Security Target for Cisco PIX Security Appliances 515/515E, 525, 535 and Cisco Adaptive Security Appliances 5510, 5520, and 5540, Version 1.0

March 2007

Contents

This document includes the following sections:

Security Target Introduction

This section includes the following topics:

Security Target Identification

TOE Identification: Cisco PIX Security Appliances 515/515E, PIX 525, PIX 535 and Adaptive Security Appliances 5510, ASA 5520 and ASA 5540, Version 7.0(6).

ST Identification: Security Target for Cisco PIX Security Appliances 515/515E, PIX 525, PIX 535 and Cisco Adaptive Security Appliances 5510, ASA 5520 and ASA 5540, Version 1.0, March 2007.

Assurance Level: Evaluation Assurance Level (EAL) 4 augmented with Common Criteria (CC) component ALC_FLR.1.

ST Author: Cisco Systems, 170 West Tasman Drive, San Jose CA 95124-1706.

Keywords: Firewall, Packet Filtering, Application-level.

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004, plus applicable CCIMB and US National interpretations up to 25 March 2004. Where specific changes result from application of an interpretation or precedent, this is noted in the security target.

Security Target Overview

The Cisco PIX Security Appliance and the Cisco ASA Adaptive Security Appliance are stateful packet filtering firewalls. 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 authorized administrator. 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. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated.

In addition to IP header information, Cisco PIX and ASA appliances mediate information flows on the basis of other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface. 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.

CC Conformance

The TOE is Part 2 conformant, Part 3 conformant, and meets the requirements of EAL 4 augmented with the CC component, ALC_FLR.1.

Related Documents

[FWPP] “U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments,” Version 1.0, June 28, 2000.

[FIPS140] “Security Engineering Requirements for Cryptographic Modules,” FIPS 140-1, National Institute of Standards and Technology, 11 January 1994, and “Security Engineering Requirements for Cryptographic Modules,” FIPS 140-2, National Institute of Standards and Technology, 25 May 2001 with Change Notices (12-03-2002).

Conventions

The following conventions have been applied in this document:

- All requirements in this ST are reproduced relative to the requirements defined in [FWPP].
- Security Functional Requirements–Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, refinement and iteration.
  - The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by bold text. For an example, see FMT_SMR.1 in this security target.
  - The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text*. For an example, see FDP_RIP.1 in this security target.
  - The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value]. For an example, see FIA_AFL.1 in this security target.
  - The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number). For example, see FMT_MSA in this security target.

Underlining is used to identify operations completed in the ST, to distinguish them from those completed in [FWPP].

Other sections of the ST use boldface and italics to highlight text of special interest, such as captions.

TOE Description

This section includes the following topics:

Overview

This section presents an overview of the Cisco PIX Security Appliance (PIX) and Adaptive Security Appliance (ASA), Version 7.0(6) to assist potential users in determining whether they meet their needs. The appliances control the flow of Internet Protocol (IP) traffic (datagrams) between network interfaces. The appliances are provided on a number of platforms. The PIX platforms included within the scope of

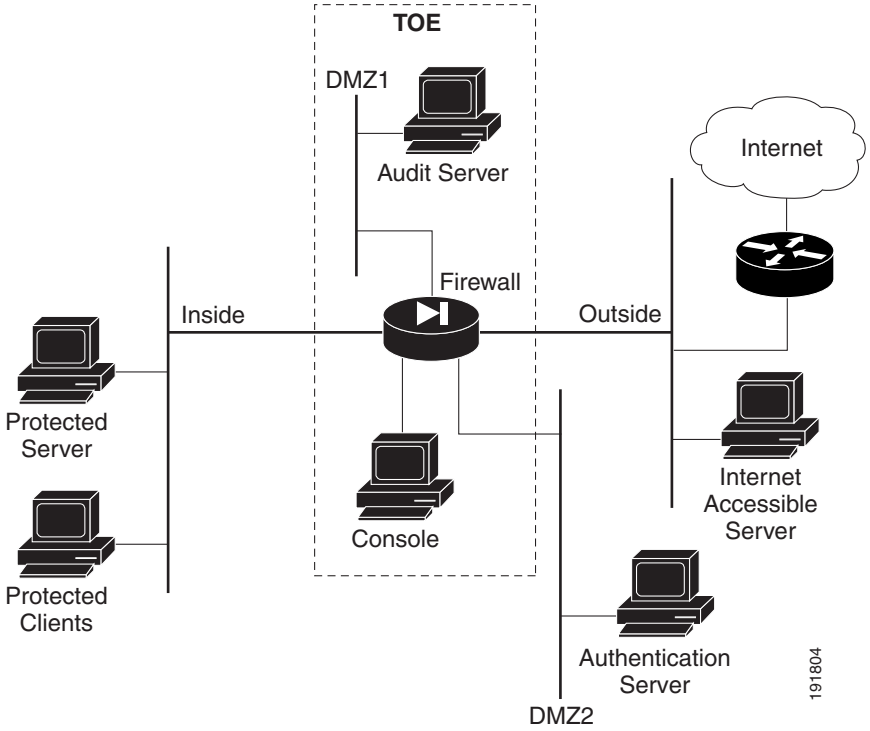
this evaluation are PIX 515/515E, PIX 525, and PIX 535. The ASA platforms included within the scope of this evaluation are ASA 5510, ASA 5520, and ASA 5540. From this point forward, these platforms will be referred to as the Target of Evaluation (TOE).

The PIX and ASA (the TOE) are purpose-built hardware devices that use an Intel processor in all models.

The PIX runs the Cisco Secure PIX Security Appliance software image Version 7.0(6), and the ASA runs the Cisco Adaptive Security Appliance software image Version 7.0(6). These software images are identical.

The TOE provides a single point of defense as well as controlled and audited access to services between networks by permitting or denying the flow of information traversing the appliance.

Figure 1 TOE Physical Boundary and Illustrative Network Connections



Physical Boundaries

The TOE physical configuration includes one PIX or one ASA, which controls the flow of IP traffic between network interfaces, and an audit server used for audit storage and analysis. The TOE physical boundary includes these components (see Figure 1). The physical scope of the TOE includes the hardware and software elements identified in Table 1.

Table 1 TOE Component Identification

Component	Description
Hardware	PIX 515 or 515E with of one of the following: • Single 433 MHz Intel Celeron processor (515E) • PI-MMX 200MHz processor (515) with up to six network interfaces PIX-VAC-PLUS Cryptographic accelerator card
	PIX 525 consisting of a 600 MHz Intel Pentium III processor with up to ten network interfaces PIX-VAC-PLUS Cryptographic accelerator card
	PIX 535 consisting of a 1000 MHz Intel Pentium III processor with up to 14 network interfaces PIX-VAC-PLUS Cryptographic accelerator card
	ASA 5510, ASA 5520, and ASA 5540 Each consisting of a 2 GHz Intel Celeron processor with up to nine network interfaces
	PC audit server platform
Software	Cisco Secure PIX Firewall Version 7.0(6)
	Windows 2000 Professional Service Pack 3 (including hotfix Q326886) or Windows XP Professional, Service Pack 2 (including hotfixes 896423, 899587, 899588, 896422, 890859, 873333, 885250, 888302, 885835, and 907865) with Service Pack 2 (for audit server)
	PIX Firewall Syslog Server (PFSS) 5.1(3)

All appliances 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:

PIX

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

ASA

- Four-port Gigabit Ethernet Security Services Module (part number ASA-SSM-4GE=)

All models are available with either AC or DC power. Because the power supplies do not provide any security enforcing functionality, the AC and DC-powered models are treated identically.

Other than the connection to the audit server, the physical boundaries of the TOE are the physical port connections on the TOE external casing. One such port is to connect to the management console. Management of the TOE may be conducted either from a directly connected console (shown in Figure 1), or from a network console linked via SSH. There are no constraints on the location of the network console. In both cases, the console must be physically protected.

Separate secure management networks are used (see DMZ1 and DMZ2 in Figure 1) for the audit and authentication servers.

The TOE includes a Windows 2000 or Windows XP server for the purpose of storing the audit data generated by the TOE. The certified versions of these operating systems, as listed in Table 2.1, must be used. This server may be combined with the network console if desired.

The TOE provides interconnections between two or more networks depending on the number of interface cards installed within the product. A combination of network cards can be installed in the PIX 515/515E, PIX 525, PIX 535, ASA 5510, ASA 5520, and ASA 5540. 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 TOE against those outside of the firewall. The TOE can provide protection between networks connecting to the different internal network interfaces of the TOE.

The TOE environment includes a commercially available, single-use TACACS+ or RADIUS authentication server.

All traffic between each network attached to the TOE must flow through the TOE to maintain security.

Logical Scope and Boundaries

The scope of the TOE includes the following security functions:

- Security management to enable, disable, or modify the behavior of the TOE
- Security auditing
- Information flow control between interfaces of the firewall
- Identification and authentication of administrators
- Provision of a secure multitasking environment with residual information protection and assured invocation of security functions
- Provision of accurate date and time information

This section includes the following topics:

The TOE controls the flow of IP traffic (datagrams) between network interfaces by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's authorized administrator. 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. 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 TOE mediates information flows on the basis of other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface. 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.

The types of traffic through or to the TOE that are within the scope of the evaluation include, but are not limited to: Ethernet, ARP, CTIQBE, DNS, Echo, Finger, H.323, IP, ICMP, TCP, UDP, FTP, GTP, HTTP, ILS, MGCP, POP3, RSH, RTSP, Skinny, SIP, ESMTP, SunRPC, Telnet, TFTP and XDMCP. Application inspection is also provided within the TOE for the following protocols and applications: CTIQBE, H.323, ICMP, FTP, GTP, HTTP, ILS, MGCP, RSH, RTSP, Skinny, SIP, ESMTP, SunRPC, TFTP, and XDMCP.

