GeNUGate Firewall 6.0

Security Target

Version 242

22. August 2006

GeNUA mbH

Domagkstr. 7, D-85551 Kirchheim, Germany

Table of Contents

1 ST INTRODUCTION

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

1.1 Identification

ST Title:	**GeNUGate Firewall 6.0** Security Target, Version 242
TOE Identification:	**GeNUGate Firewall 6.0**
Product Identification:	**GeNUGate 6.0 Z** Patchlevel 11
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.1, 1999
Assurance Level:	EAL 4, augmented by **AVA_VLA.4** and **ALC_FLR.2**
Keywords:	Two-Tiered Firewall, Application Level Gateway, Packet filter, Proxy server, Network security, Information flow control,

1.2 Overview

The TOE **GeNUGate Firewall 6.0** is part of a larger product, the firewall **GeNUGate 6.0 Z**, which consists of hardware and software. The TOE **GeNUGate Firewall 6.0** itself is part of the shipped software. The operating system is a modified OpenBSD.

GeNUGate 6.0 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. Both systems are shipped in one case. 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. The PFL has a second interface which is connected to the internal network.

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 send to and from the internal network.

The TOE, **GeNUGate Firewall 6.0**, 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.

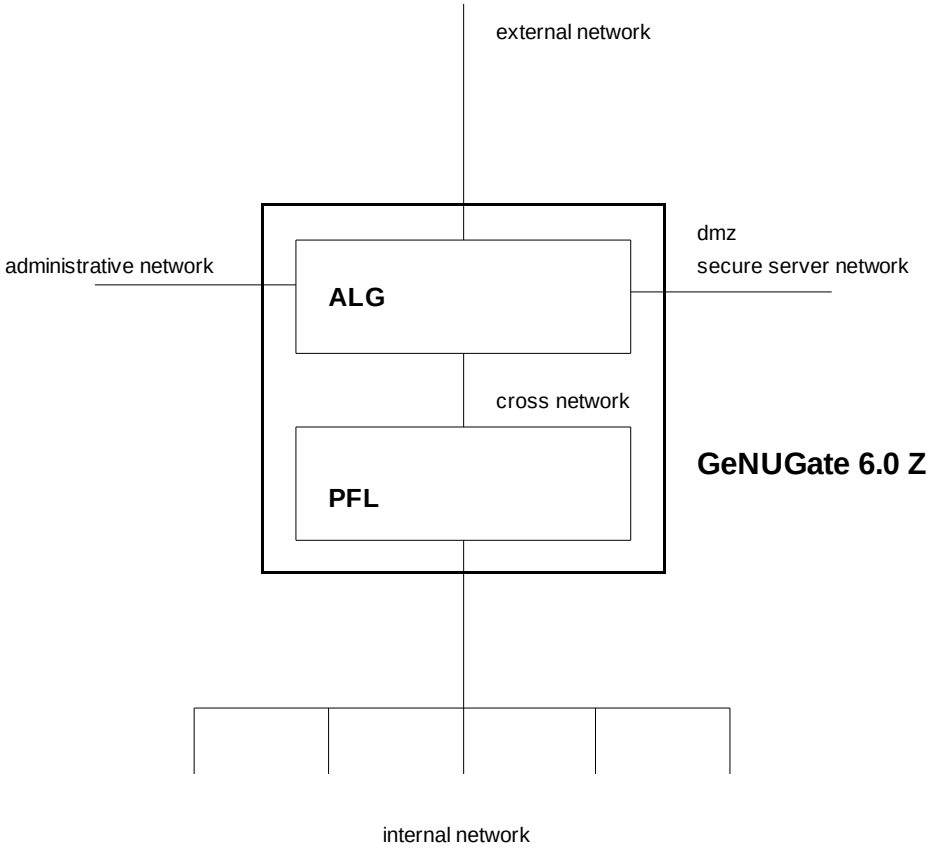


Figure 1: **GeNUGate 6.0 Z** overview

The design of the 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 ALG and 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).

1.3 ISO/IEC 15408 Conformance

The TOE is Part 2 extended and Part 3 conformant of the CC Version 2.1.

[CC_1]: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 2.1, 1999.

[CC_2]: Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 2.1, 1999.

[CC_3]: Common criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.1, 1999.

2 TOE DESCRIPTION

The TOE **GeNUGate Firewall 6.0** 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 6.0 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.
- *administration 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.
- *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.

The TOE includes the following security features:

- The ALG does not perform IP forwarding.
- The modified OpenBSD kernel performs extra IP spoofing checks.
- The modified OpenBSD kernel logs all events that occur while checking incoming IP packets.
- The filter rules of ALG and 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).

2.1 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.
- *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.
- *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.

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.

2.2 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.

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	6.0	21.08.2006	CD-ROM
Software	GeNUGate Platform	6.0 Z Patchlevel 11	21.08.2006	CD-ROM
Documentation	Administrator and user guidance manual	6.0 Z	21.08.2006	Manual and CD-ROM
Hardware	PFL floppy/USB stick	N/A		

2.3 Physical Scope and Boundary

Both ALG and PFL run on Intel compatible hardware that works with OpenBSD. As the product **GeNUGate 6.0 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 2 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.

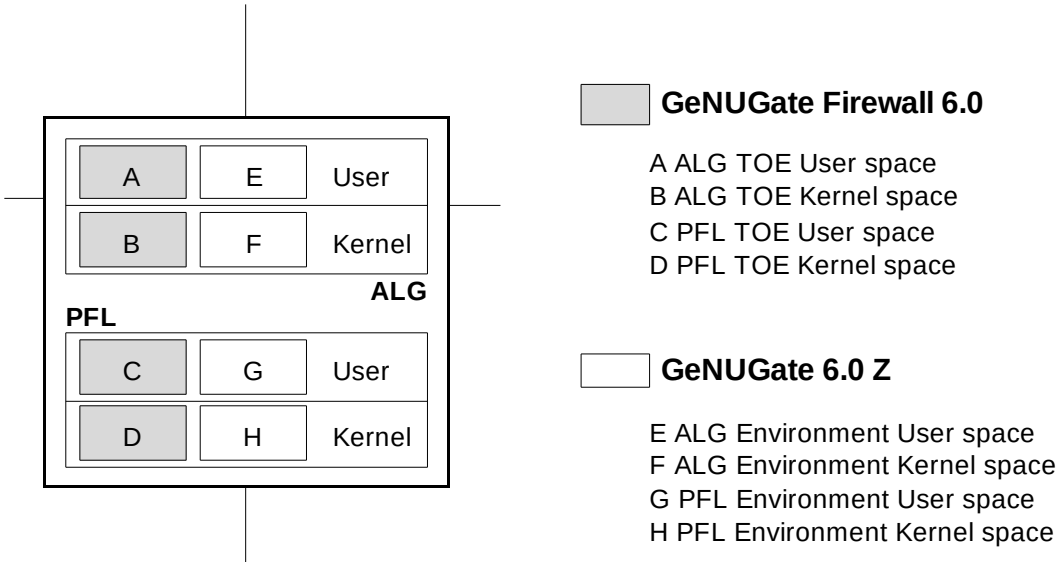


Figure 2: Scope and boundary

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	squid, sendmail, bind, ntpd, GeNUGate options: VPN , HA , 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

2.4 Logical Scope and Boundary

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 high availability option for **GeNUGate 6.0 Z**
- the VPN option for **GeNUGate 6.0 Z**
- the Secure Proxy option for **GeNUGate 6.0 Z**
- the GeNUAuth option for **GeNUGate 6.0 Z**
- the URL filter option for **GeNUGate 6.0 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

3 TOE SECURITY ENVIRONMENT

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

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

3.1 Users and Assets

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

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 role authorises them to view the TOE configuration. Their assumed attack potential is undefined.

