GeNUScreen 1.0

Security Target

Version 431

11 Jun 2007

GeNUA mbH

Domagkstr. 7, D-85551 Kirchheim, Germany

Table of Contents

1 ST Introduction

The introductory section presents the unique identifiers for the security target (ST) and the Target of Evaluation (TOE). A brief overview of the ST and the standards conformance claim follow.

1.1 ST Identification

ST Title:	**GeNUScreen 1.0** Security Target, Version 431
TOE Identification:	**GeNUScreen 1.0**
Product Identification:	**GeNUScreen 1.0 Z**
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.3
Assurance Level:	**EAL4**, augmented by **ALC_FLR.2**
Keywords:	Packet filter, Network security, Information flow control, Virtual Private Network, Encrypting Gateway

Table 1: Identification

1.2 ST Overview

1.2.1 Introduction

Readers are assumed to be familiar with the concept of firewalls, encryption, authentication and evaluation terms, as well as TCP/IP networking concepts.

1.2.2 Overview

The TOE GeNUScreen 1.0 makes VPN and firewall functionality available and easy to manage. It protects networks at the border to the Internet by filtering incoming and outgoing data traffic. It protects the data flowing between several protected networks against unauthorised inspection and modification. It consists of software on a number (at least 2) of machines (**GeNUScreen Appliances**) that work as network filters, hereafter called Firewall components, and another machine to manage this network of Firewall components. This machine, the Management Server (**GeNUCenter Management System**), is a central component. The Firewall components are initialised on a secure network from the Management Server.

After initialization, the Firewall components can be distributed to the locations of the networks they are protecting.

The GeNUScreen 1.0 Firewall components filter incoming and outgoing traffic for multiple

networks and can thus enforce a given security policy on the data flow. The filter is implemented in the kernel of the Firewalls components' operating system, OpenBSD. The Firewall components can work as bridges or routers.

At the same time the Firewall components can provide confidentiality and integrity for data traffic passing between the networks. This Virtual Private Network function is achieved by IPsec encryption and authentication mechanisms using up-to-date ciphers and key sizes. The IPsec transforms are implemented in the kernel. The key agreement for IPsec follows the ISAKMP Internet standard [RFC2409], and is implemented in user space outside the TOE by OpenBSD's `isakmpd`.

The Management Server component provides Administrators with a Graphical User Interface (GUI) to initialize and manage the Firewall components from a central server. The Management Server also allows to collect audit data and monitoring.

1.3 CC Conformance

The TOE is Part 2 extended and Part 3 conformant to the CC Version 2.3

[CC_1]: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 2.3, 2005.

[CC_2]: Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 2.3, 2005.

[CC_3]: Common criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.3, 2005.

1.4 Notational Conventions

Throughout this document, CC operations on security requirements as defined

in paragraph 6.4.1.3.2 of Part 1 of the CC are marked as follows:

- Selections are denoted by [***bold italicised text in square brackets***].
- Assignments are denoted in [**bold text in square brackets**].
- Refinements are denoted in **bold text** or ~~crossed-out~~.
- Iterations are denoted by affixing annotational text in parentheses to the component name.

2 TOE Description

The TOE consists of

1. several Firewall components that work as network filters and encrypting gateways,
2. a central Management Server that is used to configure, administrate and monitor the Firewall components.

The Management Server allows authorised administrators to configure filter rules and protection policies on the Firewall components by use of a web-based graphical user interface (GUI) at the Management Server. It also enables authorised administrators to update the software on the Firewall components. The GUI must be used from a trusted machine connected to the Management Server through a trusted network.

After installation, all communication between the Management Server and the Firewall components is protected by Secure Shell (SSH) transforms against eavesdropping and modification.

The Firewalls components employ IPsec encryption and authentication to protect data flows between the subnets assigned to them by the authorised administrators.

Management consists of definition/modification and transmission of firewall policies and security policies for network traffic. The GUI also allows transfer of audit data from the Firewall components.
The TOE components must be configured correctly so that the security features can work reliably later. It is required that the initial configuration follows a special procedure.

2.1 Secure Initialization

To guarantee that all Firewall components are set up correctly and know each other's and the Management Server's public keys, the following procedure is required:

1. A secure network is set up with only the Management Server and the Firewall components on it.
2. The management server must be installed from CD. During installation, public/private key pairs are generated which are used later to identify and authorize the Administrator.
3. The Administrator initializes his/her account with a non-guessable password.
4. The Administrator uses the GUI to create configurations for all the Firewall components. The configuration includes the creation of public/private key pairs for the Firewall components for later authentication by the Internet Key Exchange (IKE) and Secure Shell (SSH) protocols.
5. The Firewall components are installed by PXE boot from the Management Server. Among other things, the process installs on each Firewall component
    1. the authorised administrator's public key
    2. the individual Firewall component's public/private key pair
    3. all the public keys of all the Firewall components with which the individual Firewall component is configured to communicate directly.

2.2 TOE Physical scope

The GeNUScreen TOE consists of two classes of components, the Management Server and the Firewall components.

The operating system in both cases is OpenBSD. The IPsec transforms and the packet filter are part of the TOE. All other parts of the operating system are considered to be part of the TOE environment.

2.2.1 Management Server Physical Scope

The Management Server consists of an administrative GUI running on OpenBSD. The hardware is an Intel i386 compatible machine with at least the following configuration:

- 256 MB of RAM
- 20 GB of hard disk
- two 100Mbit Ethernet Interface Controllers
- CD drive

The hardware must be compatible with the OpenBSD operating system.

The physical connections are:

- network interfaces to the Internet and to the secure network where the authorised administrator's machine is connected
- connections for keyboard, monitor
- power supply

The Management Server communicates with the Firewall components by Internet. The information flowing between Management Server and Firewall components is protected by Secure Shell (SSH) cryptographic transforms, SSH is part of the OpenBSD operating system but not of the TOE.

2.2.2 Firewall component Physical Scope

Firewall components are embedded communication appliances with each at least the following components:

- an Intel i386 compatible CPU
- three 100Mbit Ethernet Interface Controllers
- a serial console interface (RS232)
- at least 32 MB of RAM
- at least 64 MB of persistent memory (Compact Flash or hard disk)

The hardware must be compatible with the OpenBSD operating system.

If configured to do so, the Firewall components communicate with each other using the IPsec protocol suite. The actual encryption and authentication of datagrams is performed by the IPsec implementation in the kernel, which is part of the TOE. The key agreement and algorithm negotiation as specified in the IKE RFCs [RFC2409] and [RFC3526] is done by programs included in OpenBSD, which are not part of the TOE.

The physical connections are:

- network interfaces for external and internal networks
- connections for a serial console
- power supply

2.3 TOE Logical Scope

2.3.1 Audit

The Firewall components collect audit data which can be collected, stored, displayed, sorted and searched at the Management Server. Auditable events are attempts to violate a policy. This allows the authorised administrator to inspect the current state of all Firewall components.

2.3.2 Information Flow Protection

There are two information flow policies enforced by the TOE.

Each Firewall component will only forward data from and to the protected networks if the firewall information flow policy allows it.

Data flowing between the networks protected by different Firewall components is encrypted and authenticated if the IPsec information flow policy requires it (the authorised administrator may choose not to protect flows).

2.3.3 Security Management

Authorised administrators can modify security policies at the Management Server and transfer them to the Firewall components.

2.3.4 Authentication and Identification

There is only one role in the TOE which can be incorporated by a human user, i.e. the authorised administrator. Authorised administrators must identify to the Management Server with a user name and must authenticate successfully by password before they can perform any security function.

2.3.5 Modules

The GeNUScreen product consists of several modules, part of which are implemented in the kernel whereas others are implemented in user space. The table 2 illustrates this and shows which modules are part of the GeNUScreen TOE.

	Environment	***TOE***
User Space	Internet Key Exchange SSH transforms	Graphical User Interface Audit mechanisms
Kernel		IPsec transforms Packet filter

Table 2: TOE and environment

2.4 TOE Scope of Delivery

The Scope of Delivery consists of

- Management Server installation CD: **GeNUScreen Version 1.0 Z**
- Management Server hardware (Models: **200**, **400**, **600**, or **800**)
- Two or more Firewall components' hardware (Models: **100C**, **300S**, **500S**, **200**, **400**, **600**, or **800**)
- Administration documentation [DOC]

3 TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.

Those parts of the OpenBSD operating systems which are not part of the TOE are part of the environment.

3.1 Users and Assets

The following users and assets will be used in the description of the threats and policies.

	Users
User	Any person or software agent sending IP packets to or receiving from the components of the TOE. This includes users on the protected networks behind the Firewall components as well as all users outside those networks. Their assumed attack potential is **low**. It must be noted however, that the TOE Firewall components are exposed to unrestricted attackers, simply because they are exposed to the Internet. The product aims to protect against more capable attackers.
Authorised administrator	These are authenticated users at the Management Server that have the role of an administrator. This role authorises them to change the Firewall component's and the Management Server's configuration on the Management Server.
IPsec Key Exchange (IKE) Daemon	The processes running on the Firewall components that are responsible for the initiation of IPsec connections. They can be distinguished by their public keys. The attack potential of the persons that administrate the IKE daemon is undefined.

Table 3: Users

	Assets
Resources in the connected networks	The resources in the connected networks that the TOE components are supposed to protect. These are outside the TOE components.

	Assets
Security sensitive data on the TOE	The data on the TOE components that contains security sensitive information.
Information flow between the connected networks	The potentially sensitive data passing between the connected networks. This data resides outside the TOE components.
Information flow between Management and Firewall components	The configuration data transmitted from the Management Server to the Firewall components and the audit data from the Firewall components to the Server. This data passes inside the TOE components.

