GeNUGate 6.3

Security Target

Version 9

17 Aug 2010

GeNUA mbH

Domagkstr. 7, D-85551 Kirchheim, Germany

Table of Contents

1 ST Introduction

1.1 ST Reference

	ST Reference
ST Title	GeNUGate 6.3 Security Target
Version	Version 9
Developer	GeNUA mbH
Date	17 Aug 2010

1.2 TOE Reference

	TOE Reference
TOE Title	GeNUGate 6.3
Product Name	GeNUGate 6.3 Z Patchlevel 7

1.3 TOE Overview

The TOE **GeNUGate Firewall 6.3** is part of a larger product, the firewall **GeNUGate 6.3 Z**, which consists of hardware and software. The TOE **GeNUGate Firewall 6.3** itself is part of the shipped software. The operating system is a modified OpenBSD.

GeNUGate 6.3 Z is a combination of an application level gateway (ALG) and a packet filter (PFL), which are implemented on two different systems (see figure 1). It is thus a two-tiered firewall. The network connection between ALG and PFL is a cross cable.

Besides the network interface to the PFL, the ALG has (at least) three more interfaces to connect to the external network, the administration network and the secure server network (a DMZ). For the high availability option, the ALG needs another network interface for the HA network. The PFL has a second interface which is connected to the internal network, and optional interfaces for further DMZs.

The aim of the firewall is to control the IP-traffic between the different connected networks. Therefore the ALG uses proxies that control all data transmitted between the different networks, while the PFL uses packet filtering as an additional means to control all data that is sent to and from the internal network.

To mitigate hardware failures the GeNUGate has a high availability option where two or more GeNUGate systems are operating in parallel and take over a failing system.

The TOE, **GeNUGate Firewall 6.3**, consists of the software that implements the IP traffic control and related functionality of the firewall. This includes the proxies, the modified OpenBSD kernel modules IP-stack, packet filter, but also other supportive functionality as logging of security events (see the next section for a more accurate definition of the TOE scope and boundary).

The TOE has a special maintenance mode. During normal operation IP packets are handled as usual and the file system is secured by the BSD flags. In maintenance mode, however, the BSD flags can be altered for maintenance operation. In this mode all IP packets are dropped for security reasons.

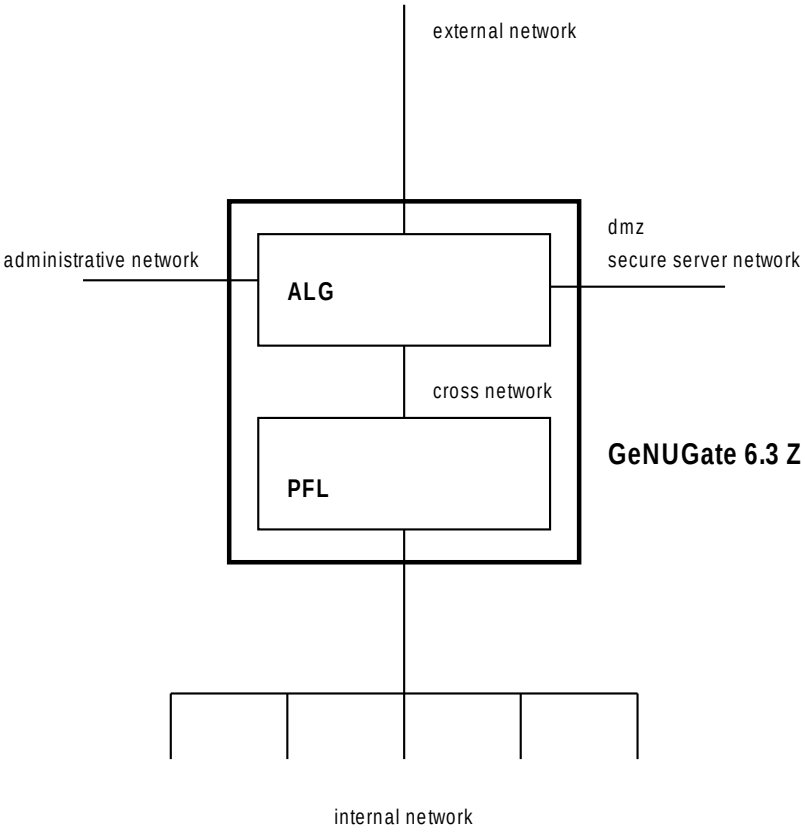


Figure 1: GeNUGate 6.3 Z Overview

GeNUGate product family includes the following security features:

- The ALG does not perform IP forwarding.
- The modified OpenBSD kernel performs extra spoofing checks. The source and destination address of the IP packet are checked against the IP address (and netmask) of the receiving interface.
- The modified OpenBSD kernel logs all events that occur while checking incoming IP packets.
- The filter rules of the PFL cannot be modified during normal operation.
- Proxies that accept connections from the connected networks run in a restricted runtime environment.
- The log files are analysed online.
- The administrators are notified about security relevant events.
- File system flags prohibit the deletion of log messages.
- The internal network is protected by a two-tiers security architecture that filter on different levels of the network stack (ALG and PFL).
- The TOE has a special maintenance mode. During normal operation IP packets are handled as usual and the file system is secured by the BSD flags. In maintenance mode, however, the BSD flags can be altered for maintenance operation. In this mode all IP packets are dropped for security reasons.

- To mitigate hardware failures the GeNUGate has a high availability option where two or more GeNUGate systems are operating in parallel and take over a failing system. The different systems synchronize their configuration with one another.

1.3.1 Required non-TOE Hardware/Software/Firmware

The product is based on OpenBSD 4.4 that runs on a large scale of hardware using different INTEL compatible processors. The ALG needs at minimum an Intel Celeron with 1 GB memory and 4 1GBit network interfaces (the high availabilit option needs at least five interfaces). The PFL needs an Intel Celeron with 512 MB memory and 2 1GBit network interfaces. Nonetheless the hardware is selected by the manufacturer in order to guarantee proper execution of the product.

For the high availability option a correctly configured OSPF router is needed in the internal network.

1.4 TOE Description

The TOE **GeNUGate Firewall 6.3** is used to control the connections and data transfer between different networks, where each network has different security needs and different threat levels for the other networks. **GeNUGate 6.3 Z** is a combination of an application level gateway (ALG) and a packet filter (PFL), which are implemented on two different systems. It is thus a two-tiered firewall. The network connection between ALG and PFL is a cross cable.

The TOE can be configured in such a way that the security needs for each network are optimally met. A standard configuration consists of the following networks connected to the TOE:

- internal network: This is the network that has to be secured against attacks from the external network. Usually only a few services from the internal network are accessible from the external network, secured by user authentication. This is the network that is secured by both the ALG and the PFL, using filtering mechanisms at two different levels of the IP stack. This network is usually controlled by a defined security policy.
- external network: This is the most insecure network, e. g. the internet. In general, no security policy exists, and all kind of attacks can occur in this network.
- administrative network: This network is used to allow a secure administration of the TOE. This network is isolated from all other networks and only administrators have access. The usual access is through the HTTPS web interface, but an SSH access for debugging and maintenance operation is also available.
- secure server network: This network allows access to common services from the external network, without the need to open the internal network. Usually, Web- and FTP-servers are installed in this network. This network is usually controlled by a defined security policy.
- HA network: This network is necessary for the high availability option. It is used to synchronize the configuration between the systems.

The TOE includes the following security features:

- The ALG does not perform IP forwarding.
- The modified OpenBSD kernel performs extra spoofing checks. The source and destination address of the IP packet are checked against the IP address (and netmask) of the receiving interface.
- The modified OpenBSD kernel logs all events that occur while checking incoming IP packets.

- The filter rules of the PFL cannot be modified during normal operation.
- Proxies that accept connections from the connected networks run in a restricted runtime environment.
- The log files are analysed online.
- The administrators are notified about security relevant events.
- File configuration of the system flags prohibit the deletion of log messages.
- The internal network is protected by a two-tiers security architecture that filter on different levels of the network stack (ALG and PFL).
- The TOE has a special maintenance mode. During normal operation IP packets are handled as usual and the file system is secured by the BSD flags. In maintenance mode, however, the BSD flags can be altered for maintenance operation. In this mode all IP packets are dropped for security reasons.
- To mitigate hardware failures the GeNUGate has a high availability option where two or more GeNUGate systems are operating in parallel and take over a failing system. The different systems synchronize their configuration with one another.

1.4.1 The Application Level Gateway

The ALG uses relays to provide and control connections between the different networks. The relays, which are user-space proxies, are necessary, because the kernel of the ALG has no capabilities to forward IP packets. All IP traffic has to be reassembled and transferred to user space by the kernel. The proxies examine the data and perform most of the filtering and controlling function. The protocol-specific proxies have enough knowledge about the respective protocol in order to filter possible threatening or insecure protocol elements. The proxies implement several access control lists that allow a fine grained control for the usage of services. All proxies can be transparent with respect to the source and/or destination address, so that the ALG can be configured transparent with respect to IP addressing. The ALG checks for source or destination spoofing attacks.

The TOE provides proxy support for the following services/protocols:

- IP: This relay can be used for all IP protocols (besides ICMP ECHO, UDP, or TCP, which are supported by their own proxies). It is a very generic proxy and has no knowledge about any application level protocol.
- PING: This relay is used if the ALG should transmit ICMP ECHO REQUEST and ICMP REPLY packets from one network into another.
- UDP: This relay is a generic proxy than can be used for almost any service that is based on UDP.
- TCP: This relay is a generic proxy that can be used for services based on TCP. It has no knowledge about application level protocols. It can handle SSL connections.
- NNTP: This relay is an application specific proxy for the NNTP protocol. All protocol commands are analysed and can be filtered. It has an interface to an optional virus scanner.
- POP: This relay is an application specific proxy for the POP protocol. All protocol commands are analysed and can be filtered. It has an interface to an optional virus scanner.
- FTP: This relay is an application specific proxy for the FTP protocol. All protocol commands are analysed and can be filtered. It has an interface to an optional virus scanner.

- HTTP: This relay is an application specific proxy for the HTTP protocol. All protocol commands are analysed and can be filtered. This proxy analyses only the protocol itself, but not the application data that is transported by the HTTP protocol. It is usually used to allow access to a web server that is located in the secure server network from the other networks.
- WWW: This relay is an application specific proxy for the HTTP protocol and its application data. This proxy analyses the HTTP protocol headers and the application data. The content-type of the application data can be used to either filter text data or to scan binary data for viruses. It has an interface to an optional virus scanner. It can handle SSL connections.
- TELNET: This relay is an application specific proxy for the TELNET protocol. All protocol commands are analysed and can be filtered.
- SMTP: This relay is an application specific proxy for the SMTP protocol. All protocol commands are analysed and can be filtered. The mail header and bodies can be filtered. It contains functionality to filter SPAM mail. It has an interface to an optional virus scanner.
- Meta-Relays: LDAP, MSSQL, MySQL, Postgres, NNTP, PPTP, RTSP and SNMPtrap. These are combinations of UDP/TCP-Relays preconfigured for the respective service.

All relays are highly configurable. The preferred configuration method is through HTML forms that are transported by secure https-connections in the administration network.

User identification and authentication can be configured in two ways. Some relays have support for authentication in the respective protocol. These relays can authenticate their users against authentication servers. The side channel authentication allows the usage of special configured relays after user identification at a special web form at the TOE.

1.4.2 The Packet Filter

The internal network has high security needs and is therefore not directly connected to the ALG, but is connected to the PFL. The PFL has at least two network interfaces. One of them is connected to the ALG with a cross cable. The (small) network is called the cross network. The other interface connects to the internal network.

The PFL works as packet filter with a set of filter rules. Only configured TCP connection requests from the cross network are allowed, but there is no restriction for TCP packets from the internal network. In order to allow UDP (and other protocols), extra rules have to be added to the filter rules by administrators.

The PFL is a minimalistic system. It boots from a removable read-only medium (floppy or USB stick with mechanical write protection) and has no other permanent memory. The medium is configured and created at the ALG. Physical access is needed to write the medium at the ALG, transfer it from the ALG to the PFL, and reboot the PFL with the new configuration.

The configuration of the PFL is done through the web based administration tool at the ALG.