The TOE allows for 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 PAT.

Logical network interfaces may be mapped to physical interfaces on a one to one basis (inside, outside, and DMZ). The TOE also supports multiple logical networks on a single physical interface.

Single or Multiple Context

A security context is a collection of processes that exist to model the logical virtual firewall into the constraints of the hardware. Each security context (virtual device) is treated as a separate independent device with its own security policy, interfaces, administrators, and configuration file.

When the firewall is operating in single routed mode one instance of a security context is present and executing. When the firewall is configured in multiple-context mode multiple security contexts are executing simultaneously. Each context in multiple-context mode is made up of the same processes used in single routed mode, only multiple instances of those processes are executing. There is no difference between the processes that are running for a single instance of a context in single, routed mode or multiple-context mode. Multiple contexts are similar to having multiple stand-alone devices.

Routed or Transparent Mode

The security appliance can run in these two firewall modes:

- Routed mode
- Transparent mode

In routed mode, the security appliance is considered to be a router hop in the network. It can perform NAT between connected networks, and can use OSPF or passive RIP (in single context mode). Routed mode supports many interfaces. Each interface is on a different subnet. Interfaces can be shared between contexts.

In transparent mode, the security appliance acts like a "bump in the wire," or a "stealth firewall," and is not a router hop. The security appliance connects the same network on its inside and outside interfaces. No dynamic routing protocols or NAT are used. However, like routed mode, transparent mode also requires access lists to allow any traffic through the security appliance, except for ARP packets, which are allowed automatically. Transparent mode can allow certain types of traffic in an access list that is blocked by routed mode, including unsupported routing protocols. Transparent mode can also optionally use EtherType access lists to allow non-IP traffic. Transparent mode only supports two interfaces, an inside interface and an outside interface, in addition to a dedicated management interface, if available for your platform.

Management

The TOE can be managed by authorized administrators via a physically secure local connection. The firewall part of the TOE can also be managed remotely from a connected network, through use of a FIPS 140-2 approved encrypted link. The TOE (both firewall and audit server) supports the authentication of authorized administrators by means of user id and password, and, with support from the environment, supports the use of third-party, single-use authentication servers.

Audit

The PIX and ASA also interact with a Windows 2000 or Windows XP server running PIX Firewall Syslog Server (PFSS) for the purpose of storage and analysis of the audit data generated by the TOE.PFSS (for firewall logs) and Windows Event Viewer (for audit server logs) are the tools that are included as part of the TOE. Use of other tools is not addressed by the evaluation. Windows access controls will ensure that the integrity of the audit logs is not compromised by use of these tools. The PIX and ASA, through the export of audit data, support the capability to perform audit analysis. The audit server is on a separate trusted network and is accessible only by trusted administrators.

Outside Scope

Features that are outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- RIP
- SNMP
- ASDM
- DHCP Server
- Virtual Private Networks

Besides these exceptions, all types of network traffic through and to the TOE are within the scope of the evaluation.

The external AAA server used provides single-use authentication is outside the scope of the TOE, although use made by the TOE of this server is within scope.

The TOE definition in this ST makes use of the following precedents under the CCEVS: PD-0113.

PP Conformance

The TOE functionality is specified to be consistent with the U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000 [FWPP].

The ST includes all security functional requirements included in [FWPP] (as modified under PD-0115 and PD-0026).

Assurance Requirements

The TOE is designed to meet the EAL4 assurance requirements, augmented with ALC_FLR.1.

TOE Security Environment

This section includes the following topics:

Assumptions

Table 2 lists the assumptions for the TOE security environment, which are the same as those for the [FWPP].

Table 2 Assumptions

No.	Assumption Name	Description
1	A.PHYSEC	The TOE is physically secure.
2	A.PROTECTPF	The PFSS is to be connected to the firewall such that the network interface of the PFSS is only accessible by the TSF. This may be achieved by either directly connecting the PFSS to the firewall, or indirectly over the trusted network. This protection of the PFSS network interface is required by PD-0113.
3	A.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
4	A.GENPUR	There are no general-purpose computing capabilities (for example, the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
5	A.PUBLIC	The TOE does not host public data.
6	A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
7	A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
8	A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (for example, a console port) if the connection is part of the TOE.
9	A.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
10	A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.

Threats to the Security of the TOE

Table 3 defines security threats for the TOE. The asset under attack is the information that transits the TOE in accordance with the security policy, as represented by the TOE rule set. In general, the threat agent includes, but is not limited to: 1) people with TOE access who are expected to possess “low” expertise, resources, and motivation, or 2) failure of the TOE.

Table 3 Threats for the TOE

No.	Threat Name	Threat Description
1	T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE, so as to access and use security functions and/or non-security functions provided by the TOE.
2	T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
3	T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
4	T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (for example., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
5	T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
6	T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
7	T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
8	T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
9	T.SELPRO	An unauthorized person may read, modify, or destroy security-critical TOE configuration data.
10	T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
11	T.MODEXP	An attacker with low attack potential may attempt to bypass the TSF to gain access to the TOE or the assets it protects.

Threats to the Security of the Environment

This section defines the threats to the IT Environment, which are listed in Table 4. The asset under attack is the information transiting the TOE. In general, the threat agent includes, but is not limited to: 1) people with TOE access who are expected to possess "average" expertise, few resources, and moderate motivation, or 2) failure of the TOE.

Table 4 Threats to Security for the IT Environment

No.	Threat Name	Threat Description
1	T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

Organizational Security Policies

Table 5 lists the organizational security policies.

Table 5 Organizational Security Policies

No.	Policy Name	Policy Description
1	P.CRYPTO	Triple DES encryption (as specified in FIPS 46-3 [3]) or AES encryption (as specified in FIPS 197) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1) or FIPS 140-2 (level 1).

Security Objectives

This section includes the following topics:

Security Objectives for the TOE

Table 6 lists security objectives for the TOE.

Table 6 Security Objectives for the TOE

No.	Objective Name	Objective Description
1	O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
2	O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.
3	O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols and ensuring that residual information from a previous information flow is not transmitted in any way.
4	O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
5	O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
6	O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
7	O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
8	O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
9	O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
10	O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
11	O.EAL	The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.

Security Objectives for the Environment

Table 7 lists security objectives for the IT environment.

Table 7 Security Objectives for the IT Environment

No.	Objective Name	Objective Description
1	OE.IDAUTH	The claimed identity of a remote user must be uniquely identified and authenticated, before granting the user access to TOE functions or, for certain specified services, to a connected network. Note: The objective IDAUTH is present for both the TOE and the TOE environment. This reflects the use of an authentication server in the environment to generate authentication credentials where single-use authentication is applied for remote users.
2	OE.SINUSE	The reuse of authentication data must be prevented for users attempting to authenticate at the TOE from a connected network.
3	OE.PHYSEC	The TOE and its operating environment are physically secure, and the network interface of the PFSS is only accessible by the TSF.
4	OE.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
5	OE.GENPUR	There are no general-purpose computing capabilities (for example, the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
6	OE.PUBLIC	The TOE and the authentication server do not host public data.
7	OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
8	OE.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
9	OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (for example, a console port) if the connection is part of the TOE.
10	OE.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
11	OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
12	OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
13	OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.

IT Security Requirements

This section includes the following topics:

TOE Security Functional Requirements

All security functional requirements are drawn from Part 2 of the CC. They are repeated in Table 8 in the ST to demonstrate the refinements. See Conventions, page 3 for the conventions used for refinements.

This section includes the following topics:

Table 8 TOE Security Functional Requirements

Security Functional Requirements Class	Security Functional Requirements Components
Security Audit (FAU)	*Audit data generation (FAU_GEN.1)*
	Audit review (FAU_SAR.1)
	Selectable audit review (FAU_SAR.3)
	Protected audit trail storage (FAU_STG.1)
	Prevention of audit data loss (FAU_STG.4)
Cryptographic Operation (FCS)	*Cryptographic operation (FCS_COP.1)*
User Data Protection (FDP)	*Subset information flow control 1 (FDP_IFC.1)*
	Subset information flow control 2 (FDP_IFC.1)
	Simple security attributes1 (FDP_IFF.1)
	Simple security attributes2 (FDP_IFF.1)
	Subset residual information protection (FDP_RIP.1)
Identification and Authentication (FIA)	*Authentication failure handling (FIA_AFL.1)*
	User attribute definition (FIA_ATD.1)
	Multiple authentication mechanisms (FIA_UAU.5)
	User identification before any action (FIA_UID.2)

Table 8 TOE Security Functional Requirements (continued)

Security Management (FMT)	*Management of security functions behavior 1 (FMT_MOF.1)*
	Management of security functions behavior 2 (FMT_MOF.1)
	Management of security attributes 1 (FMT_MSA.1)
	Management of security attributes 2 (FMT_MSA.1)
	Management of security attributes 3 (FMT_MSA.1)
	Management of security attributes4 (FMT_MSA.1)
	Static attribute initialization (FMT_MSA.3)
	Management of TSF data 1 (FMT_MTD.1)
	Management of TSF data 2 (FMT_MTD.1)
	Management of limits on TSF data (FMT_MTD.2)
	Specification of management functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	*Non-bypassability of the TSP (FPT_RVM.1)*
	TSF domain separation (FPT_SEP.1)
	Reliable time stamps (FPT_STM.1)

Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

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

a. Startup and shutdown of the audit functions.

b. All auditable events for the *not specified* level of audit.

c. [The events in Table 9].

