genuscreen 5.0

Security Target

Version 2

14 Aug 2015

genua gmbh

Domagkstr. 7, D-85551 Kirchheim, Germany

Table of Contents

1 ST Introduction

1.1 ST Reference

	ST Reference
ST Title	**genuscreen 5.0 Security Target**
Version	Version 2
Developer	genua gmbh
Date	14 Aug 2015

1.2 TOE Reference

	TOE Reference
TOE Title	**genuscreen 5.0**
Product Name	**genuscreen 5.0 Z**

1.3 TOE Overview

This chapter gives an overview about the Target Of Evaluation with it's two components genuscreen and genucenter.

1.3.1 genuscreen and genucenter

The TOE **genuscreen 5.0** makes VPN and firewall functionality available and easy to manage. It protects networks at the border to the Internet by filtering incoming and outgoing data traffic. It protects the data flowing between several protected networks against unauthorised inspection and modification. It consists of software on a number (at least 2) of machines (**genuscreen** appliances) that work as network filters, hereafter called firewall components, and another machine to manage this network of firewall components. This machine, the management system (**genucenter** management system), is a central component. The firewall components are initialised on a secure network from the management system. The TOE provides basic IPv6 support.

After initialisation, the firewall components can be distributed to the locations of the networks they are protecting.The **genuscreen** firewall components filter incoming and outgoing traffic for multiple networks and can thus enforce a given security policy on the data flow. The filter is implemented in the kernel of the firewall components' operating system, OpenBSD. The firewall components can work as bridges or routers. The firewall components can be used in an optional high availability (HA) setup where the firewall components synchronize their internal states.

At the same time the firewall components can provide confidentiality and integrity for data traffic passing between the networks. This Virtual Private Network function is achieved by IPsec encryption and authentication mechanisms using up-to-date ciphers and key sizes. The IPsec transforms are implemented in the kernel. The key agreement for IPsec follows

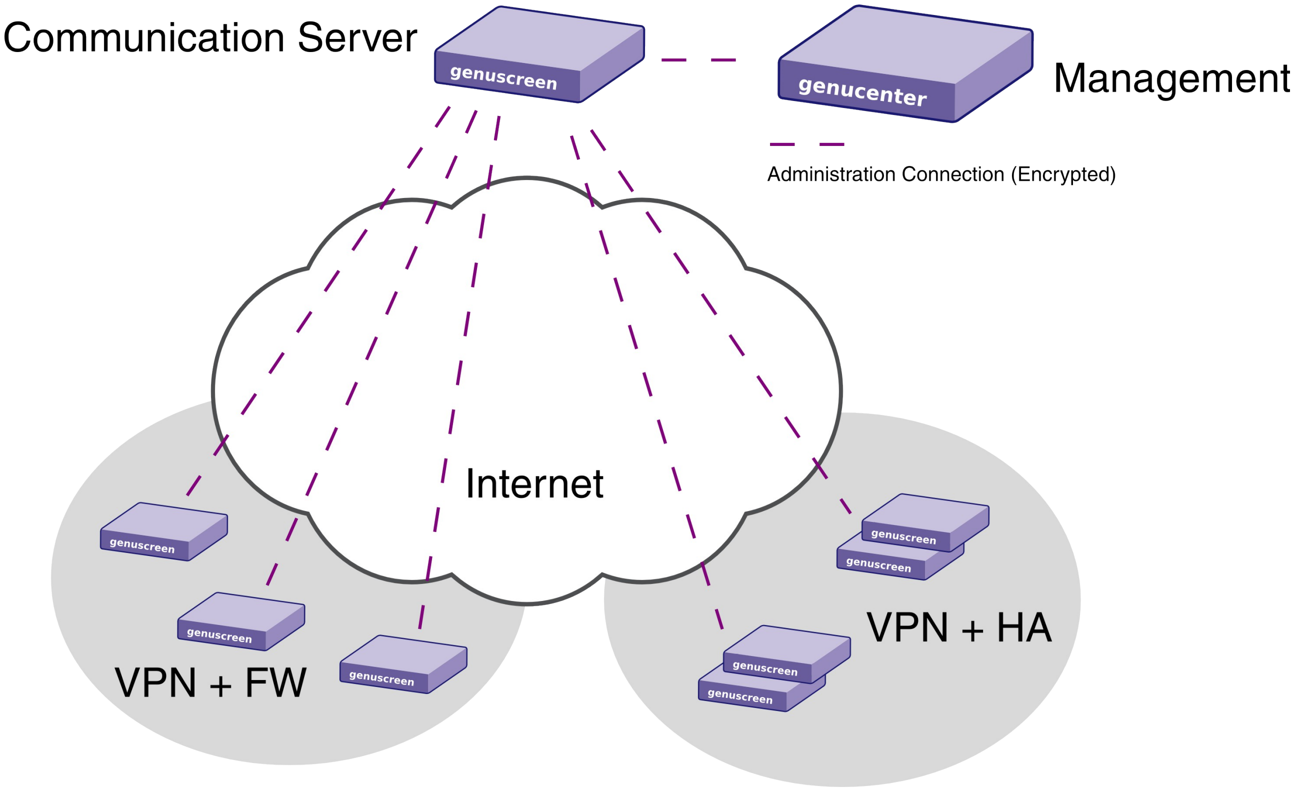


Figure 1: Two genuscreen virtual private networks managed by genucenter. The VPN on the left has additional packet filter rules for unencrypted communication. The VPN on the right is using the HA option. The appliances contact the genucenter through the communication server.

the ISAKMP Internet standard [RFC2409], and is implemented in user space by OpenBSD's `isakmpd`.

Alternatively, an encrypted tunnel not using the transport layer but the application layer can be build up with SSH connections. This scenario is useful if the full IP connectivity provided by IPsec is unwanted. This composition is referred to as the SSH launch daemon.

Interfaces of the firewall components can be classified at level high or low. Traffic on interfaces with a low classification is not transferred as cleartext.