Table 4: Assets

3.2 Assumptions

This section lists the assumptions that are to be met by the environment of the GeNUScreen TOE in order for the TOE to be considered secure.

	Assumptions
A.PHYSEC	Each component of the TOE is physically secure. Only authorised administrators have physical access to the TOE. This must hold for the Management Server and the Firewall components.
A.INIT	The TOE was initialised according to the procedure described in the documentation [DOC] (summarised in section 2.1).
A.NOEVIL	Authorised administrators are non-hostile and follow all administrator guidance; however, they are capable of error. They use passwords that are not easily guessable.
A.SINGEN	Information can not flow between the internal and external network, unless it passes through the TOE.
A.NOADDSERV	The Management Server is exclusively configured to manage the Firewall components. No incoming traffic from untrusted networks is allowed to the HTTP service on the Management Server.
A.NOFWSERV	The Firewall components are configured to accept no incoming connections except SSH-protected data from the Management Server, IPsec Key agreement protocol connections and IPsec connections initiated by IPsec Key agreement from other Firewall components of the TOE.
A.TIMESTMP	The environment provides reliable timestamps.
A.ADMIN	Authorised Administrators using the GUI on the Management Server work in a trusted network directly connected to the Server.

Table 5: Assumptions

3.3 Threats

	Threats
T.NOAUTH	A user might attempt to bypass the security functions of the TOE to gain unauthenticated access to resources in the protected networks.
T.SNIFF	A user outside the TOE might gain access to the sensitive data passing between the protected networks. Attack method is packet inspection of Internet traffic.

	Threats
T.SELPRO	A user from inside or outside the networks protected by the TOE components might gain access to the TOE and read, modify or destroy security sensitive data on the TOE, by sending IP packets to the TOE and exploiting a weakness of the protocol used.
T.MEDIAT	A user might send non-permissible data from outside the protected networks through the TOE that result in gaining access to resources in protected networks which is not allowed by the policy. The attack method is construction of IP packets to circumvent filters.
T.MSNIFF	A user outside the TOE might gain access to the configuration or audit data passing between the Management Server and a Firewall component. Attack method is packet inspection of Internet traffic.
T.MODIFY	A user outside the TOE might modify the sensitive data passing between the protected networks. Attack method is packet interception and modification of Internet traffic.
T.MMODIFY	A user outside the TOE might modify the configuration or audit data passing between the Management Server and a Firewall component. Attack method is packet interception and modification of Internet traffic.

Table 6: Threats

3.4 Organizational Security Policies

No organizational security policies are enforced by the TOE.

4 Security Objectives

The purpose of the security objectives is to describe the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment. The CC identifies two categories of security objectives:

- security objectives for the TOE
- security objectives for the operating environment

4.1 Security Objectives for the TOE

This section defines the security objectives for the GeNUScreen TOE. Security objectives counter the identified threats.

	Objectives
O.AUTH	The TOE must assure that only authorised users can initiate connections in the VPN and between Management Server and Firewall components. The only such users are the IKE daemons and the authorised Administrator.
O.MEDIAT	The TOE must mediate the flow of all data between all connected networks.
O.CONFID	The TOE must assure that data transferred between the networks protected by Firewall components is kept confidential unless explicitly configured otherwise.
O.INTEG	The TOE must assure that data transferred between the networks protected by Firewall components cannot be modified unnoticed.
O.NOREPLAY	The TOE must assure that data transferred between the networks behind the Firewall components cannot be reinjected at a later time.
O.AUDREC	The TOE must provide an audit trail of security-related events, and a means to present a readable and searchable view to authorised users.

Table 7: Objectives

4.2 Security Objectives for the Environment

	Objectives for the environment
OE.PHYSEC	Those responsible for the TOE must assure that the Management Server and the Firewall components are placed at a secured place where only authorised people have access.
OE.INIT	Those responsible for the TOE must ensure that the initial configuration is performed according to [DOC]. A summary of the procedure is given in section 2.1.
OE.NOEVIL	Those responsible for the TOE must assure that all authorised administrators are competent, regularly trained and execute the administration in a responsible way. The administrators must choose passwords which cannot be guessed easily.
OE.SINGEN	Those responsible for the TOE must assure that the Firewall components provide the only connection for the different networks.
OE.NOADDSERV	The Management Server must be exclusively configured to manage the Firewall components. No incoming traffic from untrusted networks must be allowed to the administrative GUI on the Management Server.
OE.NOFWSERV	The Firewall components must be configured to accept no incoming connections except SSH-protected data from the Management Server, IPsec Key agreement protocol connections from other Firewall components of the TOE and IPsec connections initiated by IPsec Key agreement.
OE.TIMESTMP	The IT environment must supply reliable timestamps for the TOE.
OE.ADMIN	The authorised administrators must use the GUI on the Management Server only from a trusted network directly connected to the Server.
OE.CRYPTO	The IT environment must supply SSH authorization and SSH transport protection as defined in [RFC4253]. The IT environment must supply Internet key agreement and the necessary algorithms as defined in [RFC2409], [PKCS #1, v2.0], [RFC2104], [RFC3526], [RFC3602], [FIPS-180-2] and [FIPS-197].

Table 8: Objectives for the environment

5 IT Security Requirements

This section lists the principal Security Functional Requirements claimed by the TOE. Most are derived from requirements in [CC_2]. In the statement of the requirements, the abbreviation in parentheses defines the specific iteration of the associated Part 2 requirement. Explicitly stated requirements carry the label 'EX'. Their exact definition can be found in the Appendix.

5.1 TOE Security Functional Requirements

The listing of SFRs represents the groups of information flow and access control Security Function Policies (SFPs) of the TOE. These are:

1. FW-SFP regulating the flow of network traffic through Firewall components.
2. IPSEC-SFP ensuring that connections between the individual Firewall components are protected by IPsec.

5.1.1 FW-SFP

This section lists the SFRs necessary for the Firewall components to enforce Firewall Security Policies defined by the authorised Administrator.

The FW-SFP is concerned with the creation, modification, deletion and application of firewall security policy rules. It also provides protection against unauthorised access to the platform running the Firewall component.

5.1.1.1 FDP_IFC.1 (FW) Subset information flow control

FDP_IFC.1.1 (FW)

The TSF shall enforce the [**FW-SFP**] on [**:**

- **subjects: entities that send and/or receive data through the TOE to one another;**
- **information: the data sent from one subject through the TOE to another;**
- **operation: pass the data**].

5.1.1.2 FDP_IFF.1 (FW) Simple security attributes

FDP_IFF.1.1 (FW)

The TSF shall enforce the [**FW-SFP**] based on the following types of subject and information security attributes: [

1. **subject security attributes: none**
2. **information security attributes:**
    - **address of source subject;**
    - **address of destination subject;**
    - **transport layer protocol;**
    - **interface on which traffic arrives and departs;**

- **service**].

FDP_IFF.1.2 (FW)

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

1. **Subjects on a network connected to the TOE can cause information to flow through the TOE to a subject on another connected network only if all the information security attribute values are permitted by all information flow policy rules**].

FDP_IFF.1.3 (FW)

The TSF shall enforce the [**reassembly of fragmented IP datagrams before inspection**].

FDP_IFF.1.4 (FW)

The TSF shall provide the following [**: the capability to modify parts of the TCP/IP headers to make the connections less vulnerable against hijacking attacks**].

FDP_IFF.1.5 (FW)

The TSF shall explicitly authorise an information flow based on the following rules: [**none**]

FDP_IFF.1.6 (FW)

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

1. **The TOE shall reject requests of access or services where the information arrives on a network interface and the source address of the requesting subject does not belong to the network associated with the interface (spoofed packets);**
2. **The TOE shall drop IP datagrams with the source routing option;**
3. **The TOE shall reject fragmented IP datagrams which cannot be re-assembled completely within a bounded interval**].

5.1.1.3 FMT_SMF.1 (FW) Specification of Management Functions

FMT_SMF.1.1 (FW)

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

Creation and modification of network traffic filter rules.

The rules filter for the following attributes of datagrams:

- **address of source subject;**
- **address of destination subject;**
- **transport layer protocol;**
- **interfaces on which traffic arrives and departs;**
- **service**].

5.1.1.4 FMT_MSA.3 (FW) Static attribute initialization

FMT_MSA.3.1 (FW)

The TSF shall enforce the [**FW-SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (FW)

The TSF shall allow ~~the~~ [**nobody**] to specify alternative initial values to override the default values when an object or information is created.

5.1.2 IPSEC-SFP

This section identifies the SFRs associated with the flow control functions in relation to the VPN connections between the Firewall components. The IPSEC-SFP is the policy that models this aspect of information flow control.

5.1.2.1 FDP_ITT.1 (IPSEC) Basic internal transfer protection

FDP_ITT.1.1 (IPSEC)

The TSF shall enforce the [**IPSEC-SFP**] to prevent the [***disclosure* and *modification***] of user data when it is transmitted between physically-separated parts of the TOE.

5.1.2.2 FDP_IFC.1 (IPSEC) Subset information flow control

FDP_IFC.1.1 (IPSEC)

The TSF shall enforce the [**IPSEC-SFP**] on [**:**

1. **subjects: Firewall components;**
2. **information: the data sent from one subject to another;**
3. **operation: pass the data**].

5.1.2.3 FCS_COP.1 (IPSEC-AES) Cryptographic operation

FCS_COP.1.1 (IPSEC-AES)

The TSF shall perform [**data encryption**] in accordance with a specified cryptographic algorithm [**AES in CBC mode**] and cryptographic key sizes [**128 bit**] that meet the following: [**[FIPS-197]**].