FAU_GEN.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.

b. For each audit event type, based on the auditable event definitions of the functional components included in the ST, [information specified in column three of Table 9].

Dependencies: FPT_STM.1 Reliable time stamps

Table 9 Auditable Events

Functional Component	Auditable Event	Additional Audit Record Contents
FCS_COP.1	Success and failure, and the type of cryptographic operation	The identity of the external IT entity attempting to perform the cryptographic operation.
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent **restoration by the authorized administrator of the user's capability to authenticate**.	The identity of the offending user and the authorized administrator.
FIA_UAU.5	The final decision on authentication.	The user identity and the success or failure of the authentication.
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE.
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation.
FMT_SMR.1	Modifications to the group of users that are part of the authorized administrator role. Unsuccessful attempts to authenticate **the authorized administrator**.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role. The user identity and the role.
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation.

Application Note: The boldface text in Table 9 is an addition to the CC Part 2 requirement.

FAU_SAR.1 Audit review

Hierarchical to	No other components.
FAU_SAR.1.1	The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] 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.
Dependencies	FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to	No other components.

FAU_SAR.3.1	The TSF shall provide the ability to perform *searches and sorting* of audit data based on [: **a.** User identity **b.** Presumed subject address **c.** Ranges of dates **d.** Ranges of times **e.** Ranges of addresses].
Dependencies	FAU_SAR.1 Audit review

FAU_STG.1 Protected audit trail storage

Hierarchical to	No other components.
FAU_STG.1.1	The TSF shall protect the stored audit records from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to *prevent* modifications to the audit records**.**
Dependencies	FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss

Hierarchical to	FAU_STG.3
FAU_STG.4.1	The TSF *shall prevent auditable events, except those taken by the authorized* ***administrator*** and [shall limit the number of audit records lost] if the audit trail is full.
Dependencies	FAU_GEN.1 Audit data generation

Cryptographic Operation

FCS_COP.1 Cryptographic operation

Hierarchical to	No other components.
FCS_COP.1.1	The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with a specified cryptographic algorithm: [Triple Data Encryption Standard (DES) as specified in FIPS PUB 46-3 and implementing any mode of operation specified in FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys)] and cryptographic key sizes [that are 192 binary digits in length and Advanced Encryption Standard (AES), as specified in FIPS PUB 197 and cryptographic key sizes [that are 128, 192 or 256 binary digits in length] that meet the following: [FIPS PUB 46-3 with Keying Option 1 and FIPS PUB 140-1 (Level 1)].

Dependencies	[FDP_ITC.1 Import of user data without security attributes or: • FCS_CKM.1 Cryptographic key generation] • FCS_CKM.4 Cryptographic key destruction • FMT_MSA.2 Secure security attributes
Application Note	This requirement is applicable as the firewall part of the TOE includes the capability for the authorized administrator to perform security functions remotely from a connected network.

User Data Protection

FDP_IFC.1 (1) Subset information flow control

Hierarchical to	No other components.
FDP_IFC.1.1	The TSF shall enforce the [UNAUTHENTICATED SFP] on [: **a.** Subjects—Unauthenticated external IT entities that send and receive information through the TOE to one another. **b.** Information—Traffic sent through the TOE from one subject to another. **c.** Operation—Pass information].
Dependencies	FDP_IFF.1 Simple security attributes

FDP_IFC.1 (2) Subset information flow control

Hierarchical to	No other components.
FDP_IFC.1.1	The TSF shall enforce the [AUTHENTICATED SFP] on [: **a.** Subjects—A human user or external IT entity that sends and receives FTP and Telnet information through the TOE to one another, only after the human user initiating the information flow has authenticated at the TOE per FIA_UAU.5. **b.** FTP and Telnet traffic sent through the TOE from one subject to another. **c.** Operation—Initiate service and pass information].
Dependencies	FDP_IFF.1 Simple security attributes

FDP_IFF.1 (1) Simple security attributes

Hierarchical to	No other components.

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

a. Subject security attributes:

- Presumed address
- No other subject security attributes

b. Information security attributes:

- Presumed address of source subject
- Presumed address of destination subject
- Transport layer protocol
- TOE interface on which traffic arrives and departs
- Service
- No other information security attributes].

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

a. [Subjects on an internal network can cause information to flow through the TOE to another connected network if the following are true:

- The human user initiating the information flow authenticates according to FIA_UAU.5.
- All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator.
- The presumed address of the source subject, in the information, translates to an internal network address.
- The presumed address of the destination subject, in the information, translates to an address on the other connected network.

b. Subjects on an external network can cause information to flow through the TOE to another connected network if the following are true:

- All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator.
- The presumed address of the source subject, in the information, translates to an external network address.
- The presumed address of the destination subject, in the information, translates to an address on the other connected network].

FDP_IFF.1.3 The TSF shall enforce the [none].

FDP_IFF.1.4 The TSF shall provide the following [none].

FDP_IFF.1.5 The TSF shall explicitly label an information flow based on the following rules: [none].

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

a. The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b. The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;

e. The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f. For application protocols supported by the TOE (for example, DNS, HTTP. SMTP, and POP3), the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (for example RFC). This shall be accomplished through protocol filtering proxies that are designed for that purpose].

Application Notes

1. Rule 6 applies when an application-level proxy is provided for DNS, HTTP, SMTP and POP3.
2. NAT and PAT were specifically tested, even though they were not explicitly referenced in an SFR.

Dependencies FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1 (2) Simple security attributes

Hierarchical to No other components.

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

a. Subject security attributes:

- Presumed address
- No other subject security attributes

b. Information security attributes:

- User identity
- Presumed address of source subject
- Presumed address of destination subject
- Transport layer protocol
- TOE interface on which traffic arrives and departs
- Service (that is, FTP and Telnet)
- Security-relevant service command
- No other information security attributes].

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

a. Subjects on an internal network can cause information to flow through the TOE to another connected network if:

- The human user initiating the information flow authenticates according to FIA_UAU.5.
- All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator.
- The presumed address of the source subject, in the information, translates to an internal network address.
- The presumed address of the destination subject, in the information, translates to an address on the other connected network.

b. Subjects on an external network can cause information to flow through the TOE to another connected network if:

- The human user initiating the information flow authenticates according to FIA_UAU.5.
- All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator.
- The presumed address of the source subject, in the information, translates to an external network address
- The presumed address of the destination subject, in the information, translates to an address on the other connected network].

FDP_IFF.1.3 The TSF shall enforce the [none].

FDP_IFF.1.4 The TSF shall provide the following [none].

FDP_IFF.1.5 The TSF shall explicitly label an information flow based on the following rules: [none].

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

a. The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network.

b. The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network.

c. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network.

d. The TOE shall reject requests for access or services, in which the information arrives on an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network].

e. The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject.

f. The TOE shall reject Telnet or FTP command requests that do not conform to generally accepted published protocol definitions (for example, RFCs). This must be accomplished through protocol filtering proxies designed for that purpose.

Dependencies FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_RIP.1 Subset residual information protection

Hierarchical to No other components.

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* [all objects].

Dependencies No dependencies

Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to No other components.

FIA_AFL.1.1 The TSF shall detect when [**a non-zero number** determined by the authorized administrator] **of** unsuccessful authentication attempts occur related to [authorized TOE administrator access or authorized TOE IT entity access].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending external IT entity from successfully authenticating until an authorized administrator takes some action to make authentication possible for the external IT entity in question].

Dependencies FIA_UAU.1 Timing of authentication

Application Notes

1. Although the TOE is capable of limiting the number of authentication attempts by external IT entities, in practice this represents an opportunity for denial of service attack and is not recommended.
2. This requirement applies only to authentication against the local user database, and not to local or remote authentication deferred through FIA_UAU.5 to a remote AAA server. This does not represent a dilution of the requirement, because such deferred remote authentication is not within the scope of the TOE.

FIA_ATD.1 User attribute definition

Hierarchical to No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

a. Identity
b. Association of a human user with the authorized administrator role
c. Password].

Dependencies No dependencies

FIA_UAU.5 Multiple authentication mechanisms

Note that in accordance with US PD-115, items 1, 2, and 3 of this security functional requirement are partially addressed by the TOE environment.

Hierarchical to No other components.

FIA_UAU.5.1 The TSF shall provide [password and single-use authentication mechanisms] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules:

a. Single-use authentication mechanism shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator.

b. Single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity.

c. Single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other non-TSF-mediated actions on behalf of that human user.

d. Reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator.]

Dependencies: No dependencies

Application Note: The TOE shall be responsible for correctly invoking the external single-use authentication mechanism, and for taking the correct actions based on authentication decisions. In keeping with industry practice the choice of authentication server is not mandated by this ST.

FIA_UID.2 User identification before any action

Hierarchical to: No other components.

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

Dependencies: No dependencies

Security Management

FMT_MOF.1 (1) Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1(1) The TSF shall restrict the ability to *enable, disable* the functions [:

a. Operation of the TOE

b. Single-use authentication function described in FIA_UAU.5] to [an authorized administrator].

Dependencies FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MOF.1 (2) Management of security functions behavior

Hierarchical to No other components.

FMT_MOF.1.1 (2) The TSF shall restrict the ability to *enable, disable, determine and modify the behavior of* the functions [:

a. Audit trail management

b. Backup and restore for TSF data, information flow rules, and audit trail data

c. Communication of authorized external IT entities with the TOE] to [an authorized administrator].