Table 3: Assets

	Assets
resources in the connected networks	The resources in the connected networks that the TOE is supposed to protect.

	Assets
security sensitive data on the TOE	The data on the TOE that contains security sensitive data.

3.2 Assumptions

Table 4: Assumptions

	Assumptions
A.PHYSEC	The TOE is physically secure. Only authorised persons have physical access to the TOE.
A.NOEVIL	Administrators are non-hostile and follow all administrator 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.
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.

3.3 Threats

Table 5: 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.

	Threats
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 Organizational Security Policies

Table 6: Policies

	Policies
P.AUDIT	All users must be accountable for their actions.

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

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.
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.

4.2 Security Objectives for the Environment

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.

	Objectives for the environment
OE.NOEVIL	Those responsible for the TOE must assure that all administrators 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.
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.

5 IT SECURITY REQUIREMENTS

All of the security functional requirements in subsection 5.1 have been drawn from the CC Part 2.

The functional requirements in the subsection 5.2 (**FPT_SST**, **FPT_RTE**, **FAU_GEN.1EX** and **FIA_UAU.5EX**) are not drawn from CC Part 2. The SFRs are listed in the appendix.

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 operation assignment is set in a bold 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.

5.1 TOE Security Functional Requirements

5.1.1 Class FAU: Security audit

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.

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 TSP.
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***.

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	**Audit review**
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 perform *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).***

Security audit event storage (FAU_STG)

FAU_STG.2	**Guarantees of audit data availability**
FAU_STG.2.1	The TSF shall protect the stored audit records from unauthorised deletion.
FAU_STG.2.2	The TSF shall be able to *prevent* unauthorised modifications to the audit records in the audit trail.
FAU_STG.2.3	The TSF shall ensure that ***a configurable amount (default 10%) of the total disc partition space available*** *for* audit records will be maintained when the following conditions occur: *audit storage exhaustion, failure, attack*.

FAU_STG.4	**Prevention of audit data loss**
FAU_STG.4.1	The TSF shall *prevent auditable 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.

5.1.2 Class FDP: User data protection

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 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***.

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.1:1	**Simple security attributes**
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.*** ***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 provide the following ***none***.
FDP_IFF.1.5:1	The TSF shall explicitly authorise an information flow based on the following rules: ***none***.

FDP_IFF.1:1	**Simple security attributes**
FDP_IFF.1.6:1	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 provide the following ***none***.
FDP_IFF.1.5:2	The TSF shall explicitly authorise an information flow based on the following rules: ***none***.

FDP_IFF.1:2	**Simple security attributes**
FDP_IFF.1.6:2	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 provide the following ***none***.
FDP_IFF.1.5:3	The TSF shall explicitly authorise an information flow based on the following rules: ***none***.
FDP_IFF.1.6:3	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 provide the following ***none***.
FDP_IFF.1.5:4	The TSF shall explicitly authorise an information flow based on the following rules: ***none***.
FDP_IFF.1.6:4	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 provide the following ***none***.
FDP_IFF.1.5:5	The TSF shall explicitly authorise an information flow based on the following rules: ***none***.
FDP_IFF.1.6:5	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)***.

5.1.3 Class FIA: Identification and authentication

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 3)*** 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 met or 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***.

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***.

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***.

The strength of function claim for **FIA_SOS.1** is **SOF-high**.

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.

The strength of function claim for **FIA_UAU.2** is **SOF-high**.

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)***.

User identification (FIA_UID)

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

5.1.4 Class FMT: Security management

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***.

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.

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;*** ***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***.

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.***

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***.

5.1.5 Class FPT: Protection of the TSF

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.

5.2 Tailored or new SFR

This chapter contains the extended or new Security Functional Requirements. See also the appendix for their description.

5.2.1 Class FAU: Security audit

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.***

5.2.2 Class FIA: Identification and authentication

User authentication (FIA_UAU)

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)***.

The strength of function claim for **FIA_UAU.5EX** is **SOF-high**.

5.2.3 Class FPT: Protection of the TSF

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.***

Runtime Environment (FPT_RTE)

FPT_RTE.1	**Restricted Runtime Environment**
FPT_RTE.1.1	The restricted runtime environment implements the following restrictions: ***a) chroot environment;*** ***b) restricted system calls for (chroot, kill, strace, ptrace, mknod)***.
FPT_RTE.1.2	The TSF shall maintain a restricted runtime environment for ***all TOE processes that accept connections from the connected interfaces***.

5.3 TOE Security Assurance Requirements

The TOE claims compliance to EAL4 level of assurance plus augmentations AVA_VLA.4 and ALC_FLR.2. For a complex product like the two-tiered firewall **GeNUGate 6.0 Z**, this is considered to be the highest possible level, when considering the drastically increasing efforts at higher levels of assurance. As part 3 of the CC describe it, the level EAL4 indicates that the product is methodically designed, tested, and reviewed.

To counter the high threat of malicious attacks that firewalls must handle, the level EAL4 has been augmented with the vulnerability assurance requirement AVA_VLA.4 (Highly resistant), which is only mandatory for level EAL6 and higher. The assurance requirements for life cycle support has been augmented by ALC_FLR.2 (Flaw reporting procedures) to account for regular bug fixes for **GeNUGate 6.0 Z**.

In the following table all security assurance requirement descriptions mandated by EAL4 are printed in normal weight. The descriptions for the augmented security assurance requirements are printed in bold text. The requirement AVA_VLA.2 has been left in parenthesis in the table to indicate that it is still required although only the stronger requirement AVA_VLA.4 should appear.

Table 9: Security Assurance Requirements

	Security Assurance Requirement
Configuration management	**ACM_AUT.1** Partial CM automation **ACM_CAP.4** Generation support and acceptance procedures **ACM_SCP.2** Problem tracking CM coverage
Delivery and operation	**ADO_DEL.2** Detection of modification **ADO_IGS.1** Installation, generation, and start-up procedures

	Security Assurance Requirement
Development	**ADV_FSP.2** Fully defined external interfaces **ADV_HLD.2** Security enforcing high-level design **ADV_IMP.1** Subset of the implementation of the TSF **ADV_LLD.1** Descriptive low-level design **ADV_RCR.1** Informal correspondence demonstration **ADV_SPM.1** Informal TOE security policy model
Guidance documents	**AGD_ADM.1** Administrator guidance **AGD_USR.1** User guidance
Life cycle support	**ALC_DVS.1** Identification of security measures **ALC_LCD.1** Developer defined life-cycle model **ALC_TAT.1** Well-defined development tools **ALC_FLR.2 Flaw reporting procedures**
Tests	**ATE_COV.2** Analysis of coverage **ATE_DPT.1** Testing: high-level design **ATE_FUN.1** Functional testing **ATE_IND.2** Independent testing - sample
Vulnerability assessment	**AVA_MSU.2** Validation of analysis **AVA_SOF.1** Strength of TOE security function evaluation (**AVA_VLA.2** Independent vulnerability analysis) **AVA_VLA.4 Highly resistant**

5.4 Security Requirements for the IT Environment

The security functional requirements have been drawn from the CC Part 2.