5.1.2.4 FCS_COP.1 (IPSEC-HMAC) Cryptographic operation

FCS_COP.1.1 (IPSEC-HMAC)

The TSF shall perform [**message authentication**] in accordance with a specified cryptographic algorithm [**HMAC-SHA**] and cryptographic key sizes [**160 bit**] that meet the following: [**[RFC2104] and [FIPS-180-2]**].

Application note: [RFC2104] also defines a mechanism for replay protection, which is implied in the specification of the HMAC mechanism. Thus **FCS_COP.1.1 (IPSEC-HMAC)** also protects against re-injection of earlier data.

5.1.2.5 FCS_CKM.4 (IPSEC) Cryptographic key destruction

FCS_CKM.4.1 (IPSEC)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting with zeros**] that meets the following: [**OpenBSD implementation**].

Application note: The key generation SFR **FCS_CKM.1** is not required because the keys for **FCS_COP.1.1 (IPSEC-AES)** and **FCS_COP.1.1 (IPSEC-HMAC)** are generated by the IKE daemon in the environment (cf. section 5.4.1.7 **FCS_COP.1 (IKE-DH)**)

Application note: The key destruction function is identical for **FCS_COP.1 (IPSEC-AES)** and **FCS_COP.1 (IPSEC-HMAC)**, so there is only one iteration of **FCS_CKM.4 (IPSEC)**.

5.1.2.6 FMT_MSA.3 (IPSEC) Static attribute initialisation

FMT_MSA.3.1 (IPSEC)

The TSF shall enforce the [**IPSEC-SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (IPSEC)

The TSF shall allow ~~the~~ [**nobody**] to specify alternative initial values to override the default values when an object or information is created.

5.1.2.7 FMT_SMF.1 (IPSEC) Specification of Management Functions

FMT_SMF.1.1 (IPSEC)

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

Definitions of IPsec tunnels between Firewall components].

5.1.3 Audit

This section provides SFRs that identify the audit and monitoring capabilities of the TOE.

5.1.3.1 FAU_GEN.1EX Audit data generation

This SFR is derived from FAU_GEN.1. See Appendix 9.1.1.1 for a full explanation.

FAU_GEN.1EX.1

The TSF shall generate an audit record of the following auditable events:

1. All auditable events for the [***not specified***] level of audit; and
2. [
    - **Starting of Firewall components**
    - **IP datagrams matching log filters in firewall rules**].

FAU_GEN.1EX.2

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

1. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
2. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**no other audit relevant information**].

5.1.3.2 FAU_SAR.1 Audit review

FAU_SAR.1.1

The TSF shall provide [**the authorised administrator**] with the capability to read [**all audit 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.

Application note: The restriction to one role is not meaningful for the TOE, since there is only one user.

5.1.3.3 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1

The TSF shall provide the ability to perform [***searches***] of audit data based on: [

1. **ranges of dates;**
2. **ranges of times;**
3. **the Firewall component that produced the audit data;**
4. **for log data of firewall rules: IP addresses and ports, where applicable**

].

5.1.4 General Management Facilities

This section provides SFRs relating to the general management of the TOE.

5.1.4.1 FMT_SMF.1 (Gen) Security management functions

FMT_SMF.1.1 (Gen)

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

- **Initial configuration of the Firewall components**
- **Transfer of configuration data onto the Firewall components**
- **Update of software on the Firewall components**].

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.

5.1.4.3 FIA_UID.2 User identification before any action

FIA_UID.2.1

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

5.2 TOE Strength of Function Claim

The TOE relies on the following SFRs implemented by probabilistic or permutational mechanisms that perform encryption and authentication:

- **FCS_COP.1 (IPSEC-AES)**
- **FCS_COP.1 (IPSEC-HMAC)**
- **FIA_UAU.2**

In accordance with the requirements of the national scheme no strength of function claim is made for the cryptographic mechanisms.

The minimum strength of function claim for **FCS_COP.1 (IPSEC-AES)** and **FCS_COP.1 (IPSEC-HMAC)** is 'not applicable'.

The minimum strength of function claim for **FIA_UAU.2** is 'SOF-medium'.

Therefore the minimum strength of function claim for the TOE is 'SOF-medium'.

5.3 TOE Security Assurance Requirements

5.3.1 Statement of Security Assurance Requirements

The security assurance requirement for the TOE comprise the requirements corresponding to the EAL4 level of assurance, as defined in [CC_3], augmented by **ALC_FLR.2**.

Table 9 below lists the relevant requirements by assurance components.

	Security Assurance Requirement
Configuration management	**ACM_AUT.1** Partial CM automation **ACM_CAP.4** Generation support and acceptance procedures **ACM_SCP.2** Problem tracking CM coverage
Delivery and operation	**ADO_DEL.2** Detection of modification **ADO_IGS.1** Installation, generation, and start-up procedures
Development	**ADV_FSP.2** Fully defined external interfaces **ADV_HLD.2** Security enforcing high-level design **ADV_IMP.1** Subset of the implementation of the TSF **ADV_LLD.1** Descriptive low-level design **ADV_RCR.1** Informal correspondence demonstration **ADV_SPM.1** Informal TOE security policy model
Guidance documents	**AGD_ADM.1** Administrator guidance **AGD_USR.1** User guidance
Life cycle support	**ALC_DVS.1** Identification of security measures **ALC_LCD.1** Developer defined life-cycle model **ALC_TAT.1** Well-defined development tools **ALC_FLR.2** Flaw reporting procedures
Tests	**ATE_COV.2** Analysis of coverage **ATE_DPT.1** Testing: high-level design **ATE_FUN.1** Functional testing **ATE_IND.2** Independent testing - sample
Vulnerability assessment	**AVA_MSU.2** Validation of analysis **AVA_VLA.2** Independent vulnerability analysis **AVA_SOF.1** Strength of TOE security function evaluation

Table 9: Security Assurance Requirements

5.4 Security requirements for the IT environment

5.4.1 IKE-SFP

This section identifies the SFRs associated with cryptographic functions in relation to the key management of the VPN connections between the Firewall components. The IKE-SFP is the policy that models this aspect of information flow control.

5.4.1.1 FDP_ITT.1 (IKE) Basic internal transfer protection

FDP_ITT.1.1 (IKE)

The ~~TSF~~ **IT environment** shall enforce the [**IKE-SFP**] to prevent the [***disclosure* and *modification***] of user data when it is transmitted between physically-separated parts of the TOE.

Application Note: The data transmitted is in fact the key agreement for subsequent IPsec transforms.

5.4.1.2 FDP_IFC.1 (IKE) Subset information flow control

FDP_IFC.1.1 (IKE)

The ~~TSF~~ **IT environment** shall enforce the [**IKE-SFP**] on [**:**

1. **subjects: Firewall components;**
2. **information: the data sent from one subject through the environment to another;**
3. **operation: pass the data**].

5.4.1.3 FDP_IFF.1 (IKE) Simple security attributes

FDP_IFF.1.1 (IKE)

The ~~TSF~~ **IT environment** shall enforce the [**IKE-SFP**] based on **at least** the following types of subject and information security attributes: [

1. **subject security attributes: public keys associated with the subject.**
2. **information security attributes: none**].

FDP_IFF.1.2 (IKE)

The ~~TSF~~ **IT environment** shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- **Subjects can cause information to flow through their respective components of the TOE if based on the subjects' public keys a secure IPsec connection can be negotiated between the subjects via the IKE protocol**].

FDP_IFF.1.3 (IKE)

The ~~TSF~~ **IT environment** shall enforce the [**none**].

FDP_IFF.1.4 (IKE)

The ~~TSF~~ **IT environment** shall provide the following [**none**].

FDP_IFF.1.5 (IKE)

The ~~TSF~~ **IT environment** shall explicitly authorise an information flow based on the following rules: [**none**]

FDP_IFF.1.6 (IKE)

The ~~TSF~~ **IT environment** shall explicitly deny an information flow based on the following rules: [**none**].

Application note: The decisions necessary to enforce the IKE-SFP by the IT environment are completely determined by the IPsec configuration in the TOE defined in **FMT_SMF.1 (IPSEC)**.

5.4.1.4 FCS_CKM.1 (IKE-AES) Cryptographic key generation

FCS_CKM.1.1 (IKE-AES)

The ~~TSF~~ **IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**symmetric key generation**] and specified cryptographic key sizes [**128 bit**] that meet the following: [**[RFC3602]**]**.**

5.4.1.5 FCS_COP.1 (IKE-AES) Cryptographic operation

FCS_COP.1.1 (IKE-AES)

The ~~TSF~~ **IT environment** shall perform [**data encryption**] in accordance with a specified cryptographic algorithm [**AES in CBC mode**] and cryptographic key sizes [**128 bit**] that meet the following: [**[FIPS-197]**].

5.4.1.6 FCS_CKM.1 (IKE-DH) Cryptographic key generation

FCS_CKM.1.1 (IKE-DH)

The ~~TSF~~ **IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Diffie-Hellman exponent generation**] and specified cryptographic key sizes [**2048 bit**] that meet the following: [**[RFC2409] and [RFC3526]**].

5.4.1.7 FCS_COP.1 (IKE-DH) Cryptographic operation

FCS_COP.1.1 (IKE-DH)

The ~~TSF~~ **IT environment** shall perform [**cryptographic key agreement**] in accordance with a specified cryptographic algorithm [**Diffie-Hellman**] and cryptographic key sizes [**2048 bit**] that meet the following: [**[RFC2409] and [RFC3526]**].