The management system component provides administrators with a Graphical User Interface (GUI) to initialise and manage the firewall components from a central server. The management system also allows collecting audit data and monitoring. It can be used to configure other appliances than genuscreen, such as genugate, genucrypt, or third party products. However, this document only targets genuscreen.

The communication server between the genuscreen appliances and the genucenter management system avoids exposing the genucenter to the Internet.

Figure 1 shows an example setup with two separate VPNs managed by one genucenter. The connection between the genucenter and genuscreens is encrypted with SSH. The VPNs are encrypted either by IPsec or by SSH.

1.3.2 Alternative: Local Administration

The genuscreen firewall components also have a local GUI that can be activated when needed. This case is useful if the firewall component can not be reached by the management system due to missing (Internet) connectivity. Also, the log files of the firewall component can be stored locally.

1.3.3 Required non-TOE Hardware/Software/Firmware

The product is based on OpenBSD that runs on a large scale of hardware using different processors.

The following sections list the required non-TOE components of the product.

1.3.3.1 genucenter Management System

The following items are required for the management system:

- Hardware: Intel i386 compatible CPU with at least two network interfaces, a CD ROM, an optional USB interface, and a hard drive as permanent storage for the configuration and log files.

  Currently, the supported hardware variants gz200, gz400, gz600 and gz800.
- Software: OpenBSD Version 5.5, kernel and user space programs, HTTP/S server, DHCP server, TFTP server.

1.3.3.2 genuscreen Firewall Components

The following items are required for the firewall components:

- Hardware: Intel i386 compatible CPU with at least three network interfaces, an optional USB interface, and a hard drive or CompactFlash card as permanent storage for the configuration and log files. At least one of the network interfaces must support the PXE boot protocol.

  Currently, the supported hardware variants gs100b, gs100c, gs300, gs400, gs500, gs600, gs700 and gs800.
- Software: OpenBSD Version 5.5, kernel and user space programs, HTTP/S server.

1.4 TOE Description

The TOE is a distributed stateful packet filter firewall system with VPN capabilities and central configuration. It provides basic IPv6 support.

The TOE consists of software on a number of machines. The following sections describe the contribution of each part to the total TOE.

Not included in the TOE is the OpenBSD kernel, besides the IPsec and *pf* implementations.

1.4.1 genuscreen Appliances

These firewall components perform the network filtering and encryption between peers. The network filtering is done either as a bridge or as a packet filter, using the *pf* from OpenBSD.

The encryption between genuscreen peers is done using IPsec. See section 1.4.4 for a description of the possible features.

When using the SSH launch daemon, encrypted TCP connections are build by establishing a SSH connection to the peer and creating a TCP forwarding channel to tunnel the TCP connection. The SSH uses the SOCKS protocol to determine the destination address for the tunnelled TCP connection.

As good random numbers are a requirement for proper cryptographic operation, the genuscreen checks the quality of the random numbers at start-up and initiates an action if the quality is insufficient.

Network interfaces can be marked as belonging to two different classifications (low and high). The default classification is high. The firewall components then assure that traffic sent to or received from interfaces with the low classification is properly encrypted. No cleartext traffic is sent or received by these interfaces.

The genuscreen appliances have a local administrative GUI that must explicitly be activated. This GUI should only be used if a central administration by genucenter is not feasible, e. g. if there is no network connectivity between the two systems. The switch of the administration mode (local or remote) has to be initiated by an administrator. This administrative interface can only be reached through a separate administrative network. The local administrative GUI has only one administrator and one revisor.

The appliances operate in standalone mode either by installing from the genuscreen 5.0 Z installation CD or by enabling the local administrative GUI at the command line.

On startup the genuscreen appliances check the available entropy. If the entropy is not sufficient, they write a log message and disable VPN functionality (IPsec and SSH Launch Daemon), if configured accordingly.

The firewall components genuscreen can be operated in an optional high availability mode. If two genuscreens are configured as a high available pair their pf states and SA states are synced by two daemons. Thus a takeover can take place without interrupting connections and VPNs. The high availability option for genucenter is *not* part of the TOE.

1.4.2 genucenter Management System

The genucenter management system is used as a central for all appliances. It allows to configure the appliances, update them and to collect the log data. The genuscreen appliances are installed at the management system in a secure way using a dedicated installation network. The administrative GUI allows for a tree-like hierarchical organisation of appliances in nested domains. Each domain has a list of administrators, revisors and service users that are allowed to configure or review the domain and its contained appliances and their audit data. The intermediate role service is allowed to perform maintenance activities i.e. updating applications and collecting log data. They are not allowed to do any configuration. Administration can only happen from a dedicated administrative network.

The update of the genuscreen appliances is started by the appliances. They contact and authenticate at a communication server. By using particular SSH configurations, the management server can then transfer the configuration through SSH tunnels onto the genuscreen appliances. The communication server is a specially configured genuscreen appliance meant to protect the genucenter.

Also the log data from the genuscreen appliances is transferred over an SSH channel to the genucenter when they are configured for central storage. The log messages can be viewed and sorted in the GUI inside the respective domain.

The genucenter is installed from the genucenter 5.0 Z installation CD. This medium also contains all software to install the genuscreen appliances.

The genucenter can also configure other appliances than genuscreen. However, they are not part of the TOE.

The following sections describe non-obvious special features of the TOE.

1.4.3 PF Features

The *pf* is a powerful stateful packet filter, that can also be used for NAT and RDR rules (redirect to another recipient). It can perform packet defragementation and normalization of TCP (and IP) options. The outgoing packets can be put in different queues allowing for Quality of Service. Packet tagging and filtering by tag help to enforce security policies.

1.4.4 IPsec Features

The genuscreen appliances implement the protocol IKEv1. The following IPsec configurations are possible for the TOE:

- **Full meshed net**: All appliances talk directly to each other. This is the most general configuration. There is no central.
- **Central and satellites**: The satellites can only talk to the central.
- **Central and satellites with forwarding**: The central forwards packets that are destined to the satellites network. This works by decrypting the received packet and encrypting once more for the destination satellite.
- **Transport mode**: If there are several networks attached to an appliance, an IPsec association has to be established for each network. With this transport mode, only one IPsec association to the target appliance is established and the packets for its attached networks are put in an IP over IP tunnel.

The following cryptographic settings are used:

- Data encryption and decryption: This operation uses an AES block cipher in CBC mode with a cryptographic key size of 128 bit, 192 bit or 256 bit according to FIPS-197 and NIST-SP800-38A.
- Cryptographic key agreement: This operation uses the Diffie-Hellman exponent generation with a key size of 2048 bit, according to RFC2409 and RFC3526.
- Generation and verification of message authentication code: This operation uses the HMAC-SHA256 with a key size of 256 bit according to RFC2104 and FIPS-180-4.
- Authentication: This operation uses RSA signatures with a key size of 2048 bit according to PKCS#1, v2.1**using RSASSA-PKCS1-v1_5**.
- Key destruction: Expired keys are overwritten with zeros.

1.4.5 SSH Features

The TOE uses the following SSH features respective enhancements:

- **SSH Launch Daemon**: Redirect of TCP-packets by the *pf* and tunnelling the TCP stream through an SSH port forwarding with added SOCKS protocol.
- **Log messages:** Forwarding of UDP-packets of the `syslogd` through an SSH channel.

The following cryptographic settings are used:

- Data encryption and decryption: This operation uses an AES block cipher in CTR mode with a cryptographic key size of 128 bit according to FIPS-197 and NIST-SP800-38A.
- Cryptographic key agreement: This operation uses the elliptic curve algorithm ecdh-sha2-brainpoolp256r1 with a key size of 256 bit, according to RFC5639 and [EBP].
- Generation and verification of message authentication code: This operation uses the UMAC-128-ETM algorithm with a key size of 256 bit according to RFC4418.
- Authentication: This operation uses RSA signatures with a key size of 2048 bit according to PKCS#1, v2.1**using RSASSA-PKCS1-v1_5**.
- Key destruction: Expired keys are overwritten with zeros.

1.4.6 Basic IPv6 Support

The TOE can operate in IPv6 environments (see [RFC2460]). It supports basic IPv6 functionality, but makes no automatic translation between IPv4 and IPv6 addresses. Further, there is no support for DHCPv6.

1.4.7 Secure Initialisation of genuscreen (Firewall Component)

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

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

1.4.8 Excluded Features

The following features are excluded from the TOE.

1.4.8.1 No Cryptocard

The firewall components can use a cryptocard to perform cryptographic operations for IPsec operations. However, usage of the cryptocard is out of scope for this TOE.

1.4.8.2 No USB update

The management system genucenter can write configuration updates for the genuscreen firewall components on an USB stick. The firewall component will update its configuration when the USB stick is plug into the firewall component. However, usage of the USB update is out of scope for this TOE.

1.4.8.3 No FTP and SIP Relays

The product allows the configuration of FTP and SIP relays. They only function with IPv4 and are not part of the TOE. These relays *must* not be configured.

1.4.8.4 No VPN to Other Appliances or Mobile Clients

It is possible to build VPN connections to third party (other) VPN appliances or directly to third party computers (mobile clients). These are not part of the TOE and *must* not be configured.

1.4.8.5 No L2TP VPN

Although the firewall components support the L2TP for VPN, it is excluded from the TOE and *must* not be configured.

1.4.8.6 No LDAP Authentication

Although the management server allows LDAP for administrator authentication, it is excluded from the TOE and *must* not be configured.

1.4.8.7 No Dynamic Routing

The dynamic routing feature which uses OSPF only works with IPv4 and is out of scope for this TOE.

1.4.8.8 No virtual genucenter

The genucenter must be operated on real hardware. Running the genucenter in a virtual machine is out of scope for this TOE.

1.4.9 Physical Scope

The physical scope of TOE consists only of software and documentation. The TOE does not include any hardware or firmware. The scope of delivery can be seen in table 1.1.

The TOE software is contained in the installation CD. The CD also has additional non-TOE software that is needed to get a running system.

The optional HA setup for the genuscreens is only useful for appliances with similar hardware and comparable performance.

Table 1.1: Scope of delivery

Type	Name	Release	Medium
Hardware genuscreen	gs100b, gs100c, gs300, gs400, gs500, gs600, gs700, and gs800	N/A	
Hardware genucenter	gz200, gz400, gz600, and gz800	N/A	
Software	genuscreen	5.0 Z Patchlevel 4	CD-ROM
Software	genucenter	5.0 Z Patchlevel 4	CD-ROM

1.4.10 Logical Scope

The following sections define the logical scope of the TOE.

1.4.10.1 Audit

The firewall components collect audit data which can be collected, stored, displayed, sorted and searched at the management system. Auditable events are attempts to violate a policy. This allows the administrators, service users and revisors to view the configuration and log data.

For appliances that are administered locally, the local GUI allows to inspect the current state of the respective component and the audit data.

1.4.10.2 Information Flow Protection

The most important user information flow policies enforced by the TOE are:

- Each firewall component will only forward data from and to the protected networks if the firewall information flow policy allows it.
- Data flowing between the networks protected by different firewall components is encrypted and authenticated if the IPsec/IKE information flow policy requires it (the administrators may choose not to protect flows).
- Data flowing between the networks protected by different firewall components is encrypted and authenticated if the SSH launch daemon information flow policy requires it (the administrators may choose not to protect flows).
- Data sent or received from an interface with a low classification is encrypted.

1.4.10.3 Security Management

Administrators can modify security policies at the management system and transfer them to the firewall components. Alternatively, administration can be done locally.

Service users can perform maintenance operations but are not allowed to do any configuration.

Revisors can view the configuration and log files.

1.4.10.4 Authentication and Identification

Administrators, revisors and service users must identify to the management system with a user name and must authenticate successfully by password before they can perform any security function.

Administrators and revisors at the local GUI of the firewall components must identify with a user name and must authenticate successfully by password before they can perform any security function.

1.4.10.5 Cryptographic Functionality

The TOE contains cryptographic functionality. The cryptographic algorithms are part of the TOE. This includes the random number generator which is of class DRG.3 (see [AIS20]).

2 Conformance Claims

2.1 CC conformance Claim

This Security Target is *Part 2 extended* and *Part 3 conformant* to the Common Criteria Version 3.1 Revision 4 (September 2012).

2.2 PP Claim, Package Claim

There are no Protection Profile claims. This Security Target claims to be conformant to the Assurance Packet EAL4 augmented with ALC_FLR.2, ASE_TSS.2 and AVA_VAN.4. These components are defined in CC Part 3.

2.3 Conformance Rationale

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

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

3 Security Problem Definition

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

- All different users.
- 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.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

3.1 Users

Table 3.1 lists all users. From these users only the **anonymous user** is not considered trustworthy. The threats that follow therefore only consider anonymous users as threat agents. The other user are needed for the SFRs.

The general term administrators describes the union of the genucenter administrators, the genucenter root administrators, the genucenter root shell account, and the genuscreen administrator.[1]

The general term service user describes the genucenter service users.[2]

The general term revisors describes the union of the genucenter revisors and the genuscreen revisor.[3]

Table 3.1: Users

	Users
Anonymous users	Any person or software agent sending IP packets to or receiving from the components of the TOE. This includes users on the protected networks behind the firewall components as well as all users outside those networks. Their assumed attack potential is **moderate**. It must be noted however, that the TOE firewall components are exposed to unrestricted attackers, simply because they are exposed to the Internet. The product therefore aims to protect against more capable attackers.
genucenter administrators	These are authenticated users at the management system that have administrative rights to change the firewall component's configuration on the management system inside their domain.
genucenter root administrators	These are authenticated users at the management system that have administrative rights to configure the attributes of the genucenter administrators, the genucenter root administrators, the genucenter revisors, the genucenter service users, the genuscreen administrator, and the genuscreen revisor, and to change the firewall component's and the management system's configuration at the management system.
genucenter revisors	These are authenticated users at the management system that are allowed to view the firewall component's and the management system's configuration and audit data on the management system inside their domains.
genucenter service users	These are authenticated users at the management system that are allowed to view the firewall component's and the management system's configuration and audit data on the management system inside their domains. They are also allowed to perform all maintenance activities in the "Maintenance" menu.
genucenter root shell account	This is an authenticated user that has a root shell account for administrative maintenance purposes.
genuscreen administrator	This is an authenticated user at the firewall components that has the administrative rights to change the firewall component's

[1] The singular term is also used for the administrator role.

[2] The singular term is used for the service role.

[3] The singular term is also used for the revisor role.

	Users
	configuration on the firewall component. The user also has a root shell account for administrative maintenance purposes.
genuscreen revisor	This is an authenticated user at the firewall components that has the administrative rights to view the firewall component's configuration on the firewall component.

3.2 Threats

The two different components of the TOE (management system and firewall component) fulfil different purposes and therefore must confront different threats.

Table 3.2: Threats

	Threats
T.NOAUTH	An anonymous user might attempt to bypass the security functions of the TOE to gain unauthenticated access to resources in the protected networks. This threat must be countered by the firewall components.
T.SNIFF	An anonymous user might gain access to the sensitive data passing between the protected networks. Attack method is packet inspection of Internet traffic. This threat must be countered by the firewall components.
T.SELPRO	An anonymous user might gain access to the TOE and read, modify or destroy security sensitive data on the TOE, by sending IP packets to the TOE and exploiting a weakness of the protocol used. This threat must be countered by the management system and the firewall components.
T.MEDIAT	An anonymous user might send non-permissible data that result in gaining access to resources which is not allowed by the policy. The attack method is construction of IP packets to circumvent filters. This threat must be countered by the firewall components.
T.MSNIFF	An anonymous user might gain access to the configuration or audit data passing between the management system and a firewall component. Attack method is packet inspection of Internet traffic. This threat must be countered by the management system and the firewall components.
T.MODIFY	An anonymous user might modify the sensitive data passing between the protected networks. Attack method is packet interception and modification of Internet traffic. This threat must be countered by the firewall components.
T.MMODIFY	An anonymous user might modify the configuration or audit data

	Threats
	passing between the management system and a firewall component. Attack method is packet interception and modification of Internet traffic. This threat must be countered by the management system and the firewall components.

3.3 Organisational Security Policies

The Security Target defines the following Organisational Security Policies.

Table 3.3: Policies

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

Application note: This policy only applies if the HA setup is used.

3.4 Assumptions

The following assumptions are made in order to be able to provide security functionality.

Table 3.4: Assumptions

	Assumptions
A.PHYSEC	The management system and the firewall components of the TOE are physically secure. Only administrators have physical access to the TOE. This must hold for the management system and the firewall components.
A.INIT	The TOE was initialised according to the procedure described in the documentation [DOC-GS] and [DOC-GZ] (summarised in section 1.4.7).
A.NOEVIL	Administrators, service users and revisors are non-hostile and follow all administrator guidance; however, they are capable of error. They use passwords that are not easily guessable.
A.SINGEN	Information can not flow between the internal and external network, unless it passes through the TOE.
A.TIMESTMP	The environment provides reliable timestamps.
A.ADMIN	Administrators, service users and revisors using the administrative GUI on the management system or the firewall components work in a trusted network directly connected to the system.
A.HANET	The environment provides a physical separate network for TSF data

	Assumptions
	transfer for the optional high availability setup.

Application note: **A.HANET** only applies if the HA setup is used.

4 Security Objectives

This chapter lists all security objectives of the TOE and it's operational environment.

4.1 Security Objectives for the TOE

The TOE must ensure the following objectives.

Table 4.1: Objectives

	Objectives
O.AUTH	The TOE must assure that only administrators can change the packet filter, VPN and SSH launch daemon configuration.
O.MEDIAT	The TOE must mediate the flow of all data between all connected networks.
O.CONFID	The TOE must assure that data transferred between the networks protected by firewall components is kept confidential unless explicitly configured otherwise.
O.INTEG	The TOE must assure that data transferred between the networks protected by firewall components cannot be modified unnoticed unless explicitly configured otherwise.
O.NOREPLAY	The TOE must assure that data transferred between the networks behind the firewall components cannot be reinjected at a later time unless explicitly configured otherwise.
O.AUDREC	The TOE must provide an audit trail of security-related events, and a means to present a readable and searchable view to administrators, service users and revisors.
O.RS	The TOE must prevent sending or receiving of unencrypted traffic on interfaces with low classification.
O.AVAIL	The TOE must optionally provide a fail over solution where the services of a failing system are taken over by a peer machine.

Application note: The TOE can be configured to work as a pure packet filter without cryptographic support in cases where O.CONFID, O.INTEG and O.NOREPLAY are not needed or not possible. However, when cryptographic operations are needed, the objectives must be fulfilled.

Application note: **O.AVAIL** only applies if the HA setup is used.

4.2 Security Objectives for the Operational Environment

The operational environment must ensure the following security objectives.

Table 4.2: Objectives for the Environment

	Objectives for the Operational Environment
OE.PHYSEC	Those responsible for the TOE must assure that the management system and the firewall components are placed at a secured place where only administrators have access. The communication server must be used to isolate the management system from the Internet.
OE.INIT	Those responsible for the TOE must ensure that the initial configuration is performed according to [DOC-GS] and [DOC-GZ]. A summary of the procedure is given in section 1.4.7.
OE.NOEVIL	Those responsible for the TOE must assure that all administrators, service users and revisors are competent, regularly trained and execute the administration in a responsible way. They must choose passwords which cannot be guessed easily.
OE.SINGEN	Those responsible for the TOE must assure that the firewall components provide the only connection for the different networks.
OE.TIMESTMP	The IT environment must supply reliable timestamps for the TOE.
OE.ADMIN	The administrators, service users and revisors must use the administrative GUI on the management system or the firewall components only from a trusted network directly connected to the system. They log in with SSH only from this network and use SSH keys but no passwords to authenticate.
OE.HANET	The IT-environment must supply a physical network for transfer of TSF data between nodes for the optional high availability setup.

Application note: **OE.HANET** only applies if the HA setup is used.

4.3 Security Objectives Rationale

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

Table 4.3 shows that all security objectives stated in this ST can be mapped to the stated threats and assumptions. All threats and assumptions are matched by at least one security objective.

Table 4.3: TOE Rationale

	OE.PHYSEC	OE.INIT	OE.NOEVIL	OE.SINGEN	OE.TIMESTMP	OE.ADMIN	OE.HANET	O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC	O.RS	O.AVAIL
A.PHYSEC	X														
A.INIT		X													
A.NOEVIL			X												
A.SINGEN				X											
A.TIMESTMP					X										
A.ADMIN						X									
A.HANET							X								
T.NOAUTH	X	X		X				X							
T.SNIFF		X								X				X	
T.SELPRO								X		X	X	X	X		
T.MEDIAT				X					X		X			X	
T.MSNIFF		X								X					
T.MODIFY		X									X	X		X	
T.MMODIFY		X									X	X			
P.AVAIL															X

4.3.1 Assumption Rationale

The following shows how the assumptions are satisfied by the environmental objectives.

4.3.1.1 A.PHYSEC

The objective **OE.PHYSEC** assures that the assumption about a physically secure TOE can be made and that a communication server is used.

4.3.1.2 A.INIT

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

4.3.1.3 A.NOEVIL

The objective **OE.NOEVIL** assures that the administrators, service users and revisors are trained and therefore that they are no threat to the TOE.

4.3.1.4 A.SINGEN

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

4.3.1.5 A.TIMESTMP

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

4.3.1.6 A.ADMIN

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

4.3.1.7 A.HANET

The objective **OE.HANET** assures that the IT environment provides a secure HA network.

4.3.2 Threat Rationale

The following shows that all threats are addressed by the objectives.

4.3.2.1 T.NOAUTH

The threat that an anonymous user might bypass the security functions of the TOE is countered by **OE.PHYSEC**, **OE.INIT**, **OE.SINGEN**, and **O.AUTH**. The objectives assure that no anonymous user can interfere with the initial setup, the physical setup of the firewall components, or use routes around the firewall components. The **O.AUTH** objective assures that only administrators can configure the system.

4.3.2.2 T.SNIFF

The threat that an anonymous user might gain access to the sensitive data passing between the protected networks is countered by objectives **OE.INIT** and **O.CONFID**. These assure that the firewalls components' public keys are initialised over an authenticated network and that all data flowing between the firewall components is protected against eavesdropping by IPsec or SSH transforms.

The objective **O.RS** assures that only encrypted traffic is allowed to pass from or to interfaces of the TOE with a low classification.

4.3.2.3 T.SELPRO

The threat that an anonymous user might gain access to the TOE and read, modify or destroy security sensitive data on the TOE is countered by objectives **O.AUTH**, **O.CONFID**, **O.INTEG**, **O.NOREPLAY**, and **O.AUDREC**. **O.AUTH** assures that only administrators can configure the TOE. **O.CONFID**, **O.INTEG** and **O.NOREPLAY** assure that the communication between the management system and the firewall components is secured by encryption. **O.AUDREC** assures that attempts to compromise the TOE are audited.

4.3.2.4 T.MEDIAT

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

The objective **O.RS** assures that only encrypted traffic is allowed to pass from or to interfaces of the TOE with a low classification.

4.3.2.5 T.MSNIFF

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

4.3.2.6 T.MODIFY

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

The objective **O.RS** assures that only encrypted traffic is allowed to pass from or to interfaces of the TOE with a low classification.

4.3.2.7 T.MMODIFY

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

4.3.3 Organisational Security Policy Rationale

The following shows that all organisational security policies are addressed by the objectives.

4.3.3.1 P.AVAIL

The objective O.AVAIL assures that the policy P.AVAIL is met.