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 operation assignment is set in a bold 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.

5.4.1 Class FPT: Protection of the TSF

Time stamps (FPT_STM)

FPT_STM.1	**Reliable time stamps**
FPT_STM.1.1	The ~~TSF~~*IT environment* shall be able to provide reliable time stamps for ~~its own use~~*the TOE use*.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functions

6.1.1 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 administrator Id. 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.

6.1.2 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 arts checked like non encoded messages.

6.1.3 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 succesful 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 3. 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.

6.1.4 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, 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.

6.1.5 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.

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: All incoming data that is mediated between the networks shall be processed in a restricted runtime environment that does not provide the full system to the process handling the data.

SF_PT.4: 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.5: During normal operation the packet filter rules cannot be modified. They are sealed when changing into normal operation mode.

6.1.6 Probabilistic or Permutational Security Functions

The TOE defines security functions that use probabilistic or permutational algorithms. This are the functions **SF_IA.3**, **SF_IA.4**, and **SF_IA.5**. The strength of function for these functions is **SOF-high**.

6.2 Assurance Measures

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

6.2.1 Configuration management

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

6.2.2 Delivery and operation

The developer will provide documentation that describe how the product **GeNUGate 6.0 Z** is delivered and installed. The document will contain enough details to show how the requirements **ADO_DEL.2** and **ADO_IGS.1** are met.

6.2.3 Development

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

6.2.4 Guidance documents

The **GeNUGate 6.0 Z** manual contains the administrator guide. It explains in great detail how to operate the **GeNUGate 6.0 Z** securely. It also contains a chapter for normal users that describes how to interact correctly with **GeNUGate 6.0 Z**. The manual meets the requirements **AGD_ADM.1** and **AGD_USR.1**.

6.2.5 Life cycle support

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

6.2.6 Tests

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

6.2.7 Vulnerability assessment

The developer will provide the required analysis documentation that shows that guidance is given for secure operation in all modes of operation. It will contain a vulnerability analysis. The documentation will provide enough information to meet **AVA_MSU.2** and **AVA_VLA.4**, and **AVA_SOF.1**.

7 PP CLAIMS

There are no Protection Profile claims.

8 RATIONALE

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

8.1 Security Objectives Rationale

The following table demonstrates that each threat is met by at least one security objective and that all threats have been addressed.

Table 10: 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.

The following table demonstrates that each policy is met by at least one security objective and that all policies have been addressed.

Table 11: 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.

The following discussion shows that all assumptions are met by objectives for the environment.

Table 12: 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 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.
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.

8.2 Security Requirements Rationale

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

8.2.1 Objectives

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

Table 13: 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.

Objectives	SFR
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 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. **FPT_RTE.1**: This component defines how the runtime environments of different processes are separated. The SFRs are mutually supportive. They are sufficient to meet the objective.

Objectives	SFR
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.2**: This component makes sure that the audit log can be written. **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.

Objectives	SFR
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. **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.
OE.TIMESTMP	**FPT_STM.1**: This component requires reliable timestamps from the IT environment. The SFR is sufficient to meet the objective.

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

Table 14: SFR coverage

SFR	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELFPRO	O.AUDREC	O.ACCOUN	O.SECFUN	OE.TIMESTMP
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.2					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						
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	

SFR	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SELFPRO	O.AUDREC	O.ACCOUN	O.SECFUN	OE.TIMESTMP
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_RTE.1				X				
FPT_STM.1								X

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

Table 15: 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**.

SFR	Rationale
FAU_SAR.3	This component allows the searching of the audit log and contributes to **O.AUDREC**.
FAU_STG.2	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 administrator SFP and contributes to **O.MEDIAT**.

SFR	Rationale
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**.

SFR	Rationale
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**.
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_RTE.1	This component defines how the runtime environments of different processes are separated. It contributes to **O.SELPRO**.
FPT_STM.1	This component requires reliable timestamps from the IT environment. It aids in meeting **OE.TIMESTMP**.

8.2.2 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.

FPT_RTE.1: The single component of this new family **FPT_RTE** is somewhat modelled after **FPT_SEP.1**. The other components of the family **FPT_SEP** clearly indicate that using this family requires the implementation of a reference monitor. Separated runtime environments can, however, also be implemented 'ad-hoc' without a full reference monitor concept. In order to avoid the association with the reference monitor, a new family was introduced. Also, the runtime environment must not necessarily only be only restricted to the TSFs.

8.2.3 Dependencies between the SFR and SAR

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

Table 16: Dependencies

Id	SFR/SAR	Dependencies	Satisfied by	Security Function
1-1	**FAU_ARP.1**	**FAU_SAA.1**	1-3	**SF_SA.4**
1-2	**FAU_GEN.1EX**	**FPT_STM.1**	5-4	**SF_SA.1**, **SF_SA.2**, **SF_SA.3**
1-3	**FAU_SAA.1**	**FAU_GEN.1**	1-2	**SF_SA.4**
1-4	**FAU_SAR.1**	**FAU_GEN.1**	1-2	**SF_SA.5**
1-5	**FAU_SAR.2**	**FAU_SAR.1**	1-4	**SF_SA.5**
1-6	**FAU_SAR.3**	**FAU_SAR.1**	1-4	**SF_SA.5**
1-7	**FAU_STG.2**	**FAU_GEN.1**	1-2	**SF_SA.4**, **SF_SA.6**
1-8	**FAU_STG.4**	**FAU_STG.1**	1-7	**SF_SA.6**
2-1-1	**FDP_IFC.1:1**	**FDP_IFF.1:1**	2-2-1	**SF_DF.1**, **SF_DF.2**, **SF_DF.3**, **SF_DF.4**, **SF_DF.5**