5.4.1.8 FCS_CKM.1 (IKE-HMAC) Cryptographic key generation

FCS_CKM.1.1 (IKE-HMAC)

The ~~TSF~~ **IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**authentication key generation**] and specified cryptographic key sizes [**160 bit**] that meet the following: [**[RFC2409]**].

5.4.1.9 FCS_COP.1 (IKE-HMAC) Cryptographic operation

FCS_COP.1.1 (IKE-HMAC)

The ~~TSF~~ **IT environment** shall perform [**message authentication**] in accordance with a specified cryptographic algorithm [**HMAC-SHA**] and cryptographic key sizes [**160 bit**] that meet the following: [**[RFC2104] and [FIPS-180-2]**].

5.4.1.10 FCS_CKM.1 (IKE-RSA) Cryptographic key generation

FCS_CKM.1.1 (IKE-RSA)

The ~~TSF~~ **IT environment** shall generate cryptographic keys in accordance with a specified

cryptographic key generation algorithm [**RSA key generation**] and specified cryptographic key sizes [**2048 bit**] that meet the following: [**[PKCS #1, v2.0]**].

5.4.1.11 FCS_COP.1 (IKE-RSA) Cryptographic operation

FCS_COP.1.1 (IKE-RSA)

The ~~TSF~~ **IT environment** shall perform [**authentication**] in accordance with a specified cryptographic algorithm [**RSA signature**] and cryptographic key sizes [**2048 bit**] that meet the following: [**[PKCS #1, v2.0]**].

5.4.1.12 FCS_CKM.4 (IKE) Cryptographic key destruction

FCS_CKM.4.1 (IKE)

The ~~TSF~~ **IT environment** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting with zeros**] that meets the following: [**OpenBSD ISAKMP implementation**].

Application note: The key destruction function is identical for **FCS_COP.1 (IKE-DH)**, **FCS_COP.1 (IKE-AES)**, **FCS_COP.1 (IKE-HMAC)** and **FCS_COP.1 (IKE-RSA)**, so there is only one iteration of **FCS_CKM.4** for all four SFRs.

5.4.1.13 FMT_SMF.1 (IKE) Specification of Management Functions

FMT_SMF.1.1 (IKE)

The ~~TSF~~ **IT environment** shall be capable of performing the following security management functions: [**modification and deletion of public and secret keys associated with Firewall components by the IKE daemon**].

Application note: The public and secret keys are essential for the IKE protocol, which is part of the environment. After successful authentication, the IKE protocol generates the keys for the IPsec operations in the kernel, which are functions of the TOE.

5.4.1.14 FMT_MSA.2 (IKE) Secure security attributes

FMT_MSA.2.1 (IKE)

The ~~TSF~~ **IT environment** shall ensure that only secure values are accepted for security attributes.

5.4.1.15 FMT_MSA.3 (IKE) Static attribute initialisation

FMT_MSA.3.1 (IKE)

The ~~TSF~~ **IT environment** shall enforce the [**IKE-SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (IKE)

The ~~TSF~~ **IT environment** shall allow the [**authorised administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.4.2 Flow Control Secure Internal Communication

This section identifies the SFRs associated with the flow control functions in relation to the communication between the Management Server and the Firewall components. The SSH-SFP is the policy that models this aspect of information flow control.

5.4.2.1 FDP_ITT.1 (SSH) Basic internal transfer protection

FDP_ITT.1.1 (SSH)

The ~~TSF~~ **IT environment** shall enforce the [**SSH-SFP**] to prevent the [***disclosure* and *modification***] of user data when it is transmitted between physically-separated parts of the TOE.

5.4.2.2 FDP_IFC.1 (SSH) Subset information flow control

FDP_IFC.1.1 (SSH)

The ~~TSF~~ **IT environment** shall enforce the [**SSH-SFP**] on [**:**

1. **subjects: Management Server and Firewall components;**
2. **information: the data sent from one subject through the environment to another;**
3. **operation: pass the data**].

5.4.2.3 FDP_IFF.1 (SSH) Simple security attributes

FDP_IFF.1.1 (SSH)

The ~~TSF~~ **IT environment** shall enforce the [**SSH-SFP**] based on **at least** the following types of subject and information security attributes: [

1. **subject security attributes:**
   - **SSH host keys and user keys installed on the platforms hosting the TOE components.**
2. **information security attributes: none**].

FDP_IFF.1.2 (SSH)

The ~~TSF~~ **IT environment** shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- **Subjects can cause information to flow through their respective components of the TOE if based on the subjects' host keys and user keys a secure connection can be negotiated between the subjects via the SSH protocol**].

FDP_IFF.1.3 (SSH)

The ~~TSF~~ **IT environment** shall enforce the [**none**].

FDP_IFF.1.4 (SSH)

The ~~TSF~~ **IT environment** shall provide the following [**none**].

FDP_IFF.1.5 (SSH)

The ~~TSF~~ **IT environment** shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.6 (SSH)

The ~~TSF~~ **IT environment** shall explicitly deny an information flow based on the following rules: [**none**].

5.4.2.4 FCS_CKM.1 (SSH-AES) Cryptographic key generation

FCS_CKM.1.1 (SSH-AES)

The ~~TSF~~ **IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**symmetric key generation**] and specified cryptographic key sizes [**128 bit**] that meet the following: [**[RFC4253]]**.

5.4.2.5 FCS_COP.1 (SSH-AES) Cryptographic operation

FCS_COP.1.1 (SSH-AES)

The ~~TSF~~ **IT environment** shall perform [**data encryption**] in accordance with a specified cryptographic algorithm [**AES in CBC mode**] and cryptographic key sizes [**128 bit**] that meet the following: [**[FIPS-197]**].

5.4.2.6 FCS_CKM.1 (SSH-DH) Cryptographic key generation

FCS_CKM.1.1 (SSH-DH)

The ~~TSF~~ **IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Diffie-Hellman exponent generation**] and specified cryptographic key sizes [**2048 bit**] that meet the following: [**[RFC4253] and [RFC3526]**].

5.4.2.7 FCS_COP.1 (SSH-DH) Cryptographic operation

FCS_COP.1.1 (SSH-DH)

The ~~TSF~~ **IT environment** shall perform [**cryptographic key agreement**] in accordance with a specified cryptographic algorithm [**Diffie-Hellman**] and cryptographic key sizes [**2048 bit**] that meet the following: [**[RFC4253] and [RFC3526]**].

5.4.2.8 FCS_CKM.1 (SSH-HMAC) Cryptographic key generation

FCS_CKM.1.1 (SSH-HMAC)

The ~~TSF~~ **IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**authentication key generation**] and specified cryptographic key sizes [**160 bit**] that meet the following: [**[RFC4253]**].

5.4.2.9 FCS_COP.1 (SSH-HMAC) Cryptographic operation

FCS_COP.1.1 (SSH-HMAC)

The ~~TSF~~ **IT environment** shall perform [**message authentication**] in accordance with a specified cryptographic algorithm [**HMAC-SHA**] and cryptographic key sizes [**160 bit**] that meet the following: [**[RFC2104] and [FIPS-180-2]**].

5.4.2.10 FCS_CKM.1 (SSH-RSA) Cryptographic key generation

FCS_CKM.1.1 (SSH-RSA)

The ~~TSF~~ **IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA key generation**] and specified cryptographic key sizes [**2048 bit**] that meet the following: [**[PKCS #1, v2.0]**].

5.4.2.11 FCS_CKM.4 (SSH) Cryptographic key destruction

FCS_CKM.4.1 (SSH)

The ~~TSF~~ **IT environment** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting with zeros**] that meets the following: [**OpenBSD SSH implementation**].

Application note: The key destruction function is identical for **FCS_COP.1 (SSH-DH)**, **FCS_COP.1 (SSH-AES)**, **FCS_COP.1 (SSH-HMAC)** and **FCS_COP.1 (SSH-RSA)**, so there is only one iteration of **FCS_CKM.4** for all four SFRs.

5.4.2.12 FCS_COP.1 (SSH-RSA) Cryptographic operation

FCS_COP.1.1 (SSH-RSA)

The ~~TSF~~ **IT environment** shall perform [**authentication**] in accordance with a specified cryptographic algorithm [**RSA signatures**] and cryptographic key sizes [**2048 bit**] that meet the following: [**[PKCS #1, v2.0]**].

5.4.2.13 FMT_SMF.1 (SSH) Specification of Management Functions

FMT_SMF.1.1 (SSH)

The ~~TSF~~ **IT environment** shall be capable of performing the following security management functions: [**modification and deletion of public and secret keys associated with Firewall components by the SSH daemon**].

5.4.2.14 FMT_MSA.2 (SSH) Secure security attributes

FMT_MSA.2.1 (SSH)

The ~~TSF~~ **IT environment** shall ensure that only secure values are accepted for security attributes.

5.4.2.15 FMT_MSA.3 (SSH) Static attribute initialisation

FMT_MSA.3.1 (SSH)

The ~~TSF~~ **IT environment** shall enforce the [**SSH-SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (SSH)

The ~~TSF~~ **IT environment** shall allow the [**authorised administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.4.3 Audit

5.4.3.1 FPT_STM.1 (ENV) Reliable timestamps

FPT_STM.1.1 (ENV)

The ~~TSF~~ **IT environment** shall be able to provide reliable timestamps for ~~its own~~ **the TOE's** use.

6 TOE summary specification

6.1 TOE security functions

6.1.1 Introduction

This section defines the TOE security functions. Each section contains a set of labelled statements, one for each function or sub-function. These statements taken together specify the TOE's security functionality.

6.1.2 Audit

SF_AU.1: The TOE shall generate audit records for

1. Starting of Firewall components
2. Datagrams received or sent through a Firewall component's network interfaces if they match configured patterns.

