Part Number: 00-0937467-B
Version Date: 5 March 2003

3Com Embedded Firewall
Version 1.5.1 Security Target

Secure Computing Corporation
2675 Long Lake Road
Saint Paul, Minnesota 55113

Prepared by:

Logica CLEF (LFL)
Logica UK Ltd.
Chaucer House
The Office Park
Springfield Drive
Leatherhead
Surrey KT22 7LP

Table Of Contents

Glossary of Terms

CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ISO	International Standards Organisation
IT	Information Technology
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

References

Standards and Criteria

CC	Common Criteria for Information Technology Security Evaluation (Comprising Parts 1-3: [CC1], [CC2], and [CC3])
CC1	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model CCIMB-99-031, Version 2.1, August 1999
CC2	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-99-032, Version 2.1, August 1999
CC3	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements CCIMB-99-033, Version 2.1, August 1999
CEM	Common Methodology for Information Technology Security Evaluation Part 2: Evaluation Methodology CEM-99/045, Version 1.0, August 1999

Source Documents

FIPS-46-3	Federal Information Processing Standard Publication (FIPS-PUB) 46-3, Data Encryption Standard (DES), October 1999.
FIPS-81	Federal Information Processing Standard Publication (FIPS-PUB) 81, DES Modes of Operation, December 1980.

1 Introduction

1.1 ST Identification

Title: 3Com® Embedded Firewall Version 1.5.1 Security Target.

Secure Computing Part Number: 00-0937467-B

Version of CC used for development: CC Version 2.1 (also known as ISO 15408).

1.2 Purpose

This document is the Security Target (ST) for 3Com® Corporation Embedded Firewall (EFW) Version 1.5.1.

The role of the security target within the development and evaluation process is described in the CC: the Common Criteria for Information Technology Security Evaluation [CC].

1.3 Security Target Overview

The 3Com® Embedded Firewall is a distributed firewall and access control security platform designed for the enterprise. EFW is software that applies security policy enforcement (packet filtering) capabilities to all traffic transmitted from and received by individual server and workstation (desktop or laptop) machines. Network interface cards (NICs) running EFW software (called EFW Devices) enforce policies in the EFW System. In particular, the TOE uses a NIC from the family of the 3Com NICs that support 3-DES encryption. Note that the EFW Policy Server automatically adjusts its level of encryption to match that of the devices it is managing.

EFW software provides transparent packet filtering in accordance with rules that are set up by an administrator. The rules are defined through a centralized Management Console, and are communicated to EFW Devices via the Policy Server. Figure 1 demonstrates security organization using EFW. EFW supports management of EFW devices that have a UDP connection available to the Policy Server, including remote devices for which UDP traffic is encrypted under a VPN between the EFW device and some computer (typically a VPN gateway) on the network on which the Policy Server resides.

EFW allows an administrator to specify policies for EFW Devices using the Management Console. A policy is a set of security criteria enforced by an EFW Device. A policy comprises various settings and an ordered list of rules, called an access control list (ACL), that determine what actions will take place and what events will be audited for any EFW Device associated with that policy. A rule consists of

various parameters that determine the characteristics for which incoming and outgoing packets will be screened, and specifies what action will be taken if a match occurs. EFW devices in a computer that roams between two locations can detect their location and load a different policy for each of these locations. The typical example is a laptop computer that may connect directly to the enterprise LAN, or may connect to the LAN via the enterprise VPN gateway when remote.

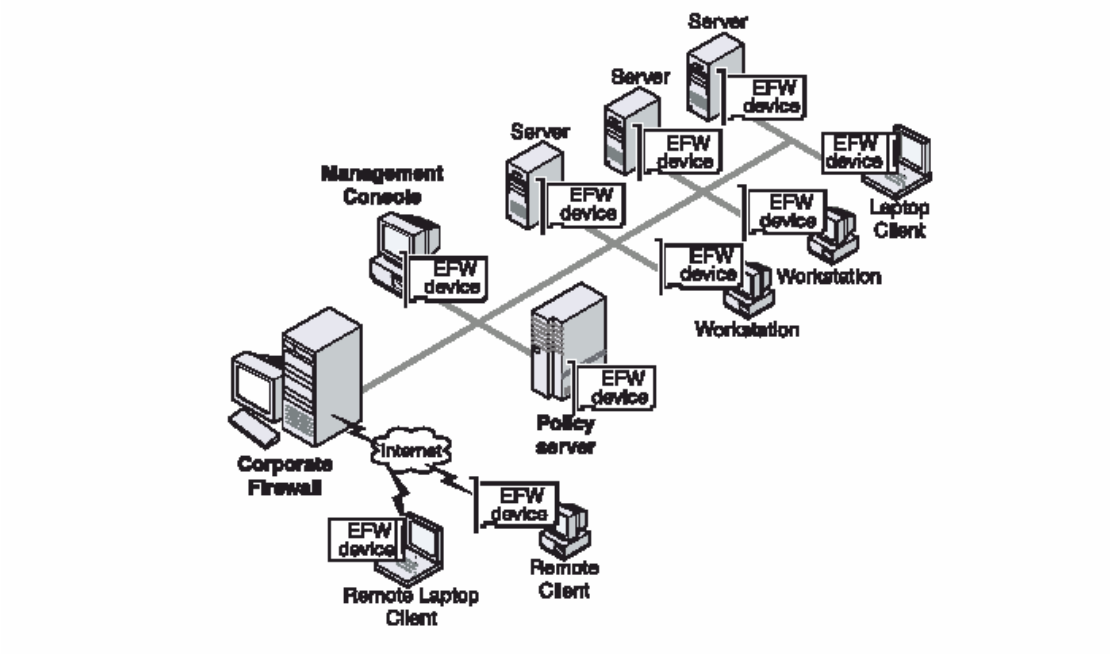

Figure 1 Security Organization using EFW

Although the EFW product supports desktop, server and laptop clients as pictured above, this evaluation is limited in scope to a configuration consisting of:

- **EFW laptop clients using a 3Com model 3CRFW102 or 3CRFW103 mobile card as an EFW device.**

- **Any 3DES 3Com desktop or server model card that supports EFW, used as an EFW device to protect the Policy Server host itself.**

1.4 CC Conformance Claim

The TOE is conforms to the CC as follows:

- CC Part 2 conformant
- CC Part 3 conformant
- EAL2 augmented
- Conformant to no PPs.

1.5 Document Structure

This ST is divided into 7 sections, as follows:

- Section 1 (this section) provides an introduction to the ST.
- Section 2 provides a description of the TOE.
- Section 3 provides the statement of TOE security environment, which defines the security problem the TOE is intended to meet.
- Section 4 provides the statement of security objectives, defining what is expected of the TOE and its environment, in order to address the security problem defined in Section 3.
- Section 5 provides the statement of IT security requirements, defining the functional and assurance requirements on the TOE (and its IT environment) that are needed to achieve the relevant security objectives defined in Section 4.
- Section 6 provides the TOE summary specification, which defines how the TOE meets the IT security requirements defined in Section 5.
- Section 7 provides the ST Rationale, which demonstrates that:
  - the security problem defined in Section 3 will be suitably addressed if the TOE and its environment meets the stated security objectives in Section 4;
  - the TOE and IT environment security objectives will be achieved if the TOE and IT environment satisfies the IT security requirements in Section 5;
  - the TOE security requirements will be met if it correctly implements the security functions and assurance measures defined in Section 6.

1.6 Amendment History

Date	New Version	Details of Change
30/7/02	1 draft A	All new
02/8/02	1 draft B	Including review comments.
04/9/02	1 draft C	Including resolution of OR.
13/11/02	1 Definitive	Including additional review comments and updates.
4 MAR 03	00-0937467-A	Revised cover sheet and identification information.
5 MAR 03	00-0937467-B	Updated for mobile only.

1.7 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

ACL: Access Control List.

aka: Also Known As.

Cryptographic module: A cryptographic module is that part of a system or application that provides cryptographic services such as encryption, authentication, or electronic signature generation and verification.

DBMS: Database Management System.

DES: Data Encryption Standard (see FIPS-46-3, FIPS-81).

3-DES: Triple DES Encryption.

DHCP: Dynamic Host Configuration Protocol.

DNS: Domain Name System.

EFW: Embedded FireWall.

EFW Agent: A supporting software agent that runs on a computer secured by an EFW policy providing addressing information.

EFW Device: A network interface card implementing EFW system policy.

EFW Domain: A collection of EFW Policy Servers that hold in common EFW related data notably the security policies and the audit data of the domain, and the EFW Devices which they serve.

EFW Management Console: The administrative interface to the Policy Server.

EFW Policy Server: A server administering, maintaining and controlling the policy and auditing for the set of EFW Devices in its domain.

ESP: Encapsulation Security Payload .

ICMP: Internet Control Message Protocol.

IP: Internet Protocol.

IPSEC: IP Security.

LAN: Local Area Network.

Local Administrators: Administrators of the Secured Computers who are not Network Administrators.

MD5: A message digest algorithm.

NAT: Network Address Translation.

Network Administrators: Administrators of the Policy Server. Those users able to administer and set the policy of the EFW system.

NIC: Network Interface Card.

PCI: Peripheral Component Interconnect – a self configuring PC local bus.

RSA: Rivest, Shamir and Adelman Public Key Cryptosystem.

Secured computer: A computer attached to the network by an EFW Device.

SHA-1: Secure hash algorithm.

TCP: Transmission Control Protocol.

UDP: User Datagram Protocol.

VPN: Virtual Private Network.