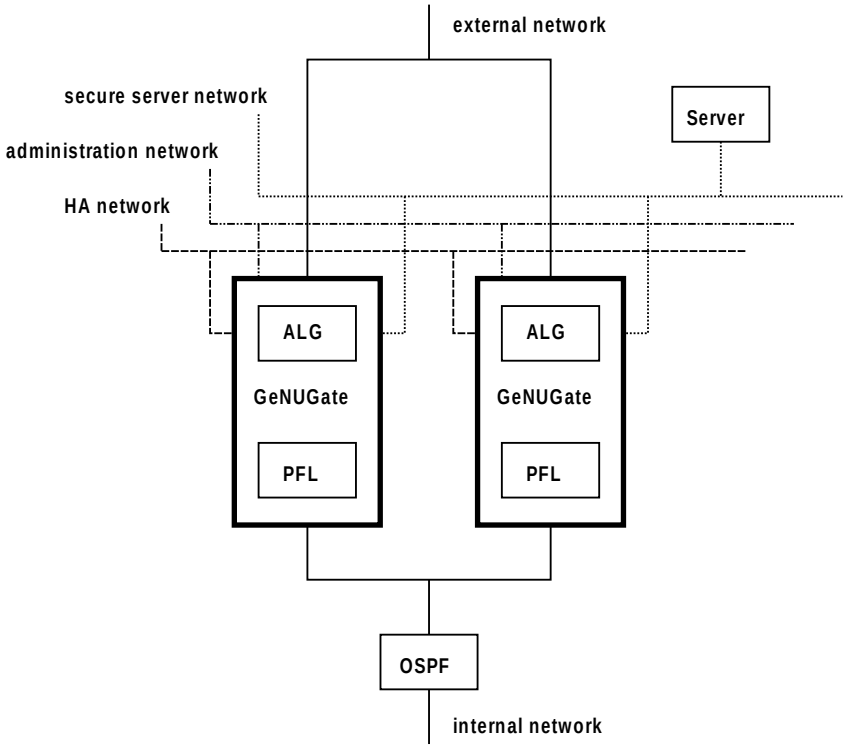


Figure 2: High availability

1.4.3 High Availability (GeNUGate-Cluster)

For a high availability (HA) setup, the HA option is installed on two or more GeNUGates (peers) and they are connected by a separate HA network that is used to synchronise the configuration and negotiate the active HA nodes. If a system fails some other system takes over its services and IP addresses. For this operation an external OSPF router is needed in the internal network. Figure 2 gives an overview for two parallel systems, although more than two are possible.

Table 1: Scope of delivery

Type	Name	Release	Date	Medium
Hardware	GeNUGate 400, 600, 800 or 200 with fourth network interface	N/A		
Software	GeNUGate Firewall	6.3	12.08.2010	CD-ROM
Software	GeNUGate Platform	6.3 Z Patchlevel 7	12.08.2010	CD-ROM
Documentation	Administrator and user guidance manual	6.3 Z	12.08.2010	Manual and CD-ROM
Hardware	PFL floppy/USB stick	N/A		

1.4.4 Physical Scope

Both ALG and PFL run on Intel compatible hardware that works with OpenBSD. As the product **GeNUGate 6.3 Z** is a combination of hardware and software, the hardware components are selected by GeNUA. The end user has no need to check for compatibility. The scope of delivery can be seen in table 1. The TOE is located as software on the CD-ROM.

The physical connections are:

- the network interfaces to the external, internal, secure server and administration networks
- connections for the keyboard, monitor, and serial interfaces at the ALG and PFL
- power supply

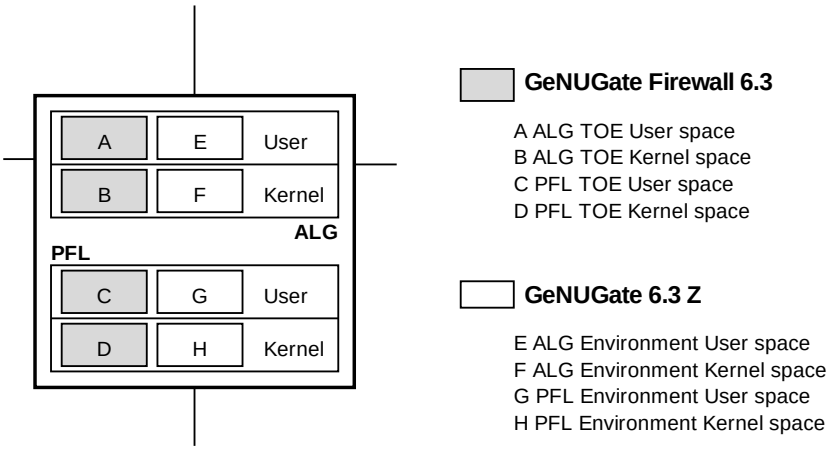


Figure 3: Scope and boundary

Figure 3 gives a schematic overview on the TOE and its environment. It divides the software on ALG and PFL into user and kernel space parts. On both systems, the user and the kernel space contain part of the TOE, and part of the environment. The following table lists the components in each part. The components for the parts **A**, **B**, **C** and **D** are part of the TOE. The components for **E**, **F**, **G**, and **H** are part of the environment.

A ALG TOE User space	relays, logging, administration webserver, user webserver, configuration commands, system startup.
B ALG TOE Kernel space	network layer, logging, system call interface.
C PFL TOE User space	logging, system startup.
D PFL TOE Kernel space	network layer, logging, system call interface.
E ALG Environment User space	sip-relay, squid, sendmail, bind, ntpd, GeNUGate options: VPN, GeNUAuth, URL filter, virus scanner; authentication methods, os environment.
F ALG Environment Kernel space	process management, memory management, device drivers, socket layer, tty driver, I/O system, IPC operation, file systems.
G PFL Environment User space	os environment.
H PFL Environment Kernel space	process management, memory management, device drivers, socket layer, tty driver, I/O system, IPC operation, file systems.

The different parts have the following interfaces with one another:

A	**B**	System call interface
A	**E**	Interprocess communication (via system call interface)
B	**F**	Kernel interfaces between the kernel components
C	**D**	System call interface
C	**G**	Interprocess communication (via system call interface)
D	**H**	Kernel interfaces between the kernel components
ALG	**PFL**	serial connection
ALG	**PFL**	network connection

Depending on their roles, the users interact with the product in the following ways:

- user: Relay usage (sending and receiving IP packets to and from the TOE)
- user: Authentication dialogues for protocols that allow for authentication.
- user: user web interface to change password
- user: user web interface for the side channel authentication to activate IP addresses
- administrator: administration web interface
- administrator: interactive access at the shell level at the console

1.4.5 Logical Scope

The TOE has the following logical scope:

- the kernel components `network', `packet filter', and `restricted runtime' for ALG and PFL. This components perform the spoofing checks, packet filtering and access control for incoming data. The spoofing checks contain detecting any mismatch between the source and destination address of the IP packet and the IP address and netmask of the receiving interface.
- the relays for IP, ICMP, PING, UDP, TCP, TELNET, FTP, NNTP, POP, SMTP, HTTP and WWW. These components perform the filtering on application level, ACL checks, and calls to the optional virus scanner. The virus scanning functionality is not part of the TOE. The TELNET- and FTP-relay allow for user authentication. The authentication methods themselves are not part of the TOE.
- system startup. This component performs the secure startup of the system and the conversion to maintenance mode.
- the logging and self-monitoring tools. These components perform the accounting and auditing functions.
- administration web server. This component allows the configuration by administrators.
- user web server. This component allows users to change their passwords.
- side channel webserver. This component allows users to activate IP addresses through the side channel mechanism.

The TOE has the following logical boundaries:

- virus scanner interface: delivering the data to the virus scanner and obtaining the scanner result. The virus scanner itself is not part of the TOE.
- external authentication methods: interaction with the authentication service. The authentication methods themselves are not part of the TOE.
- configuration interface: sending forms to and receiving form data from a web browser

The TOE excludes the following options or services from its logical scope:

- the VPN option for GeNUGate 6.3 Z
- the Secure Proxy option for GeNUGate 6.3 Z
- the GeNUAuth option for GeNUGate 6.3 Z
- the URL filter option for GeNUGate 6.3 Z
- authentication services (password, radius, LDAP, S/Key, or cryptocard) either local or remote
- virus scanner engines
- the HTTP proxy squid
- the mail delivery program sendmail
- the bind domain name service
- the ntpd network time protocol daemon
- the relay sip-pair
- although the TCP- and the WWW-Relay support encryption with SSL, the cryptographic support is not part of the TOE.

2 Conformance Claims

2.1 CC conformance Claim

This Security Target is *Part 2 extended* and *Part 3 conformant* to the Common Criteria Version 3.1 Revision 3 (July 2009).

2.2 PP Claim, Package Claim

There are no Protection Profile claims. This Security Target claims to be conformant to the Assurance Packet EAL4 augmented with ALC_FLR.2, ASE_TSS.2 and AVA_VAN.5. These components are defined in CC Part 3.

2.3 Conformance Rationale

The Security Target has no Protection Profile claim, therefore no conformance rationale has to be given.

This Security Target uses extended functional component definitions (see section 5). Therefore it is Part 2 extended. It does not use extended assurance requirements. Therefore it is Part 3 conformant.

3 Security Problem Definition

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.

3.1 Users

The users are listed in table 2.

Table 2: Users

	Users
user	Any person or software agent sending IP packets to or receiving from the TOE. The assumed attack potential is **high**. The general term user is used when it does not matter whether the user did authenticate at the TOE or not.
unauthenticated user	Any person or software agent sending IP packets to or receiving from the TOE that did not authenticate at the TOE. The assumed attack potential is **high**. This term is used for users that did not (yet) authenticate at the TOE.
authenticated user	Any person or software agent sending IP packets to or receiving from the TOE that authenticated at the TOE. The assumed attack potential is **high**.
administrator	These are authenticated users that have the role of an administrator. This role authorises them to change the TOE configuration. Their assumed attack potential is undefined.
auditor	These are authenticated users that have the role of an auditor. This is a restricted administrator role and authorises them to view the TOE configuration. Their assumed attack potential is undefined.

3.2 Assets

The assets are listed in table 3:

Table 3: Assets

	Assets
resources in the connected networks	The resources in the connected networks that the TOE is supposed to protect.
security sensitive data on the TOE	The data on the TOE that contains security sensitive data.

3.3 Threats

The threats are listed in table 4.

Table 4: Threats

	Threats
T.NOAUTH	An unauthenticated user may attempt to bypass the security functions of the TOE and gain unauthenticated access to resources in other connected networks or read, modify or destroy security sensitive data on the TOE. The attack method is exploiting authentication protocol weaknesses.
T.SPOOF	A user may attempt to send spoofed IP packets to the TOE in order to gain unauthorised access to resources in other connected networks. Without spoofing checks the TOE would route a response to the spoofed IP packet into a connected network that the user is not authorised to access.
T.MEDIAT	A user may send non-permissible data through the TOE that result in gaining access to resources in other connected networks.
T.SELPRO	A user may 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.

3.4 Organisational Security Policies

The organisational security policies are listed in table 5.

Table 5: Policies

	Policies
P.AUDIT	All users must be accountable for their actions.
P.AVAIL	A high availability operation must be possible where peers can take over the services of a failing system. (This policy only applies if needed.)

3.5 Assumptions

The assumptions are listed in table 6.

Table 6: Assumptions

	Assumptions
A.PHYSEC	The TOE is physically secure. Only authorised persons have physical access to the TOE.
A.NOEVIL	Administrators and auditors are non-hostile and follow all administrator and auditor guidance; however, they are capable of error. They use passwords that are not easily guessable.
A.ADMIN	All administration is done only in the administration network during normal operation mode.

	Assumptions
A.SINGEN	Information can not flow among the internal, external, or secure server network, unless it passes through the TOE.
A.POLICY	The security policy of the internal network allows only the administrators access to the network components and the network configuration.
A.TIMESTMP	The environment provides reliable timestamps.
A.HANET	The environment provides a physical separate network for TSF data transfer for the optional high availability setup.
A.USER	The users use passwords that are not easily guessable and keep them secret.
A.TRUSTK	The non-TOE parts of the kernel space are trustworthy and do not interfere with the security functions of the TOE.
A.TRUSTU	The non-TOE parts of the user space are trustworthy and do not interfere with the security functions of 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

The security objectives for the TOE are listed in table 7.

Table 7: Objectives

	Objectives
O.IDAUTH	The TOE must identify all network packets from the connected networks. It must check the IP addresses of the packet with the receiving interface to recognize IP-spoofing. It must identify all users before granting access to the security functions of the TOE. It must authenticate the users where an authentication is required.
O.MEDIAT	The TOE must mediate the flow of all data between all connected networks.
O.SECSTA	On start-up, the TOE must not compromise its resources or those of the connected networks.
O.SELPRO	The TOE must have self-protection mechanisms that hinder attempts by users to bypass, deactivate or tamper with TOE security functions.
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.
O.ACCOUN	The TOE must provide user accountability for data flows through the TOE and for the use of the security functions of administrators.

	Objectives
O.SECFUN	The TOE must allow administrators to use the TOE security functions and must ensure that only authorised administrators have access to the functionality.
O.AVAIL	The TOE must optionally provide a fail over solution where the services of a failing system are taken over by a peer machine.

4.2 Security Objectives for the Environment

The security objectives for the environment are listed in table 8.

Table 8: Objectives for the environment

	Objectives for the environment
OE.PHYSEC	Those responsible for the TOE must assure that the TOE is placed at a secured place where only authorised people have access.
OE.NOEVIL	Those responsible for the TOE must assure that all administrators and auditors are competent, regularly trained and execute the administration in a responsible way.
OE.ADMIN	Those responsible for the TOE must assure that administration is only done in the administration network during normal operation mode.
OE.SINGEN	Those responsible for the TOE must assure that the TOE is the only connection between the different networks.
OE.POLICY	Those responsible for the TOE must assure that the security policy for the internal network allows only administrators access to the network components and the network configuration. They must assure that the policy is maintained.
OE.TIMESTMP	The IT-environment must supply reliable timestamps for the TOE.
OE.HANET	The IT-environment must supply a physical network for transfer of TSF data between nodes for the optional high availability setup.
OE.USER	Those responsible for the TOE must assure that the users follow the user guidance, especially that they choose not easily guessable passwords and that they keep them secret.
OE.TRUSTK	The IT-environment must assure that the non-TOE parts of the kernel space do not interfere with the security functions of the TOE.
OE.TRUSTU	The IT-environment must assure that the non-TOE parts of the user space do not interfere with the security functions of the TOE.

4.3 Security Objectives Rationale

This chapter contains the ST security objectives rationale. It must show that the security objectives are consistent.

Table 9 shows that all security objectives stated in this ST can be mapped to the stated threats, assumptions and OSP. All threats, assumptions and OSP are matched by at least one security objective.

Table 9: Threat rationale

Threat	Objective	Security Objectives Rationale
T.NOAUTH	**O.IDAUTH** **O.SECSTA** **O.SECFUN**	The objective O.IDAUTH guarantees that all interactions with the TOE are identified. Only authenticated users can use functions that need authorisation. The objective O.SECSTA assures that the threat is also met at start up. The objective O.SECFUN guarantees that only authorised administrators can change the configuration of the TOE.
T.SPOOF	**O.IDAUTH**	The objective O.IDAUTH makes sure that the identification of the IP addresses of every received packet recognises IP spoofing attacks. The objective requires checking the IP address and netmask of the receiving interface, and the source and destination IP address of the packet. The check has to recognize IP spoofing attacks, i.e. the IP packet was not expected at that interface.
T.MEDIAT	**O.MEDIAT**	The objective O.MEDIAT (mediation of all network data) prevents that non-permissible data is sent across the TOE.
T.SELPRO	**O.SELPRO** **O.SECSTA** **O.IDAUTH** **O.SECFUN**	The self protection objective O.SELPRO prevents reading, modifying or destroying security sensitive data on the TOE. The objective O.SECSTA assures that the threat is also met at start-up. O.IDAUTH and O.SECFUN guarantees that only authorised administrators can read, modify, or destroy security sensitive data on the TOE.

Table 10 shows that each policy is met by at least one security objective and that all policies have been addressed.

Table 10: Policy rationale

Policy	Objective	Security Objectives Rationale
P.AUDIT	**O.ACCOUN** **O.AUDREC**	The objective O.ACCOUN (accounting of all user interactions and all security related events), make sure that all audit trails are written. The (possible) loss of audit data is recognised by O.AUDREC.
P.AVAIL	**O.AVAIL**	The objective O.AVAIL provides the optional high availability policy request.

Table11 shows that all assumptions are met by objectives for the environment.

Table 11: Assumption rationale

Assumption	Objective	Security Objectives Rationale
A.PHYSEC	**OE.PHYSEC**	This objective assures that the assumption about a physically secure TOE can be made.
A.NOEVIL	**OE.NOEVIL**	This objective assures that the administrators and auditors are trained and therefore that they are no threat to the TOE.
A.ADMIN	**OE.ADMIN**	This objective assures that the administration only occurs in a distinct network, only used for administration during normal operation mode.
A.SINGEN	**OE.SINGEN**	This objective assures that the TOE can not be bypassed and therefore assures that the assumption is met.
A.POLICY	**OE.POLICY**	This objective assures that an assumption about the security policy can be made.
A.TIMESTMP	**OE.TIMESTMP**	This objective provides reliable timestamps.
A.HANET	**OE.HANET**	This objective provides the extra network to transfer TSF data between nodes in the optional HA setup.
A.USER	**OE.USER**	This objective assures that the users use approriate passwords and keep them secret.
A.TRUSTK	**OE.TRUSTK**	This objective assures that the non-TOE parts of the kernel space are trustworthy.
A.TRUSTU	**OE.TRUSTU**	This objective assures that the non-TOE parts of the user space are trustworthy.

5 Extended Components Definition

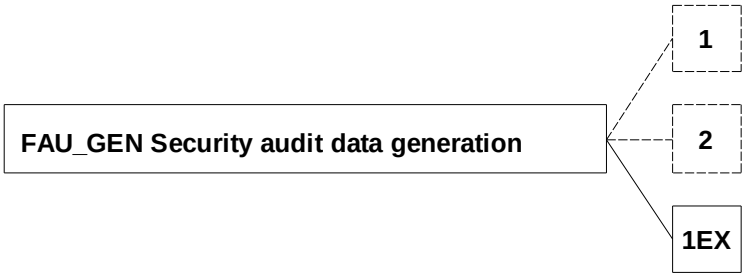
5.1 Class FAU: Security audit

5.1.1 Security audit data generation (FAU_GEN)

5.1.1.1 Family behaviour

The family has been enhanced by one component **FAU_GEN.1EX**. It is thought as a replacement for **FAU_GEN.1** when the security function do not support audit generation for startup and shutdown of the audit functions. 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**.

5.1.1.2 Component levelling



The components **FAU_GEN.1** and **FAU_GEN.2** are already described in CC Part2. Only **FAU_GEN.1EX** is new and described in this chapter.

5.1.1.3 Management: for FAU_GEN.1EX

There are no management activities foreseen.

5.1.1.4 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.

5.1.1.5 FAU_GEN.1EX Audit data generation

Hierarchical to: No other components.

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

a) All auditable events for the [selection: choose one of: minimum, basic, detailed, not specified] level of audit; and

b) [assignment: other specifically defined auditable events].

FAU_GEN.1EX.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, [assignment: other audit relevant information]

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

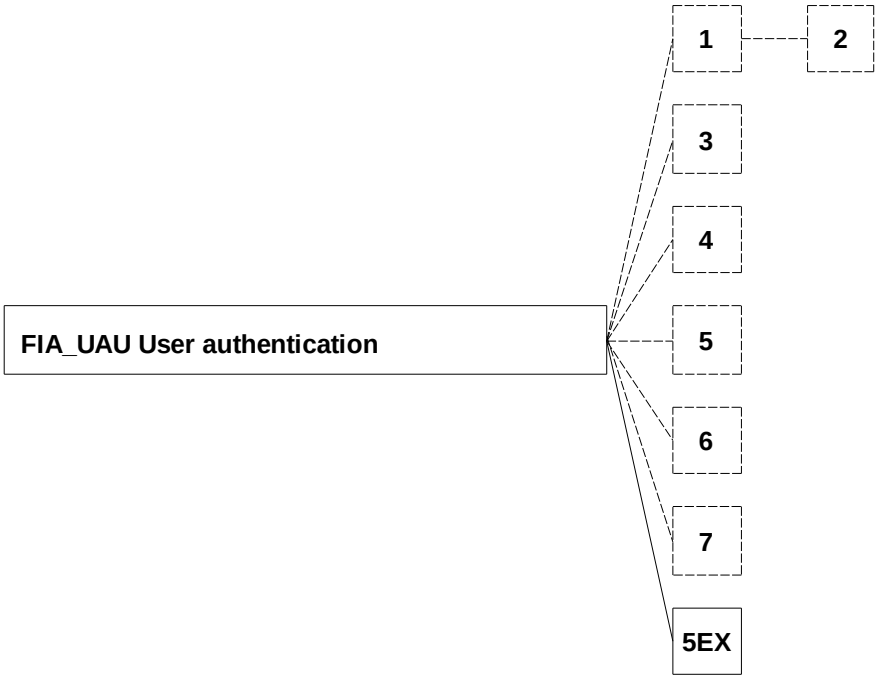
5.2 Class FIA: Identification and authentication

5.2.1 User authentication (FIA_UAU)

5.2.1.1 Family behaviour

The family has been enhanced by one component **FIA_UAU.5EX**. It is thought as a replacement for **FIA_UAU.5** when the proper authentication is done by an external means. This component can also be used as a replacement for the dependencies on **FIA_UAU.5**, because it requires the same functionality.

5.2.1.2 Component levelling



The components **FIA_UAU.1**, **FIA_UAU.2**, **FIA_UAU.3, FIA_UAU.4**, **FIA_UAU.5**, **FIA_UAU.6** and **FIA_UAU.7** are already described in CC Part2. Only **FIA_UAU.5EX** will be described in this chapter.

5.2.1.3 Management: for FIA_UAU.5EX

The following actions could be considered for the management functions in FMT:

a) the management of authentication mechanisms;

b) the management of the rules for authentication.

5.2.1.4 Audit: for FIA_UAU.5EX

The following actions should be auditable if **FAU_GEN** Security audit data generation is included in the PP/ST:

a) Minimal: The final decision on authentication;

b) Basic: The result of each activated mechanism together with the final decision.

5.2.1.5 FIA_UAU.5EX External authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5EX.1 The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication by external means.

FIA_UAU.5EX.2 The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].

Dependencies: No dependencies

5.3 Class FPT: Protection of the TSF

5.3.1 Simple Self Test (FPT_SST)

5.3.1.1 Family behaviour

The family defines the requirements for the self-testing of the TOE with respect to some expected correct operation. Examples are expected running processes or expected files at some location in the file system. These tests can be carried out at start-up, periodically, at the request of the authorised user, or when other conditions are met. The actions to be taken by the TOE as the result of self testing are defined in other families.

The requirements of this family are also needed to detect the corruption of TOE executable code (i.e. TOE software) and TOE data by various failures that do not necessarily stop the TOE's operation (which would be handled by other families). These checks must be performed because these failures may not necessarily be prevented. Such failures can occur either because of unforeseen failure modes or associated oversights in the design of hardware, firmware, or software, or because of malicious corruption of the TOE due to inadequate logical and/or physical protection.

5.3.1.2 Component levelling

FPT_SST.1 TOE testing, provides the ability to test the TOE's correct operation. These tests may be performed at start-up, periodically, at the request of the authorised user, or when other conditions are met. It also provides the ability to verify the integrity of TOE data and executable code.

5.3.1.3 Management: for FPT_SST.1

The following actions could be considered for the management functions in FMT:

a) management of the conditions under which TOE self testing occurs, such as during initial start-up, regular interval, or under specified conditions;

b) management of the time interval if appropriate.

5.3.1.4 Audit: for FPT_SST.1

The following actions should be audited if **FAU_GEN** Security audit data generation is included in the PP/ST:

a) Basic: Execution of the TOE self tests and the results of the tests.

5.3.1.5 FPT_SST.1 TOE testing

Hierarchical to: No other components.

FPT_SST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] to perform the following checks: [assignment: list of self tests]

FPT_SST.1.2 The TSF shall provide authorised users with the capability to query the results of the following checks:[assignment: list of self tests]

Dependencies: No dependencies

6 Security Requirements

This section contains the security functional requirements, the security assurance requirements, and the rationale.

6.1 Security Functional Requirements

All of the security functional requirements in subsection have been drawn from the CC Part 2.

The functional requirements in the subsection (**FPT_SST**, **FAU_GEN.1EX** and **FIA_UAU.5EX**) are not drawn from CC Part 2. The SFRs are listed in this chapter.

In the following, the unmodified text from the functional requirement templates is displayed in a sanserif font. The operation assignment is set in a ***bold italic serif font***. The operations selection and refinement are set in an *italic serif font*.The iterations are done by repeating the requirements and adding a colon and a sequence number. In a few occasions, the text has been modified slightly. The replacement text is placed directly after the crossed-out original text, and is set in an italic serif font.

6.1.1 Class FAU: Security audit

6.1.1.1 Security audit automatic response (FAU_ARP)

FAU_ARP.1	**Security alarms**
FAU_ARP.1.1	The TSF shall take ***configurable actions (log, digest, wall, exec, mail, down, halt)*** upon detection of a potential security violation.

6.1.1.2 Security audit data generation (FAU_GEN)

FAU_GEN.1EX	Audit data generation
FAU_GEN.1EX.1	The TSF shall be able to generate an audit record of the following auditable events: a) All auditable events for the *not specified* level of audit; and b) ***Starting and stopping of the system, changing operation modes, relay configuration, loading of packet filter rules; relay usage, administration, authentication***.
FAU_GEN.1EX.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, ***unspecified log data***.

6.1.1.3 Security audit analysis (FAU_SAA)

FAU_SAA.1	Potential violation analysis
FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the SFR.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of ***configurable events (packet filter violations, selected messages of daemons, selected messages of the relays, selected kernel messages and messages from the processes that implement the self-tests)*** known to indicate a potential security violation; b) ***none***.

6.1.1.4 Security audit review (FAU_SAR)

FAU_SAR.1	Audit review
FAU_SAR.1.1	The TSF shall provide ***administrators and auditors*** with the capability to read ***all audit information*** from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2	Restricted audit review
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3	Selectable audit review
FAU_SAR.3.1	The TSF shall provide the ability to apply ***searches*** of audit data based on ***time, date, process id, additional log data (for relay audit data: relay type, connection state, IP addresses and ports, status of logged event, bytes transferred)***.

6.1.1.5 Security audit event storage (FAU_STG)

FAU_STG.1	**Protected audit trail storage**
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to *prevent* unauthorised modifications to the audit records in the audit trail.

FAU_STG.4	**Prevention of audit data loss**
FAU_STG.4.1	The TSF shall *prevent audited events, except those taken by the authorised user with special rights* and ***execute a configurable action (default: inform the administrators)*** if the audit trail is full.

6.1.2 Class FDP: User data protection

6.1.2.1 Information flow control policy (FDP_IFC)

FDP_IFC.1:1	**Subset information flow control**
FDP_IFC.1.1:1	The TSF shall enforce the ***unauthenticated user SFP*** on ***a) subjects:*** *users* ***that send and receive information through the TOE to one another;*** ***b) information: traffic sent through the TOE from one subject to another;*** ***c) operation: pass information.***

FDP_IFC.1:2	**Subset information flow control**
FDP_IFC.1.1:2	The TSF shall enforce the ***authenticated user SFP*** on ***a) subjects:*** *users* ***that send and receive FTP or TELNET information through the TOE to one another, only after the user initiating the information flow has authenticated at the TOE through the FTP or TELNET authentication mechanism;*** ***b) information: FTP and TELNET traffic sent through the TOE from one subject to another;*** ***c) operation: pass information***.

FDP_IFC.1:3	**Subset information flow control**
FDP_IFC.1.1:3	The TSF shall enforce the ***identified side channel user SFP*** on ***a) subjects:*** *users* ***that send and receive information through the TOE to one another, only after identifying the user by IP address;*** ***b) information: traffic sent through the TOE from one subject to another;*** ***c) operation: pass information***.

FDP_IFC.1:4	**Subset information flow control**
FDP_IFC.1.1:4	The TSF shall enforce the ***authenticated gui user SFP*** on ***a) subjects:*** *users* ***that send and receive information to /from the TOE;*** ***b) information: html form data for side channel authentication and user***

FDP_IFC.1:4	Subset information flow control
	password changes; ***c) operation: pass information***.

FDP_IFC.1:5	Subset information flow control
FDP_IFC.1.1:5	The TSF shall enforce the ***authenticated administrator SFP*** on ***a) subjects:*** *administrators* ***from the administration network that send and receive information to/from the TOE;*** ***b) information: html form data for administration;*** ***c) operation: pass information***.

Application Note: All SFRs in this section have been refined by using (external) users instead of (internal) subjects for item a).

6.1.2.2 Information flow control functions (FDP_IFF)

FDP_IFF.1:1	Simple security attributes
FDP_IFF.1.1:1	The TSF shall enforce the ***unauthenticated user SFP*** based on the following types of subject and information security attributes: ***The header information of network packets, depending on their type:*** ***a) TCP: IP and TCP header;*** ***b) UDP: IP and UDP header;*** ***c) ICMP: IP header and ICMP message;*** ***d) IP: IP header;*** ***The actual date and time.*** ***The incoming and outgoing interfaces.*** ***Additional information depending on the handling relay:*** ***a) IP-relay: none;*** ***b) PING-relay: none;*** ***c) UDP-relay: none;*** ***d) TCP-relay: none;*** ***e) NNTP-relay: protocol and application data;*** ***f) POP-relay: protocol and application data;*** ***g) SMTP-relay: protocol and application data;*** ***h) FTP-relay: protocol data;*** ***i) TELNET-relay: protocol data;*** ***j) HTTP-relay: protocol data;*** ***k) WWW-relay: protocol and application data***.
FDP_IFF.1.2:1	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: ***IP spoofing check pass.*** ***IP option check pass.*** ***The 'connection' is configured:*** ***a) PING-relay: source and destination IP are allowed;*** ***b) IP-relay: source and destination IP and protocol are allowed;*** ***c) UDP-relay: source and destination IP and port are allowed;*** ***d) TCP-relay: source and destination IP and port are allowed;*** ***e) all other relays: source and destination IP and port are allowed.*** ***The ALG packet filter rules pass.***

FDP_IFF.1:1	Simple security attributes
	All ACL checks for the respective relay pass. ***For packets that have a source or destination address from the internal network:*** ***The PFL packet filter rules pass***.
FDP_IFF.1.3:1	The TSF shall enforce the ***none***.
FDP_IFF.1.4:1	The TSF shall explicitly authorise an information flow based on the following rules: ***none***.
FDP_IFF.1.5:1	The TSF shall explicitly deny an information flow based on the following rules: ***The protocol data is filtered:*** ***NNTP-relay: configurable protocol elements from the client are discarded.*** ***POP-relay: configurable protocol elements from the client are discarded.*** ***SMTP-relay: configured checks for mail sender and recipient, greylisting, mail relay lead to the rejection of mail.*** ***FTP-relay: configurable protocol elements from the client are discarded.*** ***TELNET-relay: none*** ***HTTP-relay: The request URIs are blocked if they contain configurable string pattern.*** ***WWW-relay: configurable protocol elements from the client or server are discarded; configurable cookies are filtered.*** ***The application data is filtered:*** ***NNTP-relay: Application data of content-type text/html can be filtered for active contents, if configured. A virus scanner can check the application data. MIME-encoded messages are (recursively) parsed their parts checked like non encoded messages.*** ***POP-relay:Application data of content-type text/html can be filtered for active contents, if configured. A virus scanner can check the application data. MIME-encoded messages are (recursively) parsed their parts checked like non encoded messages.*** ***SMTP-relay: E-mail contents of content-type text/html can be filtered for active contents, if configured. A virus scanner can check the application data. MIME-encoded e-mails are (recursively) parsed their parts checked like non encoded e-mails.*** ***WWW-relay: Server replies of content-type text/html can be filtered for active contents, if configured. A virus scanner can check the application data. MIME-encoded replies are (recursively) parsed their parts checked like non encoded contents***.

FDP_IFF.1:2	**Simple security attributes**
FDP_IFF.1.1:2	The TSF shall enforce the ***authenticated user SFP*** based on the following types of subject and information security attributes: ***The header information of network packets, depending on their type:*** ***a) TCP: IP and TCP header.*** ***The actual date and time.*** ***The interfaces from which the packets are received and to which they are delivered.*** ***Additional information depending on the configurable handling relay:*** ***a) FTP-relay: protocol data;*** ***b) TELNET-relay: protocol data***.
FDP_IFF.1.2:2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: ***IP spoofing check pass.*** ***IP option check pass.*** ***The 'connection' is configured:*** ***Source and destination IP and port are allowed.*** ***The ALG packet filter rules pass.*** ***All ACL checks for the relay pass.*** ***The user can be authenticated by the authentication data.*** ***For packets that have a source or destination address from the internal network:*** ***The PFL packet filter rules pass***.
FDP_IFF.1.3:2	The TSF shall enforce the ***none***.
FDP_IFF.1.4:2	The TSF shall explicitly authorise an information flow based on the following rules: ***none***.
FDP_IFF.1.5:2	The TSF shall explicitly deny an information flow based on the following rules: ***The protocol data is filtered:*** ***FTP-relay: configurable protocol elements from the client are discarded.*** ***TELNET-relay: none***.

FDP_IFF.1:3	Simple security attributes
FDP_IFF.1.1:3	The TSF shall enforce the ***identified side channel user SFP*** based on the following types of subject and information security attributes: ***The header information of network packets, depending on their type:*** ***a) TCP: IP and TCP header.*** ***The actual date and time.*** ***The interfaces from which the packets are received and to which they are delivered***.
FDP_IFF.1.2:3	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: ***IP spoofing check pass.*** ***IP option check pass.*** ***The 'connection' is configured:*** ***TCP-relay: source and destination IP and port are allowed.*** ***The ALG packet filter rules pass.*** ***All ACL checks for the respective relay pass.*** ***For packets that have a source or destination address from the internal network:*** ***The PFL packet filter rules pass.*** ***The sender IP has been registered as a side channel IP address by a authenticated side channel user***.
FDP_IFF.1.3:3	The TSF shall enforce the ***none***.
FDP_IFF.1.4:3	The TSF shall explicitly authorise an information flow based on the following rules: ***none***.
FDP_IFF.1.5:3	The TSF shall explicitly deny an information flow based on the following rules: ***timeout: no data is transported on this connection for a configurable time (default 10 minutes)***.

FDP_IFF.1:4	Simple security attributes
FDP_IFF.1.1:4	The TSF shall enforce the ***authenticated gui user SFP*** based on the following types of subject and information security attributes: ***The header information of network packets, depending on their type:*** ***a) TCP: IP and TCP header.*** ***The actual date and time.*** ***The interfaces from which the packets are received and to which they are delivered.*** ***The authentication data (cookie)***.
FDP_IFF.1.2:4	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: ***IP spoofing check pass.*** ***IP option check pass.*** ***The 'connection' is configured:*** ***TCP-relay: source and destination IP and port are allowed.*** ***The ALG packet filter rules pass.*** ***All ACL checks for the respective relay pass.*** ***For packets that have a source or destination address from the internal network:*** ***The PFL packet filter rules pass.*** ***The authentication data (cookie) is accepted as a valid***.
FDP_IFF.1.3:4	The TSF shall enforce the ***none***.
FDP_IFF.1.4:4	The TSF shall explicitly authorise an information flow based on the following rules: ***none***.
FDP_IFF.1.5:4	The TSF shall explicitly deny an information flow based on the following rules: ***timeout: no data is transported on this connection for a configurable time (default 10 minutes)***.

FDP_IFF.1:5	Simple security attributes
FDP_IFF.1.1:5	The TSF shall enforce the ***authenticated administrator SFP*** based on the following types of subject and information security attributes: ***The header information of network packets, depending on their type:*** ***a) TCP: IP and TCP header.*** ***The actual date and time.*** ***The interfaces from which the packets are received and to which they are delivered.*** ***The authentication data (cookie)***.
FDP_IFF.1.2:5	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: ***IP spoofing check pass.*** ***IP option check pass.*** ***The 'connection' is configured:*** ***TCP-relay: source and destination IP and port are allowed.*** ***The ALG packet filter rules pass.*** ***All ACL checks for the respective relay pass.*** ***For packets that have a source or destination address from the internal network:*** ***The PFL packet filter rules pass.*** ***The request comes from the administration network.*** ***The authentication data (cookie) is accepted as a valid***.
FDP_IFF.1.3:5	The TSF shall enforce the ***none***.
FDP_IFF.1.4:5	The TSF shall explicitly authorise an information flow based on the following rules: ***none***.
FDP_IFF.1.5:5	The TSF shall explicitly deny an information flow based on the following rules: ***timeout: no data is transported on this connection for a configurable time (default 10 minutes)***.

6.1.3 Class FIA: Identification and authentication

6.1.3.1 Authentication failures (FIA_AFL)

FIA_AFL.1	Authentication failure handling
FIA_AFL.1.1	The TSF shall detect when *an administrator configurable positive integer within* ***1 to infinite (default 5)*** unsuccessful authentication attempts occur related to ***authentication for administration, FTP- and TELNET-relay and side channel authentication***.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been *surpassed*, the TSF shall ***prevent the offending user from successfully authentication until an authorised administrator takes some action to make authentication possible for the user in question***.

6.1.3.2 User attribute definition (FIA_ATD)

FIA_ATD.1	User attribute definition
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: ***a) administrative role (or none);*** ***b) user password***.

6.1.3.3 Specification of secrets (FIA_SOS)

FIA_SOS.1	Verification of secrets
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet ***the following metric: the user name is not part of the password; the minimal password length is 6 characters; it consists not exclusively of lower- or uppercase letters***.

6.1.3.4 User authentication (FIA_UAU)

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.

FIA_UAU.5EX	External authentication mechanisms
FIA_UAU.5EX.1	The TSF shall provide ***password, radius, LDAP, S/Key, and cryptocard mechanisms*** to support user authentication by external means.
FIA_UAU.5EX.2	The TSF shall authenticate any user's claimed identity according to the ***following list:*** ***a) administrator authentication: password authentication;*** ***b) user side channel authentication: password, radius, LDAP, S/Key, or cryptocard (as configured by the administrator);*** ***c) user authentication (FTP- and TELNET-relay): password, radius, LDAP, S/Key, or cryptocard (as configured by the administrator)***.

FIA_UAU.6	Re-authenticating
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions: ***a) administrator authentication: timeout after inactivity (default 10 minutes, can be configured by an administrator);*** ***b) user side channel authentication: after inactivity (default 10 minutes, can be configured by an administrator)***.

6.1.3.5 User identification (FIA_UID)

FIA_UID.2	User identification before any action
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 Class FMT: Security management

6.1.4.1 Management of functions in TSF (FMT_MOF)

FMT_MOF.1:1	Management of security functions behaviour
FMT_MOF.1.1:1	The TSF shall restrict the ability to *disable, enable, modify the behaviour of* the functions ***a) the authentication methods for the side channel users, TELNET- and FTP-relays;*** ***b) the generation of audit trails;*** to ***the administrator***.

FMT_MOF.1:2	Management of security functions behaviour
FMT_MOF.1.1:2	The TSF shall restrict the ability to *determine the behaviour of* the functions ***a) the authentication methods for the side channel users;*** ***b) the generation of audit trails;*** to ***the administrator and auditor***.

FMT_MOF.1:3	Management of security functions behaviour
FMT_MOF.1.1:3	The TSF shall restrict the ability ~~to determine the behaviour of, disable, enable, modify the behaviour of~~ *perform* the functions ***start-up and shut-down, change to maintenance and normal operation mode;*** to ***the administrator***.

6.1.4.2 Management of security attributes (FMT_MSA)

FMT_MSA.1:1	Management of security attributes
FMT_MSA.1.1:1	The TSF shall enforce the ***authenticated administrator SFP*** to restrict the ability to *change_default, modify, delete,* the security attributes ***a) the administrative role*** to ***the administrator***.

FMT_MSA.1:2	**Management of security attributes**
FMT_MSA.1.1:2	The TSF shall enforce the ***authenticated administrator SFP*** to restrict the ability to *query* the security attributes ***a) the administrative role*** to ***the administrator and the auditor***.

FMT_MSA.1:3	**Management of security attributes**
FMT_MSA.1.1:3	The TSF shall enforce the ***authenticated gui user SFP*** to restrict the ability to *modify* the security attributes ***a) the user password*** to ***the user***.

FMT_MSA.1:4	**Management of security attributes**
FMT_MSA.1.1:4	The TSF shall enforce the ***authenticated administrator SFP*** to restrict the ability to *modify* the security attributes ***a) the user passwords;*** ***b) the administrator password*** to ***the administrator***.

FMT_MSA.3:1	**Static attribute initialisation**
FMT_MSA.3.1:1	The TSF shall enforce the ***authenticated user SFP*** to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA3.2:1	The TSF shall allow the ***administrator*** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3:2	**Static attribute initialisation**
FMT_MSA.3.1:2	The TSF shall enforce the ***authenticated gui user SFP*** to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA3.2:2	The TSF shall allow the ***administrator*** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3:3	**Static attribute initialisation**
FMT_MSA.3.1:3	The TSF shall enforce the ***authenticated administrator SFP*** to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA3.2:3	The TSF shall allow the ***administrator*** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 Management of TSF data (FMT_MTD)

FMT_MTD.1:1	**Management of TSF data**
FMT_MTD.1.1:1	The TSF shall restrict the ability to *modify, delete,* ***create*** the ***a) users;***

FMT_MTD.1:1	Management of TSF data
	b) network configuration; ***c) relay configuration;*** ***d) name server configuration;*** ***e) mail server configuration;*** ***f) packet filter rules;*** ***g) http-proxy squid configuration;*** ***h) virus scanner configuration;*** ***i) audit configuration;*** to ***the administrator***.

FMT_MTD.1:2	Management of TSF data
FMT_MTD.1.1:2	The TSF shall restrict the ability to *query* the ***a) users;*** ***b) network configuration;*** ***c) relay configuration;*** ***d) name server configuration;*** ***e) mail server configuration;*** ***f) packet filter rules;*** ***g) http-proxy squid configuration;*** ***h) virus scanner configuration;*** ***i) audit configuration;*** to ***the administrator and auditor***.

6.1.4.4 Specification of Management Functions (FMT_SMF)

FMT_SMF.1	Specification of Management Functions
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: ***a) user configuration;*** ***b) network configuration;*** ***c) relay configuration;*** ***d) name server configuration;*** ***e) mail server configuration;*** ***f) packet filter rule configuration;*** ***g) http-proxy squid configuration;*** ***h) virus scanner configuration;*** ***i) audit configuration***.

6.1.4.5 Security management roles (FMT_SMR)

FMT_SMR.2	Restrictions on security roles
FMT_SMR.2.1	The TSF shall maintain the roles ***administrator, auditor, user***.
FMT_SMR.2.2	The TSF shall be able to associate users with roles.
FMT_SMR.2.3	The TSF shall ensure that the conditions***:*** ***the source IP addresses for traffic controlled by the authenticated administrator SFP is from the administration network,*** are satisfied.

FMT_SMR.3	Assuming roles
FMT_SMR.3.1	The TSF shall require an explicit request to assume the following roles: ***administrator, auditor***.

6.1.5 Class FPT: Protection of the TSF

6.1.5.1 Trusted recovery (FPT_RCV)

FPT_RCV.2	Automated recovery
FPT_RCV.2.1	When automated recovery from ***a failure or service discontinuity*** is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.
FPT_RCV.2.2	For ***configurable events (default: none),*** the TSF shall ensure the return of the TOE to a secure state using automated procedures.

6.1.5.2 Simple Self Test (FPT_SST)

FPT_SST.1	TOE testing
FPT_SST.1.1	The TSF shall run a suite of self tests *periodically during normal operation* to perform the following checks: ***a) specified processes are running (default: all relays, named, xntpd, sendmail)*** ***b) the file system usage is below a threshold (default: 90%)*** ***c) the file system permissions and flags***.
FPT_SST.1.2	The TSF shall provide authorised users with the capability to query the results of the following checks: ***a) specified processes are running (default: all relays, named, xntpd, sendmail)*** ***b) the file system usage is below a threshold (default: 90%)*** ***c) the file system permissions and flags***.

6.1.5.3 Internal TOE TSF data replication consistency (FPT_TRC)

FPT_TRC.1	Internal TSF consistency
FPT_TRC.1.1	The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.
FPT_TRC.1.2	When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for ***services provided by the unauthenticated user SFP, the authenticated user SFP, the identified side channel use SFP, the authenticated gui user SFP, and the authenticated administrator SFP***.

6.2 Security Assurance Requirements

Table 12 shows the Security Assurance Requirements for the level EAL4. The augmented components ALC_FLR.2, ASE_TSS.2 and AVA_VAN.5 are set in a bold font. For the level EAL4, the SARs ADV_INT and ADV_SPM are not needed.

Table 12: SAR

Class	**Family**	**Level**	**Name**
Development	ADV_ARC	ADV_ARC.1	Security architecture description
	ADV_FSP	ADV_FSP.4	Complete functional specification
	ADV_IMP	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT		
	ADV_SPM		
	ADV_TDS	ADV_TDS.3	Basic modular design
Guidance	AGD_OPE	AGD_OPE.1	Operational user guidance
	AGD_PRE	AGD_PRE.1	Preparative procedures
Life-cycle	ALC_CMC	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL	ALC_DEL.1	Delivery procedures
	ALC_DVS	ALC_DVS.1	Identification of security measures
	ALC_FLR	**ALC_FLR.2**	Flaw reporting procedures
	ALC_LCD	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT	ALC_TAT.1	Well-defined development tools
Security Target	ASE_CCL	ASE_CCL.1	Conformance claims
	ASE_ECD	ASE_ECD.1	Extended components definition
	ASE_INT	ASE_INT.1	ST introduction
	ASE_OBJ	ASE_OBJ.2	Security objectives
	ASE_REQ	ASE_REQ.2	Derived security requirements
	ASE_SPD	ASE_SPD.1	Security problem definition
	ASE_TSS	**ASE_TSS.2**	TOE summary specification with architectural design summary
Tests	ATE_COV	ATE_COV.2	Analysis of coverage
	ATE_DPT	ATE_DPT.1	Testing: security enforcing modules
	ATE_FUN	ATE_FUN.1	Functional testing
	ATE_IND	ATE_IND.2	Independent testing - sample
Vulnerability	AVA_VAN	**AVA_VAN.5**	Advanced methodical vulnerability analysis

6.3 Security Functional Requirements Rationale

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

Table 13: SFR Dependencies

Id	SFR	Dependencies	Satisfied by
1-1	FAU_ARP.1	FAU_SAA.1	1-3
1-2	FAU_GEN.1EX	FPT_STM.1	environment (OE.TIMESTMP)
1-3	FAU_SAA.1	FAU_GEN.1	1-2
1-4	FAU_SAR.1	FAU_GEN.1	1-2
1-5	FAU_SAR.2	FAU_SAR.1	1-4
1-6	FAU_SAR.3	FAU_SAR.1	1-4
1-7	FAU_STG.1	FAU_GEN.1	1-2
1-8	FAU_STG.4	FAU_STG.1	1-7
2-1-1	FDP_IFC.1:1	FDP_IFF.1:1	2-2-1
2-1-2	FDP_IFC.1:2	FDP_IFF.1:2	2-2-2
2-1-3	FDP_IFC.1:3	FDP_IFF.1:3	2-2-3
2-1-4	FDP_IFC.1:4	FDP_IFF.1:4	2-2-4
2-1-5	FDP_IFC.1:5	FDP_IFF.1:5	2-2-5
2-2-1	FDP_IFF.1:1	FDP_IFC.1:1 FMT_MSA.3:X	2-1-1 N/A
2-2-2	FDP_IFF.1:2	FDP_IFC.1:2 FMT_MSA.3:1	2-1-2 4-3-1
2-2-3	FDP_IFF.1:3	FDP_IFC.1:3 FMT_MSA.3:X	2-1-3 N/A
2-2-4	FDP_IFF.1:4	FDP_IFC.1:4 FMT_MSA.3:2	2-1-4 4-3-2
2-2-5	FDP_IFF.1:5	FDP_IFC.1:5 FMT_MSA.3:3	2-1-5 4-3-3
3-1	FIA_AFL.1	FIA_UAU.1	3-4 (hierarchical)
3-2	FIA_ATD.1		
3-3	FIA_SOS.1		
3-4	FIA_UAU.2	FIA_UID.1	3-7 (hierarchical)
3-5	FIA_UAU.5EX		
3-6	FIA_UAU.6		
3-7	FIA_UID.2		
4-1-1	FMT_MOF.1:1	FMT_SMF.1 FMT_SMR.1	4-5 4-6 (hierarchical)
4-1-2	FMT_MOF.1:2	FMT_SMF.1 FMT_SMR.1	4-5 4-6 (hierarchical)
4-1-3	FMT_MOF.1:3	FMT_SMF.1 FMT_SMR.1	4-5 4-6 (hierarchical)

Id	SFR	Dependencies	Satisfied by
4-2-1	FMT_MSA.1:1	FDP_IFC.1:5 FMT_SMF.1 FMT_SMR.1	2-1-5 4-5 4-6 (hierarchical)
4-2-2	FMT_MSA.1:2	FDP_IFC.1:5 FMT_SMF.1 FMT_SMR.1	2-1-5 4-5 4-6 (hierarchical)
4-2-3	FMT_MSA.1:3	FDP_IFC.1:4 FMT_SMF.1 FMT_SMR.1	2-1-4 4-5 4-6 (hierarchical)
4-2-4	FMT_MSA.1:4	FDP_IFC.1:5 FMT_SMF.1 FMT_SMR.1	2-1-5 4-5 4-6 (hierarchical)
4-3-1	FMT_MSA.3:1	FMT_MSA.1:3 FMT_MSA.1:4 FMT_SMR.1	4-2-3 4-2-4 4-6 (hierarchical)
4-3-2	FMT_MSA.3:2	FMT_MSA.1:3 FMT_MSA.1:4 FMT_SMR.1	4-2-3 4-2-4 4-6 (hierarchical)
4-3-3	FMT_MSA.3:3	FMT_MSA.1:1 FMT_MSA.1:2 FMT_SMR.1	4-2-1 4-2-2 4-6 (hierarchical)
4-4-1	FMT_MTD.1:1	FMT_SMF.1 FMT_SMR.1	4-5 4-6 (hierarchical)
4-4-2	FMT_MTD.1:2	FMT_SMF.1 FMT_SMR.1	4-5 4-6 (hierarchical)
4-5	FMT_SMF.1		
4-6	FMT_SMR.2	FIA_UID.1	3-7 (hierarchical)
4-7	FMT_SMR.3	FMT_SMR.1	4-6 (hierarchical)
5-1	FPT_RCV.2	AGD_OPE.1	R05, table 17
5-2	FPT_SST.1		
5-3	FPT_TRC.1	FPT_ITT.1	environment (OE.HANET)

The SFR FAU_GEN.1EX depends on FPT_STM.1 that requires reliable timestamps. The objective OE.TIMESTMP exactly provides these reliable timestamps, therefore the dependency is satisfied by the environment.

The SFR FPT_TRC.1 depends on FPT_ITT.1 which requires the protection of the TSF transfer against disclosure (or modification). This requirement is satisfied by the objective OE.HANET that requires a physical network for the transfer that prohibits disclosure.

The SFR FIA_UAU.2 depends on FIA_UID.1 which is met by FIA_UID.2 which is hierarchical.

FDP_IFC.1:1: The policy for the unauthenticated user SFP is FDP_IFF.1:1.

FDP_IFC.1:2: The policy for the authenticated user SFP is FDP_IFF.1:2.

FDP_IFC.1:3: The policy for the identified side channel user SFP is FDP_IFF.1:3.

FDP_IFC.1:4: The policy for the authenticated gui user SFP is FDP_IFF.1:4.

FDP_IFC.1:5: The policy for the authenticated administrator SFP is FDP_IFF.1:5.

FDP_IFF.1:1: This is the flow control function for the unauthenticated user SFP defined in FDP_IFC.1:1. The dependency of FMT_IFF.1:1 on FMT_MSA.3:X is not applicable because the users that fall under this SFP do not have the security attributes administrative role or password.

FDP_IFF.1:2: This is the flow control function for the authenticated user SFP defined in FDP_IFC.1:2.

FDP_IFF.1:3: This is the flow control function for the identified side channel user SFP defined in FDP_IFC.1:3.The dependency of FMT_IFF.1:3 on FMT_MSA.3:X is not applicable because the users that fall under this SFP do not have the security attributes administrative role or password.

FDP_IFF.1:4: This is the flow control function for the authenticated gui user SFP defined in FDP_IFC.1:4.

FDP_IFF.1:5: This is the flow control function for the authenticated administrator SFP defined in FDP_IFC.1:5.

FMT_MOF.1:1: The management functions are specified in FMT_SMF.1. The security role administrator is defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MOF.1:2: The management functions are specified in FMT_SMF.1. The security roles administrator and auditor are defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MOF.1:3: The management functions are specified in FMT_SMF.1. The security role administrator is defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MSA.1:1: The flow control function for the authenticated administrator SFP is defined in FDP_IFC.1:5. The management functions are specified in FMT_SMF.1. The security role administrator is defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MSA.1:2: The flow control function for the authenticated administrator SFP is defined in FDP_IFC.1:5. The management functions are specified in FMT_SMF.1. The security roles administrator and auditor are defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MSA.1:3: The flow control function for the authenticated gui user SFP is defined in FDP_IFC.1:4. The management functions are specified in FMT_SMF.1. The security role user is defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MSA.1:4: The flow control function for the authenticated administrator SFP is defined in FDP_IFC.1:5. The management functions are specified in FMT_SMF.1. The security role administrator is defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MSA.3:1: The management of the respective password can be done by the user (FMT_MSA.1:3) or the administrator (FMT_MSA.1:4). Their roles are defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MSA.3:2: The management of the user password can be done by the user (FMT_MSA.1:3) or the administrator (FMT_MSA.1:4). Their roles are defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MSA.3:3: The administrative role can be changed by the administrator (FMT_MSA.1:1) and viewed by the auditor (FMT_MSA.1:2). Their roles are defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MTD.1:1: The management functions are specified in FMT_SMF.1. The security role administrator is defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

FMT_MTD.1:2: The management functions are specified in FMT_SMF.1. The security role auditor is defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

The SFR FMT_SMR.2 depends on FIA_UID.1 which is met by FIA_UID.2 which is hierarchical.

FMT_SMR.3: The security roles are defined in FMT_SMR.2 which is hierarchical to FMT_SMR.1.

6.3.1 Objectives

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

The following table shows how the objectives are met by the SFR.

Table 14: Objectives rationale

Objectives	SFR
O.IDAUTH	FIA_AFL.1: This component describes the actions of authentication failure handling. FIA_ATD.1: This component defines the user attributes. FIA_SOS.1: This component specifies the used secrets. FIA_UAU.2: This component requires a user authentication before any action. FIA_UAU.5EX: This component describes all possible authentication mechanisms. FIA_UAU.6: This component describes under which circumstances a reauthentication is necessary. FIA_UID.2: This component requires a user identification before any action. The SFRs are mutually supportive. They are sufficient to meet the objective.
O.MEDIAT	FDP_IFC.1:1: This component defines the unauthenticated user SFP that describes the data flow control for users of the firewall. FDP_IFC.1:2: This component defines the authenticated user SFP that describes the data flow control for users of the firewall that use the FTP- or TELNET-relay. FDP_IFC.1:3: This component defines the identified side channel user SFP that describes the data flow control for users of the firewall that use the side channel authentication. FDP_IFC.1:4: This component defines the authenticated gui user SFP that describes the data flow control for users of the firewall that change their password or register a side channel. FDP_IFC.1:5: This component defines the authenticated administrator SFP that describes the data flow control for administrators of the firewall. FDP_IFF.1:1: This component describes the access control for the unauthenticated user SFP. FDP_IFF.1:2: This component describes the access control for the authenticated user SFP. FDP_IFF.1:3: This component describes the access control for the identified side channel user SFP. FDP_IFF.1:4: This component describes the access control for the authenticated gui user SFP. FDP_IFF.1:5: This component describes the access control for the

Objectives	SFR
	authenticated administrator SFP. The SFRs describe all possible access ways to the TOE and their related policies. The SFRs are mutually supportive. They are sufficient to meet the objective.
O.SECSTA	FPT_RCV.2: This component describes a recovery after failures. The SFR is sufficient to meet the objective.
O.SELPRO	FPT_SST.1: This component defines simple self-tests.
O.AUDREC	FAU_ARP.1: This component detects potential security violations. FAU_GEN.1EX: This component describe the data generated for the audit. FAU_SAA.1: The component describes the security violation analysis. FAU_SAR.1: The component requires an audit review. FAU_SAR.2: This component assigns who can view the audit log. FAU_SAR.3: This component allows the searching of the audit log. FAU_STG.1: This component makes sure that the audit log is protected. FAU_STG.4: This component requires a prevention of audit data loss. The SFRs are mutually supportive. They are sufficient to meet the objective.
O.ACCOUN	FAU_GEN.1EX: This component describes the data generated for the audit. FIA_UID.2: This component requires a user identification before any action. FIA_UAU.2: This component requires a user authentication before any action. The SFRs are mutually supportive. They are sufficient to meet the objective.
O.SECFUN	FMT_MOF.1:1: This component defines who can modify the behaviour of the security functions. FMT_MOF.1:2: This component defines who can read the settings of the security functions. FMT_MOF.1:3: This component defines who can start and stop the TOE or enter maintenance or normal operation. These actions also modify the behaviour of the security functions. FMT_MSA.3:1: This component describes that the authenticated user SFP has restrictive default values of the security attributes (the user password). FMT_MSA.3:2: This component describes that the authenticated gui user SFP has restrictive default values of the security attributes (the user password). FMT_MSA.3:3: This component describes that the authenticated administrator SFP has restrictive default values of the security attributes (the administrator password). FMT_MTD.1:1: This component describes who can modify the TSF data. FMT_MTD.1:2: This component describes who can query the TSF data. FMT_SMF.1: This component lists the configuration data of the TSF. FMT_SMR.2: The component defines the security roles. FMT_SMR.3: This component describe that in order to assume the administrator or the auditor role, an explicit request must be required.

Objectives	SFR
	FMT_MSA.1:1: This component defines who can change the administrative role, i.e. who is administrator. FMT_MSA.1:2: This component defines who can query the administrative role. FMT_MSA.1:3: This component describes that the users can change their own password. FMT_MSA.1:4: This component describes that the administrator can change the user and the administrative passwords. The SFRs describe the security sensitive data on the TOE and the configurable security functions. The SFRs describe who can read/read the data and change the security functions. The SFRs are mutually supportive. They are sufficient to meet the objective.
O.AVAIL	FPT_TRC.1: This component requires that replicated data is consistent between parts of the TOE and that they check the consistency of the replicated data before accepting user connections.

The following table 15 shows that all SFR contribute to (at least one objective) and all objectives are met by (at least) one SFR.

Table 15: SFR coverage

SFR	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELFPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.AVAIL
FAU_ARP.1					X			
FAU_GEN.1EX					X	X		
FAU_SAA.1					X			
FAU_SAR.1					X			
FAU_SAR.2					X			
FAU_SAR.3					X			
FAU_STG.1					X			
FAU_STG.4					X			
FDP_IFC.1:1		X						
FDP_IFC.1:2		X						
FDP_IFC.1:3		X						
FDP_IFC.1:4		X						
FDP_IFC.1:5		X						
FDP_IFF.1:1		X						
FDP_IFF.1:2		X						

SFR	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELFPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.AVAIL
FDP_IFF.1:3		X						
FDP_IFF.1:4		X						
FDP_IFF.1:5		X						
FIA_AFL.1	X							
FIA_ATD.1	X							
FIA_SOS.1	X							
FIA_UAU.2	X					X		
FIA_UAU.5EX	X							
FIA_UAU.6	X							
FIA_UID.2	X					X		
FMT_MOF.1:1							X	
FMT_MOF.1:2							X	
FMT_MOF.1:3							X	
FMT_MSA.1:1							X	
FMT_MSA.1:2							X	
FMT_MSA.1:3							X	
FMT_MSA.1:4							X	
FMT_MSA.3:1							X	
FMT_MSA.3:2							X	
FMT_MSA.3:3							X	
FMT_MTD.1:1							X	
FMT_MTD.1:2							X	
FMT_SMF.1							X	
FMT_SMR.2							X	
FMT_SMR.3							X	
FPT_RCV.2			X					
FPT_SST.1				X				
FPT_TRC.1								X

The following table 16 shows how the SFR help to maintain the objectives.

Table 16: SFR rationale

SFR	Rationale
FAU_ARP.1	This component detects potential security violations and aids in meeting the objective O.AUDREC.
FAU_GEN.1EX	This component describes the data generated for the audit and aids in meeting the objective O.AUDREC. It also aids in meeting O.ACCOUN.
FAU_SAA.1	The component describes the security violation analysis and aids in meeting the objective O.AUDREC.
FAU_SAR.1	The component requires an audit review and contributes to the objectives O.AUDREC.
FAU_SAR.2	This component assigns who can view the audit log and contributes to O.AUDREC.
FAU_SAR.3	This component allows the searching of the audit log and contributes to O.AUDREC.
FAU_STG.1	This component makes sure that the audit log can be written and contributes to O.AUDREC.
FAU_STG.4	This component requires a prevention of audit data loss and contributes to O.AUDREC.
FDP_IFC.1:1	This component defines the unauthenticated user SFP that describes the data flow control for users of the firewall. The component aids in meeting O.MEDIAT.
FDP_IFC.1:2	This component defines the authenticated user SFP that describes the data flow control for users of the firewall that use the FTP- or TELNET-relay. The component aids in meeting O.MEDIAT.
FDP_IFC.1:3	This component defines the identified side channel user SFP that describes the data flow control for users of the firewall that use the side channel authentication. The component aids in meeting O.MEDIAT.
FDP_IFC.1:4	This component defines the authenticated gui user SFP that describes the data flow control for users of the firewall that change their password or register a side channel. The component aids in meeting O.MEDIAT.
FDP_IFC.1:5	This component defines the authenticated administrator SFP that describes the data flow control for administrators of the firewall. The component aids in meeting O.MEDIAT.
FDP_IFF.1:1	This component describes the access control for the unauthenticated user SFP and contributes to O.MEDIAT.
FDP_IFF.1:2	This component describes the access control for the authenticated user SFP and contributes to O.MEDIAT.
FDP_IFF.1:3	This component describes the access control for the identified side channel user SFP and contributes to O.MEDIAT.
FDP_IFF.1:4	This component describes the access control for the authenticated gui user SFP and contributes to O.MEDIAT.
FDP_IFF.1:5	This component describes the access control for the authenticated

SFR	Rationale
	administrator SFP and contributes to O.MEDIAT.
FIA_AFL.1	This component describes the actions of authentication failure handling and contributes to O.IDAUTH.
FIA_ATD.1	This component defines the user attributes and aids in meeting the objective O.IDAUTH.
FIA_SOS.1	The verification of secrets contributes to O.IDAUTH.
FIA_UAU.2	This component requires a user authentication before any action. It contributes to O.IDAUTH. It also aids in meeting O.ACCOUN, as the users are authenticated.
FIA_UAU.5EX	This component describes all possible authentication mechanisms and helps to meet O.IDAUTH.
FIA_UAU.6	This component describes under which circumstances a re-authentication is necessary and contributes to O.IDAUTH.
FIA_UID.2	This component requires a user identification before any action. It contributes to O.IDAUTH. It also aids in meeting O.ACCOUN, because log entries can be associates with users.
FMT_MOF.1:1	This component defines who can modify the behaviour of the security functions. It contributes to O.SECFUN.
FMT_MOF.1:2	This component defines who can read the settings of the security functions. It contributes to O.SECFUN.
FMT_MOF.1.3	This component defines who can start and stop the TOE or enter maintenance or normal operation. These actions also modify the behaviour of the security functions. The component contributes to O.SECFUN.
FMT_MSA.1:1	This component defines who can change the administrative role, i.e. who is administrator. The component contributes to O.SECFUN.
FMT_MSA.1:2	This component defines who can query the administrative role. It contributes to O.SECFUN.
FMT_MSA.1:3	This component describes that the users can change their own password. It contributes to O.SECFUN.
FMT_MSA.1:4	This component describes that the administrator can change the user and the administrative passwords. It contributes to O.SECFUN.
FMT_MSA.3:1	This component describes that the authenticated user SFP has restrictive default values of the security attributes. The component contributes to O.SECFUN.
FMT_MSA.3:2	This component describes that the authenticated gui user SFP has restrictive default values of the security attributes. The component contributes to O.SECFUN.
FMT_MSA.3:3	This component describes that the authenticated administrator SFP has restrictive default values of the security attributes. The component contributes to O.SECFUN.

SFR	Rationale
FMT_MTD.1:1	This component describes who can modify the TSF data. It contributes to O.SECFUN.
FMT_MTD.1:2	This component describes who can query the TSF data. It contributes to O.SECFUN.
FMT_SMF.1	This component lists the configuration data of the TSF. It contributes to O.SECFUN.
FMT_SMR.2	The component defines the security roles. It contributes to O.SECFUN.
FMT_SMR.3	This component describes that in order to assume the administrator or the auditor role, an explicit request must be required. This component contributes to O.SECFUN.
FPT_RCV.2	This component describes a recovery after failures and contributes to O.SECSTA.
FPT_SST.1	This component defines simple self-tests. It contributes to O.SELPRO.
FPT_TRC.1	This component requires consistency in the TSF data when it is replicated internal to the TOE. It avoids inconsistent states in the takeover case and aids to meet O.AVAIL.

6.3.2 New or tailored SFR

The following rationale justifies the introduction of new SFR components and families.

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 still supported security functions. 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 close connected to FAU_GEN.1, it has been added to the same family.

FIA_UAU.5EX: This component is derived from FIA_UAU.5, with the clarification that the SFR itself does not implement authentication methods, but uses methods outside of the TOE. This component is introduced only in order to clearly state the situation to the reader. As FIA_UAU.5EX provides the same functionality as FIA_UAU.5, it can be used as a replacement for FIA_UAU.5. The dependency on FIA_UAU.5 of other SFRs can be substituted by FIA_UAU.5EX. Because FIA_UAU.5EX is close connected to FIA_UAU.5, it has been added to the same family.

FPT_SST.1: The single component of this new family FPT_SST is modelled after component FPT_TST.1. The component FPT_TST.1 has a dependency on FPT_AMT.1. Self-tests can, however, also be performed without having a formal abstract state machine. In order to avoid any associations with these concept, a new family has been introduced. In addition, the tests do not just check the TSFs, but perform tests that can also check any other targets. Therefore, a new family seems justified.

6.4 Security Assurance Requirements Rationale

The overall security claim of this Security Target is aimed at ELA4.

The attack potential of the anonymous users is high. The firewall components are exposed to unrestricted attackers, simply because they are exposed to the Internet. Therefore the vulnerability

analysis has been augmented to AVA_VAN.5 in order to match the resistance to attackers with a high attack potential.

For the same reason the TOE summary specification has been augmented to ASE_TSS.2. This augmentation explains the security architecture of the product.

The life cycle support has been augmented by ALC_FLR.2 to demonstrate GeNUA's flaw handling procedures.

Table shows 17 that all dependencies are met.

Table 17: SAR Dependencies

ID	**Requirement**	**Dependency**	**Solution**
R01	ADV_ARC.1	ADV_FSP.1	R02
		ADV_TDS.1	R04
R02	ADV_FSP.4	ADV_TDS.1	R04
R03	ADV_IMP.1	ADV_TDS.3	R04
		ADV_TAT.1	R13
R04	ADV_TDS.3	ADV_FSP.4	R02
R05	AGD_OPE.1	ADV_FSP.1	R02
R06	AGD_PRE.1	-	-
R07	ALC_CMC.4	ALC_CMS.1	R08
		ALC_DVS.1	R10
		ALC_LCD.1	R12
R08	ALC_CMS.4	-	-
R09	ALC_DEL.1	-	-
R10	ALC_DVS.1	-	-
R11	**ALC_FLR.2**	-	-
R12	ALC_LCD.1	-	-
R13	ALC_TAT.1	ADV_IMP.1	R03
R14	ASE_CCL.1	ASE_INT.1	R16
		ASE_ECD.1	R15
		ASE_REQ.1	R18
R15	ASE_ECD.1	-	-
R16	ASE_INT.1	-	-
R17	ASE_OBJ.2	ASE_SPD.1	R19
R18	ASE_REQ.2	ASE_OBJ.2	R17
		ASE_ECD.1	R15
R19	ASE_SPD.1	-	-

ID	Requirement	Dependency	Solution
R20	**ASE_TSS.2**	ASE_INT.1	R16
		ASE_REQ.1	R18
		ADV_ARC.1	R01
R21	ATE_COV.2	ADV_FSP.2	R02
		ATE_FUN.1	R23
R22	ATE_DPT.1	ADV_ARC.1	R01
		ADV_TDS.2	R04
		ATE_FUN.1	R23
R23	ATE_FUN.1	ATE_COV.1	R21
R24	ATE_IND.2	ADV_FSP.2	R02
		AGD_OPE.1	R05
		AGD_PRE.1	R06
		ATE_COV.1	R21
		ATE_FUN.1	R23
R25	**AVA_VAN.5**	ADV_ARC.1	R01
		ADV_FSP.2	R02
		ADV_TDS.3	R04
		ADV_IMP.1	R03
		AGD_OPE.1	R05
		AGD_PRE.1	R06

7 TOE Summary

7.1 TOE Summary Specification

7.1.1 SF_SA: Security audit

SF_SA.1: The TOE generates log data whenever important events occur. This includes starting and stopping of the system, and changing from normal to the maintenance mode. Starting and stopping or reconfiguration of the relays generate log data. Creation and loading of packet filters for ALG and PFL generate log data.

SF_SA.2: All relays generate log data when the connection state changes. Log data includes the IP address of source and destination, Ports for TCP and UDP-based protocols, the timestamps for connection and disconnection and the amount of data transferred in both directions for the source and the destination side. The protocol specific relays log part of the protocol data (e.g. URLs, SMTP-Envelope-lines, ...). The TELNET- and FTP-relay log information about authentication. All unsuccessful connection attempts are logged.

SF_SA.3: All administration through the administration web generates log data. The administration action is logged together with the administrative role. Successful and unsuccessful login attempts are logged. The log contains a time stamp.

SF_SA.4: The log data is analysed by automated tools that look for pattern in the log data. The pattern include packet filter violations, daemon messages, relay messages, kernel messages, and messages from other processes, e.g. the processes that implement the self-tests. If a pattern matches, a security event is generated. The actions include logging of the event, adding the event to an event digest, use of `wall' to show the event on the consoles, mail the event to the administrators, shut down network interfaces, and system halt. The extracted log data is written to the audit log. In normal operation mode the audit log is protected by file system append-only flag. It can only be changed in maintenance mode (e.g. rotated).

SF_SA.5: The log data can be transformed into a human readable form and can be searched by all administrators and auditors. Other roles are not allowed to read the log. The possible search criteria are: time, date, process id and additional log data. For relays the log data contains: the relay type, connection state, IP addresses and ports, bytes transferred.

SF_SA.6: The system checks for available log space and notifies the administrator in a configurable way. Loss of log data is noticed and a configurable action is executed in that case.

This Security Function addresses the following SFRs: FAU_GEN.1EX (audit data generation); FAU_ARP.1 (automatic response); FAU_SAA.1 (audit analysis); FAU_STG.1 and FAU_STG.4 (event storage); FAU_SAR.1, FAU_SAR.2, and FAU_SAR.3 (audit review).