SF_AU.2: Each audit record shall include the following information:

1. Time and Date
2. The affected Firewall component
3. The type of the event
4. The subject identity (source IP)

For log data of firewall rules, the following additional information shall be included:

1. The affected interface
2. Direction
3. Action (''pass'' or ''block'')
4. Optional further information, e.g. IP addresses and ports. This depend on the protocols.

SF_AU.3: The TOE shall provide the administrator with a display of audit data on the Management Server. The audit data shall be searchable by

1. Time and/or Date
2. Firewall component that created the audit record
3. For log data of firewall rules: IP addresses and ports, where applicable.

6.1.3 Information Flow Protection

SF_DF.1: The Firewall components implement the flow control as routers or as bridges, on the network layer (IP) and transport layer (TCP/UDP/ICMP). The filter takes the information from the IP and TCP/UDP/ICMP-Header (where applicable) in order to apply the filter rules.

The filter rules allow to filter by the criteria:

1. address of source
2. address of destination

3. transport layer protocol
4. interface on which traffic arrives and departs
5. service

The TOE sets restrictive default values for the filter rules.

SF_DF.2: The Firewall components reassemble fragmented IP datagrams before further processing is performed on the data. IP datagrams which cannot be reassembled in a predefined span of time are dropped.

SF_DF.3: Packets with spoofed source- or destination-IP addresses are dropped. Packets with source routing options are dropped.

SF_DF.4: Connections between networks protected by different Firewall components can be protected by IPsec transforms against eavesdropping, modification and replay attacks. The default settings are restrictive. The transforms use the following probabilistic or permutational functions: AES block cipher in CBC mode with a key size of 128 bits for confidentiality and the SHA1 HMAC with a key size of 160 bits for integrity. Expired keys are overwritten with zeros.

SF_DF.5: The Firewall components can modify headers to make the information flows less susceptible to hijacking attacks.

6.1.4 Security Management

SF_AC.1: The TOE provides the capability for the authorised administrator to configure network traffic filter rules and IPsec tunnels on the Management Server. The TOE sets restrictive default values for the filter rules. The TOE allows to transfer the configuration data to the Firewall components and to update software on the Firewall components.

6.1.5 Authentication and Identification

SF_AI.1: The TOE guarantees that the authorised administrator has to identify himself to the Management Server with a user name and authenticate himself successfully by password before he can perform any security function.

6.2 Probabilistic or Permutational Security Functions

The TOE defines the security functions **SF_DF.4** and **SF_AI.1** that use probabilistic or permutational algorithms.

The strength of function claim is 'not applicable' for **SF_DF.4** and 'SOF-medium' for **SF_AI.1** as explained in Section 5.2 above.

6.3 Assurance Measures

The following sections show how the security assurance requirements are met.

6.3.1 Configuration management

The developer will provide documentation that describes the configuration management system used at GeNUA. The document will contain enough details to show how the requirements **ACM_AUT.1**, **ACM_CAP.4**, and **ACM_SCP.2** are met.

6.3.2 Delivery and operation

The developer will provide documentation that describe how the TOE is delivered and installed. The document will contain enough details to show how the requirements **ADO_DEL.2** and **ADO_IGS.1** are met.

6.3.3 Development

The developer will provide several development documents that cover the requirements of **ADV_FSP.2**, **ADV_HLD.2**, **ADV_IMP.1**, **ADV_LLD.1**, **ADV_RCR.1**, and **ADV_SPM.1**.

6.3.4 Guidance documents

The [DOC] manual contains the administrator guide. It explains in great detail how to operate the TOE securely. The manual meets the requirements **AGD_ADM.1** and **AGD_USR.1**.

6.3.5 Life cycle support

The developer will provide documentation that describe the life cycle support. The documentation will be detailed enough to cover the requirements **ALC_DVS.1**, **ALC_LCD.1**, **ALC_TAT.1**, and **ALC_FLR.2**.

6.3.6 Tests

The developer will provide test documentation that meet the requirements **ATE_COV.2**, **ATE_DPT.1**, **ATE_FUN.1**. The developer will provide the TOE to the evaluator in a form that satisfies **ATE_IND.2**. This allows the evaluator to do the independent testing.

6.3.7 Vulnerability assessment

The developer will provide the required analysis documentation that shows that guidance is given for secure operation in all modes of operation. It will contain a vulnerability analysis. The documentation will provide enough information to meet **AVA_MSU.2**, **AVA_SOF.1** and **AVA_VLA.2.**

7 PP Claims

No claim of PP compliance is made for the TOE.

8 TOE Rationale

8.1 Security Objectives Rationale

8.1.1 Introduction

This chapter contains the ST Rationale. It must show that the ST is consistent.

The following table shows that all security objectives stated in this ST can be mapped to the stated threats and assumptions. All threats and assumptions are matched by at least one security objective.

	OE.PHYSEC	OE.INIT	OE.NOEVIL	OE.SINGEN	OE.NOADDSERV	OE.NOFWSERV	OE.TIMESTMP	OE.ADMIN	OE.CRYPTO	O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC
A.PHYSEC	X														
A.INIT		X													
A.NOEVIL			X												
A.SINGEN				X											
A.NOADDSERV					X										
A.NOFWSERV						X									
A.TIMESTMP							X								
A.ADMIN								X							
T.NOAUTH	X	X		X					X	X					
T.SNIFF		X										X			
T.SELPRO					X	X				X					X
T.MEDIAT				X							X		X		
T.MSNIFF		X							X						
T.MODIFY		X											X	X	
T.MMODIFY		X							X				X	X	

Table 10: Security Objectives

8.1.2 Assumption Rationale

In the following table it is explained how the assumptions are satisfied by the environmental objectives.

8.1.3 A.PHYSEC

The objective **OE.PHYSEC** assures that the assumption about a physically secure TOE can be made.

8.1.4 A.INIT

The objective **OE.INIT** assures that the TOE was correctly initialised.

8.1.5 A.NOEVIL

The objective **OE.NOEVIL** assures that the authorised administrators are trained and therefore that they are no threat to the TOE.

8.1.6 A.SINGEN

The objective **OE.SINGEN** assures that the TOE can not be bypassed and therefore assures that the assumption is met.

8.1.7 A.NOADDSERV

The objective **OE.NOADDSERV** assures that no additional services run on the Management Server.

8.1.8 A.NOFWSERV

The objective **OE.NOFWSERV** assures that no additional services run on the Firewall components.

8.1.9 A.TIMESTMP

The objective **OE.TIMESTMP** provides reliable timestamps.

8.1.10 A.ADMIN

The objective **OE.ADMIN** assures that the administration only occurs from a trusted network.

8.2 Threat Rationale

8.2.1 T.NOAUTH

The threat that a user might bypass the security functions of the TOE is countered by **OE.PHYSEC**, **OE.INIT**, **OE.SINGEN**, **OE.CRYPTO** and **O.AUTH**. The environmental objectives assure that no user can interfere with the initial setup, the physical setup of the Firewall components, or use routes around the Firewall components. The **OE.CRYPTO** environmental objective assures that data flow between the Firewall components and the Management Server is protected by cryptographic transforms, so that sessions of users already authenticated cannot be taken over. The **O.AUTH** objective assures that only authorised users can open connections to other Firewall components directly. The authorised administrator and the IKE daemons are the only such users.

8.2.2 T.SNIFF

The threat that a user might gain access to the sensitive data passing between the

protected networks is countered by objectives **OE.INIT** and **O.CONFID**. These assure that the Firewalls components' public keys are initialised over an authenticated network and that all data flowing between the Firewall components is protected against eavesdropping by IPsec transforms.

8.2.3 T.SELPRO

The threat that a user might gain access to the TOE and read, modify or destroy security sensitive data on the TOE is countered by objectives **OE.NOADDSERV**, **OE.NOFWSERV**, **O.AUTH** and **O.AUDREC**. These assure that

- no externally reachable services run on the Management Server
- no services besides SSH and IKE run on the Firewall components
- only authorised users can use the available services
- attempts to compromise the TOE are audited

8.2.4 T.MEDIAT

The threat that a user may send non-permissible data through the TOE that result in gaining access to resources in other connected networks is countered by **OE.SINGEN**, **O.MEDIAT** and **O.INTEG**. These assure that all data passes through the TOE, so that it is always checked and filtered according to the policy, and that data thus checked cannot be modified on it's way to gain access to machines in the protected networks.

8.2.5 T.MSNIFF

The threat that a user might gain access to the configuration or audit data passing between the Management Server and the Firewall components is countered by objectives **OE.INIT** and **OE.CRYPTO**. These assure that the Management Server's and the Firewall components' public keys are initialised over an authenticated network and that all data flowing between the Management Server and the Firewall components is protected against eavesdropping by SSH transforms.

8.2.6 T.MODIFY

The threat that a user might modify the sensitive data passing between the protected networks is countered by objectives **OE.INIT**, **O.NOREPLAY** and **O.INTEG**. These assure that the Firewall components' public keys are initialised over an authenticated network and that all data flowing between the Firewall components is protected by IPsec transforms against unauthorised modification and re-injection of earlier data.

8.2.7 T.MMODIFY

The threat that a user might modify the configuration or audit data passing between the Management Server and the Firewall component is countered by objectives **OE.INIT**, **OE.CRYPTO**, **O.NOREPLAY** and **O.INTEG**. These assure that the Management Server's and the Firewall components' public keys are initialised over an authenticated network and that all data flowing between the Management Server and the Firewall components is protected by SSH transforms against modification and re-injection of earlier data.