Id	SFR/SAR	Dependencies	Satisfied by	Security Function
2-1-2	**FDP_IFC.1:2**	**FDP_IFF.1:2**	2-2-2	**SF_DF.1**, **SF_DF.2**, **SF_IA.3**
2-1-3	**FDP_IFC.1:3**	**FDP_IFF.1:3**	2-2-3	**SF_DF.1**, **SF_DF.2**, **SF_IA.4**, **SF_IA.6**, **SF_IA.7**
2-1-4	**FDP_IFC.1:4**	**FDP_IFF.1:4**	2-2-4	**SF_DF.1**, **SF_DF.2**, **SF_IA.6**, **SF_IA.7**
2-1-5	**FDP_IFC.1:5**	**FDP_IFF.1:5**	2-2-5	**SF_DF.1**, **SF_DF.2**, **SF_IA.6**, **SF_IA.7**
2-2-1	**FDP_IFF.1:1**	**FDP_IFC.1:1** **FMT_MSA.3:X**	2-1-1 N/A	**SF_DF.1**, **SF_DF.2**, **SF_DF.3**, **SF_DF.4**, **SF_DF.5**
2-2-2	**FDP_IFF.1:2**	**FDP_IFC.1:2** **FMT_MSA.3:1**	2-1-2 4-3-1	**SF_DF.1**, **SF_DF.2**, **SF_IA.3**
2-2-3	**FDP_IFF.1:3**	**FDP_IFC.1:3** **FMT_MSA.3:X**	2-1-3 N/A	**SF_DF.1**, **SF_DF.2**, **SF_IA.4**, **SF_IA.6**, **SF_IA.7**
2-2-4	**FDP_IFF.1:4**	**FDP_IFC.1:4** **FMT_MSA.3:2**	2-1-4 4-3-2	**SF_DF.1**, **SF_DF.2**, **SF_IA.6**, **SF_IA.7**
2-2-5	**FDP_IFF.1:5**	**FDP_IFC.1:5** **FMT_MSA.3:3**	2-1-5 4-3-3	**SF_DF.1**, **SF_DF.2**, **SF_IA.6**, **SF_IA.7**
3-1	**FIA_AFL.1**	**FIA_UAU.1**	3-4	**SF_IA.6**
3-2	**FIA_ATD.1**			**SF_SM.1**
3-3	**FIA_SOS.1**			**SF_IA.3**, **SF_IA.4**, **SF_IA.5**
3-4	**FIA_UAU.2**	**FIA_UID.1**	3-7	**SF_IA.3**, **SF_IA.4**, **SF_IA.5**
3-5	**FIA_UAU.5EX**			**SF_IA.3**, **SF_IA.4**, **SF_IA.5**, **SF_IA.8**
3-6	**FIA_UAU.6**			**SF_IA.7**
3-7	**FIA_UID.2**			**SF_IA.1**, **SF_IA.2**, **SF_IA.3**, **SF_IA.4**, **SF_IA.5**, **SF_IA.8**
4-1-1	**FMT_MOF.1:1**	**FMT_SMF.1** **FMT_SMR.1**	4-5 4-6	**SF_SM.5**

Id	SFR/SAR	Dependencies	Satisfied by	Security Function
4-1-2	**FMT_MOF.1:2**	**FMT_SMF.1** **FMT_SMR.1**	4-5 4-6	**SF_SM.5**
4-1-3	**FMT_MOF.1:3**	**FMT_SMF.1** **FMT_SMR.1**	4-5 4-6	**SF_IA.8**
4-2-1	**FMT_MSA.1:1**	**FDP_IFC.1:5** **FMT_SMF.1** **FMT_SMR.1**	2-1-5 4-5 4-6	**SF_SM.3**, **SF_SM.4**
4-2-2	**FMT_MSA.1:2**	**FDP_IFC.1:5** **FMT_SMF.1** **FMT_SMR.1**	2-1-5 4-5 4-6	**SF_SM.3**, **SF_SM.4**
4-2-3	**FMT_MSA.1:3**	**FDP_IFC.1:4** **FMT_SMF.1** **FMT_SMR.1**	2-1-4 4-5 4-6	**SF_SM.3**, **SF_SM.4**
4-2-4	**FMT_MSA.1:4**	**FDP_IFC.1:5** **FMT_SMF.1** **FMT_SMR.1**	2-1-5 4-5 4-6	**SF_SM.3**, **SF_SM.4**
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	**SF_SM.3**
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	**SF_SM.3**
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	**SF_SM.3**
4-4-1	**FMT_MTD.1:1**	**FMT_SMF.1** **FMT_SMR.1**	4-5 4-6	**SF_SM.1**, **SF_SM.2**
4-4-2	**FMT_MTD.1:2**	**FMT_SMF.1** **FMT_SMR.1**	4-5 4-6	**SF_SM.1**, **SF_SM.2**
4-5	**FMT_SMF.1**			**SF_SM.2**
4-6	**FMT_SMR.2**	**FIA_UID.1**	3-7	**SF_IA.5**, **SF_SM.1**
4-7	**FMT_SMR.3**	**FMT_SMR.1**	4-6	**SF_SM.1**, **SF_IA.5**

Id	SFR/SAR	Dependencies	Satisfied by	Security Function
5-1	**FPT_RCV.2**	**FPT_TST.1** **AGD_ADM.1** **ADV_SPM.1**	5-2 9-1 8-6	**SF_PT.1**, **SF_PT.2**, **SF_PT.5**
5-2	**FPT_SST.1**			**SF_PT.4**
5-3	**FPT_RTE.1**			**SF_PT.3**
5-4	**FPT_STM.1**			**Environment**
6-1	**ACM_AUT.1**	**ACM_CAP.3**	6-2	
6-2	**ACM_CAP.4**	**ALC_DVS.1**	10-1	
6-3	**ACM_SCP.2**	**ACM_CAP.3**	6-2	
7-1	**ADO_DEL.2**	**ACM_CAP.3**	6-2	
7-2	**ADO_IGS.1**	**AGD_ADM.1**	9-1	
8-1	**ADV_FSP.2**	**ADV_RCR.1**	8-5	
8-2	**ADV_HLD.2**	**ADV_FSP.1** **ADV_RCR.1**	8-1 8-5	
8-3	**ADV_IMP.1**	**ADV_LLD.1** **ADV_RCR.1** **ALC_TAT.1**	8-4 8-5 10-3	
8-4	**ADV_LLD.1**	**ADV_HLD.2** **ADV_RCR.1**	8-2 8-5	
8-5	**ADV_RCR.1**			
8-6	**ADV_SPM.1**	**ADV_FSP.1**	8-1	
9-1	**AGD_ADM.1**	**ADV_FSP.1**	8-1	
9-2	**AGD_USR.1**	**ADV_FSP.1**	8-1	
10-1	**ALC_DVS.1**			
10-2	**ALC_LCD.1**			

Id	SFR/SAR	Dependencies	Satisfied by	Security Function
10-3	**ALC_TAT.1**	**ADV_IMP.1**	8-3	
10-4	**ALC_FLR.2**			
11-1	**ATE_COV.2**	**ADV_FSP.1** **ATE_FUN.1**	8-1 11-3	
11-2	**ATE_DPT.1**	**ADV_HLD.1** **ATE_FUN.1**	8-2 11-3	
11-3	**ATE_FUN.1**			
11-4	**ATE_IND.2**	**ADV_FSP.1** **AGD_ADM.1** **AGD_USR.1** **ATE_FUN.1**	8-1 9-1 9-2 11-3	
12-1	**AVA_MSU.2**	**ADO_IGS.1** **ADV_FSP.1** **AGD_ADM.1** **AGD_USR.1**	7-2 8-1 9-1 9-2	
12-2	**AVA_SOF.1**	**ADV_FSP.1** **ADV_HLD.1**	8-1 8-2	
12-3	**AVA_VLA.4**	**ADV_FSP.1** **ADV_HLD.2** **ADV_IMP.1** **ADV_LLD.1** **AGD_ADM.1** **AGD_USR.1**	8-1 8-2 8-3 8-4 9-1 9-2	

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

The following discusses cases where the dependencies are not met, and those cases, where iteration can lead to dependencies on different iterations:

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**.

FPT_RCV.2: The dependency on **FPT_TST.1** has been replaced by **FPT_SST.1**. This is possible because **FPT_SST.1** is modelled after **FPT_TST.1**, without the requirement for an abstract state

machine. It is noted that **FPT_RCV.2** has no direct dependency on the abstract state machine.