7.1.2 SF_DF: Data flow control

SF_DF.1: The packet filter at the ALG and PFL implement the flow control at the network layer (IP) and transport layer (TCP/UDP). The filter rules take the information from the IP and TCP/UDP-Header (where applicable) in order to apply the filter rules.

Packets with spoofed source- or destination-IP addresses are dropped. Packets with source routing are dropped. Packets are not forwarded at the ALG; so that packets that cannot be transmitted to the socket layer are dropped.

The packet filter of the PFL has a restrictive default filter set. Any TCP-connections (or UDP packets) from the ALG into the internal net have to be activated by a administrator.

SF_DF.2: The relays check the following attributes:

The header information of network packets, depending on their type:

TCP: IP and TCP header;

UDP: IP and UDP header;

ICMP: IP header and ICMP message;

IP: IP header;

The actual date and time.

The incoming and outgoing interfaces.

Additional information depending on the handling relay:

IP-relay: none;

PING-relay: none;

UDP-relay: none;

TCP-relay: none;

NNTP-relay: protocol and application data;

POP-relay: protocol and application data;

SMTP-relay: protocol and application data;

FTP-relay: protocol data;

TELNET-relay: protocol data;

HTTP-relay: protocol data;

WWW-relay: protocol and application data;

A virus scanner can be used to scan the application data of SMTP-relay, POP-relay, NNTP-relay, FTP-relay and WWW-relay.

SF_DF.3: The SMTP-relay can block mails depending on the mail data (virus, blocked extension type of a MIME part). The mail stays on the TOE and must be handled by an administrator.

SF_DF.4: WWW-relay: For data of the content-type text/html a filter can remove the following tags that imply active content: <applet>, <embed>, <object>, <script>, and comments. Typical javascript-fragments, like event handler (on-tags) can also be removed.

SF_DF.5: MIME-encoded messages are (recursively) parsed. Their parts are checked like non encoded messages.

This Security Function addresses the SFRs: FDP_IFC.1:1, FDP_IFC.1:2, FDP_IFC.1:3, FDP_IFC.1:4, and FDP_IFC.1:5 (information flow control policy); FDP_IFF.1:1, FDP_IFF.1:2, FDP_IFF.1:3, FDP_IFF.1:4, and FDP_IFF.1:5 (information flow control functions). They cover the policies ***unauthenticated user SFP****,* ***authenticated user SFP****,* ***identified side channel user SFP****,* ***authenticated gui user SFP****, and* ***authenticated administrator SFP****.*

7.1.3 SF_IA: Identification and Authentication

SF_IA.1: All IP packets are identified at the network layer by their source and destination IP addresses (and ports if applicable).

SF_IA.2: The TCP-based relays are already connection oriented. The UDP- and IP-related relays introduce a UDP-association or IP-association respectively. Packages with the same destination IP, (destination port,) source IP, (source port,) and packets where source and destination are reversed are treated as belonging to a connection if they appear within a short timespan one after the other. The connections time out after an idle time with no traffic. As with TCP connections, the connection establishment can be configured to be initiated only by one side. For the IP-relay, the IP protocol takes the role of the port.

SF_IA.3: For the TELNET- and FTP-relays a compulsory user authentication at the TOE can be configured by the administrator. The authentication method can be configured and either be password, radius, LDAP, S/Key, or cryptocard. The password can be changed by the users themselves, but a minimum quality is checked by the TOE. The password must be of minimum length 6, must not only contain uppercase- or lowercase letters, and must not contain the user name.

The TELNET- and FTP-relay capture the eventual option-negotiation commands sent before the authentication proceeds, and replay them to the destination, if the authentication completes successfully.

SF_IA.4: The side channel authentication allows users to activate configurable TCP-relays after a successful authentication at the side channel web site. The authentication method can be configured by the administrators and either be password, radius, LDAP, S/Key, or cryptocard. The password can be changed by the users themselves, but a minimum quality is checked by the TOE. The password must be of minimum length 6, must not only contain uppercase- or lowercase letters, and must not contain the user name.

SF_IA.5: Administration is only possible after successful authentication at the administration web server. Auditors (administrators with read-only rights) can view the configuration after successful authentication at the administration web server. Connections to the administration webserver are only accepted from the administration network. The authentication method is password. The password can be changed by the respective administrators themselves, but a minimum quality is checked by the TOE. The password must be of minimum length 6, must not only contain uppercase- or lowercase letters, and must not contain the user name.

SF_IA.6: All of the different authentication methods disable a user/administrator account after a configurable number of unsuccessful attempts. The default value is 5. An administrator has to reactivate the user account.

SF_IA.7: The side channel, user and the administration web server have a timeout for inactivity, after which the user/administrator have to re-authenticate. The default timeout is 10 minutes.

SF_IA.8: To gain interactive access (shell access) to the console, the administrator has to authenticate. Other interactions at the console require administrator input. On (re)boot the system waits for keyboard input but does not require a password. The application of boot install scripts in maintenance mode continue without applying the scripts, if the password is not entered during the timeout period. Changing the kernel requires keyboard input but does not require a password.

This Security Function addresses the SFRs: FIA_AFL.1 (authentication failures), FIA_SOS.1 (specification of secrets), FIA_UAU.2, FIA_UAU.5EX, FIA_UAU.6 (user authentication), FIA_UID.2 (user identification); FDP_IFC.1:2, FDP_IFC.1:3, FDP_IFC.1:4, and FDP_IFC.1:5 (Information flow control policy); FDP_IFF.1:2, FDP_IFF.1:3, FDP_IFF.1:4, and FDP_IFF.1:5 (Information flow control functions), FMT_MOF.1:3 (management of functions in TSF), FMT_SMR.2 and FMT_SMR.3 (security management roles). They cover the policies ***authenticated user SFP****,* ***identified side channel user SFP****,* ***authenticated gui user SFP****, and* ***authenticated administrator SFP****.*

7.1.4 SF_SM: Security management

SF_SM.1: The security management can be divided into three different roles: normal users do not have any rights, auditors (administrators with read-only rights) can view the configuration, and (normal) administrators can change the configuration. All users have the security attributes administrative role and password.

SF_SM.2: The configuration is divided into the following fields:

System, Services, Connection, User, Packet filter, Statistics, Logging

SF_SM.3: Only administrators can change the password and security role of users, auditors and administrators. The auditors can view the settings. All security attributes for new users and administrators are set to a restrictive default. The user can change their passwords at the user webserver.

SF_SM.4: Only administrators can change the timeouts for the administrator, user and side channel web server. The auditors can view the settings.

SF_SM.5: Only administrators can change the log details and authentication methods. The auditors can view the settings.

SF_SM.6: The attributes synchronized between HA peers are
a) user configuration (but not their blocked status);
b) network configuration;
c) relay configuration;
d) name server configuration;
e) mail server configuration;
f) packet filter rule configuration;
g) http-proxy squid configuration;
h) virus scanner configuration;
i) audit configuration.

This Security Function addresses the SFRs: FIA_ATD.1 (user attribute definition); FMT_SMR.2 and FMT_SMR.3 (security management roles); FMT_MTD.1:1 and FMT_MTD.1:2 (management of TSF data); FMT_SMF.1 (specification of management functions); FMT_MSA.1:1, FMT_MSA.1:2, FMT_MSA.1:3, FMT_MSA.1:4, FMT_MSA.3:1, FMT_MSA.3:2, and FMT.MSA.3:3 (management of security attributes); FMT_MOF.1:1 and FMT_MOF.1:2 (management of functions in TSF).

7.1.5 SF_PT: Protection of the TSF

SF_PT.1: After a shutdown due to a failure or service discontinuity, the TOE does not reboot automatically, but requires an administrator interaction at the console.

For the high availability system this stop of service is not desired. Therefore a peer will take over the services of the failed system. The HA peers synchronize the attributes given in SF_SM.6.

SF_PT.2: In maintenance mode, system flags can be modified and therefore protected files can be manipulated. To allow an interactive session at the TOE only for the administrator at the console, all network packets (and ethernet frames) are dropped silently in maintenance mode.

SF_PT.3: The TOE executes self tests regularly. The self tests consist of checking that (a configurable number) of processes are running, the file system usage is below a configurable threshold, and of tests for the file system consistency (file system permissions and flag settings). Administrators and auditors (the authorized users) can view the results of the self tests.

SF_PT.4: During normal operation the packet filter rules of the PFL cannot be modified. They are sealed when changing into normal operation mode.

This Security Function addresses the SFRs: FPT_SST.1 (simple self test); FPT_RCV.2 (trusted recovery); FPT_TRC.1 (internal TOE TSF data replication consistency)

7.2 Self-Protection against Interference and Logical Tampering

The product takes the following self-protection measures, supplied by the TOE:

- The system is a two-tiered firewall. Both systems have to be overcome to gain unauthorised access from the external network on the internal network.
- On the ALG all connections are accepted by relay which are located in a reduced runtime environment (cages). An attacker has only limited capabilities.
- The ALG has a hardened kernel, some system calls are modified and deviate from their POSIX-conformant behaviour. This prevents attackers from escape out of the cages. The system calls are `chroot`, `mknod`, `ktrace`, and `strace`.

- All central processes of the ALG are controlled by the processmaster. In case of strange behaviour the processmaster can take actions.
- The ALG uses the BSD file system flags and runs at `securelevel=2`. The flags are used to mark most files as read-only and logfiles as append-only. The securelevel prevents changing the flags without going through single user mode.
- A reboot requires a manual interaction at the console. An attacker cannot modify the flags by going through single user mode.
- The PFL runs at `securelevel=3`. This means that the packet filter rules are immutable.

The following self-protection measures are supplied by the environment:

- The OpenBSD kernel uses a randomized stack top, a stack canary to detect stack overflow, and exclusive write or executable memory segments (W^X) to mitigate exploits.
- The OpenBSD applications use a randomized stack top, a stack canary to detect stack overflow, and exclusive write or executable memory segments (W^X) to mitigate exploits. Further, they use random library memory locations, random `mmap` and `malloc` function results, a read-only data segment `.rodata` for constant data to mitigate exploits.
- The OpenBSD daemons use either privilege revocation or privilege separation if they temporary need enhanced privileges.
- Both the OpenBSD kernel and the core OpenBSD applications use the functions `strlcat` and `strlcpy` to replace `strncat` and `strncpy` that guarantee to null-terminate the result.

The measures together build up a multi-layered security barrier that results in a sufficient level of self-protection:

- The low level `strlcat` and `strlcpy` functions prohibit overwriting the allocated memory.
- The stack and memory protection mechanisms make it difficult to insert shell code.
- The privilege reduction functions inhibit a successful attacker to gain further privileges.

Further, encryption of the TOE data when it is transported over an insecure path prevent an attacker to obtain information for continued attacks.

The TOE supplies a configuration GUI that check the parameters entered in the HTML forms. This helps to mitigate misconfiguration by administrators. It also gives a clear user interface for the administrators and revisors.

7.3 Self-Protection against Bypass

As the TOE is a firewall system, there can be no bypassing if it is installed properly. The assumption A.SINGEN reflects this.

8 Abbreviations

ALG Application Level Gateway

BSD Berkeley Software Distribution

DMZ demilitarised zone

DNS Domain Name Service or Domain Name System

FTP File Transfer Protocol

HTTP Hyper Text Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

ICMP Internet Control Message Protocol

IP Internet Protocol

LDAP Lightweight Directory Access Protocol

MSSQL Microsoft SQL Server relational database management system

MySQL a relational database management system

NNTP Network News Transfer Protocol

NTP Network Time Protocol

PING send ICMP ECHO_REQUEST packets to network hosts

POP Post Office Protocol

Postgres PostgreSQL object-relational database management system

RTSP Real Time Streaming Protocol

SSH Secure Shell

S/KEY Secure Key

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

Telnet Telecommunication network

TCP Transmission Control Protocol

UDP User Datagram Protocol

URL Uniform Resource Locator

VPN Virtual Private Network

WWW World Wide Web

9 Bibliography

[CC_1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1
[CC_3]	Common criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1
[OpenBSD]	http://www.openbsd.org/