8.3 Security Requirements Rationale

This section must show that the SFR address the objectives, and that all dependencies between the SFRs and SARs are met.

8.3.1 TOE Functional Requirements Rationale

Table 11 below shows that all TOE SFRs contribute to stated TOE objectives, and all TOE security objectives are mapped to at least one TOE SFR.

The rest of this section describes the coverage of security objectives by SFRs and reasons why the SFRs are sufficient for the objectives.

	O.MEDIAT	O.CONFID	O.INTEG	O.AUTH	O.NOREPLAY	O.AUDREC
FDP_IFC.1 (FW)	**X**					
FDP_IFF.1 (FW)	**X**					
FMT_SMF.1 (FW)	**X**					
FMT_MSA.3 (FW)	**X**					
FAU_GEN.1EX						**X**
FAU_SAR.1						**X**
FAU_SAR.3						**X**
FMT_SMF.1 (Gen)	**X**					
FIA_UID.2				**X**		
FIA_UAU.2				**X**		
FDP_ITT.1 (IPSEC)		**X**	**X**		**X**	
FDP_IFC.1 (IPSEC)	**X**					
FCS_COP.1 (IPSEC-AES)		**X**				
FCS_COP.1 (IPSEC-HMAC)			**X**		**X**	
FCS_CKM.4 (IPSEC)		**X**	**X**			
FMT_MSA.3 (IPSEC)		**X**	**X**		**X**	
FMT_SMF.1 (IPSEC)		**X**	**X**		**X**	

Table 11: TOE Functional Requirements Rationale

8.3.1.1 O.MEDIAT

FDP_IFC.1 (FW), **FDP_IFC.1 (IPSEC)** and **FDP_IFF.1 (FW)** describe the information flow controls and information flow control policy.

FMT_SMF.1 (FW) and **FMT_MSA.3 (FW)** describe the management functions and the restrictive defaults for security attributes concerned with flow controls.

FMT_SMF.1 (Gen) SFR defines the general management functions including the initial installation and configuration without which there would be no filters.

Together, the SFRs describe how firewall policies are enforced on flows, which restrictive default policies apply and who is allowed to modify the policies. The SFRs are therefore sufficient to satisfy the **O.MEDIAT** objective and mutually supportive.

8.3.1.2 O.AUDREC

FAU_GEN.1EX describes the creation of audit logs.

FAU_SAR.1 and **FAU_SAR.3** describe the selectable audit review of the authorised administrator.

Taken together, the SFRs suffice to satisfy the **O.AUDREC**, because they describe who is allowed to cause creation of audit data, who is allowed to read it, what events can be audited and how the audit data can be searched. The SFRs are mutually supportive.

8.3.1.3 O.AUTH

The **FIA_UAU.2** SFR requires every user to authenticate before any action.

The **FIA_UID.2** SFR requires every user to identify themselves before any action.

The SFRs describe that only authorised administrators are allowed to operate the TOE. The SFRs are therefore sufficient.

8.3.1.4 O.INTEG

FDP_ITT.1 (IPSEC) identifies the requirement to protect data flow between Firewall components by IPsec transforms.

The **FCS_COP.1 (IPSEC-HMAC)** SFR describes the cryptographic transforms to be applied to protect the data flow from unauthorised modifications. The **FCS_CKM.4 (IPSEC)** SFR assures that keys are securely deleted.

The **FMT_SMF.1 (IPSEC)** SFR describes the management functions concerned with IPsec transforms.

The **FMT_MSA.3 (IPSEC)** SFR enforces restrictive defaults on the IPsec transforms.

8.3.1.5 O.CONFID

FDP_ITT.1 (IPSEC) identifies the requirement to protect data flow between Firewall components by IPsec transforms.

The **FCS_COP.1 (IPSEC-AES)** SFR describes the cryptographic transforms to be applied to protect the data flow from unauthorised inspections. The **FCS_CKM.4 (IPSEC)** SFR assures that keys are securely deleted.

The **FMT_SMF.1 (IPSEC)** SFR describes the management functions concerned with IPsec transforms.

The **FMT_MSA.3 (IPSEC)** SFR enforces restrictive defaults on the IPsec transforms.

8.3.1.6 O.NOREPLAY

FDP_ITT.1 (IPSEC) identifies the requirement to protect data flow between Firewall components by IPsec transforms.

The **FCS_COP.1 (IPSEC-HMAC)** SFR describes the cryptographic transforms to be applied to protect the data flow from unauthorised modifications including the re-injection of data.

The **FMT_SMF.1 (IPSEC)** SFR describes the management functions concerned with IPsec transforms.

The **FMT_MSA.3 (IPSEC)** SFR enforces restrictive defaults on the IPsec transforms.

This addresses the integrity, confidentiality and replay protection objectives sufficiently.

8.3.2 Environment Functional Requirements Rationale

The **OE.PHYSEC**, **OE.NOEVIL**, **OE.SINGEN**, **OE.NOADDSER**, **OE.NOFWSERV** and **OE.ADMIN** are covered by assumptions about the environment, not by any SFRs.

The **FDP_ITT.1 (IKE)**, **FDP_IFC.1 (IKE)**, **FDP_IFF.1 (IKE)**, **FCS_CKM.1 (IKE-AES)**, **FCS_COP.1 (IKE-AES)**, **FCS_CKM.1 (IKE-DH)**, **FCS_COP.1 (IKE-DH)**, **FCS_CKM.1 (IKE-HMAC)**, **FCS_COP.1 (IKE-HMAC)**, **FCS_CKM.1 (IKE-RSA)**, **FCS_COP.1 (IKE-RSA)**, **FCS_CKM.4 (IKE)**, **FMT_SMF.1 (IKE)**, **FMT_MSA.2 (IKE)**, **FMT_MSA.3 (IKE)** define the requirements for the Internet Key Exchange protocol which is one part of the **OE.CRYPTO** objective for the environment.

The **FDP_ITT.1 (SSH)**, **FDP_IFC.1 (SSH)**, **FDP_IFF.1 (SSH)**, **FCS_CKM.1 (SSH-AES)**, **FCS_COP.1 (SSH-AES)**, **FCS_CKM.1 (SSH-DH)**, **FCS_COP.1 (SSH-DH)**, **FCS_CKM.1 (SSH-HMAC)**, **FCS_COP.1 (SSH-HMAC)**, **FCS_CKM.1 (SSH-RSA)**, **FCS_CKM.4 (SSH)**, **FCS_COP.1 (SSH-RSA)**, **FMT_SMF.1 (SSH)**, **FMT_MSA.2 (SSH)**, **FMT_MSA.3 (SSH)** define the requirements for the Secure Shell protocol which is the other part of the **OE.CRYPTO** objective for the environment.

So the SFRs in total map to **OE.CRYPTO** exactly.

The **FPT_STM.1 (ENV)** covers the **OE.TIMESTMP** environmental objective.

8.3.3 New or tailored SFR

The following rationale justifies the introduction of a new SFR component.

FAU_GEN.1EX: This component is derived from **FAU_GEN.1**, but omits the audit events on start-up and shutdown of the audit functions. The replacement can be used if the omitted functionality is not supported. All other requirements are taken literally from **FAU_GEN.1**. The SFR that depend on **FAU_GEN.1** usually require only the security functions still supported. **FAU_GEN.1EX** can therefore be used as a replacement for **FAU_GEN.1**. The dependency on **FAU_GEN.1** of other SFRs can be substituted by **FAU_GEN.1EX**. Because **FAU_GEN.1EX** is closely connected to **FAU_GEN.1**, it has been added to the same family.

8.3.4 Dependencies between the SFR and SAR

The following tables shows that all dependencies are met (see notes at end of table):

ID	*SFR*	*Depends*	*Satisfied by*
A1	**FDP_IFC.1 (FW)**	**FDP_IFF.1**	**A2**
A2	**FDP_IFF.1 (FW)**	**FDP_IFC.1** **FMT_MSA.3**	**A1** **A4**
A3	**FMT_SMF.1 (FW)**	**-/-**	
A4	**FMT_MSA.3 (FW)**	**FMT_MSA.1** **FMT_SMR.1**	**N/A** **N/A**
B1	**FDP_ITT.1 (IPSEC)**	**FDP_IFC.1**	**B2**
B2	**FDP_IFC.1 (IPSEC)**	**FDP_IFF.1**	**E3**
B3	**FCS_COP.1 (IPSEC-AES)**	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	**E6** **B5** **E14**
B4	**FCS_COP.1 (IPSEC-HMAC)**	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	**E6** **B5** **E14**
B5	**FCS_CKM.4 (IPSEC)**	**FCS_MSA.2** **FCS_CKM.1**	**E14** **E6**
B6	**FMT_MSA.3 (IPSEC)**	**FMT_MSA.1** **FMT_SMR.1**	**N/A** **N/A**
B9	**FMT_SMF.1 (IPSEC)**	**-/-**	
C1	**FAU_GEN.1EX**	**FPT_STM.1**	**G1**
C2	**FAU_SAR.1**	**FAU_GEN.1**	**C1**
C3	**FAU_SAR.3**	**FAU_SAR.1**	**C2**
D1	**FMT_SMF.1 (Gen)**	**-/-**	
D2	**FIA_UAU.2**	**FIA_UID.1**	**D3**
D3	**FIA_UID.2**	**-/-**	
E1	**FDP_ITT.1 (IKE)**	**FDP_IFC.1**	**E2**
E2	**FDP_IFC.1 (IKE)**	**FDP_IFF.1**	**E3**
E3	**FDP_IFF.1 (IKE)**	**FDP_IFC.1** **FMT_MSA.3**	**B2, E2** **E15**