5 Extended Components Definition

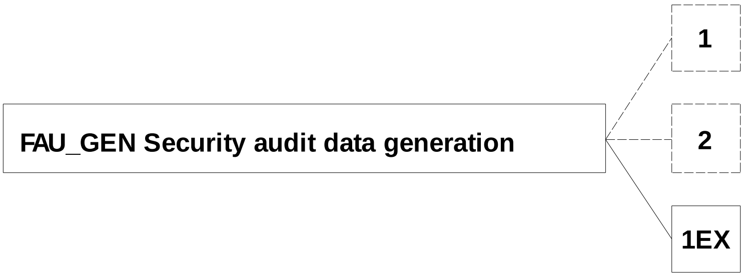
5.1 Extended Components Definition

5.1.1 Class FAU: Security audit

5.1.1.1 Security audit data generation (FAU_GEN)

Family behaviour

The family has been enhanced by one component **FAU_GEN.1EX**. It is intended to be a replacement for **FAU_GEN.1** when the security function does not support audit generation for startup and shutdown of the audit functions. This component can also be used as a replacement for the de-



pendencies on **FAU_GEN.1**, because all other audit events can be specified as in **FAU_GEN.1**.

Component levelling

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

Management: FAU_GEN.1EX

There are no management activities foreseen.

Audit: 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.

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

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 (if applicable), 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]**.

5.1.2 Class FCS: Cryptographic Support

The following family has been defined in [KS2011], a supporting document for [AIS20] and [AIS31]. For the rationale of the definition of this extended component, see [KS2011].

5.1.2.1 FCS_RNG: Generation of random numbers

Family Behaviour

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling:

FCS_RNG Generation of random numbers
1

FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

6 Security Requirements

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

Throughout this document, CC operations on security requirements are marked as follows:

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

6.1 Security Functional Requirements

This section lists the principal Security Functional Requirements claimed by the TOE. Most are derived from requirements in [CC_2]. In the statement of the requirements, the abbreviation in parentheses defines the specific iteration of the associated Part 2 requirement.

6.1.1 FW-SFP

This section lists the SFRs necessary for the firewall components to enforce firewall security policies defined by the administrators.

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

6.1.1.1 FDP_IFC.1_(FW) Subset information flow control

FDP_IFC.1.1_(FW)

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

- **subjects: anonymous users;**
- **information: the data sent from one subject through the TOE to another;**
- **operation: pass the data**].

6.1.1.2 FDP_IFF.1_(FW) Simple security attributes

FDP_IFF.1.1_(FW)

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

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

FDP_IFF.1.2_(FW)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**subjects on a network connected to the TOE can cause information to flow through the TOE to a subject on another connected network only if all the information security attribute values are permitted by all information flow policy rules**].

FDP_IFF.1.3_(FW)

The TSF shall enforce the [

- **reassembly of fragmented IPv4 and IPv6 datagrams before inspection**
- **possibility to modify parts of the TCP/IP headers to make the connections less vulnerable against hijacking attacks**].

FDP_IFF.1.4_(FW)

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

FDP_IFF.1.5_(FW)

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

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

6.1.1.3 FMT_MSA.1_(FW-A) Management of security attributes

FMT_MSA.1.1_(FW-A)

The TSF shall enforce the [**FW-SFP**] to restrict the ability to [***modify***] the security attributes [**packet filter rules**] to [**the genucenter administrators, the genucenter root administrators, and the genuscreen administrator**].

6.1.1.4 FMT_MSA.1_(FW-R) Management of security attributes

FMT_MSA.1.1_(FW-R)

The TSF shall enforce the [**FW-SFP**] to restrict the ability to [***query***] the security attributes [**packet filter rules**] to [**the genucenter administrators, the genucenter root administrators, the genuscreen administrator, the genucenter service users, the genucenter revisors, and the genuscreen revisor**].

6.1.1.5 FMT_MSA.3_(FW) Static attribute initialisation

FMT_MSA.3.1_(FW)

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

FMT_MSA.3.2_(FW)

The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.

6.1.1.6 FMT_SMF.1_(FW) Specification of management functions

FMT_SMF.1.1_(FW)

The TSF shall be capable of performing the following security management functions: [**creation and modification of network traffic filter rules. The rules filter for the following attributes of datagrams:**

- **address of source subject;**
- **address of destination subject;**

- **transport layer protocol;**
- **interfaces on which traffic arrives and departs;**
- **IP version;**
- **service**].

6.1.2 RS-SFP

This section lists the SFRs necessary for the firewall components to enforce the interface classification

6.1.2.1 FDP_IFC.2_(RS) Complete information flow control

FMT_IFC.2.1_(RS)

The TSF shall enforce the [**RS-SFP**] on [

- **subjects: anonymous users;**
- **information: the data sent from one subject through the TOE to another;**
- **operation: pass the data**]

and all operations that cause that information to flow to and from subjects covered by the SFP.

FMT_IFC.2.2_(RS)

The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.1.2.2 FDP_IFF.1_(RS) Simple security attributes

FDP_IFF.1.1_(RS)

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

- **subject security attributes: none**
- **information security attributes:**
  - **the incoming interface and its classification**
  - **the outgoing interface and its classification**].

FDP_IFF.1.2_(RS)

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

- **the incoming and the outgoing interface have a different classification;**
- **packets send into the unclassified network are encrypted;**
- **packets received from the unclassified network are encrypted**].

FDP_IFF.1.3_(RS)

The TSF shall enforce the [**none**].

FDP_IFF.1.4_(RS)

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

FDP_IFF.1.5_(RS)

The TSF shall explicitly deny an information flow based on the following rules: [**the traffic is not encrypted**].

6.1.2.3 FMT_MSA.1_(RS-A) Management of security attributes

FMT_MSA.1.1_(RS-A)

The TSF shall enforce the [**RS-SFP**] to restrict the ability to [***modify***] the security attributes [**network interface classification**] to [**the genucenter administrators, the genucenter root administrators, and the genuscreen administrator**].

6.1.2.4 FMT_MSA.1_(RS-R) Management of security attributes

FMT_MSA.1.1_(RS-R)

The TSF shall enforce the [**RS-SFP**] to restrict the ability to [***query***] the security attributes [**network interface classification**] to [**the genucenter administrators, the genucenter root administrators, the genuscreen administrator, the genucenter service users, the genucenter revisors, and the genuscreen revisor**].

6.1.2.5 FMT_MSA.3_(RS) Static attribute initialisation

FMT_MSA.3.1_(RS)

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

FMT_MSA.3.2_(RS)

The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.

6.1.2.6 FMT_SMF.1_(RS) Specification of management functions

FMT_SMF.1.1_(RS)

The TSF shall be capable of performing the following security management functions: [**classification of the interface**].

6.1.3 IPSEC

This section identifies the SFRs associated with the flow control functions in relation to the VPN connections between the firewall components. The IKE-SFP is the policy that models this aspect of information flow control. This section is separated from the IKE-SFP because these SFRs are handled by the kernel but configured from user space. When cryptographic standards are referenced, the requirements only apply to the mandatory parts.

6.1.3.1 FDP_ITT.1_(IPSEC) Basic internal transfer protection

FDP_ITT.1.1_(IPSEC)

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

6.1.3.2 FDP_IFC.1_(IPSEC) Subset information flow control

FDP_IFC.1.1_(IPSEC)

The TSF shall enforce the [**IKE-SFP**] on [

- **subjects: firewall components;**
- **information: the data sent from one subject to another;**
- **operation: pass the data**].

6.1.3.3 FCS_COP.1_(IPSEC-AES) Cryptographic operation

FCS_COP.1.1_(IPSEC-AES)

The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in CBC mode**] and cryptographic key sizes [**128 bit, 192 bit (default), or 256 bit**] that meet the following: [**[FIPS-197] and [NIST-SP800-38A]**].

6.1.3.4 FCS_COP.1_(IPSEC-HMAC) Cryptographic operation

FCS_COP.1.1_(IPSEC-HMAC)

The TSF shall perform [**generation and verification of message authentication code**] in accordance with a specified cryptographic algorithm [**HMAC-SHA256**] and cryptographic key sizes [**256 bit**] that meet the following: [**[RFC2104] and [FIPS-180-4]**].

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

6.1.3.5 FCS_CKM.4_(IPSEC) Cryptographic key destruction

FCS_CKM.4.1_(IPSEC)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting with zeros**] that meets the following: [**none**].

6.1.4 IKE-SFP

This section identifies the SFRs associated with cryptographic functions in relation to the key management of the VPN connections between the firewall components. The IKE-SFP is the policy that models this aspect of information flow control. When cryptographic standards are referenced, the requirements only apply to the mandatory parts.

6.1.4.1 FDP_ITT.1_(IKE) Basic internal transfer protection

FDP_ITT.1.1_(IKE)

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

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

6.1.4.2 FDP_IFC.1_(IKE) Subset information flow control

FDP_IFC.1.1_(IKE)

The TSF shall enforce the [**IKE-SFP**] on [

- **subjects: firewall components;**
- **information: the data sent from one subject through the environment to another;**
- **operation: pass the data**].

6.1.4.3 FDP_IFF.1_(IKE) Simple security attributes

FDP_IFF.1.1_(IKE)

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

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

FDP_IFF.1.2_(IKE)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**subjects can cause information to flow through their respective components of the TOE if based on the subjects' public keys a secure IPsec connection can be negotiated between the subjects via the IKE protocol**].

FDP_IFF.1.3_(IKE)

The TSF shall enforce the [**none**].

FDP_IFF.1.4_(IKE)

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

FDP_IFF.1.5_(IKE)

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

6.1.4.4 FCS_CKM.1_(IKE-AES) Cryptographic key generation

FCS_CKM.1.1_(IKE-AES)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**symmetric key generation**] and specified cryptographic key sizes [**128 bit, 192 bit (default), or 256 bit**] that meet the following: [**[RFC2409]].**

6.1.4.5 FCS_COP.1_(IKE-AES) Cryptographic operation

FCS_COP.1.1_(IKE-AES)

The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in CBC mode**] and cryptographic key sizes [**128 bit, 192 bit (default), or 256 bit**] that meet the following: [**[FIPS-197] and [NIST-SP800-38A]**].

6.1.4.6 FCS_CKM.1_(IKE-DH) Cryptographic key generation

FCS_CKM.1.1_(IKE-DH)

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

6.1.4.7 FCS_COP.1_(IKE-DH) Cryptographic operation

FCS_COP.1.1_(IKE-DH)

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

6.1.4.8 FCS_CKM.1_(IKE-HMAC) Cryptographic key generation

FCS_CKM.1.1_(IKE-HMAC)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**authentication key generation**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**[RFC2409]**].

6.1.4.9 FCS_COP.1_(IKE-HMAC) Cryptographic operation

FCS_COP.1.1_(IKE-HMAC)

The TSF shall perform [**generation and verification of message authentication code**] in accordance with a specified cryptographic algorithm [**HMAC-SHA256**] and cryptographic key sizes [**256 bit**] that meet the following: [**[RFC2104] and [FIPS-180-4]**].

6.1.4.10 FCS_CKM.1_(IKE-RSA) Cryptographic key generation

FCS_CKM.1.1_(IKE-RSA)

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

6.1.4.11 FCS_COP.1_(IKE-RSA) Cryptographic operation

FCS_COP.1.1_(IKE-RSA)

The TSF shall perform [**digital signature creation and verification**] in accordance with a specified cryptographic algorithm [**RSA signature**] and cryptographic key sizes [**2048 bit**] that meet the following: [**[PKCS #1, v2.1] using RSASSA-PKCS1-v1_5**].

6.1.4.12 FCS_CKM.4_(IKE) Cryptographic key destruction

FCS_CKM.4.1_(IKE)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting with zeros**] that meets the following: [**none**].