The **SFR FPT_STM.1** is met by the environment.

8.3 Assurance Requirements Rationale

The TOE claims compliance to EAL4 level of assurance plus augmentations AVA_VLA.4 and ALC_FLR.2. For a complex product like the two-tiered firewall **GeNUGate 6.0 Z**, this is considered to be the highest possible level, when considering the drastically increasing efforts at higher levels of assurance. As part 3 of the CC describe it, the level EAL4 indicates that the product is methodically designed, tested, and reviewed.

To counter the high threat of malicious attacks that firewalls must handle, the level EAL4 has been augmented with the vulnerability assurance requirement AVA_VLA.4 (Highly resistant), which is only mandatory for level EAL6 and higher. The assurance requirements for life cycle support has been augmented by ALC_FLR.2 (Flaw reporting procedures) to account for regular bug fixes for **GeNUGate 6.0 Z**.

8.4 Strength of Function Rationale

The overall strength of function claim for the TOE is **SOF-high**. The claim is applicable to the SFRs **FIA_SOS.1**, **FIA_UAU.2**, and **FIA_UAU.5EX**.

The TOE has security functions that are realized by a probabilistic or permutational mechanism. The functions are **SF_IA.3**, **SF_IA.4**, and **SF_IA.5**.

Firewalls are exposed to attacks of high attack potential, therefore it seems reasonable to claim a high strength of function for an evaluation at level EAL4+.

8.5 TOE Summary Specification Rationale

The tables shows how the SFR are mapped onto the SF.

SF_SA: Security audit

SF	Rationale
SF_SA.1	This SF describes audit data generation and aids to meet **FAU_GEN.1EX**.
SF_SA.2	This SF describes audit data generation and aids to meet **FAU_GEN.1EX**.
SF_SA.3	This SF describes audit data generation and aids to meet **FAU_GEN.1EX**.
SF_SA.4	This SF describes audit analysis and security alarms. It aids to meet **FAU_ARP.1** and **FAU_SAA.1**. It also describes the prevention of unauthorized deletion or unauthorized modification. It aids to meet **FAU_STG.2**.
SF_SA.5	This SF describes audit data review and aids to meet **FAU_SAR.1**, **FAU_SAR.2**, and **FAU_SAR.3**.

SF	Rationale
SF_SA.6	This SF describes measures taken to ensure enough audit storage space. It aids to meet **FAU_STG.2** and **FAU_STG.4**.

SF_DF: Data flow control

SF	Rationale
SF_DF.1	This SF describes the kernel part of the data flow control and aids to meet **FDP_IFC.1:1**, **FDP_IFC.1:2**, **FDP_IFC.1:3**, **FDP_IFC.1:4**, **FDP_IFC.1:5**, **FDP_IFF.1:1**, **FDP_IFF.1:2**, **FDP_IFF.1:3**, **FDP_IFF.1:4**, and **FDP_IFF.1:5**.
SF_DF.2	This SF describes the application level part of the data flow control and aids to meet **FDP_IFC.1:1**, **FDP_IFC.1:2**, **FDP_IFC.1:3**, **FDP_IFC.1:4**, **FDP_IFC.1:5,** **FDP_IFF.1:1**, **FDP_IFF.1:2**, **FDP_IFF.1:3**, **FDP_IFF.1:4**, and **FDP_IFF.1:5**.
SF_DF.3	This SF describes additional data flow control for the unauthenticated user SFP and aids to meet **FDP_IFC.1:1** and **FDP_IFF.1:1**.
SF_DF.4	This SF describes additional data flow control for the unauthenticated user SFP and aids to meet **FDP_IFC.1:1** and **FDP_IFF.1:1**.
SF_DF.5	This SF describes additional data flow control for the unauthenticated user SFP and aids to meet **FDP_IFC.1:1** and **FDP_IFF.1:1**.

SF_IA: Identification and Authentication

SF	Rationale
SF_IA.1	This SF describes the identification at IP-level and aids to meet **FIA_UID.2**.
SF_IA.2	This SF describes the connections at the transport layer and aids to meet **FIA_UID.2**.
SF_IA.3	This SF describes the security measures for the authenticated user SFP. It aids to meet **FIA_SOS.1**, **FIA_UAU.2**, **FIA_UAU.5EX**, **FIA_UID.2**, **FDP_IFC.1:2**, and **FDP_IFF.1:2**.
SF_IA.4	This SF describes the security measures for the authenticated gui user SFP. It aids to meet **FIA_SOS.1**, **FIA_UAU.2**, **FIA_UAU.5EX**, **FIA_UID.2**, **FDP_IFC.1:3** and **FDP_IFF.1:3**.

SF	Rationale
SF_IA.5	This SF describes the security measures for the authenticated administrator SFP. It aids to meet **FIA_SOS.1**, **FIA_UAU.2**, **FIA_UID.2**, **FIA_UAU.5EX**, **FMT_SMR.2**, and **FMT_SMR.3**.
SF_IA.6	This SF describes the disabling of passwords after authentication failure. It aids to meet **FIA_AFL.1**, **FDP_IFC.1:3**, **FDP_IFC.1:4**, **FDP_IFC.1:5**, **FDP_IFF.1:3**, **FDP_IFF.1.4** and **FDP_IFF.1:5**.
SF_IA.7	This SF describes the timeout for web based access. It aids to meet **FAI_UAU.6**, **FDP_IFC.1:3**, **FDP_IFC.1:4**, **FDP_IFC.1:5**, **FDP_IFF.1:3**, **FDP_IFF.1:4**, and **FDP_IFF.1:5**.
SF_IA.8	This SF describes the interaction at the console. It aids to meet **FIA_UID.2**, **FIA_UAU.5EX**, and **FMT_MOF.1:3**.

SF_SM: Security management

SF	Rationale
SF_SM.1	This SF describes the security roles. It aids to meet **FMT_SMR.2**, **FMT_SMR.3**, **FMT_MTD.1:1**, **FMT_MTD.1:2**, and **FIA_ATD.1**.
SF_SM.2	This SF lists the main configuration topics. It aids to meet **FMT_SMF.1**, **FMT_MTD.1:1**, **FMT_MTD.1:2**.
SF_SM.3	This SF describes the rights to change security roles. It aids to meet **FMT_MSA.1:1**, **FMT_MSA.1:2**, **FMT_MSA.1:3**, **FMT_MSA.1:4**, **FMT_MSA.3:1**, **FMT_MSA.3:2**, **FMT_MSA.3:3**.
SF_SM.4	This SF describes the rights to change timeouts. It aids to meet **FMT_MSA.1:1**, **FMT_MSA.1:2**, **FMT_MSA.1:3**, and **FMT_MSA.1:4**.
SF_SM.5	This SF describes the rights to change security functionality. It aids to meet **FMT_MOF.1:1** and **FMT_MOF.1:2**.

SF_PT: Protection of the TSF

SF	Rationale
SF_PT.1	This function describes the recovery after failure or maintenance. It aids to meet **FPT_RCV.2**.
SF_PT.2	This function describes the security in maintenance mode. It aids to meet **FPT_RCV.2**.

SF	Rationale
SF_PT.3	This function describes the acceptance of incoming connections. It aids to meet **FPT_RTE.1**.
SF_PT.4	This function describes the self tests. It aids to meet **FPT_SST.1**.
SF_PT.5	This function describes the sealing of the packet filter rules during normal operation. It aids to meet **FPT_RCV.2**.

The following table shows that all SFR are met by the SF.

Table 17: SFR

SFR	Security Function
FAU_ARP.1	**SF_SA.4**: This function describes the log analysis and alarm generation. It searches all relevant log files, so that no log entry is missed. The security function does not interfere with any other function. It meets the requirement.
FAU_GEN.1EX	**SF_SA.1**: This function describes the general audit data generation. **SF_SA.2**: This function describes the additional audit data generation from the relays. **SF_SA.3**: This function describes the audit data generation for the administration web. This functions cover the audit generating TOE parts. Together they meet the requirement.
FAU_SAA.1	**SF_SA.4**: This function describes the automated search of the log files for relevant software failures. It does not interfere with other functions and meets the requirement.
FAU_SAR.1	**SF_SA.5**: This function describes the readability of the log files by humans. It does not interfere with other functions and meets the requirement.
FAU_SAR.2	**SF_SA.5**: This function describes that only administrators and auditors can view the log files. It does not interfere with other functions and meets the requirement.
FAU_SAR.3	**SF_SA.5**: This function describes the searchability of the log files. It does not interfere with other functions and meets the requirements.

SFR	Security Function
FAU_STG.2	**SF_SA.4**: This function describes the prevention of unauthorized deletion or modification of the log data. **SF_SA.6**: This function describes the check for available log file space and guarantees audit data availability. It does not interfere with other functions and meets the requirements.
FAU_STG.4	**SF_SA.6**: This function describes the actions taken in the event of a full audit trail. It does not interfere with other functions and meets the requirements.
FDP_IFC.1:1	**SF_DF.1**: This function implements the data flow control at the IP level and provides parts of the requirements for the unauthenticated user SFP. **SF_DF.2**: This function implements the data flow control at the relay level and provide parts of the requirements for the unauthenticated user SFP. **SF_DF.3**: This function implements the extra data flow control for the SMTP-relay and provide parts of the requirements for the unauthenticated user SFP. **SF_DF.4**: This function implement the extra data flow control for the WWW-relay and provides parts of the requirements for the unauthenticated user SFP. **SF_DF.5**: This function implements the extra data flow control for MIME-encoded messages and provides parts of the requirements for the unauthenticated user SFP. Every function performs only one specified part of the data flow control. The functions do not interfere and together they meet the requirements.
FDP_IFC.1:2	**SF_DF.1**: This function implements the data flow control at the IP level and provides parts of the requirements for the authenticated user SFP. **SF_DF.2**: This function implements the data flow control at the relay level and provide parts of the requirements for the authenticated user SFP. **SF_IA.3**: This function describes the authentication needed for the authenticated user SFP. Every function performs only one specific part of the data flow control. The functions do not interfere and together they meet the requirements.

SFR	Security Function
FDP_IFC.1:3	**SF_DF.1**: This function implements the data flow control at the IP level and provides parts of the requirements for the identified side channel user SFP. **SF_DF.2**: This function implements the data flow control at the relay level and provide parts of the requirements for the identified side channel user SFP. **SF_IA.4**: This function describes the activation of a sender IP address for relay usage by the side channel authentication. **SF_IA.6**: This function describes the handling of unsuccessful authentication attempts for the side channel authentication. **SF_IA.7**: This function describes the inactivity timeout for the identified side channel user SFP. Every function performs only one specific part of the data flow control. The functions do not interfere and together they meet the requirements.
FDP_IFC.1:4	**SF_DF.1**: This function implements the data flow control at the IP level and provides parts of the requirements for the authenticated gui user SFP. **SF_DF.2**: This function implements the data flow control at the relay level and provide parts of the requirements for the authenticated gui user SFP. **SF_IA.6**: This function describes the handling of unsuccessful authentication attempts for the user web. **SF_IA.7**: This function describes the inactivity timeout for the authenticated gui user SFP. Every function performs only one specific part of the data flow control. The functions do not interfere and together they meet the requirements.

SFR	Security Function
FDP_IFC.1:5	**SF_DF.1**: This function implements the data flow control at the IP level and provides parts of the requirements for the authenticated administrator SFP. **SF_DF.2**: This function implements the data flow control at the relay level and provide parts of the requirements for the authenticated administrator SFP. **SF_IA.6**: This function describes the handling of unsuccessful authentication attempts for the administration web. **SF_IA.7**: This function describes the inactivity timeout for the authenticated administrator SFP. Every function performs only one specific part of the data flow control. The functions do not interfere and together they meet the requirements.
FDP_IFF.1:1	**SF_DF.1**: This function implements the data flow control at the IP level and provides parts of the requirements for the unauthenticated user SFP. **SF_DF.2**: This function implements the data flow control at the relay level and provide parts of the requirements for the unauthenticated user SFP. **SF_DF.3**: This function implements the extra data flow control for the SMTP-relay and provide parts of the requirements for the unauthenticated user SFP. **SF_DF.4**: This function implement the extra data flow control for the WWW-relay and provides parts of the requirements for the unauthenticated user SFP. **SF_DF.5**: This function implements the extra data flow control for MIME-encoded messages and provides parts of the requirements for the unauthenticated user SFP. Every function performs only one specified part of the data flow control. The functions do not interfere and together they meet the requirements.

SFR	Security Function
FDP_IFF.1:2	**SF_DF.1**: This function implements the data flow control at the IP level and provides parts of the requirements for the authenticated user SFP. **SF_DF.2**: This function implements the data flow control at the relay level and provide parts of the requirements for the authenticated user SFP. **SF_IA.3**: This function describes the authentication needed for the authenticated user SFP. Every function performs only one specific part of the data flow control. The functions do not interfere and together they meet the requirements.
FDP_IFF.1:3	**SF_DF.1**: This function implements the data flow control at the IP level and provides parts of the requirements for the identified side channel user SFP. **SF_DF.2**: This function implements the data flow control at the relay level and provide parts of the requirements for the identified side channel user SFP. **SF_IA.4**: This function describes the activation of a sender IP address for relay usage by the side channel authentication. **SF_IA.6**: This function describes the handling of unsuccessful authentication attempts for the side channel authentication. **SF_IA.7**: This function describes the inactivity timeout for the identified side channel user SFP. Every function performs only one specific part of the data flow control. The functions do not interfere and together they meet the requirements.
FDP_IFF.1:4	**SF_DF.1**: This function implements the data flow control at the IP level and provides parts of the requirements for the authenticated gui user SFP. **SF_DF.2**: This function implements the data flow control at the relay level and provide parts of the requirements for the authenticated gui user SFP. **SF_IA.6**: This function describes the handling of unsuccessful authentication attempts for the user web. **SF_IA.7**: This function describes the inactivity timeout for the authenticated gui user SFP. Every function performs only one specific part of the data flow control. The functions do not interfere and together they meet the requirements.

SFR	Security Function
FDP_IFF.1:5	**SF_DF.1**: This function implements the data flow control at the IP level and provides parts of the requirements for the authenticated administrator SFP. **SF_DF.2**: This function implements the data flow control at the relay level and provide parts of the requirements for the authenticated administrator SFP. **SF_IA.6**: This function describes the handling of unsuccessful authentication attempts for the administration web. **SF_IA.7**: This function describes the inactivity timeout for the authenticated administrator SFP. Every function performs only one specific part of the data flow control. The functions do not interfere and together they meet the requirements.
FIA_AFL.1	**SF_IA.6**: The function describes the handling of authentication failures for user authentication, side channel authentication and administrator authentication. It meets the requirement.
FIA_ATD.1	**SF_SM.1**: The function lists the security attributes of the users.
FIA_SOS.1	**SF_IA.3**: This function describes the verifying of authentication information for the TELNET- and FTP-relay. It provides parts to the requirement. **SF_IA.4**: This function describes the verifying of authentication information for the side channel authentication. It provides parts to the requirement. **SF_IA.5**: This function describes the verifying of authentication information for the administrator authentication. It provides parts to the requirement. Every function performs only one specified part of the requirements. The functions do not interfere and together they meet the requirements.
FIA_UAU.2	**SF_IA.3**: This function describes the authentication procedure for the TELNET- and FTP-relay usage. It provides parts to the requirement. **SF_IA.4**: This function describes the authentication procedure for the side channel authentication. It provides parts to the requirement. **SF_IA.5**: This function describes the authentication procedure for the administrator authentication. It provides parts to the requirements. Every function performs only one specified part of the requirements. The functions do not interfere and together they meet the requirements.

SFR	Security Function
FIA_UAU.5EX	**SF_IA.3**: This function describes the usage of external authentication methods for the TELNET- and FTP-relay. It provides parts to the requirement. **SF_IA.4**: This function describes the usage of external authentication methods for the side channel authentication. It provides parts to the requirement. **SF_IA.5**: This function describes the administrator authentication at the administrative webserver. **SF_IA.8**: This function describes the administrator authentication at the console. Every function performs only one specified part of the requirements. The functions do not interfere and together they meet the requirements.
FIA_UAU.6	**SF_IA.7**: This function describes the reauthentication that is required after inactivity. The function meets the requirement.
FIA_UID.2	**SF_IA.1**: This function describes the identification at the IP level. It meets parts of the requirement. **SF_IA.2**: This function describes the connections for TCP-based services and the association for IP- and UDP-based services. It helps in identifying the users and meets part of the requirement. **SF_IA.3**: This function describes the user identification at application level for the TELNET- and FTP-relay. It helps to meet the requirement. **SF_IA.4**: This function describes the user identification at application level for the side channel authentication. It helps to meet the requirement. **SF_IA.5**: This function describes the administrator identification at application level. It helps to meet the requirement. **SF_IA.8**: This function describes the administrator authentication at the console. Every function performs only one specified part of the requirements. The functions do not interfere and together they meet the requirements.
FMT_MOF.1:1	**SF_SM.5**: This function describes changing the authentication methods and generation detail of the log messages. This function meet the requirement.
FMT_MOF.1:2	**SF_SM.5**: This function describes viewing the settings for the authentication methods and log messages. This function meet the requirements.

SFR	Security Function
FMT_MOF.1:3	**SF_IA.8**: This function describes the restrictions to start or stop the security functions. The function meets the requirements.
FMT_MSA.1:1	**SF_SM.3**: This function describes that only administrators can change the administrative roles of users. **SF_SM.4**: This function describes the rights to change timeouts. Every function performs only one specific part of the requirements. The functions do not interfere and together they meet the requirements.
FMT_MSA.1:2	**SF_SM.3**: This function describes that administrators and auditors can view the administrative roles of users. **SF_SM.4**: This function describes the rights to change timeouts. Every function performs only one specific part of the requirements. The functions do not interfere and together they meet the requirements.
FMT_MSA.1:3	**SF_SM.3**: This function describes that users can change their own password. **SF_SM.4**: This function describes the rights to change timeouts. Every function performs only one specific part of the requirements. The functions do not interfere and together they meet the requirements.
FMT_MSA.1:4	**SF_SM.3**: This function describes that administrators can change the administrative and the user passwords. **SF_SM.4**: This function describes the rights to change timeouts. Every function performs only one specific part of the requirements. The functions do not interfere and together they meet the requirements.
FMT_MSA.3:1	**SF_SM.3**: The function describes the default values for security attributes for the authenticated user SFP. The function meets the requirement.
FMT_MSA.3:2	**SF_SM.3**: The function describes the default values for security attributes for the authenticated gui user SFP. The function meets the requirement.
FMT_MSA.3:3	**SF_SM.3**: The function describes the default values for security attributes for the authenticated administrator user SFP. The function meets the requirement.

SFR	Security Function
FMT_MTD.1:1	**SF_SM.1**: This function describes who can edit the configuration data. **SF_SM.2**: The function specifies which configuration data exists and can be changed. Every function performs only one specified part of the requirements. The functions do not interfere and together they meet the requirements.
FMT_MTD.1:2	**SF_SM.1**: This function describes who can view the configuration data. **SF_SM.2**: The function specifies which configuration data exists and can be changed. Every function performs only one specified part of the requirements. The functions do not interfere and together they meet the requirements.
FMT_SMF.1	**SF_SM.2**: The function specifies which configuration data exists and can be changed. Every function performs only one specified part of the requirements. The functions do not interfere and together they meet the requirements.
FMT_SMR.2	**SF_IA.5**: This function specifies that administration through the web interface is only possible from the administration network. **SF_SM.1**: This function specifies the different user roles. Every function performs only one specified part of the requirements. The functions do not interfere and together they meet the requirements.
FMT_SMR.3	**SF_SM.1**: This function specifies the different user roles. **SF_IA.5**: This function describes the authentication procedure to assume administrative roles. Every function performs only one specified part of the requirements. The functions do not interfere and together they meet the requirements.
FPT_RCV.2	**SF_PT.1**: This function describes the actions taken in case of failure. **SF_PT.2**: This function describes the actions taken in maintenance mode. **SF_PT.5**: This function describes the packet filter sealing during change from maintenance to normal operation.

SFR	Security Function
FPT_SST.1	**SF_PT.4**: This function describes the regular self tests. The function meets the requirement.
FPT_RTE.1	**SF_PT.3**: This function describes the functionality that runs in a restricted runtime environment. The function meets the requirement.
FPT_STM.1	**Environment**: This requirement must be met by the environment.

8.6 PP Claims Rationale

There are no Protection Profile claims.

9 Appendix

9.1 Tailored or new SFR

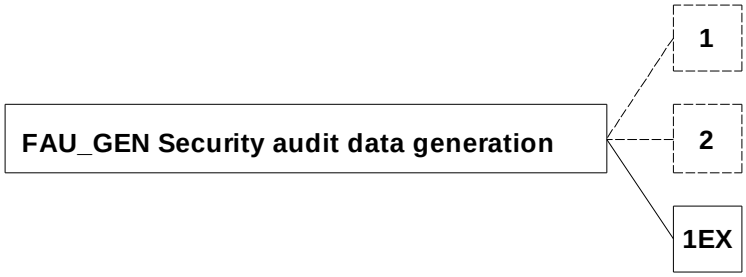
9.1.1 Class FAU: Security audit

Security audit data generation (FAU_GEN)

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**.

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 appendix.

Management: for FAU_GEN.1EX

There are no management activities foreseen.