1.8 Trademark Notices

2 TOE Description

This part of the ST describes the TOE as an aid to the understanding of its security requirements, and addresses the product or system type. The scope and boundaries of the TOE are described in general terms both in a physical way (hardware and/or software components/modules) and a logical way (IT and security features offered by the TOE).

2.1 Intended Use

The 3Com Embedded Firewall (*EFW*) is a distributed firewall and access control security platform for the enterprise. EFW is software that applies security policy enforcement (packet filtering) capabilities to all traffic transmitted from and received by network interface cards (NICs) of individual server and workstation (desktop or laptop) machines. NICs running EFW software (called *EFW Devices*) enforce policies in the EFW System.

EFW software provides transparent packet filtering in accordance with rules that are set up by an administrator. The rules are defined through a centralized *Management Console*, and are communicated to EFW Devices by an *EFW Policy Server.*

EFW allows an administrator to specify policies for EFW Devices using the Management Console. A *policy* is a set of security criteria enforced by an EFW Device. A policy comprises various settings and an ordered list of rules, called an access control list (ACL), that determine what actions will take place and what events will be audited for any EFW Device associated with that policy. A *rule* consists of various parameters that determine the characteristics for which incoming and outgoing packets will be screened, and specifies what action will be taken if a match occurs.

A device may have one or two policies. It will have two policies if it roams between two locations, as in the case of a travelling laptop. There is one policy associated with each location.

2.1.1 Application Context

EFW consists of the following major architectural components:

- EFW Management Console
- EFW Policy Server(s)
- Audit Server
- Database Management System (DBMS)
- EFW Device(s)
- EFW Agent

Each of these components is shown in Figure 2 and discussed in the following subsections.

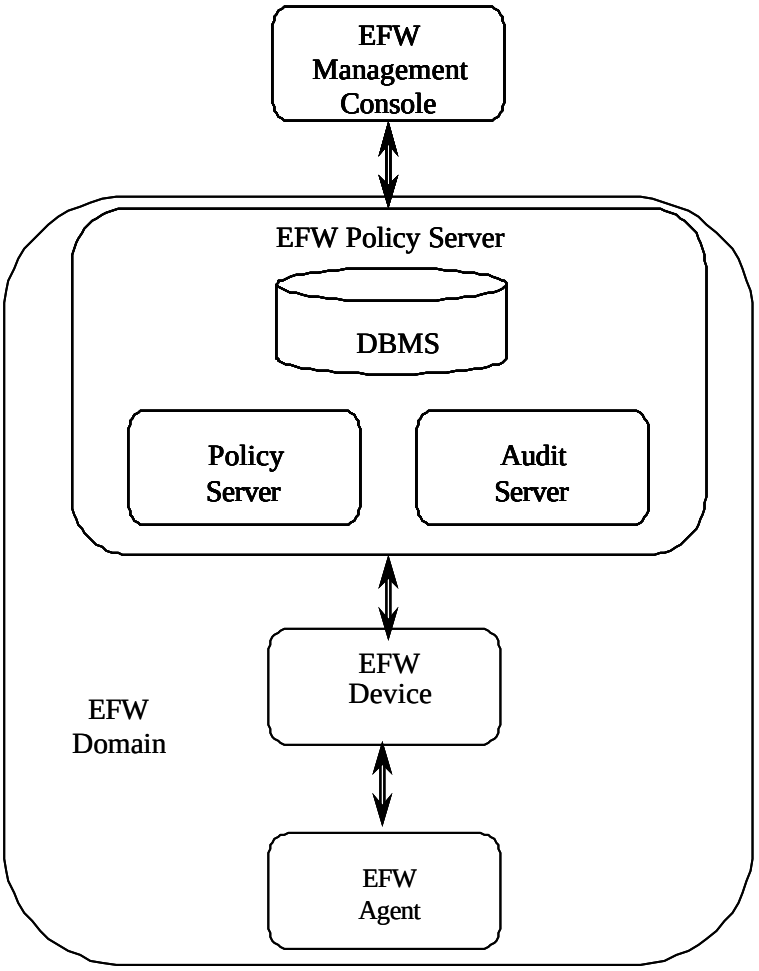

Figure 2 EFW Architectural Components

2.1.1.1 EFW Management Console

The EFW Management Console is the administrative interface to the Policy Server. Administrators configure the system and view data using the Management Console. The Management Console can be installed and run on the same machine as a Policy Server, or remotely on a different machine. The Management Console platform, and the EFW Policy Server platform, or both (if they are not co-located on the same platform) can be protected with an EFW Device.

More than one administrator may be connected to a Management Console in a single EFW Domain at the same time with read-only access. However, only one administrator in that Domain is allowed to have normal, that is full access to the administrative functions, at any one time. An EFW Domain can consist of as many as three Policy Servers and 3000 EFW Devices. A Management Console connected to any Policy Server in a domain has access to all EFW data for that domain. When a Management Console is active on any Policy Server within a domain, it can view or make changes to any EFW Device in that domain, regardless of whether that Policy Server is a primary or backup server for that EFW Device.

2.1.1.2 EFW Policy Servers

EFW Policy Servers control EFW Devices by implementing administrative actions received from the Management Console in the following ways:

- Accept the high-level commands issued from the Management Console and convert them into low-level packet filtering rules for the EFW Devices.
- Receive and process heartbeat messages from EFW Devices that contain updates on the IP addresses and resident policy version for the devices.
- Receive and process audit messages from the EFW Devices.
- Store EFW System data in a DBMS.

Each EFW Device must be assigned to a primary EFW Policy Server. A Policy Server can also specify a second Policy Server to act as a backup Policy Server if the primary server fails. If desired, a third Policy Server can also be specified in case neither the primary nor secondary servers are available or reachable.

The primary EFW Policy Server has initial responsibility for distributing policy updates to EFW Devices. Furthermore, each EFW Device caches the address of its primary Policy Server internally and contacts that Policy Server at EFW Device initialisation (for example, when the host containing an EFW Device is booted).

2.1.1.3 EFW Devices

EFW Devices filter incoming and outgoing packets based on the rules and policy settings for the specific policy they are enforcing. A policy is distributed to the EFW Devices by the Policy Servers.

Each EFW Device must be associated with a device set. A device set is a group of EFW Devices that are associated with a specific policy. Any number of device sets can be defined and EFW Devices can be assigned to any one of those device sets. An EFW Device can be placed in up to two device sets. If the device roams between two locations (called local and remote), it will have a local and a remote device set, associated with the device's local and remote policies, respectively.

A machine that is secured by an EFW Device (a Secured Computer) can be either a server or a workstation (desktop or laptop). A Secured Computer can have any number of EFW Devices, each using different policies (if desired), as long as each EFW Device has a different IP address.

A software agent, called the EFW Agent, also runs on the Secured Computer to support some of the embedded firewall operations. Figure 3 shows EFW Devices on both a workstation and server.

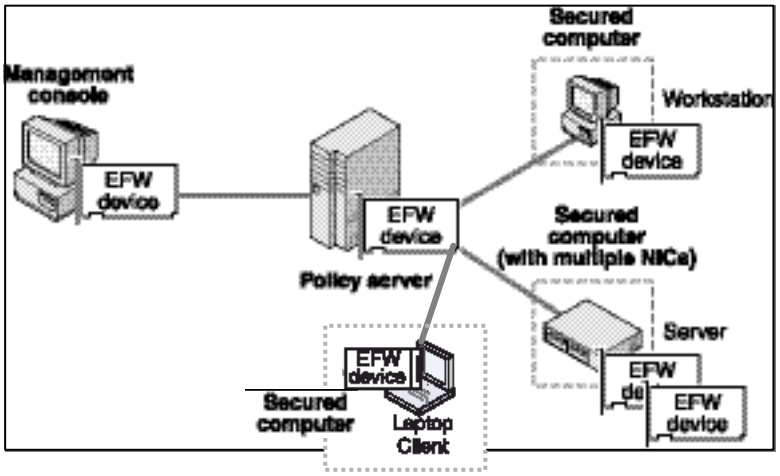

Figure 3 EFW Device Application

Although the EFW product supports desktop, server and laptop clients as pictured above, this evaluation is limited in scope to a configuration consisting of:

- **EFW laptop clients using a 3Com model 3CRFW102 or 3CRFW103 mobile card as an EFW device.**
- **Any 3DES 3Com desktop or server model card that supports EFW, used as an EFW device to protect the Policy Server host itself.**

2.2 Evaluated Configurations

The TOE configuration must conform to the following specification:

- The EFW TOE shall be installed and configured in accordance with the directives contained in the Installation, Generation and Startup (IGS) documentation.

- The configured EFW System shall support an EFW Policy Server platform protected with an EFW 3-DES Device and two Secured Computers (consisting of two laptops capable of running with Windows XP Professional on the first and Windows 2000 Professional on the second), each protected with an EFW 3-DES Device.

- The Windows XP laptop will have a network connection on the LAN on which the policy server resides. The Windows 2000 laptop shall be able to connect either directly to the LAN on which the Policy Server resides or connect to this LAN via a VPN. The Windows 2000 laptop will be equipped with an IPSEC VPN client to support the VPN connection.

- The roaming device in the laptop will be configured to detect its location using one of the two EFW "locator" criteria options "IP Address Mask – Policy Server verifies device's IP address" or "Non-VPN Connection to Policy Server." Under the first criterion the device is determined to be operating locally only if its IP address matches a specified address mask, and the Policy Server successfully verifies that the address is not being spoofed. In the second case the device is determined to be operating locally only if it has a connection to the Policy Server that is not tunnelled under a VPN.

- Physical access to the configured EFW Policy Server shall be controlled. After the configured EFW Policy Server is installed only Authorized Administrators shall be allowed physical access to it for such purposes as starting the system, managing the EFW TOE security functions, and doing complete backups or restores.

- The configured EFW Policy Server shall support administrative operations only through the direct-connected console of the EFW Policy Server.

Some functionality that is provided by an EFW System is disabled by the software set-up, and/or may be unsupported by the hardware configuration of the TOE and includes:

- EFW server or desktop workstation clients other than the policy server host itself, that use desktop, server or fiber model cards to support EFW.
- Remote instances of the EFW Management Console.
- Replicated EFW Policy Servers.
- Additional EFW "locator" options, used for automatically distinguishing remote vs. local operation: DHCP Server, DNS Server, Reachable Policy Server.
- Multiple NICs on Secured Computers.
- Management of NICs behind a NAT-configured router.
- NICs installed on systems running Windows 98 or Windows NT.
- 3Com NICs with similar hardware and firmware that can serve as a platform for EFW, but for which crypto support is limited to DES.

2.2.1 Physical Scope and Boundary

In general, EFW Policy Server software and EFW Agent software may run on a variety of computing platforms executing one of the Microsoft Windows operating systems (Windows 2000 Professional, Windows XP Professional, or Windows NT 4 – SP4 or higher), each with one card from the family of 3Com 3-DES network interface cards (NIC) installed and executing EFW firmware, and with other peripheral equipment. The systems are interconnected across an IP network through Ethernet connections. A secured computer may also connect via a VPN onto the network.

In actuality, the EFW TOE configuration consists of an EFW Policy Server system managing two Secured Computers, all of which incorporate EFW Devices to control the flow of IP traffic from the connected IP network to the Secured Computers. The EFW TOE uses the Embedded Firewall Software Version 1.5.1 (composed of the EFW Policy Server software, the EFW Agent software, and the EFW Device firmware).

Figure 4 depicts the EFW TOE configuration in the form of a simplified block diagram, and Table 1 provides a detailed description of the hardware platform requirements.

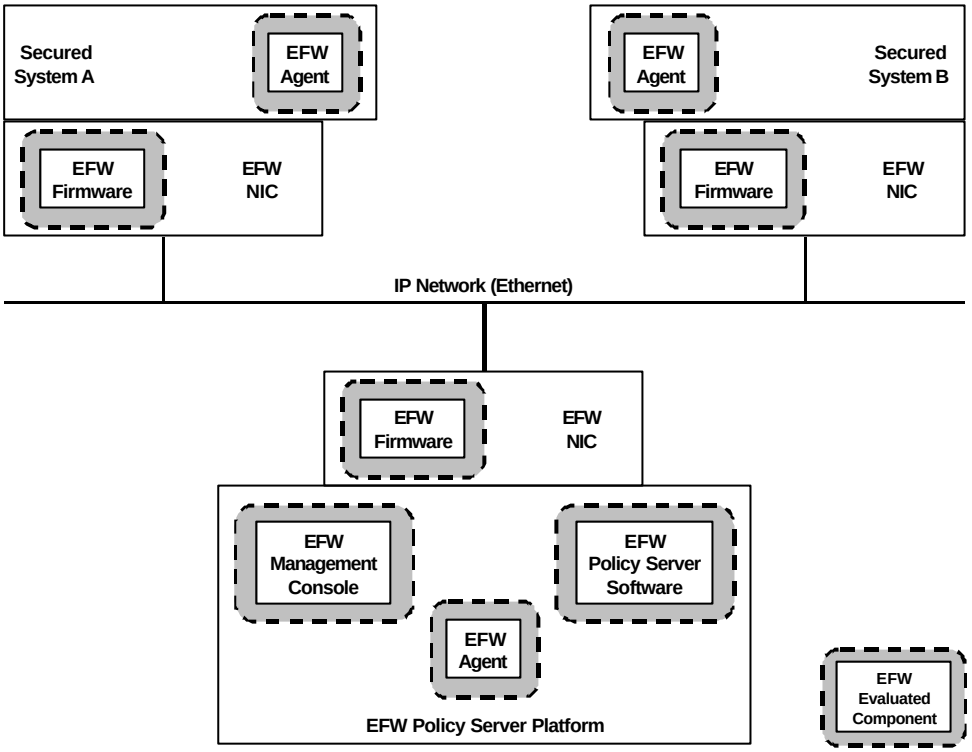

Figure 4 EFW Evaluated Components

Note: The TOE consists of the EFW Agent, the EFW Policy Server software and the EFW Firmware for the NICs. The other components, which include the operating systems and the hardware platforms of the Policy Server and Secured computers, and the NICs associated with these platforms, form part of the TOE environment.

Table 1 EFW TOE Platform Specifications

EFW Policy Server and Management Console Components [a]	**Specifications**
Operating system	Microsoft Windows 2000 Server
CPU	not less than 600 MHz Intel Pentium class or equivalent
RAM	not less than 128 MB [b]
Disk space	As dictated by the OS plus 150 MB [b] for EFW components.
Monitor/Video	256 colours or higher, screen area 800 x 600 or higher
Network Interface Card (NIC)	A server or desktop 3DES NIC in the 3CRFW or 3CR990 family.
EFW Device Host Component [a] **(Secured Computer) A (laptop)**	**Specifications**
Operating system	Microsoft Windows 2000 Professional
CPU	
RAM	not less than 16 MB
Disk space	As dictated by the OS plus 17 MB for EFW installation package.
Monitor/Video	As dictated by the OS
Network Interface Card (NIC)	A mobile model NIC in the 3CRFW family.
EFW Device Host Component [a] **(Secured Computer) B (laptop)**	**Specifications**
Operating system	Microsoft Windows XP Professional
CPU	
RAM	not less than 16 MB.
Disk space	As dictated by the OS plus 17 MB for EFW installation package.
Monitor/Video	As dictated by the OS.
Network Interface Card (NIC)	A mobile model NIC in the 3CRFW family.

[a] Installation of EFW components on Windows 2000 and Windows XP requires administrative privileges.

[b] Performance increases with additional memory and free hard drive space.

Additional information concerning key hardware components can be found in the *Embedded Firewall Administration Guide*. To the extent that this product information identifies specific components that have been tested, such components shall be used to construct the TOE.

2.3 Summary of IT and Security Features

The EFW TOE provides the following security features:

- Security Management
- Identification and Authentication
- User Data Protection
- Protection of Security Functions
- Audit

2.3.1 Security Management

2.3.1.1 EFW Management Console

The EFW Management Console is the administrative interface to the Policy Server. Administrators configure the system and view data using the Management Console. The Management Console can be installed and run on the same machine as a Policy server, or remotely on a different machine.

For the evaluated configuration of the EFW, the EFW Management Console will only be installed and run on the EFW Policy Server platform and the host machine will be protected with an EFW Device.

Remote management will be disabled by blocking any incoming console traffic at the EFW device of the Policy Server within the evaluated configuration. This configuration precludes multiple administrators interacting with the EFW management functions at one time.

2.3.1.2 Policy Dissemination

An Authorized Administrator may distribute new or changed policies at any time using the Management Console. If any Secured Computer is offline at the time of a policy distribution, it receives the new or updated policy the next time it boots up. EFW Devices periodically send heartbeats to the Policy Server. If policy distribution fails when a Secured Computer is online, the next heartbeat sent from the EFW Device to the Policy Server allows the Policy Server to determine that the Secured Computer needs a policy update, and the EFW Device receives the correct policy at that time.

2.3.2 Identification and Authentication

2.3.2.1 System Console

In the evaluated configuration, Authorized Administrators may only access EFW management functions through the direct-connected console of the EFW Policy Server.

No claims are being made for the host platform I&A functions.

2.3.2.2 Management Console I&A

Connection to the Policy Server requires a second login and password, which is valid for accessing any EFW management data in an EFW Domain. Administrator login names and passwords for the EFW System are managed under the Tools menu.

The EFW System is shipped with a built-in default login name and password, which shall be changed during system installation. To identify and authenticate Authorized Administrators, the EFW Policy Server gets the login name and password from the human user, determines its validity and enforces the result of the validity check. All I&A assurance claims for the human user of the EFW System are relative to this Security Function.

2.3.3 User Data Protection

2.3.3.1 Protected DBMS

The EFW Policy Server uses an underlying SQL database, called *MySQL*. Access to execute SQL commands for this database is protected by a password generated at installation time. In addition, access using a remote SQL client is prohibited. Direct user access to the EFW database via SQL is not necessary for EFW operations.

EFW data includes policy information, audit records that contain raw contents of packets, and the cryptographic keys used for communicating with the EFW devices. These packets may include login names and passwords that could be transmitted over the network.

2.3.3.2 Encrypted Communication

Communication is encrypted between EFW Devices and the Policy Server. For the purposes of 3-DES key resynchronisation, the Policy Server identifies itself to the EFW Devices using a public-private key pair generated upon creation of a new EFW Domain. The EFW installation procedures include a step to save this key pair to a diskette. The key pair data supports a method to recover control of EFW Devices in the event of a catastrophic loss of the Policy Server and data in a domain.

For communication between EFW Devices and the Policy Server, the system automatically determines the level of encryption used, based upon the encryption capability of the EFW Devices. For the evaluated configuration, all EFW Devices will be capable of 3-DES encryption. If EFW Devices are installed using the network installation method, they generate their own initial encryption keys and report them to the Policy Server. If installed with the diskette-keyed method, the initial key is generated by the Policy Server and distributed to the EFW Devices via a diskette. Both methods are included in the evaluation.

Mobile cards only support network installation. A diskette-keyed installation will be done for the card on the Policy Server host itself.

2.3.3.3 Information Flow Policy Enforcement

EFW Devices apply security policy enforcement (packet filtering) capabilities to all traffic transmitted from and received by individual machines. The EFW Policy Server distributes policies to the EFW Devices which then filter incoming and outgoing packets based on the rules and policy settings for the specific policy they are enforcing.

2.3.3.4 Policy Autoload

When an EFW Device is installed, it makes first contact with an EFW Policy Server upon boot-up of its host computer. The Policy Server automatically downloads the policy for that NIC. This policy is the one assigned to the default device set, unless the NIC has been registered manually in advance in another device set for a desktop or server NIC, or that of the relevant device set for a mobile NIC.

2.3.4 Protection of Security Functions

2.3.4.1 Policy Server Local EFW Device

For the evaluated configuration, the Policy Server host manages its own local EFW Device, installed directly on the Policy Server computer itself. The installation procedure for the local NIC is the same as any other EFW-Secured Computer. The EFW System provides a pre-defined policy for this NIC, which allows only traffic required for Policy Server operation. In particular, this policy prohibits remote access to the database. This policy is a second layer of defence beyond that provided by the database security mechanisms.

2.3.4.2 Encrypted Communication

Communication is encrypted between EFW Devices and the Policy Server and between the Management Console and the Policy Server. The Policy Server identifies itself to the Management Console and to the EFW Devices using public-private key pairs generated upon creation of a new EFW Domain. The installation procedure

and encrypted communications between the EFW Devices and the Policy Server are as described in section 2.4.3.2.

2.3.4.3 EFW Device self-protection

The EFW System is designed so that the EFW capability of the EFW Device cannot be disabled by any action from the Secured Computer hosting the NIC, or any action originating on the network except authorised Policy Server commands. The EFW capability on an EFW Device can only be "uninstalled" via the Management Console. Other than tampering with the physical hardware, there is no method for an end user to reconfigure the NIC to turn off or uninstall EFW. Attempts to do so may render the NIC inoperable. Uninstalling EFW using the standard Windows function removes only the EFW Agent software. To disable the EFW capability of an EFW Device, an Authorized Administrator must first remove the NIC from the EFW System via the EFW Management Console.

2.3.4.4 Fallback Mode

If a Secured Computer boots up and cannot contact any Policy Server in its domain, it enforces a policy called the *Fallback Mode*. The Fallback Mode is a setting that was specified within the policy being enforced on this computer before the reboot.

2.3.5 Audit

2.3.5.1 Audit Trail Generation and Storage

EFW Devices send audit messages to the EFW Policy Server. The events audited for an EFW Device are determined by the Device's policy. Also, the Policy Server itself generates audit messages for administrative actions. All audit messages are stored in the DBMS as audit records.

2.3.5.2 Audit Trail Review

An Authorized Administrator can query audit records directly or export them for analysis. The EFW System provides the capability for audit reporting via the EFW Management Console. A variety of custom reports can be generated. Selected audit data can be exported for processing by third-party tools.

2.3.5.3 Audit Trail Storage Management

Audit trail storage management is performed through the facilities of the EFW Policy Server platform.

3 TOE Security Environment

This part of the ST provides the statement of TOE security environment, which defines the security problem the TOE and its environment is intended to address.

To this end, the statement of TOE security environment identifies the assumptions made on the environment and the intended method of use of the TOE, defines the threats that the TOE is designed to counter, and the organisational security policies with which the TOE is designed to comply.

The EFW TOE is intended to be used in environments in which, at most, sensitive but unclassified information is processed, or where the sensitivity level of information in both the Secured Computer and the connected network is equivalent.

Identification of known or assumed threats to the assets requiring the EFW or its environments to provide specific protection further defines the EFW security environment. The assumptions and threat identification combined with any organization security policy statement or rules requiring EFW compliance completes the definition of the security environment. It is necessary that a comprehensive security policy be established for the site in which the product is operated and that it is enforced and adhered to by all users of the product. The security policy is expected to include measures for:

- Physical security - to restrict physical access to areas containing the Policy Server and associated equipment and protect physical resources, including media and hardcopy material, from unauthorized access, theft or deliberate damage.

- Procedural security - to control the use of the computer system, associated equipment, the product and information stored and processed by the product and the computer system, including use of the product's security features and physical handling of information.

- Personnel security - to limit a user's access to the Policy Server and to the computer system to those resources and information for which the user has a need-to-know and, as far as possible, to distribute security related responsibilities among different users.

3.1 Assumptions

This part of the security problem definition scopes the security problem by identifying what aspects of the TOE security environment are taken to be axiomatic.

3.1.1 Physical assumptions

These are assumptions about the physical location of the TOE.

A.PHYSEC **Physical Security:** The EFW Policy Server platform and its associated management console is only physically accessible to authorised administrators.

3.1.2 Personnel assumptions

These are assumptions made about individuals within the security environment of the TOE.

A.NOEVIL **Non-Hostile Administrators:** There are one or more individuals who are assigned to administer the TOE and its security. These authorised administrators are not careless, wilfully negligent nor hostile.

This assumption still allows the possibility that administrators are capable of human error leading to a compromise of the assets, which could, if needed, be mitigated by increasing the procedural measures within the TOE environment.

3.1.3 Connectivity assumptions

These are assumptions about the connection of the TOE to the network, or about its relationship with other software, firmware or hardware within the TOE environment.

A.NOBYPS **Controlled Network Connection:** Information cannot flow between a Secured Computer and the network except through the EFW Device.

The only connections between the secured computers and the network are via the EFW Devices.

3.1.4 Method of use assumptions

These are assumptions about the general way the TOE is to be used in terms of manner and/or purpose.

A.NOGENC **No General-Purpose Computing:** The Policy Server is used for no other purposes than those needed in the EFW system.

The Policy Server does not host public data, web applications or content, nor can it be used for some additional computing task.

A.NOREMO **No Remote Management:** The EFW System will only be administered via the dedicated management console of the EFW Policy Server platform.

The hardware and software configuration of the TOE will ensure that the EFW system may only be administered locally.

3.2 Threats

This part of the security problem definition identifies the assets requiring protection, the threat agents and the threats that may compromise the TOE.

3.2.1 Assets requiring protection

The primary IT assets to be protected are data and services available at the computers on the network including the Policy Server itself.

Secondary assets whose confidentiality and integrity must be protected consist of characteristics of the TOE important for the security of the system. These assets include:

- Cryptographic keys used by the security processes of the TOE;
- The software implementation upon which the security relies;
- The Policy Server data describing the flow control policy of the secured computers of the network.

3.2.2 Threat Agents

The threat agents can be categorised as:

- Users and local administrators of the computers on the network, with the exception of the network administrators of the Policy Server.

3.2.3 Statement of threats

This section identifies the threats to the assets that require protection.

T.APPLICATIONS A user or local administrator on a secured computer on the network may attempt to use applications on computers on the network for which they have no authorisation; conversely, a user or local administrator on a computer on the network may attempt to use applications on secured computers on the network for which they have no authorisation.

T.DATA A user or local administrator on a secured computer on the network may attempt to create, read, modify or destroy data on computers on the network for which they have no authorisation; conversely, a user or local administrator on a computer on the network may attempt to create, read, modify or destroy data on secured computers on the network for which they have no authorisation.

T.NETWORK A user or local administrator on a secured computer on the network may attempt to create or read information on the network for which they have no authorisation.

T.BYPASS A user or local administrator may attempt to bypass the information flow control policy enforced by the TOE.

That is users or local administrators may try to subvert the policy of the TOE by attacking the local components of the TOE, namely the EFW Agent and EFW Device located on a Secured computer.

T.COVERT A user or local administrator attacking the TOE or the assets it protects may seek to go undetected.

That is users or local administrators may seek to succeed by mounting an attack outside of normal hours or normal circumstances, or by some series of stealthy actions. The attacks envisaged are software attacks not attacks involving physical tampering with the TOE.

3.3 Organisational Security Policies

This part of the security problem definition refines the security problem by identifying organisational policy constraints relating to the protection of the assets identified in section 3.2.1.

The TOE and its environment is expected to comply with the following organisational security policies (OSPs).

P.CRYPTO Triple DES encryption must be used to encrypt security critical parameters transmitted on the network.

4 Security Objectives

This part of the ST defines the security objectives that the TOE and its environment must meet, in order to fully address the security problem defined in Section 3.

4.1 TOE Security Objectives

The TOE shall comply with the following security objectives.

O.ACCOUNT **Accountability:** The EFW System will provide system accountability for information flows through the EFW Device(s) and user accountability for Authorized Network Administrator use of security functions related to audit.

O.ADMSFA **Administrator Security Function Access:** The TOE will ensure that only Authorized Network Administrators are able to change the policy of the EFW Devices.

The EFW Devices uphold the network policy as defined by the authorised network administrators at the Policy Server and disseminated to these devices at the Secured computers. Only authorised network administrators have the capability to authenticate and thus change the policy maintained by these devices.

O.AUDREC **Audit Trail Recording:** The EFW Policy Server, in conjunction with the underlying operating system, will 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.

This security objective is included in both the objectives for the TOE and the objectives for the environment in accordance with [CC–Part 1;C.2.5].

O.EFWDEV **EFW Device Function:** The EFW Device(s) will be able to limit, amongst other things, the source/destination hosts and/or type of network traffic that can be utilized between the Secured Computer(s) and the connected network.

This security objective is refined in the Security Functional Requirements to clarify the manner in which control is exercised.

O.ENCRYPT **Encrypted Control Information:** The authenticity, confidentiality, and integrity of communications between the EFW Policy Server and the EFW Device(s) will be protected using encryption in accordance with the rules defined by P.CRYPTO.

O.IDAUTH **Identification and Authentication:** The EFW Policy Server will uniquely identify and authenticate the claimed identity of all users, before granting a user access to EFW security functions.

O.MEDIATE **Mediated Information Flow:** The EFW System will mediate the flow of all information between a Secured Computer and a connected network based on network layer information as configured by an Authorized Network Administrator.

O.SECSTART **Secure Start-Up:** Upon initial start-up of the EFW System or recovery from an interruption in EFW Policy Server service, the EFW Device(s) will not compromise its resources or those of any connected system(s).

O.SELFPRO **Self Protection:** The EFW System will protect itself against attempts to bypass, deactivate, or tamper with EFW security functions.

The EFW Devices enforcing the policy of the TOE are able to provide secure operation even when local software agents or the EFW Devices themselves are attacked.

4.2 Security Objectives for the Environment

The environment shall comply with the following security objectives.

OE.ADMDES **Designated Administrator:** At least one administrator will be designated with responsibility for management and configuration of the EFW System, including the management of the audit trail.

OE.ADMTRA **Trained Administrator:** Administrators will be trained to establish and maintain sound security policies and practices.

OE.AUDREC **Audit Trail Recording:** The EFW Policy Server, in conjunction with the underlying operating system, will 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.

This security objective is included in both the objectives for the TOE and the objectives for the environment in accordance with [CC-part 1,C.2.5].

OE.AUDREV **Audit Trail Review:** Procedures will exist to ensure that the audit trails are regularly analysed and that the audit trails archived by the firewall are not overwritten before they are inspected.

OE.CNFREV **Configuration Review:** The configuration of the EFW will be reviewed on a regular basis to ensure that the configuration continues to meet the organization's security objectives in the face of:

a) Changes to the configuration of the network protected by the EFW System;

b) Changes in the security policy;

c) Changes in the threats presented by the network;

d) Changes in the services made available by the Secured Computer(s).

OE.GUIDAN **Guidance is Followed:** The EFW System will be delivered, installed, administered, maintained, and operated in accordance with standard security practices and vendor-provided, evaluated documentation, and in a manner that maintains the security policy.

OE.KEYS **Keys Protected:** The Administrators of the TOE must ensure the continuing security of the Cryptographic keys used by the EFW system and kept on diskette, which must ensure only authentic keys are loaded to the EFW Devices.

OE.NOBYPS **Controlled Network Connection:** Secured Computers will be installed in a manner that provides no connection which allows the information flow between a Secured computer and the networks to physically bypass the EFW Device(s).

OE.NOGENC **No General-Purpose Computing:** The network administrators will ensure that the computing platform of the EFW Policy Server is used only for the purpose of the EFW system.

In particular, they will ensure that Policy Servers do not provide any general-purpose computing capabilities (i.e. the ability to execute arbitrary code or applications), storage repository capabilities, or host public data or applications (e.g. Web server or web content).

OE.NOREMO **No Remote Management:** The EFW System will only be able to be administered via the dedicated management console on the EFW Policy Server.

OE.PHYSEC **Physical Security:** The EFW Policy Server will be physically protected so that only Authorized Administrators have access to the platform and associated console.

For a detailed mapping from the security objectives for the environment listed in this section to the identified assumptions, threats, and organizational security policies, see Section 7.

5 Security Requirements

This part of the ST defines the security requirements that the TOE and its IT environment must meet in order to achieve the corresponding security objectives defined in Section 4. Requirements for the TOE are divided in to Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs). The CC requires that these be constructed, where possible, using security functional and assurance components defined, respectively, in [CC2] and [CC3].

This section also states the strength of TOE security function claims (SOF).

5.1 Security Functional Requirements

This section identifies the security functional requirements (SFRs) required of the TOE to meet its security objectives.

The components taken from [CC2] to specify the SFRs are listed in the table below together with an indication of whether the components are *iterated* (indicated by "(*N)" where N identifies the number of iterations) or *refined*.

Assignment and selection operations to be completed by the ST author are indicated using the same notation as used in [CC2]. Partially completed operations are denoted by *italicisation* of the word *assignment* or *selection* (as appropriate). Completed assignment and selection operations are indicated by *italicised text.* Refinements of components are indicated by **emboldened text**.

CLASS	FAMILY	COMPONENT	REFINED?
FAU	FAU_GEN	FAU_GEN.1	
	FAU_SAR	FAU_SAR.1	
	FAU_SAR	FAU_SAR.3	
FCO	FCO_NRO	FCO_NRO.2	
FDP	FDP_IFC	FDP_IFC.1	
	FDP_IFF	FDP_IFF.1	
FIA	FIA_UAU	FIA_UAU.2	
	FIA_UID	FIA_UID.2(1)	
	FIA_UID	FIA_UID.2(2)	
FMT	FMT_MOF	FMT_MOF.1	
	FMT_MSA	FMT_MSA.1	
	FMT_MSA	FMT_MSA.3	
	FMT_SMR	FMT_SMR.1	

CLASS	FAMILY	COMPONENT	REFINED?
FPT	FPT_AMT	FPT_AMT.1	Y
	FPT_FLS	FPT_FLS.1	
	FPT_ITT	FPT_ITT.1	Y
	FPT_RCV	FPT_RCV.2	Y
	FPT_RVM	FPT_RVM.1	
	FPT_SEP	FPT_SEP.1	
	FPT_TST	FPT_TST.1	

5.1.1 FAU - Security Audit

5.1.1.1 FAU_GEN.1 Audit data generation

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

a) Start-up and shutdown of the audit functions;

b) *Information flows through EFW Devices; and*

c) The administrator use of security functions related to the audit function.

Application Note: An audit level of *not specified* has been selected, and the resulting second paragraph removed for readability.

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; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the audit record will include audit event id number, the identity of the device, the identity of the Policy Server, the identity of the Network Administrator, the identity of the device set, the policy name, the policy version number, the rule number, the source address, the destination address, the IP protocol in use, the source port, the destination port, the TCP Flags, ICMP type where relevant.*

5.1.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide *authorised network administrators* with the capability to read *audit information* from the audit records.

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

5.1.1.3 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform *sorting* of audit data based on *relevant attributes*.

5.1.2 FCO - Communication

5.1.2.1 FCO_NRO.2 Enforced proof of origin

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted *communications between the EFW Policy Server and any EFW Device* at all times.

FCO_NRO.2.2 The TSF shall be able to relate *the EFW Policy Server identity or EFW Device identity* of the originator of the information, and *the Message Authentication Code* of the information to which the evidence applies.

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to *the receiving EFW Policy Server or EFW Device* given *the limitations of the encryption method used as given in P.CRYPTO*.

Application Note: The authentication of origin depends on identifying the parties involved. This requirement depends on FIA_UID.2(2).

5.1.3 FDP – User data protection

5.1.3.1 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the *EFW Policy Server information flow control SFP on EFW Devices, network information, and EFW Device operations* that cause network information to flow to and from Secured computers covered by the SFP.

5.1.3.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the *EFW Policy Server information flow control SFP* based on the following types of subject and information security attributes:

a) source and destination computers;

b) the protocols that may be used;

c) source and destination ports;

d) whether a TCP packet initiates a connection;

e) whether to match incoming packets, outgoing packets or both;

f) whether sniffing or spoofing is allowed;

g) whether fragmented IP packets are allowed;

h) whether non-IP packets are allowed;

i) whether IP packets containing IP options are allowed;

j) the identifier of the mediating EFW Device;

k) The location (local or remote) where the EFW device is operating.

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

a) The transmission of a network packet from a secured computer within the EFW system via one of its EFW Devices to another computer on the network is permitted by the rules enforced by Policy Server information flow control SFP.

b) The reception of a network packet at a secured computer within the EFW system via one of its EFW Devices from another computer on the network is permitted by the rules enforced by EFW Policy Server information flow control SFP.

c) The reception of a “request for wakeup” packet at a secured computer is always permitted.

FDP_IFF.1.3 The TSF shall enforce *no additional information flow control SFP rules.*

Application Note: The SFR has been refined by deletion of the word ‘the’ for clarity.

FDP_IFF.1.4 The TSF shall provide *no additional SFP capabilities.*

Application Note: The SFR has been refined by the deletion of the words 'the following' for clarity.

FDP_IFF.1.5 The TSF shall explicitly authorise 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: *none.*

5.1.4 FIA – Authentication and identification

5.1.4.1 FIA_UID.2 User identification before any action

FIA_UID.2.1(1) The TSF shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

FIA_UID.2.1(2) The TSF shall require each **Policy Server and EFW Device** to identify itself before allowing any other TSF mediated actions on behalf of that **Policy Server or EFW Device**.

Application Note: The Policy Server and EFW Device are required to initialise the shared key used for the MAC within the Device/Server communication function.

5.1.4.2 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 FMT – Security Management

5.1.5.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the behaviour of the EFW System security functions* to *the authorised network administrators*.

Application Note: The words "the functions" before the assignment have been removed for greater fluency.

5.1.5.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the *EFW Policy Server information flow control SFP* to restrict the ability to *change the security attributes defining the policy of the EFW Policy Server* to *authorised network administrators.*

5.1.5.3 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the *EFW Policy Server information flow control SFP* to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *authorised network administrators* to specify alternative initial values to override the default values when an object or information is created.

5.1.5.4 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: *authorised network administrator*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.6 FPT – Protection of the TOE

5.1.6.1 FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 The TSF shall run a suite of **heartbeat** tests periodically during normal operation to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.6.2 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

a) Deletion of a EFW Agent on a Secured computer;

b) Loss of communications from an EFW Device on a Secured computer;

c) Loss of communications from the EFW Policy Server.