Note For audit data, the restriction applies to the audit administrator.

Dependencies FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Application Note Determine and modify the behavior of element c) (communication of authorized external IT entities with the TOE) is intended to cover functionality such as providing a range of addresses from which the authorized external entity can connect.

FMT_MSA.1 (1) Management of security attributes

Hierarchical to No other components.

FMT_MSA.1.1 (1) The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, and add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(1)] to [the authorized firewall administrator].

Dependencies [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MSA.1 (2) Management of security attributes

Hierarchical to No other components.

FMT_MSA.1.1 (2)	The TSF shall enforce the [AUTHENTICATED_SFP] to restrict the ability to [delete attributes from a rule, modify attributes in a rule, and add attributes to a rule] the security attributes [listed in section FDP_IFF1.1(2)] to [the authorized firewall administrator].
Dependencies	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MSA.1 (3) Management of security attributes

Hierarchical to	No other components.
FMT_MSA.1.1 (3)	The TSF shall enforce the [UNAUTHENTICATED_SFP] to restrict the ability to *delete* and [create] the security attributes [information flow rules described in FDP_IFF.1.1(1)] to [the authorized firewall administrator].
Dependencies	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MSA.1 (4) Management of security attributes

Hierarchical to	No other components.
FMT_MSA.1.1 (4)	The TSF shall enforce the [AUTHENTICATED_SFP] to restrict the ability to *delete* and [create] the security attributes [information flow rules described in FDP_IFF.1.1(2)] to [the authorized firewall administrator].
Dependencies	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialization

Hierarchical to	No other components.
FMT_MSA.3.1	The TSF shall enforce the [UNAUTHENTICATED SFP and AUTHENTICATED SFP] to provide *restrictive* default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2	The TSF shall allow the [authorized firewall administrator] to specify alternative initial values to override the default values when an object or information is created.
Dependencies	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles

FMT_MTD.1 (1) Management of TSF data

Hierarchical to	No other components.
FMT_MTD.1.1(1)	The TSF shall restrict the ability to *query*, *modify*, *delete*, [and assign] the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].
Dependencies	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

FMT_MTD.1 (2) Management of TSF data

Hierarchical to	No other components.
FMT_MTD.1.1 (2)	The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1.1] to [the authorized administrator].
Dependencies	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

FMT_MTD.2 Management of limits on TSF data

Hierarchical to	No other components.
FMT_MTD.2.1	The TSF shall restrict the specification of the limits for [the number of authentication failures] to [the authorized administrator].
FMT_MTD.2.2	The TSF shall take the following actions, if the TSF data are at, or exceed the indicated limits: [actions specified in FIA_AFL.1.2].
Dependencies	FMT_MTD.1 Management of TSF data
	FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

Hierarchical to	No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a. Enable or disable the operation of the TOE.

b. Enable or disable the single-use authentication function described in FIA_UAU.5.

c. Enable, disable, determine and modify the behavior of the audit trail.

d. Enable, disable, determine and modify the behavior of the backup and restore function for TSF data, information flow rules, and audit trail data.

e. Enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE.

f. Delete attributes from a rule, modify attributes in a rule and add attributes to a rule for the security attributes listed in section FDP_IFF1.1(1).

g. Delete and create the information flow rules described in FDP_IFF.1(1).

h. Query, modify, delete and assign the user attributes defined in FIA_ATD.1.1.

i. Set the time and date used to form the timestamps in FPT_STM.1.1.

j. Specify of the limits for the number of authentication failures.

Dependencies No dependencies

FMT_SMR.1 Security roles

Hierarchical to No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [authorized firewall administrator and authorized audit administrator].

FMT_SMR.1.2 The TSF shall be able to associate **human** users with **the authorized administrator** roles.

Dependencies FIA_UID.1 Timing of identification

Application Note Where references are made in this ST, without further qualification, to administrators, then the reference includes both firewall administrators and audit administrators. This does not weaken the security functional requirements in any way, but merely identifies that the administrator role within the TOE can be split. Firewall administrators are administrators of the PIX/ASA. Audit administrators are administrators of the Windows audit server.

Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to No other components.

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.
Dependencies	No dependencies

FPT_SEP.1 TSF domain separation

Hierarchical to	No other components.
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.
FMT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.
Dependencies	No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to	No other components.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.
Dependencies	No dependencies
Application Note	The word "reliable" in the above requirement means that the order of the occurrence of auditable events is preserved. Reliable time stamps, which include both date and time, are especially important for TOEs composed of greater than one component.

The required minimum strength of function for security functional requirements is SOF-Medium. Strength of function shall be demonstrated for the password authentication mechanism such that the probability that authentication data can be guessed is no greater than one in two to the fortieth (2^{40}). The password authentication mechanism must demonstrate SOF-Medium, as defined in Part 1 of CC.

TOE Environment Security Functional Requirements

The following functional requirements are met partially by the TOE and partially by the environment.

FIA_ATD.1 User attribute definition

Hierarchical to	No other components.
FIA_ATD.1.1	The IT environment shall maintain the following list of security attributes belonging to individual users and external IT entities: **a.** [Identity **b.** Association of a human user with the authorized firewall administrator role **c.** Password].
Dependencies	No dependencies

FIA_UAU.5 Multiple authentication mechanisms

Note that in accordance with US PD-115 items 1, 2, and 3 of this security functional requirement are addressed partially by the TOE environment, while item 4 is addressed by the TOE.

Hierarchical to	No other components.
FIA_UAU.5.1	The IT environment shall provide [password and single-use authentication mechanisms] to support user authentication.
FIA_UAU.5.2	The IT environment shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules: **a.** Single-use authentication mechanism shall be used for authorized firewall administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized firewall administrator. **b.** Single-use authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity. **c.** Single-use authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet such that successful authentication must be achieved before allowing any other non-TSF-mediated actions on behalf of that human user. **d.** Reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator.].
Dependencies	No dependencies
Application Note	The TOE shall be responsible for correctly invoking the external single-use authentication mechanism, and for taking the correct actions based on authentication decisions. In keeping with industry practice, the choice of authentication server is not mandated by this ST.

FIA_UID.2 User identification before any action

Hierarchical to	No other components.
FIA_UID.2.1	The IT environment shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.
Dependencies	No dependencies

TOE Security Assurance Requirements

Table 10 describes the TOE security assurance requirements drawn from Part 3 of the CC. The security assurance requirements represent EAL4 augmented with ALC_FLR.1.

Table 10 TOE Assurance Components

Assurance Class	Assurance Components
Configuration Management (ACM)	*Partial CM Automation (ACM_AUT.1)*
	Generation support and acceptance procedures (ACM_CAP.4)
	Problem tracking CM coverage (ACM_SCP.2)
Delivery and Operation (ADO)	*Detection of modification (ADO_DEL.2)*
	Installation, generation, and start-up procedures (ADO_IGS.1)
Development (ADV)	*Fully defined external interfaces (ADV_FSP.2)*
	Security enforcing high-level design (ADV_HLD.2)
	Subset of the implementation of the TSF (ADV_IMP.1)
	Descriptive low-level design (ADV_LLD.1)
	Informal correspondence demonstration (ADV_RCR.1)
	Informal TOE security policy model (ADV_SPM.1)
Guidance Documents (AGD)	*Administrator guidance (AGD_ADM.1)*
	User guidance (AGD_USR.1)
Life Cycle Support (ALC)	*Identification of security measures (ALC_DVS.1)*
	Basic flaw remediation (ALC_FLR.1)
	Developer defined life-cycle model (ALC_LCD.1)
	Well defined development tools (ALC_TAT.1)
Tests (ATE)	*Analysis of coverage (ATE_COV.2)*
	Testing: high-level design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability Assessment (AVA)	*Validation of analysis (AVA_MSU.2)*
	Strength of TOE security function evaluation (AVA_SOF.1)
	Independent vulnerability analysis (AVA_VLA.2)

Configuration Management

This section includes the following topics:

ACM_AUT.1 Partial CM automation

Dependencies ACM_CAP.3 Authorization controls

Developer action elements:

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements:

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements:

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_CAP.4 Generation support and acceptance procedures

Dependencies ALC_DVS.1 Identification of security measures

Developer action elements:

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.7C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.8C The CM plan shall describe how the CM system is used.

ACM_CAP.4.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.11C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.12C The CM system shall support the generation of the TOE.

ACM_CAP.4.13C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.2 Problem tracking CM coverage

Dependencies ACM_CAP.3 Authorization controls

Developer action elements:

ACM_SCP.2.1D The developer shall provide a list of configuration items for the TOE.

Content and presentation of evidence elements:

ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evidence required by the assurance components in the ST.

Evaluator action elements:

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Delivery and Operation

ADO_DEL.2 Detection of modification

Dependencies ACM_CAP.3 Authorization controls

Developer action elements:

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements:

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies AGD_ADM.1 Administrator guidance

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Development

ADV_FSP.2 Fully defined external interfaces

Dependencies ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

Dependencies ADV_FSP.1 Informal functional specification

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_ HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

Application Note The elements within this family define a requirement that the evaluator determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements. This provides a direct correspondence between the TOE security functional requirements and the high level design, in addition to the pair-wise correspondences required by the ADV_RCR family. It is expected that the evaluator will use the evidence provided in ADV_RCR as an input to making this determination, and the requirement for completeness is intended to be relative to the level of abstraction of the high-level design.