ID	*SFR*	*Depends*	*Satisfied by*
E4	**FCS_CKM.1 (IKE-AES)**	**FCS_CKM.4** **FCS_COP.1** **FMT_MSA.2**	**E11** **E5** **E14**
E5	**FCS_COP.1 (IKE-AES)**	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	**E4** **E11** **E14**
E6	**FCS_CKM.1 (IKE-DH)**	**FCS_CKM.4** **FCS_COP.1** **FMT_MSA.2**	**E11** **E7** **E14**
E7	**FCS_COP.1 (IKE-DH)**	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	**E6** **E11** **E14**
E8	**FCS_CKM.1 (IKE-HMAC)**	**FCS_CKM.4** **FCS_COP.1** **FMT_MSA.2**	**E11** **E9** **E14**
E9	**FCS_COP.1 (IKE-HMAC)**	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	**E8** **E11** **E14**
E10	**FCS_CKM.1 (IKE-RSA)**	**FCS_CKM.4** **FCS_COP.1** **FMT_MSA.2**	**E11** **E12** **E14**
E11	**FCS_CKM.4 (IKE)**	**FCS_CKM.1** **FMT_MSA.2**	**E4, E6, E8, E10** **E14**
E12	**FCS_COP.1 (IKE-RSA)**	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	**E10** **E11** **E14**
E13	**FMT_SMF.1 (IKE)**	**-/-**	
E14	**FMT_MSA.2 (IKE)**	**ADV_SPM.1** **FDP_IFC.1** **FMT_MSA.1** **FMT_SMR.1**	**Table 13 AS.11** **E2** **N/A** **N/A**
E15	**FMT_MSA.3 (IKE)**	**FMT_MSA.1** **FMT_SMR.1**	**N/A** **N/A**
F1	**FDP_ITT.1 (SSH)**	**FDP_IFC.1**	**F2**

ID	*SFR*	*Depends*	*Satisfied by*
F2	**FDP_IFC.1 (SSH)**	**FDP_IFF.1**	**F3**
F3	**FDP_IFF.1 (SSH)**	**FDP_IFC.1** **FMT_MSA.3**	**F2** **F15**
F4	**FCS_CKM.1 (SSH-AES)**	**FCS_CKM.4** **FCS_COP.1** **FMT_MSA.2**	**F11** **F5** **F14**
F5	**FCS_COP.1 (SSH-AES)**	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	**F4** **F11** **F14**
F6	**FCS_CKM.1 (SSH-DH)**	**FCS_CKM.4** **FCS_COP.1** **FMT_MSA.2**	**F11** **F7** **F14**
F7	**FCS_COP.1 (SSH-DH)**	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	**F6** **F11** **F14**
F8	**FCS_CKM.1 (SSH-HMAC)**	**FCS_CKM.4** **FCS_COP.1** **FMT_MSA.2**	**F11** **F9** **F14**
F9	**FCS_COP.1 (SSH-HMAC)**	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	**F8** **F11** **F14**
F10	**FCS_CKM.1 (SSH-RSA)**	**FCS_CKM.4** **FCS_COP.1** **FMT_MSA.2**	**F11** **F12** **F14**
F11	**FCS_CKM.4 (SSH)**	**FCS_CKM.1** **FMT_MSA.2**	**F4, F6, F8, F10** **F14**
F12	**FCS_COP.1 (SSH-RSA)**	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**	**F10** **F11** **F14**
F13	**FMT_SMF.1 (SSH)**	**-/-**	
F14	**FMT_MSA.2 (SSH)**	**ADV_SPM.1** **FDP_IFC.1** **FMT_MSA.1** **FMT_SMR.1**	**Table 13 AS.11** **F2** **N/A** **N/A**

ID	*SFR*	*Depends*	*Satisfied by*
F15	**FMT_MSA.3 (SSH)**	**FMT_MSA.1** **FMT_SMR.1**	**N/A** **N/A**
G1	**FPT_STM.1 (ENV)**	**-/-**	**IT environment**

Table 12 SFRs' dependencies

Application note:
The **FMT_SMR.1** SFR that **FMT_MSA.3 (FW)**, **FMT_MSA.3 (IPSEC)**, **FMT_MSA.2 (SSH)**, **FMT_MSA.3 (SSH)**, **FMT_MSA.2 (IKE)** and **FMT_MSA.3 (IKE)** depend on is not applicable for the TOE because it does not allow users to take different roles in the environment.

Since roles do not need to be enforced on the TOE, the SFRs which specify restrictions or abilities of roles are not applicable here. This means that the **FMT_MSA.1** SFRs on which **FMT_MSA.3 (FW)**, **FMT_MSA.3 (IPSEC)**, **FMT_MSA.2 (IKE)**, **FMT_MSA.3 (IKE)**, **FMT_MSA.2 (SSH)** and **FMT_MSA.3 (SSH)** depend are not necessary.

The **FCS_COP.1 (IPSEC-AES)** and **FCS_COP.1 (IPSEC-HMAC)** depend on a **FCS_CKM.1** SFR for key creation. The keying material for the in-kernel IPSec transforms is generated dynamically by the IKE daemons, which are part of the environment. Thus the **FCS_CKM.1 (IKE)** SFR satisfies the dependency. The algorithms and key sizes are dictated by the configuration of the IKE daemons, so that requirement **FMT_MSA.2 (IKE)** also enforces a requirement on **FCS_COP.1 (IPSEC-AES)** and **FCS_COP.1 (IPSEC-HMAC)**, which makes a special **FMT_MSA.2** for the IPsec cryptographic operations unnecessary.

The **FDP_IFF.1** SFR on which **FDP_IFC.1 (IPSEC)** depends is supplied by the TOE's environment's SFR **FDP_IFF.1 (IKE)**. This is because all security attributes of IPsec transforms are the result of an IKE protocol run, which in turn will only proceed if both parties can authenticate to each other. There is no iteration of **FDP_IFF.1** for the IPSEC-SFP because of this direct causal dependency of authenticated key agreement and IPsec transforms.

FPT_STM.1 (ENV) is satisfied by the IT environment.

ID	*SAR*	*Depends*	*Satisfied by*
AS.1	**ACM_AUT.1**	**ACM_CAP.4**	AS.2
AS.2	**ACM_CAP.4**	**ALC_DVS.1**	AS.14
AS.3	**ACM_SCP.2**	**ACM_CAP.4**	AS.2
AS.4	**ADO_DEL.2**	**ACM_CAP.4**	AS.2

ID	*SAR*	*Depends*	*Satisfied by*
AS.5	**ADO_IGS.1**	**AGD_ADM.1**	AS.12
AS.6	**ADV_FSP.2**	**ADV_RCR.1**	AS.10
AS.7	**ADV_HLD.2**	**ADV_FSP.1** **ADV_RCR.1**	AS.6 AS.10
AS.8	**ADV_IMP.1**	**ADV_LLD.1** **ADV_RCR.1** **ALC_TAT.1**	AS.9 AS.10 AS.16
AS.9	**ADV_LLD.1**	**ADV_HLD.1** **ADV_RCR.1**	AS.7 AS.10
AS.10	**ADV_RCR.1**		
AS.11	**ADV_SPM.1**	**ADV_FSP.1**	AS.6
AS.12	**AGD_ADM.1**	**ADV_FSP.1**	AS.6
AS.13	**AGD_USR.1**	**ADV_FSP.1**	AS.6
AS.14	**ALC_DVS.1**		
AS.15	**ALC_LCD.1**		
AS.16	**ALC_TAT.1**	**ADV_IMP.1**	AS.8
AS.17	**ALC_FLR.2**		
AS.18	**ATE_COV.2**	**ADV_FSP.1** **ATE_FUN.1**	AS.6 AS.20
AS.19	**ATE_DPT.1**	**ADV_HLD.1** **ATE_FUN.1**	AS.7 AS.20
AS.20	**ATE_FUN.1**		

ID	*SAR*	*Depends*	*Satisfied by*
AS.21	**ATE_IND.2**	**ADV_FSP.1** **AGD_ADM.1** **AGD_USR.1** **ATE_FUN.1**	AS.6 AS.12 AS.13 AS.20
AS.22	**AVA_MSU.2**	**ADO_IGS.1** **ADV_FSP.1** **AGD_ADM.1** **AGD_USR.1**	AS.5 AS.6 AS.12 AS.13
AS.23	**AVA_SOF.1**	**ADV_FSP.1** **ADV_HLD.1**	AS.6 AS.7
AS.24	**AVA_VLA.2**	**ADV_FSP.1** **ADV_HLD.1** **ADV_IMP.1** **ADV_LLD.1** **AGD_ADM.1** **AGD_USR.1**	AS.6 AS.7 AS.8 AS.9 AS.12 AS.13

Table 13: SAR

The dependencies between the SFRs without iteration follow directly from CC. Their rationale is justified by the CC catalogue. The dependencies between the SAR follow directly from CC. The dependency rationale is justified by the CC catalogue.

8.3.5 Assurance Requirements Rationale

The TOE claims compliance to **EAL4** level of assurance augmented by **ALC_FLR.2**. As [CC_3] describes it, the level **EAL4** indicates that the product is methodically designed, tested, and reviewed.

The assurance requirements for life cycle support has been augmented by **ALC_FLR.2** (flaw reporting procedures) to account for regular bug fixes for the TOE.

This is considered appropriate for attackers who have access to publicly available exploit tools and vulnerability announcements

8.3.6 Strength of Function Claim Rationale

The overall strength of function claim for the TOE is 'SOF-medium'. The claim is applicable to the SFR **FIA_UAU.2**. The TOE has security functions that are realized by probabilistic or permutational mechanisms. While the minimal strength of function for **SF_DF.4** is 'not applicable', the minimal strength of function for **SF_AI.1** is 'SOF-medium'. This claim is reasonable for users with an attack potential higher than 'low'.