5.1.6.3 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure and modification* when it is transmitted between separate parts of the TOE **using encryption in accordance with the rules of P.CRYPTO.**

Application Note: The separate parts of the TOE are composed of the Policy server, the Management console, the EFW device(s) and the EFW Agents.

5.1.6.4 FPT_RCV.2 Automated recovery

FPT_RCV.2.1 When automated recovery from a failure or service discontinuity **of a Secured computer** is not possible, the TSF shall enter a **secure** maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2 For *initial start-up and other service discontinuities of a Secured computer*, the TSF shall ensure the return of the TOE **from a secure Fallback Mode** to a **fully functioning** secure state using automated procedures.

5.1.6.5 FPT_RVM.1 Non-bypassability of the TSP

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

5.1.6.6 FPT_SEP.1 TSF domain separation

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

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

5.1.6.7 FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests *resulting from a periodic EFW Device heartbeat* to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.2 Security Assurance Requirements

The target evaluation assurance level for the product is EAL2 augmented (see [CC3] for a definition of EAL2) with the following assurance components:

ALC_FLR.1 – Basic Flaw Remediation.

5.3 Strength of Function Claims

The SOF claim is *SOF-Basic.*

The strength of cryptographic algorithms is outside the scope of the CC, and hence the assessment of algorithmic strength will not form part of the TOE evaluation. The evaluation will however confirm the correct implementation of the specified cryptographic algorithms which (in accordance with P.CRYPTO) are considered to have the appropriate strength for the intended use.

5.4 Security Requirements for the IT Environment

The IT environment is required to meet the objectives described in section 4.2.

The confidentiality and integrity of the Policy Server software and EFW data including the SQL database (holding the rules for the required information flow control policy software, the audit records collected by the system and the keys used to communicate with and rekey the devices) needs to be protected from unauthorised users. (In this circumstance, unauthorised users include those administrators lacking authorisation for the administration of the network.) To achieve this, the TOE relies on ensuring that only authorised administrators have access to the platform and console.

Audit records are communicated to the Policy Server where they are stored in files which upon reaching a certain size are archived as zip files by the product. The network administrators are responsible for monitoring the growth of the audit archive and managing manual back-up and deletion.

However, the audit system of the TOE does rely on the underlying operating system to provide both accurate dates and times for accounting records, and the relevant security functional requirement is given in the following table.

CLASS	FAMILY	COMPONENT	REFINED?
FPT	FPT_STM	FPT_STM.1	

5.4.1.1 FPT_STM.1 Reliable time stamps

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

Application Note: It is assumed that the time is inclusive of a date (which might, for example, be time after epoch).

6 TOE Summary Specification

This section defines the IT Security Functions (SFs) and assurance measures that meet the TOE SFRs and SARs defined in Section 5.

6.1 IT Security Functions

The IT security functions to which the claimed strength of function (SOF) applies are: IT_IA.1, IT_CO.1, IT_CO.2 and IT_MST.2.

6.1.1 Audit

IT_AUD.1 The Embedded Firewall shall be able to generate an audit record for the following events:

- Start-up and shutdown of the audit functions; and
- Information flows through the EFW Devices of the Secured computers on the network; and
- The administrator's use of security functions related to audit.

IT_AUD.2 Audit records shall record at least the following information:

a) Date and time of the event, the type of the event, the subject and whether the event was a success or failure.

b) For the three types of audit events, namely the application of a rule at an EFW Device, policy-related, or network administrator initiated events, relevant parameters from the following: the audit event id number, the identity of the device, the identity of the Policy Server, the identity of the network administrator, the identity of the device set, the policy name, the policy version number, the rule number, the source address, the destination address, the IP protocol in use, the source port, the destination port, the TCP Flags, ICMP type.

IT_AUD.3 The TOE shall include:

a) Facilities to examine the audit files in a suitable manner; and

b) Facilities that allow the sorting of the audit data based on relevant attributes.

6.1.2 Encrypted Communications

IT_CO.1 The TOE shall require the Policy Server and an EFW Device to identify themselves before allowing any other security related actions on behalf of the Policy Server or EFW Device.

IT_CO.2 The TOE shall ensure the authenticity, confidentiality and integrity of the TSF data by encrypting such communications between the Policy Server and EFW Devices via the proprietary protocol modelled on the Encapsulation Security Payload using SHA-1, RSA and 3-DES.

6.1.3 Information Flow Control

IT_IF.1 The TOE shall enforce the information flow control policy of the Policy Server to control the packet flow between the Secured Computers and the rest of the network.

IT_IF.2 The TOE shall provide a means to control the packet flow between the Secured computers and other computers on the network.

See Section 5.1.3.2. FDP_IFF.1, for detail.

IT_IF.3 The TOE shall enforce permissive default values for packet flows between Secured computers and the rest of the network, unless overridden by alternative values set by the network administrator.

6.1.4 Identification and Authentication

IT_IA.1 An EFW Policy Server shall require users to identify and successfully authenticate themselves using a user name and password before gaining access to the administrative services of the EFW Policy Server.

6.1.5 Administration of Rights

IT_AR.1 Only an authorised network administrator of the TOE shall be able:

a) Create new network administration user accounts on the Policy server;

b) Change the policy of the EFW Devices of the Secured computers;

c) Change the audit parameters of the associated audit function of the flow policy.

6.1.6 Maintenance of Secure Operation

IT_MST.1 The TOE shall provide the means for the EFW Devices of the Secured computers to periodically communicate to their Policy Server, to ensure the EFW Devices update and enforce any changes to their flow policy.

IT_MST.2 The TOE shall provide authorised network administrators a means to verify the integrity of the TSF data and executable code.

IT_MST.3 The TOE shall enforce a secure fall back policy (selected at the Policy Server by a network administrator) at start-up and following minor service discontinuities at a Secured computer until its EFW Devices are able to communicate with the Policy Server and establish the current policy for the Devices.

IT_MST.4 The TOE shall enforce a secure maintenance mode at the EFW Device of a Secured computer, blocking all flows to and from the effected EFW device, following a severe service discontinuity where automated recovery is not possible.

IT_MST.5 The TOE shall ensure continued secure operation, in the event of:

a) Deletion of the EFW Agent associated with the Device;

b) A Failure to communicate with the Policy Server following re-boot.

c) Loss of communications with its Policy Server.

6.1.7 Enforcement

IT_EF.1 The TOE shall validate all actions between subjects and objects that require security enforcement before allowing the action to proceed.

IT_EF.2 The TOE shall maintain a security domain for it own trusted execution comprising the Policy Server and the EFW Devices. This shall be kept separate from untrusted subjects which operate in a separate security domain.

6.2 Required security mechanisms

IT_CO.1, IT_CO.2 and **IT_MST.2** use the following cryptographic algorithms: 3-DES, SHA-1, MD5 and RSA. The assessment of the algorithmic strength of any of these algorithms does not form part of the evaluation.

IT_IA.1 uses a proprietary password mechanism. The construction of passwords is sufficient to meet the requirements of a strength of function of SOF-basic.

6.3 Assurance Measures

Assurance measures will be adopted to address each of the EAL2 assurance requirements as summarised in Table B.1 in [CC, Part 3] with an additional assurance measure for ALC_FLR - flaw remediation, and as summarised below.

Assurance Requirement	Assurance Measure
ACM_CAP.2	Configuration Management documentation will be provided
ADO_DEL.1	Delivery procedures will be provided
ADO_IGS.1	Installation, generation and start-up procedures will be provided by the administration guide augmented with the Common Criteria evaluated configuration guide.
ADV_FSP.1	A functional specification will be provided
ADV_HLD.1	High-level design documentation will be provided
ADV_RCR.1	Representation correspondence will be evident in the relevant TSF representations
AGD_ADM.1	Administrator guidance documentation will be provided
AGD_USR.1	No user guidance documentation will be provided as the product is transparent to the user.
ALC_FLR.1	Flaw remediation documentation will be provided
ATE_COV.1	A test coverage analysis will be provided
ATE_FUN.1	Test documentation will be provided
ATE_IND.2	No specific assurance measure, although access will be provided to the TOE in its evaluated configuration for evaluator testing
AVA_SOF.1	A SOF analysis will be provided
AVA_VLA.1	A developer vulnerability analysis will be provided. Access will also be provided to the TOE in its evaluated configuration for penetration testing

7 ST Rationale

This section provides the rationale for the choice of security objectives, security requirements, and IT security functions and assurance measures, demonstrating that they are necessary and sufficient to meet the security problem as defined in Section 3. This comprises the following parts:

- the security objectives rationale, demonstrating that the security problem defined in Section 3 will be suitably addressed if the TOE and its environment that meets the stated security objectives in Section 4;
- the security requirements rationale, demonstrating that the TOE and IT environment security objectives will be achieved if the TOE and IT environment satisfies the IT security requirements in Section 5;
- the TOE summary specification rationale the TOE security requirements will be met if it correctly implements the security functions and assurance measures defined in Section 6.

7.1 Security Objectives Rationale

This section demonstrates how the threats, organisational security policies and assumptions are met by the security objectives. The correlation between the security needs and objectives is given in table 2 below.

Table 2 - Correlation between Security Needs and Objectives

Objectives:	O.ACCOUNT	O.ADMSFA	O.AUDREC	O.EFWDEV	O.ENCRYPT	O.IDAUTH	O.MEDIATE	O.SECSTART	O.SELFPRO	OE.ADMDES	OE.ADMTRA	OE.AUDREC	OE.AUDREV	OE.CNFREV	OE.GUIDAN	OE.KEYS	OE.NOBYPS	OE.NOGENC	OE.NOREMO	OE.PHYSEC
Threats																				
T.APPLICATIONS		x		x		x	x		x					x			x	x	x	x
T.BYPASS					x			x	x								x			
T.COVERT	x		x		x					x	x	x	x		x					
T.DATA		x		x		x	x		x					x			x	x	x	x
T.NETWORK		x		x	x		x		x					x		x	x			
Policies																				
P.CRYPTO					x															
Assumptions																				
A.NOBYPS																	x			
A.NOEVIL										x	x									
A.NOGENC																		x		
A.NOREMO																			x	
A.PHYSEC																				x

7.1.1 Suitability to counter the threats

The following rationale demonstrates how the objectives counter the threats:

T.APPLICATIONS A user or local administrator on a secured computer on the network may attempt to use applications on computers on the network for which they have no authorisation; conversely, a user or local administrator on a computer on the network may attempt to use applications on secured computers on the network for which they have no authorisation.

This threat is countered on the network by O.MEDIATE and O.EFWDEV which limits users and local administrators access across the network to those other computers and their applications to those that are permitted.

This is supported by OE.NOBYPS and O.SELFPRO which ensure that the TOE is able to enforce the information flow policy and that it is not circumvented, either by physical bypass or by attacks on the EFW devices. OE.CNFREV also supports by ensuring the policy of the TOE adequately reflects the perceived threats to the resources protected by the TOE. O.ADMSFA ensures that the local policy of the EFW Devices reflects the policy as defined by the network administrators.

The threat, in the guise of a local attack on the Policy Server, is countered by OE.PHYSEC and OE.NOREMO which permits only authorised network administrators access to the associated console from which the TOE may only be administered. O.IDAUTH helps to counter the threat by ensuring only authorised administrators may logon to the administrative functions of the Policy Server.

These previous objectives are further supported by OE.NOGENC which prohibits the computing platform of the Policy Server of the TOE being used to support applications that might harbour vulnerabilities which could, in turn, support an indirect attack allowing the use of applications of the Secured computers supported by the TOE (e.g. vulnerabilities in web browsers).

T.DATA A user or local administrator on a secured computer on the network may attempt to create, read, modify or destroy data on computers on the network for which they have no authorisation; conversely, a user or local administrator on a computer on the network may attempt to create, read, modify or destroy data on secured computers on the network for which they have no authorisation.

This threat is countered in a similar manner to T.APPLICATIONS as the actions of creating, reading, modifying or destroying data is mediated by processes, that is applications. The argument is re-iterated here because of some slight changes in focus.

This threat is countered on the network by O.MEDIATE and O.EFWDEV which limits users and local administrators access across the network to those other computers and their applications (that may create read or destroy data) to those that are permitted.

This is supported by OE.NOBYPS and O.SELFPRO which ensure that the TOE is able to enforce the information flow policy and that it is not circumvented, either by physical bypass or by attacks on the EFW devices. OE.CNFREV also supports by ensuring the policy of the TOE adequately reflects the perceived threats to the resources protected by the TOE. O.ADMSFA ensures that the local policy of the EFW Devices reflects the policy as defined by the network administrators.

The threat, in the guise of a local attack on the Policy Server, is countered by OE.PHYSEC and OE.NOREMO which permits only authorised network administrators access to the associated console from which the TOE may only be administered. O.IDAUTH helps to counter the threat by ensuring only authorised administrators may logon to the administrative functions of the Policy Server.

These previous objectives are further supported by OE.NOGENC which prohibits the computing platform of the Policy Server of the TOE being used to support applications that might harbour vulnerabilities which could, in turn, support an indirect attack to the data security needs of the Secured computers supported by the TOE (e.g. vulnerabilities in web browsers).

T.NETWORK A user or local administrator on a secured computer on the network may attempt to create or read information on the network for which they have no authorisation.

This threat is countered by O.MEDIATE and O.EFWDEV which can prevent unauthorised reading or unauthorised masquerading within packets on the network, and by O.ENCRYPT which ensures that security critical information for the administration and audit of the network may not be readily decrypted except by those intended.

This is supported by OE.NOBYPS and O.SELFPRO which ensure that the TOE is able to enforce the information flow policy and that it is not circumvented, either by physical bypass or by attacks on the EFW devices. OE.CNFREV also supports by ensuring the policy of the TOE adequately reflects the perceived threats to the resources protected by the TOE. O.ADMSFA ensures that the local policy of the EFW Devices reflects the policy as defined by the network administrators.

O.ENCRYPT is supported by OE.KEYS which ensures that encrypted information continues to be only readily decrypted by those intended.

T.BYPASS A user or local administrator may attempt to bypass the information flow control policy enforced by the TOE.

This threat is mainly countered by O.SELFPRO which ensures that attacks against the local components of the trusted security functions, namely the EFW Device and the EFW Agent, cannot compromise the TOE.

OE.NOBYPS ensures that the EFW devices that enforce the information flow at the Secured computers may not be physically bypassed.

O.SECSTART ensures, that neither at the initial start-up or following attacks that lead to forced recoveries of the system, these events cannot be used to compromise the information flow control policy.

O.ENCRYPT ensures that the authenticity of the communications of between the Policy Server and the EFW Devices prohibiting users or local administrators trying to masquerade as either a Policy Server or another Secured computer.

T.COVERT A user or local administrator attacking the TOE or the assets it protects may seek to go undetected.

This threat is countered by O.ACCOUNT and O.AUDREC (a.k.a. OE.AUDREC) which provides the records and the means to record and to search security related events, so that suitably trained network administrators arising from OE.ADMTRA and OE.ADMDES, may counter a sequence of actions that might lead to a security compromise by timely interventions supported by OE.AUDREV.

OE.GUIDAN ensures that, in particular, the auditing of the TOE has been installed, configured and maintained so as to uphold the security of the TOE.

O.ENCRYPT ensure the confidentiality and integrity of the accounting records as they are transmitted to the Policy Server to compose the audit log.

7.1.2 Suitability to meet the OSPs

The following rationale demonstrates how the objectives achieve the OSPs:

P.CRYPTO Triple DES encryption must be used to encrypt security critical parameters transmitted on the network.

O.ENCRYPT ensures the TOE supports cryptographic functions securely, and in accordance with P.CRYPTO.

7.1.3 Suitability to uphold the assumptions

The following rationale demonstrates how the objectives cover the assumptions:

A.PHYSEC **Physical Security:** The EFW Policy Server platform and its associated management console is only physically accessible to authorised administrators.

OE.PHYSEC upholds this assumption.

A.NOEVIL **Non-Hostile Administrators:** There are one or more individuals who are assigned to administer the TOE and its security. These authorised administrators are not careless, wilfully negligent nor hostile.

OE.ADMDES together with OE.ADMTRA upholds this assumption.

A.NOBYPS **Controlled Network Connection:** Information cannot flow between a Secured Computer and the network except through the EFW Device.

OE.NOBYPS upholds this assumption.

A.NOGENC **No General-Purpose Computing:** The Policy Server is used for no other purposes than those needed in the EFW system.

OE.NOGENC upholds this assumption.

A.NOREMO **No Remote Management:** The EFW System will only be administered via the dedicated management console of the EFW Policy Server platform.

OE.NOREMO upholds this assumption.

7.2 Security Requirements Rationale

7.2.1 Suitability to achieve the security objectives

This section provides the correlation and justification of suitability between the objectives and the Security Functional Requirements. Iteration numbers of components are given where appropriate – if an iteration number is not given than all those iterations of the component help to achieve the security objective.

OBJECTIVE to be met by TOE	Security Functional Requirement COMPONENT
O.ACCOUNT	Audit data generation FAU_GEN.1
O.ADMSFA	User identification before any action FIA_UID.2(1) Management of security functions behaviour FMT_MOF.1 Security roles FMT_SMR.1
O.AUDREC	Audit review FAU_SAR.1 Selectable audit review FAU_SAR.3
O.EFWDEV	Subset information flow control FDP_IFC.1 Simple security attributes FDP_IFF.1

OBJECTIVE to be met by TOE	Security Functional Requirement COMPONENT
O.ENCRYPT	Enforced proof of origin FCO_NRO.2 Basic internal TSF data transfer protection FPT_ITT.1 User identification before any action FIA_UID.2(2)
O.IDAUTH	User authentication before any action FIA_UAU.2 User identification before any action FIA_UID.2(1)
O.MEDIATE	Subset information flow control FDP_IFC.1 Simple security attributes FDP_IFF.1 Management of security attributes FMT_MSA.1 Static attribute initialisation FMT_MSA.3
O.SECSTART	Automated recovery FPT_RCV.2
O.SELFPRO	Abstract machine testing FPT_AMT.1 Failure with preservation of secure state FPT_FLS.1 Non-bypassability of the TSP FPT_RVM.1 TSF domain separation FPT_SEP.1 TSF testing FPT_TST.1

O.ACCOUNT **Accountability:** The EFW System will provide system accountability for information flows through the EFW Device(s) and user accountability for Authorized Network Administrator use of security functions related to audit.

FAU_GEN.1 ensures that accounting records are produced for information flows through EFW Devices and the administrators use of audit functions.

O.ADMSFA **Administrator Security Function Access:** The TOE will ensure that only Authorized Network Administrators are able to change the policy of the EFW Devices.

The EFW Devices uphold the network policy as defined by the authorised network administrators at the Policy Server and disseminated to these devices at the Secured computers. Only authorised network administrators have the capability to authenticate and thus change the policy maintained by these devices.

FIA_UID.2(1) ensures that users identify themselves before performing any other security related actions.

FMT_MOF.1 ensures that only authorised network administrators may modify the behaviour of the EFW System security functions, in particular those that ensure the local policy of the EFW Devices.

FMT_SMR.1 ensures that the role of authorised network administrator exists and that the TOE is able to associate users with roles.

O.AUDREC **Audit Trail Recording:** The EFW Policy Server, in conjunction with the underlying operating system, will 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.

FAU_SAR.1 ensures that the TOE provides audit records in a suitable manner for the user to interpret, and that authorised network administrators have the capability to read such records.

FAU_SAR.3 ensures that the audit log can perform sorting of the audit data based on relevant attributes.

The rationale for OE.AUDREC (later in this section) which is an identical objective for the environment handles the environmental aspects.

O.EFWDEV **EFW Device Function:** The EFW Device(s) will be able to limit, amongst other things, the source/destination hosts and/or type of network traffic that can be utilized between the Secured Computer(s) and the connected network.

FDP_IFC.1 ensures that there is an information flow policy between the Secured computers and the network.

FDP_IFF.1 ensures that the policy enforced by this named policy mediates the flow by assigning rules that control the flow and the type of network traffic between hosts and the Secured computers, thus restricting the utilisation of these hosts and type of network traffic.

O.ENCRYPT **Encrypted Control Information:** The authenticity, confidentiality, and integrity of communications between the EFW Policy Server and the EFW Device(s) will be protected using encryption in accordance with the rules defined by P.CRYPTO.

FCO_NRO.2 ensures that the authenticity of the communications between the EFW Policy Server and the EFW device(s) is enforced and that the identity of the originator can be verified and is in accordance with the rules defined by P.CRYPTO.

FPT_ITT.1 ensures that the confidentiality and integrity of communications (which comprise transmissions of TSF data) between the EFW Policy Server and the EFW device(s) is protected using encryption again in accordance with the rules define by P.CRYPTO.

FIA_UID.2(2) ensures that identities of the Policy Server and EFW device(s) are established before any communications takes place, thus ensuring authentication is always possible.

O.IDAUTH **Identification and Authentication:** The EFW Policy Server will uniquely identify and authenticate the claimed identity of all users, before granting a user access to EFW security functions.

FIA_UAU.2 and FIA_UID.2(1) ensure that users are successfully identified and authenticated before any actions may take place.

O.MEDIATE **Mediated Information Flow:** The EFW System will mediate the flow of all information between a Secured Computer and a connected network based on network layer information as configured by an Authorized Network Administrator.

FDP_IFC.1 ensures the TOE enforces the EFW Policy Server Information flow control policy between the Secured computers and the network.

FDP_IFF.1 ensures that the policy enforced is based on rules that control the transmission and reception of network packets.

FMT_MSA.1 and FMT_MSA.3 ensures that only authorised network administrators may change the security attributes and their default values which define the EFW Policy Server Information flow control policy.

O.SECSTART **Secure Start-Up:** Upon initial start-up of the EFW System or recovery from an interruption in EFW Policy Server service, the EFW Device(s) will not compromise its resources or those of any connected system(s).

FPT_RCV.2 ensures that the upon initial start-up, or following either service discontinuities that may be automatically fixed or not, the TOE remains in a secure state.

O.SELFPRO **Self Protection:** The EFW System will protect itself against attempts to bypass, deactivate, or tamper with EFW security functions.

FPT_AMT.1 ensures that the TOE checks in periodic manner that it is operating in a secure manner.

FPT_FLS.1 ensures that attacks on the EFW Agent leading to its deletion, or loss of communications from EFW devices to the Policy Server or vice-versa loss of communications from the EFW Policy Server to the EFW Devices do not compromise the security of the TOE.

FPT_RVM.1 ensures that the enforcement functions are invoked and succeed before performing other security related functions.

FPT_SEP.1 ensures that that the TOE keep the security domains for its trusted and untrusted subjects separate, thus protecting untrusted subjects interfering with or gaining information from the trusted subjects of the TOE.

FPT_TST.1 ensures that the administrators can check the integrity of the code and data of the TOE, and moreover that the TOE checks its own correct operation in a periodic manner.

OBJECTIVE to be met by IT environment	Security Functional Requirement COMPONENT
OE.AUDREC	Reliable time stamps FPT_STM.1

OE.AUDREC **Audit Trail Recording:** The EFW Policy Server, in conjunction with the underlying operating system, will 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.

FPT_STM.1 ensures that the underlying operating system is able to provide the EFW Policy Server with reliable time stamps for stamping audit records. The other elements of this objective are provided by TOE.

The rationale for O.AUDREC (earlier in this section) which is an identical objective for the TOE handles the aspects provided by the TOE.

7.2.2 Dependency analysis

The following table gives the dependencies between the SFRs.

	FAU_GEN.1	FAU_SAR.1	FDP_IFC.1	FDP_IFF.1	FIA_UID.2(1)	FIA_UID.2(2)	FMT_MSA.1	FMT_MSA.3	FMT_SMR.1	FPT_AMT.1	FPT_TST.1	FPT_STM.1
FAU_GEN.1												x
FAU_SAR.1	x											i
FAU_SAR.3	i	x										i
FCO_NRO.2						x						
FDP_IFC.1			i	x	i		i	i	i			
FDP_IFF.1			x		i		i	x	i			
FIA_UAU.2					x							
FIA_UID.2(1)												
FIA_UID.2(2)												
FMT_MOF.1					i				x			
FMT_MSA.1			x	i	i		i	i	x			
FMT_MSA.3			i	i	i		x	i	x			
FMT_SMR.1					x							
FPT_AMT.1												
FPT_FLS.1												
FPT_ITT.1												
FPT_RCV.2										i	x	
FPT_RVM.1												
FPT_SEP.1												
FPT_TST.1										x		

Table 3: Dependency matrix for the SFRs

Key x – direct dependencies
i – indirect dependencies

Note: The dependencies of FPT_FLS.1 and FPT_RCV.2 on ADV_SPM.1, is met by the security target as a whole which functions as an informal model. The dependence of FPT_RCV.2 on AGD_ADM.1 is met by the specification of EAL2 augmented as the assurance requirement. The dependences of FIA_UAU.2, FMT_SMR.1 and FCO_NRO.2 on FIA_UID.1 are satisfied by instances of FIA_UID.2 which is hierarchic to it. The additional assurance requirement ALC_FLR.1 introduces no additional dependencies. FCO_NRO.2 places certain requirements on the accounting events, for example, at a minimal level the use of non-repudiation should accountable. The dependency of FAU_GEN.1 on FPT_STM.1 is satisfied by the IT environment.

7.2.3 Mutual support

The Embedded Firewall is a counter-measure to the unauthorised use of the resources of one networked computer by another network computer in a manner contrary to stated information flow policy.

FDP_IFC.1 and FDP_IFF.1 ensure that the information flow policy of the network and associated Secured Computers is enforced.

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3 and FMT_SMR.1 ensure that the policy, in terms of setting the modifiable functionality and attributes that define the policy and its audit, may only be modified at the server by authorised network administrators.

FIA_UID.2(1) and FIA_UAU.2 ensure that the access to modifying the policy of the information flow and audit is reserved to properly identified and authenticated network administrators.

FIA_UID.2(2), FCO_NRO.2 and FPT_ITT.1 ensure that the Policy Server and the EFW Devices are identified within the system and that communications between them are authenticated, confidential and true.

FPT_RCV.2 and FPT_FLS.1 ensure that the TOE remains secure when subject to various service failures.

FAU_GEN.1, FAU_SAR.1 and FAU_SAR.3 aid the detection of misconfiguration of the TOE by network administrators, and series of events that may lead to a compromise of the TOE by other users, by producing accounting and audit records and the means to review them.

Finally, FPT_AMT.1, FPT_TST.1, FPT_RVM.1 and FPT.SEP.1 ensure the TOE is not bypassed and that its policy is current, by ensuring the regular testing and update of the policy and that the trusted functions of the TOE are neither bypassed nor performed in an insecure domain.

7.3 TOE Summary Specification Rationale

7.3.1 Suitability of the IT Security Functions

The following table shows how the Security Functional requirements of section 5 are correlated to the informal security functions of section 6.

Security Functional Requirement	Security Function
Audit data generation FAU_GEN.1	IT_AUD.1; IT_AUD.2
Audit review FAU_SAR.1	IT_AUD.3
Selectable audit review FAU_SAR.3	IT_AUD.3 paragraph (b)
Enforced proof of origin FCO_NRO.2	IT_CO.2
Subset information flow control FDP_IFC.1	IT_IF.1
Simple security attributes FDP_IFF.1	IT_IF.2
User identification before any action FIA_UID.2(1)	IT_IA.1
User identification before any action FIA_UID.2(2)	IT_CO.1
User authentication before any action FIA_UAU.2	IT_IA.1
Management of security functions behaviour FMT_MOF.1	IT_AR.1
Management of security attributes FMT_MSA.1	IT_AR.1
Static attribute initialisation FMT_MSA.3	IT_IF.3
Security roles FMT_SMR.1	IT_AR.1
Abstract machine testing FPT_AMT.1	IT_MST.1
Failure with preservation of secure state FPT_FLS.1	IT_MST.5
Basic internal TSF data transfer protection FPT_ITT.1	IT_CO.2

Security Functional Requirement	Security Function
Automated recovery FPT_RCV.2	IT_MST.3; IT_MST.4
Non-bypassability of the TSP FPT_RVM.1	IT_EF.1
TSF domain separation FPT_SEP.1 TSF	IT_EF.2
TSF testing FPT_TST.1	IT_MST.1; IT_MST.2

7.3.2 Suitability of the Assurance Measures

Section 6.3 demonstrates that, for each SAR, there is an appropriate assurance measure.