Audit: for FAU_GEN.1EX

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

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**

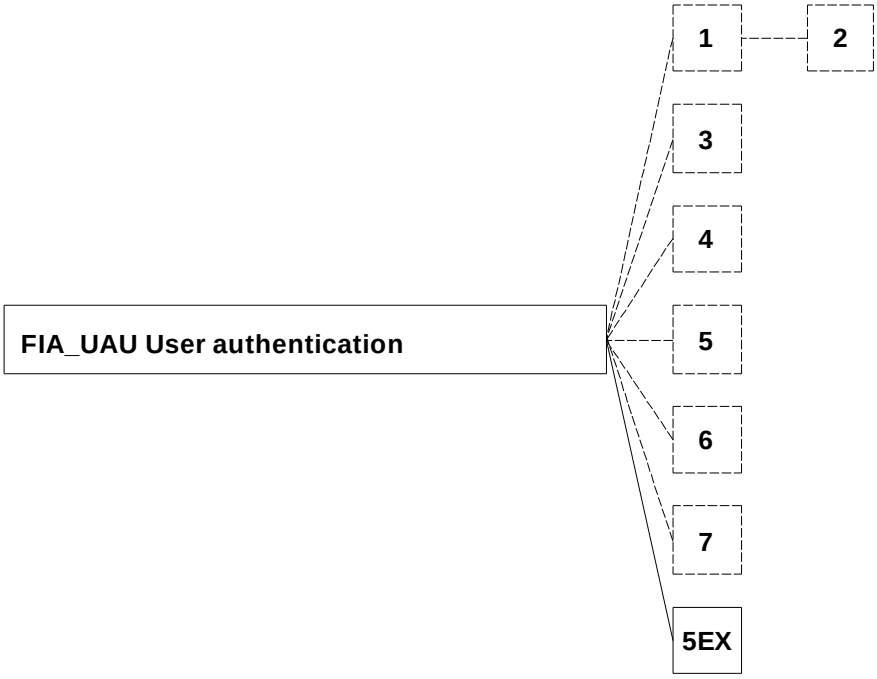
9.1.2 Class FIA: Identification and authentication

User authentication (FIA_UAU)

Family behaviour

The family has been enhanced by one component **FIA_UAU.5EX**. It is thought as a replacement for **FAU_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 **FAU_UAU.5**, because it requires the same functionality.

Component levelling



The components **FAI_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 **FAU_UAU.5EX** will be described in this appendix.

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.

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.

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

9.1.3 Class FPT: Protection of the TSF

Simple Self Test (FPT_SST)

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.

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.

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.

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.

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

Runtime Environment (FPT_RTE)

Family behaviour

The components of this family ensure that the TSF is protected from external interference and tampering (e.g. by modification of TSF code or data structures) by untrusted subjects by isolating the untrusted subjects in a restricted runtime environment. Satisfying the requirements of this family makes the TSF self protecting, meaning that an untrusted subject cannot modify or damage the TSF.

The resources of the TSF's restricted runtime environment and those of subjects and unconstrained entities external to the restricted runtime environment are separated such that the entities in the protected runtime environment cannot observe or modify TSF data or TSF code outside of the restricted runtime environment.

Component levelling

FPT_RTE.1 Restricted runtime environment, provides a distinct protected domain for the TSF and provides separation between subjects within the TSC.

Management: for FPT_RTE.1

There are no management activities foreseen.

Audit: for FPT_RTE.1

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

FPT_RTE.1 Restricted Runtime Environment

Hierarchical to: No other components.

FPT_RTE.1.1 The restricted runtime environment implements the following restrictions: [assignment: list of restrictions].

FPT_RTE.1.2 The TSF shall maintain a restricted runtime environment for [assignment: list of processes that are exposed to security threats].

Dependencies: No dependencies

10 Glossary

Runtime Environment: The POSIX chroot system call restricts the access of processes to the file system. The enhancements implemented by GeNUA restrict the access rights also for other resources and disallow the system calls chroot, kill, strace, ptrace and mknod for certain arguments.

IP Spoofing: There are different kinds of IP spoofing. Spoofing in general means that IP addresses are used for source or destination which usually are not valid in the respective network.

Source-Spoofing: The source address of the IP packets are spoofed, so that responses to the spoofed address are emitted on a different interface. This is detected by a mismatch of the source IP address and the IP address (and netmask) configured for the interface.

Destination-Spoofing: The destination address of the IP packet is spoofed, and the software dealing with the IP packet might associate the wrong interface with the packet, due to the spoofed IP address. This is detected by a mismatch of the destination address and the IP address (and netmask) configured for the interface.

Identification and Authentication: All users of the TOE are identified by their IP source address. If an authentication is necessary, the authentication data is transmitted through the (TCP-) connection. If the authentication fails, the connection is closed.

Interactive access: Administrators have an interactive access at the console both in maintenance and normal operation mode. Access control is provided by the UNIX file system permissions. The administrator has superuser (root) access and can modify all files in the maintenance mode. The revisor has no root access rights, but can read all files necessary for the revisor role. This includes the configuration files and the log files. Usually the direct access at the console is usually only used during (re-) booting the system, when e.g. installing patches, writing PFL floppies, or rotating flagged log files require an interaction.

IP Association: The relays that operate on IP packets assign all packets with the same IP protocol, source and destination IP address (and reversed addresses) to an IP association, if the packets arrive during a defined short time span. This allows to add a `connection state' to the IP data flow.

UDP Association: The UDP relay assigns all packets with the same source and destination port and IP address (and packets with reversed destination/source) to an UDP association, if the packets arrive during a defined short time span. This allows to add a `connection state' to the UDP data flow.

Demilitarised Zone: A separate network branch that is isolated from both the external net and the internal net. It is usually used to provide services to the external net.

Operation modes: The product family **GeNUGate** has two operation modes.

normal operation mode: In this operation mode the product family **GeNUGate** is transferring data between the connected networks according to its configuration. In order to resist modifications of its TOE data, the kernel variable security level is set to 2. At this level the BSD flags cannot be removed and important files are protected against tampering.

maintenance mode: In this mode no data is transferred between the connected networks. The security level is reset to a lower level that allows removing the BSD flags for maintenance (e.g. applying patches). On re-entering the normal operation mode the security level is increased before allowing network traffic.

BSD Flags: Besides the normal permission modes of the file system, BSD systems also carry so-called flags, that indicate special access restrictions. For each flag there are two variants, one for

the superuser, and one for the normal user. Of special interest here are the immutable flag and the append-only flag. In order to effectively protect files the kernel variable security level should be at least 2, this level disallows changing the flags.

11 Abbreviations

TCP Transmission Control Protocol

UDP User Datagram Protocol

IP Internet Protocol

DMZ demilitarised zone

ALG Application Level Gateway

PFL Packet Filter

ICMP Internet Control Message Protocol

NNTP Network News Transfer Protocol

SMTP Simple Mail Transfer Protocol

HTTP Hyper Text Transfer Protocol

NTP Network Time Protocol

POP Post Office Protocol

WWW World Wide Web

FTP File Transfer Protocol

URL Uniform Resource Locator

LDAP Lightweight Directory Access Protocol

S/KEY Secure Key

DNS Domain Name Service or Domain Name System

VPN Virtual Private Network