ADV_IMP.1 Subset of the implementation of the TSF

Dependencies ADV_LLD.1 Descriptive low-level design

ADV_RCR.1 Informal correspondence demonstration

ALC_TAT.1Well-defined development tools

Developer action elements:

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

Content and presentation of evidence elements:

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_ IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

ADV_LLD.1 Descriptive low-level design

Dependencies ADV_HLD.2 Security enforcing high-level design

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements:

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP enforcing and other modules.

Evaluator action elements:

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.1E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Dependencies No dependencies.

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note The intent of this requirement is for the vendor to provide, and the evaluator to confirm, that there exists accurate, consistent, and clear mappings between each level of design decomposition. Thus, there can be no TOE security functions defined at a lower layer of abstraction absent from a higher level of abstraction and vice versa.

ADV_SPM.1 Informal TOE security policy model

Dependencies ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Guidance Documents

AGD_ADM.1Administrator guidance

Dependencies ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

Dependencies ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note This assurance component is trivially met since neither authorized external IT entities nor human users who are not authorized administrators are permitted on the TOE.

Life Cycle Support

ALC_DVS.1 Identification of security measures

Dependencies No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_FLR.1 Basic flaw remediation

Dependencies No dependencies.

Developer action elements:

ALC_FLR.1.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

Content and presentation of evidence elements:

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Evaluator action elements:

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_LCD.1 Developer defined life-cycle model

Dependencies No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.1 Well-defined development tools

Dependencies ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements:

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Tests

ATE_COV.2 Analysis of coverage

Dependencies ADV_FSP.1 Informal functional specification

ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Testing: high-level design

Dependencies ADV_HLD.1 Descriptive high-level design

ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies No dependencies.

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing – sample

Dependencies ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

Vulnerability Assessment

AVA_MSU.2 Validation of analysis

Dependencies ADO_IGS.1 Installation, generation, and start-up procedures

ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of TOE security function evaluation

Dependencies ADV_FSP.1 Informal functional specification

ADV_HLD.1 Descriptive high-level design

Developer action elements:

AVA_SOF.1.1D The developer shall perform a TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim, the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim, the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.2 Independent vulnerability analysis

Dependencies	ADV_FSP.1 Informal functional specification
	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
	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance

Developer action elements:

AVA_VLA.2.1D	The developer shall perform a vulnerability analysis.
AVA_VLA.2.2D	The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.2.1C	The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.
AVA_VLA.2.2C	The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.
AVA_VLA.2.3C	The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.2.4C	The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

Evaluator action elements:

AVA_VLA.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.2.2E	The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.
AVA_VLA.2.3E	The evaluator shall perform an independent vulnerability analysis.
AVA_VLA.2.4E	The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.
AVA_VLA.2.5E	The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

TOE Summary Specification

This section includes the following topics:

TOE Security Functions

This section includes the following topics:

Security Management Function

The Security Management Function permits an authorized firewall administrator (from a physically secure local connection, or via an SSH encrypted connection (the encryption is subject to the FIPS 140 security functional requirements given under FCS_COP.1, in the first section) from an internal trusted host or a remote connected network) to perform the following actions:

1. Enable or disable the operation of the TOE.
2. Enable or disable the use of the single-use authentication function.
3. Enable or disable firewall administrator accounts, or modify their security attributes.
4. Enable, disable, determine and modify the behavior of the audit trail.
5. Enable, disable, determine and modify the behavior of the backup and restore function for TSF data, information flow rules, and audit trail data.
6. Enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE.
7. Delete attributes from a rule, modify attributes in a rule and add attributes to a rule for the security attributes.
8. Delete and create the information flow rules.
9. Set the time and date used to form the timestamps.
10. Specify of the limits for the number of authentication failures.

The management functions listed in the previous section can only be performed by an authorized administrator. Items 2, 6, 7, and 8 are relevant for the firewall administrator only.

Audit Function

The Audit Function provides auditing that can be switched on or off (this action is audited). When active, the following events are recorded:

1. All decisions on requests for information flow.
2. The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the user's capability to authenticate.
3. Any use of the identification or authentication mechanisms.
4. Modifications to the group of users that are part of the authorized administrator role.
5. Changes to the time.

6. Audit trail management activities.
7. Backup for TSF data.
8. Use of the single-use authentication function.
9. Activation or deactivation of the single-use authentication function.

For each event the Audit Function will record the following:

1. Date and time of the event.
2. Source and destination IP address (for connections only).
3. Type of event or service.
4. Specific information related to the event.
5. Success or failure of the event.

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

Audit records are sent by the firewall for storage using the Firewall Syslog Server (PFSS) on the Windows 2000 or Windows XP server. PFSS creates seven rotating syslog files named monday.log, tuesday.log, wednesday.log, thursday.log, friday.log, saturday.log, and sunday.log. If a week has passed since the last log file was created, it will rename the old log file to *day.mmddyy,* where *day* is the current day, *mm* is the month, *dd* is the day, and *yy* is the year. An authorized audit administrator can gain read access to firewall audit records through PFSS. Audit events generated on the audit server can be viewed using the Windows Event Viewer.

Note that the evaluated configuration requires use of the CC certified versions of these products (that is, Microsoft Windows 2000 Professional Server with SP3 (including hotfix Q326886) or Microsoft Windows XP Professional; SP 2 (including hotfixes 896423, 899587, 899588, 896422, 890859, 873333, 885250, 888302, 885835, and 907865).

PFSS provides the ability to search and sort audit records based on one or a combination of many of the following:

1. Source IP address or address range
2. Source port or range of ports
3. Destination IP address or address range
4. Destination port or range of ports
5. Service
6. Start date and end date
7. Start time and end time
8. System log message number
9. Interface name

Audit records are protected from modification or unauthorized deletion through permission settings in Windows 2000 or Windows XP.

If it is not possible to write audit records to the audit trail then actions other than those taken by an authorized administrator are prevented.

Information Flow Control Function

The Information Control Function of the TOE allows authorized firewall administrators to set up rules between interfaces of the firewall. These rules control whether a packet is transferred from one interface to another based on:

1. User identity
2. Source address
3. Destination address
4. Service used
5. Port number
6. Security-relevant service command
7. Network interface on which the connection request occurs

The service requested, if permitted by the information control rules may comprise of (but is not limited to) Ethernet, ARP, CTIQBE, DNS, Echo, Finger, H.323, IP, ICMP, TCP, UDP, FTP, GTP, HTTP, ILS, MGCP, POP3, RSH, RTSP, Skinny, SIP, ESMTP, SunRPC, Telnet, TFTP and XDMCP. Application inspection is also provided within the TOE for the following protocols and applications: CTIQBE, H.323, ICMP, FTP, GTP, HTTP, ILS, MGCP, RSH, RTSP, Skinny, SIP, ESMTP, SunRPC, TFTP and XDMCP. 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.

The TOE has the ability to reject requests in which the subject specifies the route in which information flows en route to the receiving subject. Through use of protocol filtering proxies, the TOE can also reject Telnet or FTP command requests that do not conform to generally accepted, published protocol definitions.

Identification and Authentication Function

Administrators are required to identify themselves and be authenticated before any further access to the TOE is granted (that is, before they become authorized administrators).

Authentication performed by the TOE makes use of a reusable password mechanism for local access to the TOE by authorized administrators. This is a permutational mechanism that meets the minimum strength of function rating of Medium.

Following a non-zero number of failed authentication attempts (set by an authorized administrator) administrator accounts will be locked until released by an authorized administrator. This function is not implemented for remote access, due to the ease with which a DOS attack could be mounted.

Single-use authentication for remote authorized firewall administrators and authorized external IT entities is provided by means of TOE functions that correctly invoke it and act correctly, based on the decisions of an external authentication server in the TOE environment.

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 TOE accounts for all packets traversing the firewall in relation to the associated information stream. Therefore, no residual information relating to other packets will be reused on that stream.

The protection function also ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. This includes use of an encrypted link (with FIPS 140 validated cryptographic modules) for remote management functions.

Clock Function

The Clock Function of the TOE provides a source of date and time information for the firewall, used in audit timestamps and in validating service requests. This function can only be accessed from within the configuration exec mode via the privileged mode of operation of the firewall. The clock function is reliant on the system clock provided by the underlying hardware.

Assurance Measures

Table 11 identifies the deliverables that will meet the assurance requirements of Common Criteria EAL 4, augmented with ALC_FLR.1. The identified deliverables describe the approach taken to meet the assurance requirements, and meet all of the assurance requirements contained in this assurance package.

Table 11 Assurance Measures

Assurance Class	Assurance Components	Assurance Measures (Cisco Documentation)
Security target (ASE)	*All*	This security target meets all of the requirements within class ASE.

Table 11 Assurance Measures (continued)

Configuration Management (ACM)	*Partial CM Automation (ACM_AUT.1)* *Generation support and acceptance procedures (ACM_CAP.4)* *Problem tracking CM coverage (ACM_SCP.2)*	Configuration Management and Delivery Procedures for Cisco Secure PIX Firewall 515/515E, PIX 525, PIX 535, and ASA 5510, ASA 5520, and ASA 5540 Version 7.0(6). Installation Guide for the Cisco Secure PIX Firewall Version 7.0(6) Configuration Guide for the Cisco Secure PIX Firewall Version 7.0(6) Release Notes for Cisco Secure PIX Firewall Version 7.0(6) The Configuration Management and Delivery Procedures describe the use of an automated configuration management system that meets the requirements of ACM_CAP.4 and ACM_AUT.1. All documentation required by ACM_SCP.1 is held under configuration control. These procedures also describe secure delivery process to preserve the integrity of the TOE, meeting the requirements of ADO_DEL.2. The Installation Guide, Configuration Guide and Release Notes provide information on how to bring the delivered TOE into an operational state in accordance with ADO_IGS.1.

Table 11 Assurance Measures (continued)

Delivery and operation (ADO)	*Detection of modification (ADO_DEL.2)*	Functional Specification for Cisco Secure PIX Firewall 515/515E, PIX 525, PIX 535, and ASA 5510, ASA 5520, and ASA 5540 Version 7.0(6). This document describes the external interfaces to the TOE in a manner consistent with the requirements of ADV_FSP.2.
	Installation, generation, and start-up procedures (ADO_IGS.1)	
Development (ADV)	*Fully defined external interfaces (ADV_FSP.2)*	
	Security enforcing high-level design (ADV_HLD.2)	High-Level Design for Cisco Secure PIX Firewall 515/ 515E, PIX 525, PIX 535, ASA 5510, ASA 5520 and ASA 5540 Version 7.0(6). This document describes the TOE in terms of subsystems, and documents the interfaces between them.
	Subset of the implementation of the TSF (ADV_IMP.1)	Various source code for Cisco Secure PIX Firewall 515/ 515E, PIX 525, PIX 535, ASA 5510, ASA 5520 and ASA 5540 Version 7.0(6). A sample of the TOE source code selected by the evaluators meets this requirement.
	Descriptive low-level design (ADV_LLD.1)	Low-Level Design for Cisco Secure PIX Firewall 515/ 515E, PIX 525, PIX 535, ASA 5510, ASA 5520 and ASA 5540 Version 7.0(6). This document describes the decomposition of the TOE subsystems into modules, and documents the interfaces between them.
	Informal correspondence demonstration (ADV_RCR.1)	Correspondence demonstration for Cisco Secure PIX Firewall 515/ 515E, PIX 525, PIX 535, ASA 5510, ASA 5520 and ASA 5540 Version 7.0(6). A description of correspondence between the TOE summary specification, the high-level design, the low-level design and source code is provided by means of cross-references in this document.
	Informal TOE security policy model(ADV_SPM.1)	Security Policy Model for Cisco Secure PIX Firewall 515/ 515E, PIX 525, PIX 535, ASA 5510, ASA 5520 and ASA 5540 Version 7.0(6). The security policy model describes in an informal style the policies that underlie the TOE security functional requirements, which are traced to the functional specification.

Table 11 Assurance Measures (continued)

Guidance documents (AGD)	*Administrator guidance (AGD_ADM.1)* *User guidance (AGD_USR.1)*	Installation Guide for the Cisco Secure PIX Firewall Version 7.0(6) Configuration Guide for the Cisco Secure PIX Firewall Version 7.0(6) Command Reference Guide for the Cisco Secure PIX Firewall Version 7.0(6) Release Notes for Cisco Secure PIX Firewall Version 7.0(6) CC Evaluated Configuration Guide for the Cisco Secure PIX Firewall Version 7.0(6) These documents provide detailed guidance on the administration of the TOE in a secure manner. They also provide information on achieving the evaluated configuration.
Life cycle support (ALC)	*Identification of security measures (ALC_DVS.1)*	Development Security for Cisco Secure PIX Firewall, Cisco Adaptive Security Appliances and Cisco Systems Firewall Services Module (FWSM). This document defines the procedures used to maintain the security of the development environment. These measures provide a combination of procedural, personnel and technical measures that safeguard the integrity and confidentiality of the TOE.
	Basic flaw remediation (ALC_FLR.1) *Developer defined life cycle model (ALC_LCD.1)* *Well-defined development tools (ALC_TAT.1)*	Configuration and delivery procedures for Cisco Secure PIX Firewall 515/ 515E, PIX 525, PIX 535, ASA 5510, ASA 5520 and ASA 5540 Version 7.0(6). This document describes the procedures and tools that are used in development and maintenance of the TOE. These procedures provide a controlled approach to management of the TOE lifecycle. Procedures covering handling of reported flaws in the TOE are also provided.
Tests (ATE)	*Analysis of coverage (ATE_COV.2)* *Testing: high-level design (ATE_DPT.1)* *Functional testing (ATE_FUN.1)* *Independent testing – sample (ATE_IND.2)*	Testing plan and analysis for Cisco Secure PIX Firewall 515/ 515E, PIX 525, PIX 535, ASA 5510, ASA 5520 and ASA 5540 Version 7.0(6). The test documentation describes how each external security functional interface is tested, and also how it is demonstrated that the subsystem interfaces are also operating correctly. The documentation describes the test environments used, the tests that are carried out, and the results that are expected and obtained. The TOE is made available to the evaluators for testing.

Table 11 Assurance Measures (continued)

Vulnerability assessment (AVA)	*Validation of analysis (AVA_MSU.2)*	Misuse analysis for Cisco Secure PIX Firewall 515/ 515E, PIX 525, PIX 535, ASA 5510, ASA 5520 and ASA 5540 Version 7.0(6). The misuse analysis provides an analysis of the guidance documentation, demonstrating that the TOE can be managed in a predictable and secure manner.
	Strength of TOE security function evaluation (AVA_SOF.1)	Strength of function analysis for Cisco Secure PIX Firewall 515/ 515E, PIX 525, PIX 535, ASA 5510, ASA 5520 and ASA 5540 Version 7.0(6). The strength of function analysis provides an analysis of the password mechanism that demonstrates that the SOF claims are upheld.
	Independent vulnerability analysis (AVA_VLA.2)	Vulnerability analysis for Cisco Secure PIX Firewall 515/ 515E, PIX 525, PIX 535, ASA 5510, ASA 5520 and ASA 5540 Version 7.0(6). Cisco carries out and documents an analysis of the TOE deliverables, searching for weaknesses that might allow an attacker to violate the TOE security policy. This analysis is provided to the evaluators.

Protection Profile Claims

This section includes the following topics:

The TOE functionality is specified to be consistent with the U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000 [FWPP].

The ST includes all security functional requirements included in [FWPP] (as modified under PD-0115 and PD-0026).

Environment Rationale

The assumptions in this ST are the same as those in the [FWPP], although an additional assumption concerning protection of the audit server has been added (A.PROTECTPF).

The threats in this ST are the same as those in the [FWPP], adjusted slightly to reflect attackers with low attack potential.

The organizational security policy in this ST has been updated that from the [FWPP] to include FIPS PUB 140-2 and AES.

Objectives Rationale

The security objectives in this ST differ from those in the [FWPP] in the following ways:

a. The TOE security objective O.IDAUTH has been abbreviated to exclude connected networks. This functionality is provided in the TOE environment, where the objective is transcribed completely. The limited objective is retained in the TOE security objectives to cover local authentication of administrators. This change is consistent with PD-0115.

b. The TOE security objective O.MEDIAT has been clarified to refer to "users," rather than "clients and servers."

c. The IT environment security objective OE.PHYSEC has been modified to include the TOE operating environment and the connection to the audit server. This clarifies the intent of the objective, but does not weaken it.

d. The IT environment security objective OE.PUBLIC has been modified to include the authentication server, and the environment security objectives OE.IDAUTH and OE.SINUSE have been added. Since PD-0115 excluded the authentication server from the scope of the TOE this renders the objectives consistent with the intent of the [FWPP].

Security Functional Requirements Rationale

The security functional requirements in this ST differ from those in the [FWPP] in the following ways:

a. All operations have been completed in a manner consistent with the [FWPP].

b. The TOE security functional requirements FIA_ATD.1, FIA_UAU.5 and FIA_UID.2 have been duplicated for the TOE and for the IT environment. This reflects the removal of the authentication server from the scope of the TOE, and is consistent with PD-0115.

Security Assurance Requirements Rationale

The assurance requirements in this ST are different from those in the [FWPP]. The differences are identified in Table 12.

Table 12 Assurance Comparison of ST with [FWPP]

[FWPP]	ST
-	ACM_AUT.1
ACM_CAP.2	ACM_CAP.4
-	ACM_SCP.2
ADO_DEL.1	ADO_DEL.2
ADV_FSP.1	ADV_FSP.2
-	ALC_DVS.1
-	ADV_SPM.1
-	ALC_FLR.1
-	ALC_LCD.1
ATE.COV.1	ATE_COV.2

Table 12 Assurance Comparison of ST with [FWPP] (continued)

-	ATE_DPT.1
-	AVA_MSU.2
AVA_VLA.3	AVA_VLA.2

Because the audit server meets the criteria established in PD-0113, the modified assurance requirements stated in this document will be applied to that part of the TOE.

Rationale

This section includes the following topics:

Security Objectives Rationale

The security objectives rationale is modeled on that for the [FWPP]. It has been included here for the sake of completeness. Also, in some areas, minor errors in the [FWPP] have been corrected. For example, O.IDAUTH objective includes not only user identification, but also user authentication.

O.IDAUTH	This security objective is necessary to counter the threat: T.NOAUTH, because it requires that users be uniquely identified and authenticated before accessing the TOE.
O.SINUSE	This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY, because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.
O.MEDIAT	This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF, which involve getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE, and that no residual information is transmitted.
O.SECSTA	This security objective ensures that no information is compromised by the TOE upon start-up or recovery, and thus counters the threats: T.NOAUTH and T.SELPRO.
O.ENCRYP	This security objective is necessary to counter the threats and policy: T.NOAUTH, T.PROCOM and P.CRYPTO by requiring that an authorized firewall administrator use encryption when performing administrative functions on the TOE remotely.