8.4 TOE Summary Specification Rationale

Table 14 shows how the SF are mapped onto the principal SFRs.

SF	Rationale
SF_AU.1	This SF describes for which classes of events audit data is generated. It meets **FAU_GEN.1EX**.
SF_AU.2	This SF describes the data that is written to the audit records for datagrams. It meets **FAU_GEN.1EX**.
SF_AU.3	This SF describes the display and search functions for audit records. It meets **FAU_GEN.1EX**, **FAU_SAR.1** and **FAU_SAR.3**.
SF_DF.1	This SF describes the flow control in the Firewall components. It meets the **FMT_MSA.3 (FW)**, **FDP_IFC.1 (FW)** and **FDP_IFF.1 (FW)** SFRs.
SF_DF.2	This SF describes IP fragment reassembly on the Firewall components and meets SFR **FDP_IFF.1 (FW)**.
SF_DF.3	This SF describes the treatment of spoofed and source-routed datagrams, it meets **FDP_IFF.1 (FW)**.
SF_DF.4	This SF describes protection of connections between the Firewall components, it meets **FDP_ITT.1 (IPSEC)**, **FDP_IFC.1 (IPSEC)**, **FCS_COP.1 (IPSEC-AES)**, **FCS_COP.1 (IPSEC-HMAC)** and **FCS_CKM.4 (IPSEC)**.
SF_DF.5	This SF describes modification of headers to inhibit hijacking attacks. It meets an element of **FDP_IFF.1 (FW)**.
SF_AC.1	This SF describes the capability of the authorised administrator for configuration. It meets **FMT_MSA.3 (FW)**, **FMT_MSA.3 (IPSEC)** and is supported by the **FMT_SMF.1 (FW)**, **FMT_SMF.1 (IPSEC)**, **FMT_SMF.1 (Gen)** SFRs.
SF_AI.1	This SF describes the enforcement of authentication and identification. It meets the **FIA_UID.2** and **FIA_UAU.2** SFRs.

Table 14: Summary Specification Rationale for SFs

Table 15 shows how the TOE's SFRs are mapped to security functions.

SFR	*Rationale*
FDP_IFC.1 (FW)	This SFR defines that flow control should be applied to data flowing through the Firewall component, and thus maps to **SF_DF.1**.
FDP_IFF.1 (FW)	The **FDP_IFF.1.1 (FW)** element defines the header fields to which filter rules may be applied as in **SF_DF.1**. Element **FDP_IFF.1.2 (FW)** defines the conditions under which information flow shall be allowed between Firewall components and thus is necessary for **SF_DF.1**. The **FDP_IFF.1.3 (FW)** element requires the re-assembly of fragments as in **SF_DF.2**. The **FDP_IFF.1.4 (FW)** element describes possible modification of headers to obstruct hijacking attacks and so maps directly to **SF_DF.5**. The **FDP_IFF.1.6 (FW)** states that no flows are explicitly allowed and so contributes to **SF_DF.1**. The **FDP_IFF.1.6 (FW)** element requires discarding spoofed packets and packets with source routing options as in **SF_DF.3**.
FMT_SMF.1 (FW)	This SFR defines the management functions available to the authorised administrator for configuration of firewall rules, and thus maps to **SF_AC.1**.
FMT_MSA.3 (FW)	This SFR enforces restrictive defaults and thus maps to **SF_AC.1** and **SF_DF.1**.
FDP_ITT.1 (IPSEC)	The SFR requires the IPSEC-SFP to be enforced and thus follows **SF_DF.4**.
FDP_IFC.1 (IPSEC)	The SFR defines on which data flows the IPSEC-SFP should apply and so maps to **SF_DF.4**.
FCS_COP.1 (IPSEC-AES)	This SFR defines a cryptographic operation to protect data against disclosure and thus maps to **SF_DF.4**.
FCS_COP.1 (IPSEC-HMAC)	This SFR defines a cryptographic operation to protect data against unauthorised modification and replay attacks and thus maps to **SF_DF.4**.
FCS_CKM.4 (IPSEC)	This SFR requires destruction of cryptographic keys by overwriting with zeros and thus maps to **SF_DF.4**.
FMT_MSA.3 (IPSEC)	This SFR enforces restrictive defaults and thus maps to **SF_AC.1**.
FMT_SMF.1 (IPSEC)	This SFR defines the management functions available for configuration of IPsec connections between Firewall components, and thus maps to **SF_AC.1**.
FAU_GEN.1EX	The SFR defines the generation of audit data and thus maps to the security functions **SF_AU.1**, **SF_AU.2**, **SF_AU.3**.

SFR	*Rationale*
FAU_SAR.1	The SFR requires the audit records to be suitable for interpretation and thus maps to **SF_AU.3**.
FAU_SAR.3	This SFR defines the search criteria for audit data and thus maps to **SF_AU.3**.
FMT_SMF.1 (Gen)	The SFR defines the general management functions available for configuration of the Firewall components and thus maps to **SF_AC.1**.
FIA_UAU.2	The SFR forbids any action before successful authentication and thus maps to **SF_AI.1**.
FIA_UID.2	The SFR forbids any action before successfully identification and thus maps to **SF_AI.1**.

Table 15: Summary Specification Rationale for SFRs

9 Appendix

9.1 Tailored SFRs

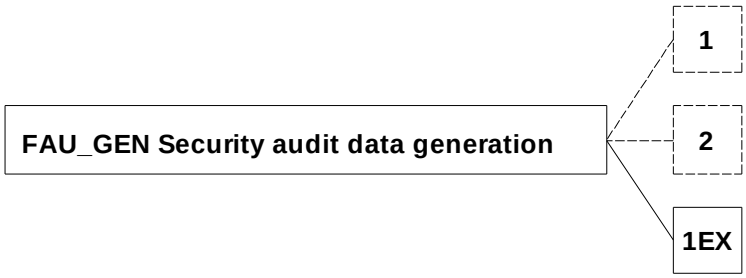
9.1.1 Class FAU: Security audit

9.1.1.1 Security audit data generation (FAU_GEN)

9.1.1.1.1 Family behaviour

The family has been enhanced by one component **FAU_GEN.1EX**. It is intended to be a replacement for **FAU_GEN.1** when the security function does not support audit generation for startup and shutdown of the audit functions. It also removes the mandatory configurability of the audit record generation. This component can also be used as a replacement for the dependencies on **FAU_GEN.1**, because all other audit events can be specified as in **FAU_GEN.1**.

Component levelling



The components **FAU_GEN.1** and **FAU_GEN.2** are already described in [CC_2]. Only **FAU_GEN.1EX** is new and described in this appendix.

Management: for **FAU_GEN.1EX**

There are no management activities foreseen.

Audit: for **FAU_GEN.1EX**

There are no actions identified that should be auditable if **FAU_GEN** Security audit data generation is included in the PP/ST.

9.1.1.1.2 FAU_GEN.1EX Audit data generation

Hierarchical to: No other components.

FAU_GEN.1EX.1 The TSF shall generate an audit record of the following auditable events:

1. All auditable events for the **[selection: choose one of: *minimum, basic, detailed, not specified*]** level of audit; and
2. **[assignment: *other specifically defined auditable events*]**.

FAU_GEN.1EX.2 The TSF shall record within each audit record at least the following information:

1. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
2. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: *other audit relevant information*]**.

Dependencies: **FPT_STM.1** Reliable time stamps.

10 Glossary

IPSec protocol suite: A set of protocols based on IP/UDP to enable two machines to initiate a key exchange, authenticate each other, negotiate encryption and authentication mechanisms, and subsequently encrypt and/or authenticate selected data passing between them.

Cryptographic (SSH or IPsec) Transform: A series of protocol steps between two parties consisting of

1. agreement on new encryption and/or authentication keys when necessary
2. application of the keys to a stream of data
3. transmission of encrypted, authenticated data between the parties
4. decryption and check of authentication on the respective endpoints

11 Abbreviations

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
DH	Diffie-Hellman
ESP	Encapsulated Security Payload
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security protocol suite
ISAKMP	Internet Security Association Key Management Protocol
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
TCP	Transmission Control protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol

12 Bibliography

[CC_1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 2.3

[CC_2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 2.3

[CC_3] Common criteria for Information Technology Security Evaluation, Part [RFC3602]3: Security assurance requirements, Version 2.3

[DOC] GeNUScreen Installations- und Konfigurationshandbuch Version 1.0 Z

[PF] OpenBSD pf.conf Manual http://www.openbsd.org/cgi-bin/man.cgi?query=pf.conf&apropos=0&sektion=0&manpath=OpenBSD+3.9&arch=i386&format=html

[PKCS #1, v2.0] RSA Cryptography Standards Version 2.0 http://www.ietf.org/rfc/rfc2437.txt

[RFC2104] HMAC: Keyed-Hashing for Message Authentication http://www.ietf.org/rfc/rfc2104.txt

[RFC2409] The Internet Key Exchange (IKE) http://www.ietf.org/rfc/rfc2409.txt

[RFC3526] More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) http://www.ietf.org/rfc/rfc3526.txt

[RFC3602] The AES-CBC Cipher Algorithm and Its Use with IPsec http://www.ietf.org/rfc/rfc3602.txt

[RFC4253] SSH Transport Layer Protocol http://www.ietf.org/rfc/rfc4253.txt

[FIPS-180-2] Secure Hash Standard http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[FIPS-197] Advanced Encryption Standard http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf