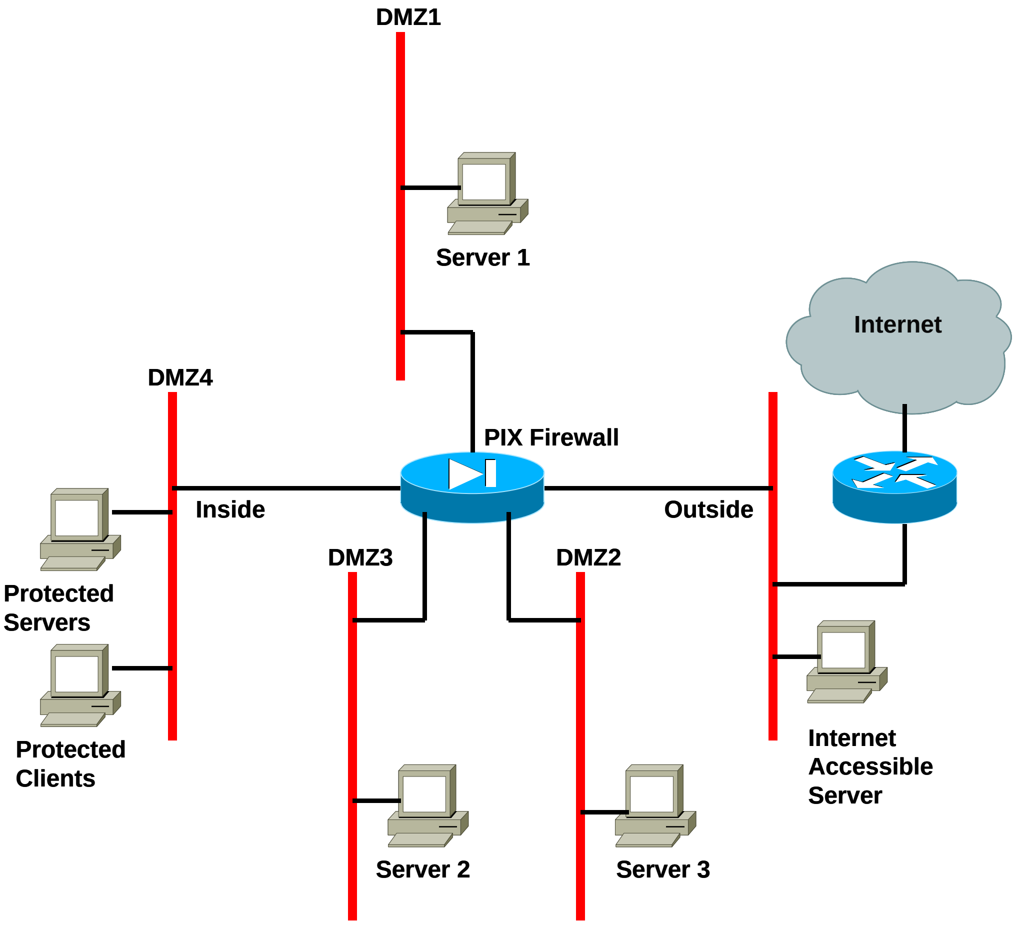
This augmentation has been included, as it is intended to maintain the assurance of the TOE under an assurance maintenance scheme.

2 TOE Description

2.1 Overview of the Cisco Secure PIX Firewall System

This section presents an overview of the Cisco Secure PIX Firewall Version 6.2 (2) to assist potential users in determining whether it meets their needs. The Cisco Secure PIX Firewall controls the flow of Internet Protocol (IP) traffic (datagrams) between network interfaces. The Cisco Secure PIX Firewall is provided on a number of platforms. The platforms included within the scope of this evaluation are 501, 506, 506E, 515, 515E, 520, 525 & 535. From hereon these platforms will referred to as the Target of Evaluation (TOE).

The Cisco Secure PIX Firewall (the TOE) is a purpose built hardware device that uses an Intel processor in all models, except the PIX 501 which uses an AMD SC520 processor. The TOE runs the Cisco Secure PIX Firewall ‘image’ version 6.2(2). It provides a single point of defence as well as controlled and audited access to services between networks by permitting or denying the flow of information traversing the firewall.



2.2 Scope and Boundaries of the Evaluated Configuration

The TOE configuration consists of:

- One Cisco Secure PIX Firewall, which controls the flow of IP traffic between network interfaces.

The TOE's physical boundary includes this single component, although the TOE relies on functionality provided by components beyond the scope of this evaluation. The physical scope of the TOE includes the hardware and software elements identified in Table 1.

Hardware	PIX 501 consisting of a **fixed configuration** with a 133 MHz AMD SC520 processor and 1 outside interface with 4 inside interfaces
	PIX 506, 506E consisting of a **fixed configuration** with a • 300 MHz Intel Celeron processor (506E); or • PI-MMX 200MHz processor (506) and 2 network interfaces.
	PIX 515, 515E consisting of a • single 433 MHz Intel Celeron processor (515E); or • PI-MMX 200MHz processor (515) with up to 6 network interfaces
	PIX 520 consisting of a 350MHz Intel Pentium II processor with up to 6 network interfaces
	PIX 525 consisting of a 600 MHz Intel Pentium III processor with up to 8 network interfaces
	PIX 535 consisting of a 1000 MHz Intel Pentium III processor with up to 10 network interfaces
Software	Cisco Secure PIX Firewall 'image' version 6.2(2)

Table 1 - TOE Component Identification

The PIX 501, 506 and 506E are fixed configuration firewalls. The PIX 515, 515E, 520, 525 and 535 models are configurable with additional modules. As well as the built-in network interfaces, three types of network module are supported. The network modules supported in this evaluation are:

- 1-port 10/100 Module (part number PIX-1FE)
- 4-port 10/100 Module (part number PIX-4FE)
- 1-port Gigabit Ethernet Module (part number PIX-1GE-66, only available on the PIX 520, 525 and 535)

The PIX 501, 506 and 506E are supplied with external AC power supplies. The PIX 515, 515E, 520, 525 and 535 are available with either AC or DC power. As the power supplies do not provide any security enforcing functionality the AC and DC powered models are treated identically.

The TOE interacts with an NT Server 4.0 machine for the purpose of storing the audit data generated by the TOE. The requirements for the component of the IT environment providing storage for the audit trail of the TOE is identified in one of the following platforms and associated software:

Operating System	**Software requirements**
NT Server 4.0	Microsoft Windows NT Server 4.0 operating system with Service Pack 6a

Table 2 Requirements of the machine storing audit data generated by the PIX firewall

Functionality provided by the component collecting audit data is beyond the scope of the evaluation.

Software and hardware features outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- Cut-through Proxies
- Failover
- RIP
- Remote Management, except via telnet from a trusted host on an inside interface
- SNMP
- DHCP Server
- Virtual Private Networks
- AAA server to provide Identification and Authentication

2.3 Application Context

The Cisco Secure PIX firewall (the TOE) provides interconnections between two or more networks depending on the number of interface cards installed within the product. For the evaluation the PIX 501, 506 and 506E will be used in their fixed configurations. A combination of network cards will be installed in the PIX 515, 515E, 520, 525 and 535. With the Cisco Secure PIX firewall it is possible to identify each network interface as either ‘internal’ or ‘external’. If an interface is identified as external then the network to which it attaches is classed as being outside of the firewall. If an interface is identified as an internal interface that the network to which it attaches is classed as being inside (or behind) the firewall. All networks inside (or behind) the firewall are protected by the Cisco Secure PIX firewall against those outside of the firewall. The Cisco Secure PIX firewall can provide protection between networks connecting to the different internal network interfaces of the TOE.

All traffic between each network attached to the TOE must flow through the Cisco Secure PIX Firewall to maintain security. The connections through the TOE that are within the scope of the evaluation are Ethernet, ARP, DNS, Echo, Finger, H.323, IP, ICMP, TCP, UDP, FTP, HTTP, POP3, RTSP, Skinny, SIP, SMTP and Telnet.

The TOE allows for Network Address Translation (NAT). NAT is used to map IP addresses from an inside interface to an outside interface. Using this feature an IP address on an inside interface is mapped to range of global IP addresses that can be addressed from the outside. The feature can also be used in the opposite direction to map addresses from the outside interface to the inside interface. Port numbers can also be mapped in this way, and this function is often referred to as Port Address Translation (PAT).

The TOE can be managed by the authorised user via a physically secure local connection or via a telnet session from an internal trusted host. The TOE must only accept Telnet sessions from trusted hosts via the inside interface.

The Cisco Secure PIX Firewall also interacts with an NT Server 4.0 machine for the purpose of storing the audit data generated by the TOE. The NT Server 4.0 platform will be used for gathering test evidence for the evaluation.

3 Security Environment

3.1 Introduction

This section provides the statement of the TOE security environment, which identifies and explains all:

1. known and presumed threats countered by either the TOE or by the security environment;

2. organisational security policies the TOE must comply with;

3. assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

3.2 Threats

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment.

3.2.1 Threats countered by the TOE

The IT assets requiring protection are the services provided by, and data accessible via, hosts on the internal network (or networks if there are multiple network interfaces on the TOE configured as being behind the firewall).

The general threats to be countered are:

- attackers on the outside the protection of the TOE may gain inappropriate access to resources within the internal network;

- users on the internal network may inappropriately expose data or resources to the external network.

If the TOE is configured to provide separation between different internal networks then the following general threats will also need to be countered:

- a user on one of the internal networks may gain inappropriate access to resources on another of the internal networks;

- a user on one of the internal networks may expose data or resources to users on other internal networks.

The following specific threats (based on the general threats) are countered:

T.INTERN A user on the internal network may attempt to connect to unauthorised hosts or access unauthorised services on the external network or other internal networks.

T.EXTERN A user on the external network may attempt to connect to unauthorised hosts or access unauthorised services on an internal network.

T.SPOOF A user may cause information to flow through the TOE into a connected network by spoofing the source IP address in the service request.

3.2.2 Threats countered by the Operating Environment

The following are specific threats that must be countered by technical and/or non-technical measures in the IT environment, or must be accepted as potential security risks.

TE.AUDATT An attempt by someone to access unauthorised hosts or services through the firewall may go undetected.

TE.AUDFUL A user may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity.

TE.SELPRO An unauthorised user may read, modify, or destroy TOE internal data.

TE.VIOLATE Users may violate the network security policy as a result of careless or wilful negligence actions by the system authorised user, resulting in an attack on the assets protected by the network security policy.

TE.MODTOE Users may not be able to detect that an unauthorised person has modified the delivered TOE image.

3.3 Organisational Security Policies

There are no organisational security policies or rules with which the TOE must comply.

3.4 Assumptions

The following conditions are assumed to exist in the operational environment.

A.PHYSICAL The TOE is physically protected so that only the authorised user of the TOE has physical access.

A.HOSTILE The firewall is physically protected to prevent hostile individuals engaging in theft, implantation of devices, or unauthorised alteration of the physical configuration (e.g. bypassing the firewall altogether by connecting the internal and external networks together).

A.AUDIT The machine used to store the audit data is physically protected so that only those authorised to access the audit data can do so.

A.AUDFUL The machine used to store the audit data has sufficient storage space to store the audit data.

A.REMOTE The authorised user must ensure that the Cisco Secure PIX firewall will only accept telnet sessions for remote management by the authorised user from trusted hosts on the internal interface.

4 Security Objectives

4.1 TOE Security Objectives

4.1.1 IT Security Objectives

The principal IT security objective of the Cisco Secure PIX firewall is to reduce the vulnerabilities of an internal network exposed to an external network (or another internal network should there be multiple internal networks) by limiting the hosts and services available. Additionally, the Cisco Secure PIX firewall has the objective of providing the ability to monitor established connections and attempted connections between networks.

The specific IT security objectives are as follows:

O.VALID The Cisco Secure PIX firewall must limit the valid range of addresses expected on each network interface.

O.HOSTILE The Cisco Secure PIX firewall must limit the internal hosts and service ports that can be accessed from the external network (or other internal networks should they exist).

O.PRIVATE The Cisco Secure PIX firewall must limit the external hosts and service ports that can be accessed from the internal network.

O.ATTEMPT The Cisco Secure PIX firewall must provide a facility for the generation of audit events of all communication attempts, both successful and unsuccessful, between each network interface.

O.SECPROC The Cisco Secure PIX firewall must provide separate areas in which to process security functions and service requests. The processing of a security function must be completed prior to invocation of subsequent security functions.

4.1.2 Non-IT Security Objectives

There are no non-IT security objectives to be satisfied by the TOE.

4.2 Environment Security Objectives

4.2.1 IT Security Objectives

The following IT security objectives are satisfied by the IT environment.

OE.AUDIT The machine used for the storage of audit data shall provide facilities to securely store audit data.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

NOE.AUDIT Authorised users of the audit facilities must ensure that the audit facilities are used and managed effectively. In particular, audit logs should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Also, the audit logs should be archived in a timely manner to ensure that the machine does not run out of audit log data storage space.

NOE.DELIV Those responsible for the Cisco Secure PIX firewall must ensure that it is delivered, installed, managed and operated in a manner that maintains the security policy.

NOE.NETWORK The Cisco Secure PIX firewall must be configured as the only network connection between the networks connected to the firewall's network interfaces.

NOE.MANAGE A Cisco Secure PIX firewall authorised user is fully trained and assigned with responsibility for day to day management and configuration of the firewall. Authorised users are trusted individuals, who have been appropriately vetted.

NOE.MODTOE The Cisco website should be secure and the downloaded TOE image must be verified by comparing the MD5 hash value for the downloaded TOE image with the value published on approved sources.

NOE.PHYSICAL The Cisco Secure PIX firewall and the audit machine must be physically protected so that only authorised users have access to Cisco Secure PIX and only authorised individuals have access to the audit machine.

NOE.REVIEW The configuration of the firewall will be reviewed on a regular basis to ensure that the configuration continues to meet the organisation's security objectives in the face of:

- Changes in the Cisco Secure PIX firewall configuration;
- Changes in the security objectives;
- Changes in the threats presented by the external network;
- Changes in the internal hosts and services available to the external network by the internal network.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

The functional security requirements are drawn from [CC] Part 2 with the exception of FAU_AUD.1 which is a bespoke security functional component based on the [CC] Part 2 component FAU_GEN.1. Table 3 below details the functional security requirements drawn from [CC] Part 2, while Table 4 details the functional security requirement not drawn from [CC] Part 2. The functional security requirements for this Security Target are discussed in detail below.

It was found to be necessary to include FAU_AUD.1 instead of FAU_GEN.1 as the requirements imposed by FAU_GEN.1 were not appropriate for the TOE.

Functional Components drawn from [CC] Part 2	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	Management of TSF data
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Access Control Functions
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
FDP_RIP.1	Subset Residual Information Protection
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps

Table 3: Functional Requirements from [CC] Part 2

Bespoke Functional Components not drawn from [CC] Part 2	
FAU_AUD.1	Audit Generation

Table 4: Functional Requirements not drawn from [CC] Part 2

5.1.1 Security Management

This section defines requirements for the management of security attributes that are used to enforce the SFP.

In the evaluated configuration, access (from a physically secure local connection or via telnet from an internal trusted host) is required to the TOE prior to management of the security attributes is possible. Once access is gained to the TOE the Authorised user needs to provide the enable (privilege mode) password to be able to manage the security attributes.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to

a) [modify] the [time];

to [an authorised user from a physically secure local connection or via telnet from an internal trusted host].

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Access Control SFP] to restrict the ability to [change_default, query, modify, delete, add] the security attributes:

a) [the interface on which the request is allowed to arrive;

b) the information flow policy rules

to [an authorised user from a physically secure local connection or via telnet from an internal trusted host].

FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the [Access Control SFP and Information Flow Control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [authorised user from a physically secure local connection or via telnet from an internal trusted host] to specify alternative initial values to override the default values when an object or information is created.

5.1.2 Security Audit[1]

This section involves recognising, recording and storing information related to security relevant activities.

FAU_AUD.1 Audit Generation

FAU_AUD.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) All auditable events for the [not specified] level of audit; and

b) [Every inbound and outbound connection].

FAU_AUD.1.2 The TSF shall record within each audit record at least the following information:

a) Date and Time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [service requested for network connections].

5.1.3 User Data Protection

This section specifies requirements for TOE security functions and TOE security function policies relating to the protection of user data.

This section consists of an Access Control Policy and an Information Flow policy. The Information Flow Policy defines the information flows of packets that are permissible for the types of inbound traffic (external to internal information flows) and outbound traffic (internal to external information flows). These policies are defined using the rules specified below.

[1] The Audit Generation component is a bespoke component based on the [CC] Part 2 component FAU_GEN.1.

FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [Access Control SFP] on

a) [Manipulation of TSF data and security attributes (as specified in FMT_MSA.1) by an authorised user]

FDP_ACF.1 Access Control Functions

FDP_ACF.1.1 The TSF shall enforce the [Access Control SFP] to objects based on [the user being an authorised user]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[Manipulation of TSF data, and security attributes (as specified in FMT_MSA.1) can only be performed by an authorised user]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [None]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [No additional rules]

FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [information flow control SFP] on:

a) [external hosts which send and receive information through the TOE;

b) internal hosts which send and receive information through the TOE].

FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [information flow control SFP] based on the following types of subject and information security attributes:

a) [the interface on which the request arrives;

b) the information flow policy rules which consists of:

- presumed source IP address of the subject, as appropriate;
- presumed destination IP address of the subject, as appropriate;
- service is allowed;

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information, via a controlled operation if the following rules hold:

a) [subjects on the internal network can cause information to flow through the TOE if:

- all information security attribute values are expressly permitted by the information flow control SFP rules;
- the request arrives on the internal interface;
- the presumed address of the destination subject does not translate to an address on network from which it originated;
- service is allowed;

b) subjects on the external network can cause information to flow through the TOE if:

- all information security attribute values are expressly permitted by the information flow control SFP rules;

- the presumed address of the source subject translates to an external network address;
- the presumed address of the destination subject translates to an address assigned to an internal interface of the TOE.
- service is allowed;

FDP_IFF.1.3 The TSF shall enforce the [additional information flow control SFP rules: none]

FDP_IFF.1.4 The TSF shall provide the following [additional SFP capabilities: Network Address Translation]

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules [no additional rules to authorise information flow]

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:

a) [there is no rule which explicitly allows it;

b) if any of the attributes identified in FDP_IFF.1.1 do not match].

FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] the following objects [resources that are used to communicate through the TOE].

5.1.4 Protection of the TOE Security Functions

This section specifies functional requirements that relate to the integrity and management of the mechanisms providing the TSF and the TSF data.

FPT_RVM.1 Non-Bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.2 Security requirements for the IT Environment

This section details the IT security requirements that to be met by the IT environment of the TOE. Table 5 lists the IT security requirements to be provided by the IT environment:

Functional Components	
FAU_STG.1	Protected Audit Trail Storage
FAU_SAR.1	Audit Review

Table 5: IT Security Requirements of the Environment

5.2.1 Security Audit

This section involves recognising, recording and storing information related to security relevant activities.

FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [detect] modifications to the audit records.

FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [authorised users] with the capability to read [all audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.3 TOE Security Assurance Requirements

The assurance requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL4 level of assurance, augmented with the Flaw Remediation assurance. The assurance components are summarised in Table 6.

Assurance Class	**Assurance Components**	
Configuration management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Basic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools

Assurance Class	Assurance Components	
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

Table 6: Assurance Requirements: EAL4 augmented with ALC_FLR.1

Further information on these assurance components can be found in [CC] Part 3.

5.4 Strength of Function Claim

A Strength of Function (SOF) claim of SOF-medium is made for the TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions provided by the TOE and the environment to meet the security functional requirements specified for the Cisco Secure PIX firewall in Section 5.1.

6.1.1 Security Management Function

The Security Management Function permits an authorised user (from a physically secure local connection or via telnet from an internal trusted host) to perform the following actions:

- Manipulate the information flow policy rules for the firewall;
- Modify the time.

6.1.2 Audit Function

The Audit Function provides auditing that can be switched on or off. When active, audit events for every connection, whether successful or not, through the firewall are generated.

For each event the Audit Function will record the following:

- Date and time of the event;
- Source and destination IP address (for connections only);
- Type of event or service;
- Success or failure of the event.

To provide date and time information the Audit Function uses the Clock Function.

6.1.3 Information Flow Control Function

The Information Control Function of Cisco Secure PIX firewall allows authorised users to set up rules between interfaces of the firewall. These rules control whether a packet is transferred from one interface to another based on:

- Source address;
- Destination address;

- Service used;
- Port number;
- Network interface on which the connection request occurs.

The service requested, if permitted by the information control rules may comprise of Ethernet, ARP, DNS, Echo, Finger, H.323, IP, ICMP, TCP, UDP, FTP, HTTP, POP3, RTSP, Skinny, SIP, SMTP, and Telnet.

Packets will be dropped unless a specific rule has been set up to allow the packet to pass.

In providing the Information Flow Control function, the TOE has the ability to translate network addresses contain within a packet, called Network Address Translation. Depending upon the TOE configuration the address can be translated into a permanently defined static address, an address selected from a range, or into a single address with a unique port number (Port Address Translation). Also Network Address Translation can be disabled, so that addresses are not changed when passing through the TOE.

6.1.4 Protection Function

The Protection function provides a multitasking environment for the firewall. Within this environment all processes are allocated separate memory locations within the RAM. Whenever memory is re-allocated it is flushed of data prior to re-allocation.

The Protection function also ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

6.1.5 Clock Function

The Clock Function of the Cisco Secure PIX firewall provides a source of date and time information for the firewall. This function can only be accessed from within the configuration exec mode via the privileged mode of operation of the firewall.

6.2 Identification and Strength of Function Claim for IT security Functions

The TOE does not provide any IT security functions that are realised by a probabilistic or permutational mechanism. This Security Target claims that the general strength of the security functions provided by the TOE is SOF-medium although there are no mechanisms to which this claim relates.

6.3 Assurance Measures

Table 7, below, identifies the deliverables that will meet the Common Criteria EAL 4 Assurance Requirements, augmented with ALC_FLR.1.

CC Assurance Components		Assurance Measures (Cisco documentation)
ACM_AUT.1	Partial CM automation	Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ACM_CAP.4	Generation support and acceptance procedures	Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ACM_SCP.2	Problem tracking CM coverage	Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ADO_DEL.2	Delivery	Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ADO_IGS.1	Installation, generation and start-up procedures	Installation Guide for the Cisco Secure PIX Firewall Version 6.2 Configuration Guide for the Cisco Secure PIX Firewall Version 6.2 Release Notes for Cisco Secure PIX Firewall Version 6.2(2) Certified Installation and Configuration for the Cisco Secure PIX Firewall Version 6.2(2)
ALC_FLR.1	Basic flaw remediation	Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).

CC Assurance Components		Assurance Measures (Cisco documentation)
ALC_LCD.1	Developer defined life-cycle model	Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ADV_FSP.2	Fully defined external interfaces	Functional Specification for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ADV_HLD.2	Security enforcing high-level design	High Level Design for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ADV_IMP.1	Subset of the implementation of the TSF	Various Source Code modules for Cisco Secure PIX Firewall Version 6.2(2)
ADV_LLD.1	Descriptive low-level design	Low Level Design for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ADV_RCR.1	Informal correspondence demonstration	Correspondence Demonstration for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ADV_SPM.1	Informal TOE security policy model	Security Policy Model for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).

CC Assurance Components		Assurance Measures (Cisco documentation)
AGD_ADM.1	Administrator guidance	Installation Guide for the Cisco Secure PIX Firewall Version 6.2 Configuration Guide for the Cisco Secure PIX Firewall Version 6.2 Release Notes for Cisco Secure PIX Firewall Version 6.2(2) Release Notes for Cisco PIX Firewall Version 6.2(x) Certified Installation and Configuration for the Cisco Secure PIX Firewall Version 6.2(2)
AGD_USR.1	User guidance	
ALC_DVS.1	Identification of security measures	Development Security for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ALC_TAT.1	Well-defined development tools	Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).

CC Assurance Components		Assurance Measures (Cisco documentation)
ATE_COV.2	Analysis of coverage	Testing Plan and Analysis for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ATE_DPT.1	Testing: high-level design	Testing Plan and Analysis for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ATE_FUN.1	Functional testing	Testing Plan and Analysis for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
ATE_IND.2	Independent testing	Testing Plan and Analysis for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
AVA_MSU.2	Validation of analysis	Misuse Analysis for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
AVA_SOF.1	Strength of TOE security function evaluation	Strength of Function Assessment for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).
AVA_VLA.2	Independent vulnerability analysis	Vulnerability Assessment for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).

Table 7: Assurance Measures

7 Protection Profiles Claims

There are no Protection Profile Claims.

8 Rationale

8.1 Introduction

This section demonstrates that the TOE provides an effective set of IT security countermeasures within the security environment and that the TOE summary specification addresses the requirements.

8.2 Security Objectives for the TOE Rationale

Table 8 demonstrates how the IT security objectives and environment objectives of the TOE counter the IT threats and environment threats identified in Section 3.2.

Threats/ Assumptions **Objectives**	T.INTERN	T.EXTERN	T.SPOOF	TE.AUDATT	TE.AUDFUL	TE.SELPRO	TE.VIOLATE	TE.MODTOE	A.PHYSICAL	A.HOSTILE	A.AUDIT	A.AUDFUL	A.REMOTE
O.VALID	✓	✓	✓										
O.HOSTILE		✓											
O.PRIVATE	✓												
O.ATTEMPT	✓	✓	✓	✓					✓				
O.SECPROC						✓							
OE.AUDIT				✓									
NOE.AUDIT	✓	✓	✓	✓	✓		✓					✓	
NOE.DELIV							✓	✓					
NOE.NETWORK	✓	✓	✓						✓				
NOE.MANAGE							✓						✓
NOE.MODTOE							✓	✓					
NOE.PHYSICAL						✓			✓	✓	✓		✓
NOE.REVIEW	✓	✓	✓				✓						✓

Table 8 Mapping of Objectives to Threats and Assumptions

As can be seen from the table above, all threats and assumptions met by at least one objective, either TOE or environment, as applicable. The coverage of the threats and assumptions countered by the TOE is discussed in the subsections below.

8.2.1 T.INTERN

The Cisco Secure PIX firewall controls the flow of information between networks; it is the only point of connection between the networks that use the TOE for interconnection. This flow is controlled based on address ranges (i.e., it will reject a packet received at an internal network interface with a source address within the external network address range) and service ports available from an internal network. The configuration is reviewed in line with the security policies. The Cisco Secure PIX firewall also provides audit events that the authorised user can review for suspicious activity.

8.2.2 T.EXTERN

The Cisco Secure PIX firewall controls the flow of information from the external to the internal network; it is the only point of connection between the internal and external networks. This flow is controlled based on address ranges (i.e., it will reject a packet received at the external network interface with an address within the internal network address range) and service ports available from the external network. The configuration is reviewed in line with the security policies. The Cisco Secure PIX firewall also provides audit events that the authorised user can review for suspicious activity.

8.2.3 T.SPOOF

As described in 8.2.1 and 8.2.2 above the Cisco Secure PIX firewall controls the flow of information between the internal and external networks. Only permitted information flows are allowed between the networks. The Cisco Secure PIX firewall provides audit events of all connection attempts to ensure that the authorised user can identify suspicious activity. The configuration is reviewed in line with the security policies.

8.2.4 TE.AUDATT

The Cisco Secure PIX firewall will audit all attempts by hosts, connected through one network interface, to access hosts or services, connected on another interface, that are not explicitly allowed by the information flow policy. The machine used for the storage of audit data will ensure that there are facilities to view the audit data. The authorised users of the firewall must ensure that the audit facilities are used and managed correctly, including inspecting the logs on a regular basis.

8.2.5 TE.AUDFUL

The Cisco Secure PIX firewall relies on the machine used for storing the audit data to ensure that audit events generated are not lost due storage capacity exhaustion.

8.2.6 TE.SELPRO

Access to the internal data of the TOE is only possible through trusted means i.e a console attached directly to the TOE, or a telnet session from a trusted host on the internal interface. The TOE relies on the physical environment to ensure that only the Authorised user has physical access to the TOE.

8.2.7 TE.VIOLATE

The authorised users of the Cisco Secure PIX firewall are trusted to install, manage and operate (including using and managing the audit facilities, as well as indication from alerts) the Cisco Secure PIX firewall in a manner consistent with the security policy. The Cisco Secure PIX firewall is installed with a software image that has been securely delivered and its integrity has been confirmed by checking the MD5 hash value with an approved source to ensure that it has not been tampered with.In addition the configuration of the firewall will be reviewed on a regular basis to ensure that the configuration continues to meet the organisation’s security objectives. The authorised users should be provided with the appropriate training in order to complete this.

8.2.8 TE.MODTOE

Any unauthorised modification of the TOE image would be detected by an inconsistency with the published MD5 hash value. The assurance component ADO_DEL.2 is also applied.

8.2.9 A.PHYSICAL

The Cisco Secure PIX firewall must be the only (physical and logical) connection between the internal and external networks. Access to firewall console must be controlled.

8.2.10 A.HOSTILE

The Cisco Secure PIX firewall must be physically protected so that only the Authorised user has access.

8.2.11 A.AUDIT

The machine used to store audit data must be physically protected so that only authorised persons have access.

8.2.12 A.AUDFUL

The authorised user of the machine used to store audit data must ensure that the audit data is archived and that the storage space does not become exhausted.

8.2.13 A.REMOTE

The authorised user must ensure that the Cisco Secure PIX firewall will only accept telnet sessions for management from trusted hosts on the internal interface.

8.3 Security Requirements Rationale

8.3.1 Requirements are appropriate

Table 9 identifies which SFRs satisfy the Objectives as defined in Section 4.1.1

Objective	Security Functional Requirement(s)
O.VALID	FDP_IFC.1, FDP_IFF.1, FMT_MSA.3, FPT_RVM.1, FMT_MSA.1, FDP_ACC.1, FDP_ACF.1
O.HOSTILE	FDP_IFC.1, FDP_IFF.1, FMT_MSA.3, FPT_RVM.1, FMT_MSA.1, FDP_ACC.1, FDP_ACF.1
O.PRIVATE	FDP_IFC.1, FDP_IFF.1, FMT_MSA.3, FPT_RVM.1, FMT_MSA.1, FDP_ACC.1, FDP_ACF.1
O.ATTEMPT	FAU_AUD.1, FPT_STM.1, FMT_MTD.1, FDP_ACC.1, FDP_ACF.1
O.SECPROC	FDP_RIP.1, FPT_SEP.1
OE.AUDIT	FAU_STG.1, FAU_SAR.1

Table 9 Mapping of Objectives to SFRs

As it can be seen in the table above, all objectives are satisfied by at least one SFR and all SFRs are required to meet at least one objective. Therefore, as demonstrated in Table 8 and Table 9, all SFRs specified for the TOE are appropriate to counter the threats and meet the objectives of the TOE.

The Cisco Secure PIX firewall allows for the enforcement of information control (FDP_IFC.1) on traffic flow through the firewall and is achieved through the packet attributes (FDP_IFF.1) that cannot be bypassed by any traffic flowing the networks interconnected by the TOE (FPT_RVM.1). This ensures that the Cisco Secure PIX firewall can restrict the range of allowed addresses on each interface (O.VALID). It also means that Cisco Secure PIX firewall can restrict the hosts (and services) available on the internal network (or internal networks) that are available to hosts on the external network(s) (O.HOSTILE) and vice versa (O.PRIVATE). As a default Cisco Secure PIX ensures that after initialisation the firewall enters a restrictive state (FMT_MSA.3) that ensures that information control flow is enforced between the internal and external hosts. In addition, in order to provide the objectives (O.VALID), (O.HOSTILE) and (O.PRIVATE) the authorised user is able to manipulate the Information Flow Policy Rules (FMT_MSA.1), (FDP_ACC.1) and (FDP_ACF.1).

In order that an authorised user has correctly configured the Cisco Secure PIX firewall, the firewall generates audit events (FAU_AUD.1) for all attempted connections, both successful and unsuccessful. These events have timestamps attached (FPT_STM.1) prior to being transferred to a remote machine for secure storage and viewing (O.ATTEMPT). In addition the authorised user has the ability to modify the time (FMT_MTD.1), (FDP_ACC.1) and (FDP_ACF.1).

All audit events transferred for secure storage (OE.AUDIT) to another machine through a dedicated link. This machine securely stores all audit events and provides facilities to view the data (FAU_STG.1, FAU_SAR.1).

As Cisco Secure PIX firewall runs multiple processes (network connections) at the same time as the configuration functionality separation of data is essential (O.SECPROC). The Cisco Secure PIX firewall achieves this allocating separate memory partitions to each process (FPT_SEP.1). To ensure that information leakage does not occur between the memory that has been de-allocated from an old process and re-allocated to a new process, Cisco Secure PIX firewall flushes the memory before reallocation (FDP_RIP.1).

8.3.2 Security Requirement dependencies are satisfied

Table 10 shows a mapping of Functional Components to there dependencies. The shaded functional components are provided by the TOE Environment.

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FMT_MTD.1	FMT_SMR.1	None[2]
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1	FDP_ACC.1[3]
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1[3]
FAU_AUD.1[3]	FPT_STM.1	FPT_STM.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1, FMT_MSA.3
FDP_RIP.1	None.	None.

[2] FMT_SMR.1 is a dependency on FMT_MTD.1, FMT_MSA.1 and FMT_MSA.3. The dependency is there because the SFRs relating to Management of TSF data and Management of security attributes refer to restricting the ability to perform certain actions to certain users. In the TOE there is only one user - the authorised user - who is defined as a user, who may, in accordance with the TSP, perform an operation. A. PHYSICAL states that 'the TOE is physically protected so that only the authorised user of the TOE has physical access'. A.REMOTE states that the TOE 'will only accept telnet sessions for remote management by the authorised user from trusted hosts on the internal interface'. Thus there are no security roles and therefore this dependency is not relevant to the evaluated configuration.

[3] The functional requirement FAU_AUD.1 is based on the [CC] Part 2 functional requirement FAU_GEN.1. Thus it is viewed that FAU_AUD.1 will have a dependency on FPT_STM.1.

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FPT_RVM.1	None	None
FPT_SEP.1	None	None
FPT_STM.1	None	None
FAU_STG.1	FAU_AUD.1	FAU_AUD.1
FAU_SAR.1	FAU_AUD.1	FAU_AUD.1

Table 10 Mapping of SFR Dependencies

All functional component dependencies, with the exception of the dependencies of FAU_STG.1 and FAU_SAR.1 on FAU_GEN.1 and FMT_SMR.1 on FMT_MTD.1 and FMT_MSA.3 are met, as shown in Table 1 - TOE Component Identification above.

The component FAU_STG.1 is concerned with audit trail storage. The dependency of this component on FAU_GEN.1 relates to the fact that there must be audit events generated in order to store them. As FAU_AUD.1 generates audit events (in much the same way as FAU_GEN.1) it is appropriate to make FAU_STG.1 dependent upon FAU_AUD.1 rather than FAU_GEN.1.

The component FAU_SAR.1 is concerned with audit review. The dependency of this component on FAU_GEN.1 relates to the fact that there must be audit events generated in order to review them. As FAU_AUD.1 generates audit events (in much the same way as FAU_GEN.1) it is appropriate to make FAU_STG.1 dependent upon FAU_AUD.1 rather than FAU_GEN.1.

The component FMT_SMR.1 is concerned with security roles. The dependency of this component on FMT_MTD.1 relates to the fact that the information policy rules and time can be modified by a specific user role. As the TOE only has authorised users this component is met.

The component FMT_SMR.1 is concerned with security roles. The dependency of this component on FMT_MSA.3 relates to the fact that a specific user may override default values. As the TOE only has authorised users this component is met.

8.3.3 Security Requirements are mutually supportive

The only interactions between the security requirements specified for the Cisco Secure

PIX firewall are those which are identified in the CC Part 2 as dependencies between the SFRs. These dependencies are documented and demonstrated to be satisfied in Section 8.3.2. These interactions are specified in the CC Part 2, and are therefore mutually supportive.

The dependencies of, and on FAU_GEN.1 have been replaced by dependencies of, and on FAU_AUD.1. The rationale for this is provided in section 8.3.2.

8.3.4 ST complies with the referenced PPs

This Security Target does not claim compliance with a Protection Profile.

8.3.5 IT security functions satisfy SFRs

Table 11 shows a mapping of Section 6 IT functions to SFRs (Section 5.1 and 5.2).

IT Function	Security Functional Requirement(s)
Security Management Function	FMT_MTD.1, FMT_MSA.1, FMT_MSA.3, FDP_ACC.1, FDP_ACF.1
Information Control Flow Function	FMT_MSA.3 FDP_IFC.1, FDP_IFF.1
Audit Function	FAU_AUD.1, FPT_STM.1
Protection Function	FDP_RIP.1, FPT_SEP.1, FPT_RVM.1
Clock Function	FPT_STM.1, FMT_MTD.1

Table 11 Mapping of IT Functions to SFRs

The Security Management Function permits the authorised user to perform the following actions:

- Modify the time (FMT_MTD.1, FDP_ACC.1 and FDP_ACF.1);
- Manipulate the Information Flow Policy Rules (FMT_MSA.1, FMT_MSA..3, FDP_ACC.1 and FDP_ACF.1).

The Information Control Flow Function allows authorised users to set up traffic flow rules between pairs of network interfaces on the firewall. As default, the firewall prevents all network connections and will only allow connections through the firewall if a rule has been set up to allow the type of communication to pass (FMT_MSA.3).

Through use of the Information Control Flow Function an authorised user can restrict and control the flow of network between the network interfaces of the firewall. This is based on the flowing attributes of the packets arriving at a network interface:

- The interface on which the request arrives (FDP_IFF.1 and FDP_IFC.1);

- The presumed source IP address of the packet (FDP_ IFF.1 and FDP_IFC.1);
- The destination IP address of the packet (FDP_ IFF.1 and FDP_IFC.1);
- The service related to the packet (FDP_ IFF.1);
- The transport layer protocol contained within the packet (FDP_IFF.1).

The packets can have their address translated into another address (FDP_IFF.1).

If a packet arrives at one of the interfaces of the firewall and fails to meet a requirement for the rules set on an interface it will be blocked. Unless a rule specifically states that a particular packet can pass from one network interface to another of the firewall the packet will be blocked (FDP_IFF.1 and FPT_RVM.1).

The Audit Function provides reliable audit trail of network connections (FAU_AUD.1). For all events the Audit Function will record the:

- Date and time of the event, using the date and time information provided by the Clock Function (FPT_STM.1 and FAU_AUD.1);
- Source and destination IP address (for network traffic only) (FAU_AUD.1);
- Type of event or service (FAU_AUD.1);
- Success or failure of the event (FAU_AUD.1).