O.SELPRO — This security objective is necessary to counter the threats: T.SELPRO, T.NOAUTH, and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC — This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

O.ACCOUN — This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

O.SECFUN — This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

O.LIMEXT — This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.

O.EAL — This security objective is necessary to counter the threat: T.MODEXP because it requires that the TOE is resistant to penetration attacks performed by an attacker possessing low attack potential.

Table 13 shows the mapping between threats and policies, and IT security objectives. A check in every row means that every security objective is necessary. A check in every column implies that all threats are countered and policies are met.

Table 13 Summary of Mappings Between Threats, Policies, and IT Security Objectives

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T.MODEXP	P.CRYPTO
O.IDAUTH	x											
O.SINUSE		x	x									
O.MEDIAT				x	x	x						
O.SECSTA	x								x			
O.ENCRYP	x						x					x
O.SELPRO	x								x	x		
O.AUDREC								x				
O.ACCOUN								x				
O.SECFUN	x		x							x		
O.LIMEXT	x											
O.EAL											x	

Rationale for Security Objectives for the Environment

The security objectives rationale for the environment is based on that for [FWPP].

OE.IDAUTH	This security objective is necessary to counter the threat: T.NOAUTH, because it requires that remote users be uniquely identified and authenticated before accessing the TOE.
OE.PHYSEC	The TOE and its operating environment are physically secure. The audit server is accessible only by the TSF.
OE.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.GENPUR	There are no general-purpose computing capabilities (for example, the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.PUBLIC	The TOE and the authentication server do not host public data.
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (for example, a console port) if the connection is part of the TOE.
OE.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
OE.REMACC	Authorized firewall administrators may access the TOE remotely from the internal and external networks.
OE.GUIDAN	This non-IT security objective is necessary to counter the threat: T.TUSAGE and T.AUDACC, because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.
OE.ADMTRA	This non-IT security objective is necessary to counter the threat: T.TUSAGE and T.AUDACC, because it ensures that authorized administrators receive the proper training.
OE.SINUSE	This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY, because it requires that the IT environment contributes to preventing the reuse of authentication data, so that even if valid authentication data is obtained, it will not be used successfully to mount an attack.

Table 14 shows the relationship between threats and four of the security objectives for the environment.

Table 14 Summary of Mappings Between Threats and Security Objectives for the Environment

T.	NOAUTH	REPEAT	REPLAY	TUSAGE	AUDACC
OE.IDAUTH	x				
OE.GUIDAN				x	x
OE.ADMTRA				x	x
OE.SINUSE		x	x		

Because the rest of the security objectives for the environment are, in part, a restatement of the security assumptions, those security objectives trace to all aspects of the assumptions.

TOE Security Functional Requirements (SFR) Rationale

The functional and assurance requirements presented in this ST are mutually supportive and their combination meets the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria. The following paragraphs and Table 13 show the mapping between the security requirements and the security objectives. Table 15 demonstrates the relationship between the threats, policies, and IT security objectives. Together these tables demonstrate the completeness and sufficiency of the requirements.

The minimum strength of function claim of SOF-Medium has been selected as appropriate to meet the security objective O.IDAUTH and the selected assurance level of EAL4. The metric required in this ST is an acceptable metric for SOF-Medium.

FAU_GEN.1 Audit data generation

This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review

This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

This component is chosen to ensure that the audit trail is always protected from tampering, the security functionality is limited to the authorized administrator, and start-up and recovery do not compromise the audit records. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SELPRO, and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

This component ensures that the authorized audit administrator will be able to take care of the audit trail if it should become full and resources will not be compromised upon recovery. This component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SELPRO and O.SECFUN.

If TCP system log messaging is enabled, the maximum that can be lost on power failure is the number of logs generated as a result of the last 50 packets. While this is not strictly quantifiable, the maximum length an audit queue can grow is limited to 8192 messages (2MB).

FCS_COP.1 Cryptographic operation

This component ensures that Triple-DES or AES are used by authorized firewall administrators to communicate with the TOE remotely from an internal or external network. This component is necessitated by the postulated threat environment. This component traces back to and aids in meeting the following objective: O.ENCRYP.

FDP_IFC.1(1) Subset information flow control

This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (that is, users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFC.1(2) Subset information flow control

This component identifies the entities involved in the AUTHENTICATED information flow control SFP (that is, users of the services FTP or Telnet sending information to servers and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1(1) Simple security attributes

This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1(2) Simple security attributes

This component identifies the attributes of the users sending and receiving the information in the AUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_RIP.1 Subset residual information protection

This component ensures that neither information that had flown through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FIA_AFL.1 Authentication failure handling

This component ensures that human users who are not authorized administrators can not endlessly attempt to authenticate. After some number of failures that the authorized administrator decides, that must not be zero, the user becomes unable from that point to authenticate. This continues until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.

FIA_ATD.1 User attribute definition

This component exists to permit the TOE to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.

FIA_UAU.5 Multiple authentication mechanisms

This component was chosen to ensure that multiple authentication mechanisms are used appropriately in all attempts to authenticate at the TOE from an internal or external network. An additional SOF metric for this requirement is defined in section 5.1 to ensure that the mechanism is of adequate cryptologic strength. This component traces back to and aids in meeting the following objectives: O.SINUSE and O.IDAUTH. Note that this requirement is partially satisfied by the TOE and partially by the TOE environment. Its presence under TOE security functional requirements is to address authentication of local administrators only.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of a user, the user is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FMT_MOF.1 Management of security functions behavior (1)

This component ensures that the TSF restricts the management of the TOE start up and shut down operation and single-use authentication function (described in FIA_UAU.5) to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN, and O.LIMEXT.

FMT_MOF.1 Management of security functions behavior (2)

This component ensures that the TSF restricts the ability to modify the behavior of functions such as audit trail management, back and restore for TSF data, and communication of authorized external IT entities with the TOE to an appropriate authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN and O.LIMEXT.

FMT_MSA.1 Management of security attributes (1)

This component ensures the TSF enforces from TOE start-up the UNAUTHENTICATED SFP to restrict the ability to add, delete and modify specified security attributes that are listed in section 0 (FDP_IFF1.1(1)). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (2)

This component ensures the TSF enforces from TOE start-up the AUTHENTICATED SFP to restrict the ability to add, delete and modify specified security attributes that are listed in section 0 (FDP_IFF1.1(2)). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN

FMT_MSA.1 Management of security attributes (3)

This component ensures the TSF enforces from TOE start-up the UNAUTHENTICATED SFP to restrict the ability to create or delete specified security attributes that are listed in information flow rules in section 0 (FDP_IFF1.1(1)). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.1 Management of security attributes (4)

This component ensures the TSF enforces from TOE start-up the AUTHENTICATED SFP to restrict the ability to create or delete specified security attributes that are listed in information flow rules in section 0 (FDP_IFF1.1(2)). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.3 Static attribute initialization

This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECSTA.

FMT_MTD.1 Management of TSF data (1)

This component ensures that the TSF restrict abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.1 Management of TSF data (2)

This component ensures that the TSF restrict abilities to set the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_MTD.2 Management of limits on TSF data

This component ensures that the TSF restrict the specification of limits on the number of unauthenticated failures to the authorized administrator and specifies the action be taken if limits are reached or exceeded. This component traces back to and aids in meeting the following objective: O.SECFUN.

FMT_SMF.1 Specification of management functions

This component requires that security management functions be implemented in the TOE. It traces back to and aids in meeting the following objective: O.SECFUN.

FMT_SMR.1 Security roles

Each of the CC class FMT components in this ST depend on this component. This component traces back to and aids in meeting the following objective: O.SECFUN.

FPT_RVM.1 Non-bypassability of the TSP

This component ensures that the TSF are always invoked from initial start-up. This component traces back to and aids in meeting the following objective: O.SELPRO and O.SECSTA.

FPT_SEP.1 TSF domain separation

This component ensures that the TSF has a domain of execution that is separate and that cannot be violated by unauthorized users. This component also ensures that the domains of execution for the various processes are isolated and cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

A check in every row in Table 15 means that every SFR is necessary. A check in every column implies that all security objectives are met. O.EAL objective is satisfied by the Security Assurance Requirements.

Table 15 Summary of Mappings Between TOE Security Functional Requirements and IT Security Objectives

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT	O.EAL
FAU_GEN.1							x	x			
FAU_SAR.1							x				
FAU_SAR.3							x				
FAU_STG.1				x		x			x		
FAU_STG.4				x		x			x		
FCS_COP.1					x						
FDP_IFC.1(1)			x								
FDP_IFC.1(2)			x								
FDP_IFF.1(1)			x								
FDP_IFF.1(2)			x								
FDP_RIP.1			x								
FIA_AFL.1						x					
FIA_ATD.1	x								x		
FIA_UAU.5	x	x									
FIA_UID.2	x							x			
FMT_MOF.1 (1)				x					x	x	
FMT_MOF.1 (2)				x					x	x	
FMT_MSA.1 (1)			x	x					x		
FMT_MSA.1 (2)			x	x					x		

Table 15 Summary of Mappings Between TOE Security Functional Requirements and IT Security Objectives (continued)

FMT_MSA.1 (3)			x	x					x		
FMT_MSA.1 (4)			x	x					x		
FMT_MSA.3			x	x							
FMT_MTD.1 (1)									x		
FMT_MTD.1 (2)									x		
FMT_MTD.2									x		
FMT_SMF.1									x		
FMT_SMR.1									x		
FPT_RVM.1				x		x					
FPT_SEP.1						x					
FPT_STM.1							x				

TOE Environment Security Functions Rationale

Apart from OE.IDAUTH and OE.SINUSE, all of the security objectives for the environment are met by non-IT measures.

The following rationale is provided to support security functional requirements that are partially met within the TOE environment.

FIA_ATD.1 User attribute definition

This component exists to permit the TOE to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: OE.IDAUTH and OE.SINUSE. Its presence under TOE environment security functional requirements is to address authentication of remote authorized administrators and external IT entities only.

FIA_UAU.5 Multiple authentication mechanisms

This component was chosen to ensure that multiple authentication mechanisms are used appropriately in all attempts to authenticate at the TOE from an internal or external network. This component traces back to and aids in meeting the following objective: OE.IDAUTH. Note that this requirement is partially satisfied by the TOE and partially by the TOE environment. Its presence under TOE environment security functional requirements is to address authentication of remote authorized firewall administrators and external IT entities only.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of a user, the user is identified to the TOE. This component traces back to and aids in meeting the following objective: OE.IDAUTH.

Security Assurance Requirements (SAR) Rationale

The ST is written with EAL4 augmented with ALC_FLR.1.

EAL4 was chosen because it permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices. EAL4 provides the developers and users a moderate to high level of independently assured security in conventional commercial TOEs.

EAL 4 is augmented by ALC_FLR.1 to help ensure that the customers can report the flaws and the flaws can be systematically corrected.

To ensure high security of information processed by the TOE, not only must vulnerability analysis by the developer be performed, but the evaluator of the TOE must perform independent penetration testing to determine that the TOE is resistant to penetration attacks performed by attackers possessing a low attack potential.

The chosen assurance level as supported by O.EAL, which is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than low, and the product will have undergone vulnerability analysis by the developer and independent penetration testing by the evaluator.

Rationale for Not Satisfying All Dependencies

With the exception of the functional component FCS_COP.1 and FIA_AFL.1 all dependencies are contained in this security target.

Functional component FCS_COP.1 depends on the following functional components: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction and FMT_MSA.2 Secure Security Attributes. Cryptographic modules must be FIPS PUB 140-1 or FIPS 140-2 compliant. Since the cryptographic modules are compliant with FIPS PUB 140-2, then the dependencies of key generation, key destruction and secure key values will have been satisfied in becoming FIPS PUB 140-2 compliant. For more information, refer to sections 4.7.2 and 4.7.6 of FIPS PUB 140-2.

FIA_AFL.1 has a dependency on FIA_UAU.1. This authentication functionality is required to support the operation of authentication failure locking. In this ST, the necessary authentication functionality is required through inclusion of FIA_UAU.5, where item 1 of the completed operation contains similar wording to FIA_UAU.2 (which is hierarchical to FIA_UAU.1).

TOE Summary Specification Rationale

This section shows that the security functions, as described in the TOE Summary Specification (see TOE Summary Specification, page 44) are necessary and sufficient to implement the SFRs and SARs. Table 16 shows a summary of the mappings between TOE security functional requirements and security functions.

Table 16 Summary of Mappings Between TOE Security Functional Requirements and TOE Security Functions

	Security Management	Audit	Information Flow Control	Identification and Authentication	Protection	Clock
FAU_GEN.1		x				x
FAU_SAR.1		x				
FAU_SAR.3		x				
FAU_STG.1		x				
FAU_STG.4		x				
FCS_COP.1	x				x	
FDP_IFC.1(1)			x			
FDP_IFC.1(2)			x			

Table 16 Summary of Mappings Between TOE Security Functional Requirements and TOE Security Functions (continued)

FDP_IFF.1(1)			x			
FDP_IFF.1(2)			x			
FDP_RIP.1					x	
FIA_AFL.1				x		
FIA_ATD.1				x		
FIA_UAU.5				x		
FIA_UID.2				x		
FMT_MOF.1(1)	x					
FMT_MOF.1(2)	x	x				
FMT_MSA.1 (1)	x		x			
FMT_MSA.1 (2)	x		x			
FMT_MSA.1 (3)	x		x			
FMT_MSA.1 (4)	x		x			
FMT_MSA.3	x		x			
FMT_MTD.1 (1)	x			x		
FMT_MTD.1 (2)	x					x
FMT_MTD.2	x			x		
FMT_SMF.1	x	x	x	x		x
FMT_SMR.1	x	x	x	x		x
FPT_RVM.1					x	
FPT_SEP.1					x	
FPT_STM.1						x

The **Security Management Function** permits the authorized administrator (FMT_SMR.1) to perform the following actions (FMT_SMF.1), locally and remotely via a FIPS 140 validated encrypted link (FCS_COP.1):

- Modify the time (FMT_MTD.1(2)).
- Control the operation of the single use authentication mechanism (firewall administrator only) (FMT_MOF.1(1)).
- Manage the audit trail and communication with the TOE by external IT entities, (FMT_MOF.1(2).
- Backup TSF data (FMT_MOF.1(2)).
- Manipulate the Information Flow Policy Rules (firewall administrator only) (FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), and FMT_MSA.3).
- Manage administrator accounts (FMT_MTD.1(1).
- Manage the authentication failure lockout mechanism (FMT_MTD.2).

The **Information Control Flow Function** allows authorized firewall administrators (FMT_SMR.1) to set up traffic flow rules between pairs of network interfaces on the firewall (FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3, FMT_SMF.1). 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 authorized firewall administrator can restrict and control the flow of network traffic between the network interfaces of the firewall. This is based on the flow attributes of the packets arriving at a network interface:

- The interface on which the request arrives (FDP_ IFF.1(1), FDP_IFF.1(2), FDP_IFC.1(1) and FDP_IFC.1(2)).
- The presumed source IP address of the packet (FDP_ IFF.1(1), FDP_IFF.1(2), FDP_IFC.1(1) and FDP_IFC.1(2)).
- The destination IP address of the packet (FDP_ IFF.1(1), FDP_IFF.1(2), FDP_IFC.1(1) and FDP_IFC.1(2)).
- The service related to the packet (FDP_ IFF.1(1) and FDP_IFF.1(2)).
- The transport layer protocol contained within the packet (FDP_ IFF.1(1) and FDP_IFF.1(2)).

The packets can have their address translated into another address (FDP_IFF.1(1) and FDP_IFF.1(2)).

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(1), FDP_IFF.1(2)and FPT_RVM.1).

The **Audit Function** provides reliable audit trail of network connections and other events (FAU_GEN.1) that can be managed by an authorized administrator (FMT_MOF1(2), FMT_SMF.1). For all events, the Audit Function will record the following information:

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

Audit records are stored securely on the audit server (FAU_STG.1), where they can be viewed and analyzed by an authorized audit administrator (FMT_SMR.1) using the PFSS (FAU_SAR.1, FAU_SAR.3). The analysis capabilities of PFSS, as described in the TOE summary specification, cover all of the security functional requirements in this area.

Loss of audit data is limited (FAU_STG.4). If TCP system log messaging is enabled, the maximum that can be lost in the event of failure is the number of logs generated as a result of last 50 packets. While this is not strictly quantifiable, the maximum length an audit queue can grow is limited to 8192 messages (2MB).

The **Protection Function** provides a separation of information streams traversing the TOE. The TOE is a dedicated firewall device, with no general purpose operating system, disk storage or programming interface. Interfaces are provided for administrators and for traffic using supported protocols. The administrative interface is protected by authentication and by physical controls, and by means of encryption when used remotely (FCS_COP.1). The protocol converters ensure traversing packets are treated as objects, and all processes running are trusted. No untrusted processes are permitted on the TOE (FPT_SEP.1). Before 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 (FPT_RVM.1).

The Identification and Authentication Function requires that administrators be identified (FIA_UID.2, FIA_ATD.1) and authenticated (FIA_UAU.5, FIA_ATD.1) before being granted access to any other TOE functions. Authentication failures are monitored, and accounts are locked if the predefined limit of failures is exceeded (FIA_AFL.1).

The function is controlled by authorized administrators (FMT_SMF.1 and FMT_SMR.1), who may modify administrator attributes (FMT_MTD.1(1)), and manage the number of permitted authentication attempts (FMT_MTD.2).

The claimed strength of function for the password mechanism is SOF-Medium. This is consistent with the overall claim for the TOE of SOF-Medium.

The **Clock Function** provides a reliable source of time and date information. This function permits authorized administrators (FMT_SMF.1, FMT_SMR.1) to set and change the time and date (FMT_MTD.1(2)). The Clock Function also provides the audit function with time stamps (FPT_STM.1).

Mutually Supportive IT Security Functions

The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (shown in TOE Security Functional Requirements (SFR) Rationale, page 57), because each of the IT functions can be mapped to one or more SFRs, as shown in Table 16.

Glossary

Table 17 lists the terms and acronyms used in this document.

Table 17 Terms and Acronyms

AAA	Authentication, Authorization, and Accounting
ARP	Address Resolution Protocol
CC	Common Criteria
CTIQBE	Computer Telephony Interface Quick Buffer Encoding
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
ESMTP	Extended Simple Mail Transfer Protocol
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GTP	GPRS Tunneling Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ILS	Internet Locator Service
IP	Internet Protocol
MGCP	Media Gateway Control Protocol

Table 17 Terms and Acronyms (continued)

POP3	Post Office Protocol 3
PP	Protection Profile
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RSH	Remote Shell
RTSP	Real Time Streaming Protocol
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
SIP	Session Initiation Protocol
Skinny (SCCP)	Skinny Client Control Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol
XDMCP	X Display Manager Control Protocol

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

This document is to be used in conjunction with the documents listed in the "Obtaining Documentation, Obtaining Support, and Security Guidelines" section.