The Protection Function provides a separate runtime memory for each process running. This function ensures that each process cannot interfere with the data held by another process (FPT_SEP.1). Prior to providing memory to a new process, this function flushes the memory to be allocated to the new process (FDP_RIP.1). Furthermore the Protection Function also ensures that before any function within the TSC is processed, the TSF ensures that that function is successfully validated by the TSF.

The Clock Function provides a reliable source of time and date information. This function permits authorised users (i.e. those who have entered the privilege mode of operation by entering the enable password) to set and change the time and date (FMT_MTD.1). The Clock Function also provides the audit function with time stamps (FPT_STM.1).

8.3.6 IT security functions mutually supportive

The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (demonstrated in Section 8.3.3), as each of the IT functions can be mapped to one or more SFRs, as demonstrated in Table 8.3.

8.3.7 Strength of Function claims are appropriate

The SoF claim made by the TOE is SOF-medium.

MEDIUM as defined in the CC Part 1 is “resistance to attackers possessing a moderate attack potential”. This is consistent with AVA_VLA.2, one of the assurance components from which the EAL4 assurance level is comprised, which determines that “the TOE provides adequate protection against attackers possessing a moderate attack potential” (CC Part 3).

This product is to be used in environments such as government departments to protect internal networks when connecting them to external networks. The guidance for such interconnections is to use Firewall products with ITSEC E3 or equivalent (CC EAL4) assurance. No strength for critical mechanisms is associated with guidance so SOF-medium can be assumed to be adequate.

Therefore, the claim of SOF-Medium made by Cisco Secure PIX firewall is viewed to be appropriate for this use.

8.3.8 Justification of Assurance Requirements

EAL4 is defined in the CC as “methodically designed, tested and reviewed”.

Products such as Cisco Secure PIX firewall are intended to be used in a variety of environments, and used to connect networks with different levels of trust in the users. The Cisco Secure PIX firewall is intended to be suitable for use in UK HMG, which requires an ITSEC E3 equivalent level of assurance, for which EAL4 assurance is suitable.

In the Internet area of IT new exploits are continually being discovered and published, which the Cisco Secure PIX firewall will be expected to protect the internal network against. It is therefore considered to be appropriate to augment the EAL4 assurance requirements for the Cisco Secure PIX firewall with the ALC_FLR.1 assurance component. This will provide additional assurance that new vulnerabilities identified and reported in the services the product supports, or in the product itself, are addressed in a controlled and suitable manner.

8.3.9 Assurance measures satisfy assurance requirements

Table 12, below, provides a tracing of the Assurance Measures identified in Table 7 of Chapter 6 to the assurance requirements that they meet. From the table it can be seen that all assurance requirements trace to at least one assurance measure.

The assurance requirements identified in the table are those required to meet the CC assurance level EAL4, augmented with Flaw Reporting (ALC_FLR.1). As all assurance requirements are traced to at least on of the assurance measures the identified assurance measures are sufficient to meet the assurance requirements. It is also asserted that the assurance measures have been produced with EAL 4 (augmented with ALC_FLR.1) in mind and as a consequence contains sufficient information to meet the assurance requirements of the TOE.

Assurance Measures (Cisco documentation)	Assurance Requirements Met by Assurance Measure	
Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
	ADO_DEL.2	Detection of modification
Installation Guide for the Cisco Secure PIX Firewall Version 6.2 Configuration Guide for the Cisco Secure PIX Firewall Version 6.2 Release Notes for Cisco Secure PIX Firewall Version 6.2(x) Certified Installation and Configuration for the Cisco Secure PIX Firewall Version 6.2(x)	ADO_IGS.1	Installation, generation and start-up procedures

Assurance Measures (Cisco documentation)	Assurance Requirements Met by Assurance Measure	
Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ALC_FLR.1	Basic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
Functional Specification for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ADV_FSP.2	Fully defined external interfaces
High Level Design for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ADV_HLD.2	Security enforcing high-level design
Various Source Code Modules for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ADV_IMP.1	Subset of the implementation of the TSF
Low Level Design for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ADV_LLD.1	Descriptive low-level design
Correspondence Demonstration for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ADV_RCR.1	Informal correspondence demonstration

Assurance Measures (Cisco documentation)	Assurance Requirements Met by Assurance Measure	
Security Policy Model for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ADV_SPM.1	Informal TOE security policy model
Installation Guide for the Cisco Secure PIX Firewall Version 6.2 Configuration Guide for the Cisco Secure PIX Firewall Version 6.2 Release Notes for Cisco Secure PIX Firewall Version 6.2(2).	AGD_ADM.1	Administrator guidance
Release Notes for Cisco Secure PIX Firewall Version 6.2(2). Certified Installation and Configuration for the Cisco Secure PIX Firewall Version 6.2(2).	AGD_USR.1	User guidance
Development Security for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ALC_DVS.1	Identification of security measures
Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ALC_TAT.1	Well-defined development tools

Assurance Measures (Cisco documentation)	Assurance Requirements Met by Assurance Measure	
Testing Plan and Analysis for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ATE_COV.2	Analysis of coverage
Testing Plan and Analysis for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ATE_DPT.1	Testing: high-level design
Testing Plan and Analysis for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ATE_FUN.1	Functional testing
Testing Plan and Analysis for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	ATE_IND.2	Independent testing
Validation of Analysis for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	AVA_MSU.2	Validation of analysis
Strength of Function Assessment for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	AVA_SOF.1	Strength of TOE security function evaluation

Assurance Measures (Cisco documentation)	Assurance Requirements Met by Assurance Measure	
Vulnerability Assessment for Cisco Secure PIX Firewall 501, 506, 506E, 515, 515E, 520, 525 & 535 Version 6.2(2).	AVA_VLA.2	Independent vulnerability analysis

Table 12 Mapping of Assurance Measures to Assurance Requirements

This page is intentionally blank.