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

6.1.4.13 FMT_MSA.1_(IKE-A) Management of security attributes

FMT_MSA.1.1_(IKE-A)

The TSF shall enforce the [**IKE-SFP**] to restrict the ability to [***modify***] the security attributes [**IKE configuration**] to [**the genucenter administrators, the genucenter root administrators and the genuscreen administrator**].

6.1.4.14 FMT_MSA.1_(IKE-R) Management of security attributes

FMT_MSA.1.1_(IKE-R)

The TSF shall enforce the [**IKE-SFP**] to restrict the ability to [***query***] the security attributes [**IKE configuration**] to [**the genucenter administrators, the genucenter root administrators, the genuscreen administrator, the genucenter service users, the genucenter revisors, and the genuscreen revisor**].

6.1.4.15 FMT_MSA.2_(IKE) Secure security attributes

FMT_MSA.2.1_(IKE)

The TSF shall ensure that only secure values are accepted for [**the IKE configuration**].

6.1.4.16 FMT_MSA.3_(IKE) Static attribute initialisation

FMT_MSA.3.1_(IKE)

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

FMT_MSA.3.2_(IKE)

The TSF shall allow the [**genucenter administrators, the genucenter root administrators, and the genuscreen administrator**] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.17 FMT_SMF.1_(IKE) Specification of management functions

FMT_SMF.1.1_(IKE)

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

6.1.5 SSH-SFP

This section identifies the SFRs associated with the flow control functions in relation to the communication between the management system and the firewall components. The SSH-SFP is the policy that models this aspect of information flow control. When cryptographic standards are referenced, the requirements only apply to the mandatory parts.

6.1.5.1 FPT_ITT.1_(SSH) Basic internal TSF data transfer protection

FPT_ITT.1.1_(SSH)

The TSF shall protect TSF data from [***disclosure* and *modification***] when it is transmitted between separate parts of the TOE.

6.1.5.2 FDP_ITT.1_(SSH) Basic internal transfer protection

FDP_ITT.1.1_(SSH)

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

6.1.5.3 FDP_IFC.1_(SSH) Subset information flow control

FDP_IFC.1.1_(SSH)

The TSF shall enforce the [**SSH-SFP**] on [

- **subjects: management system and firewall components;**
- **information: the data sent from one subject through the environment to another;**
- **operation: pass the data**].

6.1.5.4 FDP_IFF.1_(SSH) Simple security attributes

FDP_IFF.1.1_(SSH)

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

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

FDP_IFF.1.2_(SSH)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**subjects can cause information to flow through their respective components of the TOE if based on the subjects' host keys and user keys a secure connection can be negotiated between the subjects via the SSH protocol**].

FDP_IFF.1.3_(SSH)

The TSF shall enforce the [**none**].

FDP_IFF.1.4_(SSH)

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

FDP_IFF.1.5_(SSH)

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

6.1.5.5 FCS_CKM.1_(SSH-AES) Cryptographic key generation

FCS_CKM.1.1_(SSH-AES)

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

6.1.5.6 FCS_COP.1_(SSH-AES) Cryptographic operation

FCS_COP.1.1_(SSH-AES)

The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in CTR mode**] and cryptographic key sizes [**128 bit**] that meet the following: [**[FIPS-197] and [NIST-SP800-38A]**].

6.1.5.7 FCS_CKM.1_(SSH-ECDH) Cryptographic key generation

FCS_CKM.1.1_(SSH-ECDH)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**elliptic curve ecdh-sha2-brainpoolp256r1**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**[RFC5639] and [EBP]**].

Application note: The cryptographic algorithm elliptic curve ecdh-sha2-brainpoolp256r1 contains both the cryptographic key generation and the cryptographic operation. Therefore the respective SFR FCS_COP.1 is omitted.

6.1.5.8 FCS_CKM.1_(SSH-UMAC) Cryptographic key generation

FCS_CKM.1.1_(SSH-UMAC)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**authentication key generation**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**[RFC4253] with the ETM extension**].

6.1.5.9 FCS_COP.1_(SSH-UMAC) Cryptographic operation

FCS_COP.1.1_(SSH-UMAC)

The TSF shall perform [**generation and verification of message authentication code**] in accordance with a specified cryptographic algorithm [**UMAC-128-ETM**] and cryptographic key sizes [**256 bit**] that meet the following: [**[RFC4418] using AES**].

6.1.5.10 FCS_CKM.1_(SSH-RSA) Cryptographic key generation

FCS_CKM.1.1_(SSH-RSA)

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

6.1.5.11 FCS_COP.1_(SSH-RSA) Cryptographic operation

FCS_COP.1.1_(SSH-RSA)

The TSF shall perform [**authentication**] in accordance with a specified cryptographic algorithm [**RSA signature generation and verification**] and cryptographic key sizes [**2048 bit**] that meet the following: [**[PKCS #1, v2.1] using RSASSA-PKCS1-v1_5**].

6.1.5.12 FCS_CKM.4_(SSH) Cryptographic key destruction

FCS_CKM.4.1_(SSH)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting with zeros**] that meets the following: [**none**].

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

6.1.5.13 FMT_MSA.1_(SSH-A) Management of security attributes

FMT_MSA.1.1_(SSH-A)

The TSF shall enforce the [**SSH-SFP**] to restrict the ability to [***modify***] the security attributes [**SSH configuration**] to [**the genucenter administrators and the genucenter root administrators**].

6.1.5.14 FMT_MSA.1_(SSH-R) Management of security attributes

FMT_MSA.1.1_(SSH-R)

The TSF shall enforce the [**SSH-SFP**] to restrict the ability to [***query***] the security attributes [**SSH configuration**] to [**the genucenter administrators, the genucenter root administrators, the genucenter service users and the genucenter revisors**].

6.1.5.15 FMT_MSA.2_(SSH) Secure security attributes

FMT_MSA.2.1_(SSH)

The TSF shall ensure that only secure values are accepted for [**the SSH configuration**].

6.1.5.16 FMT_MSA.3_(SSH) Static attribute initialisation

FMT_MSA.3.1_(SSH)

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

FMT_MSA.3.2_(SSH)

The TSF shall allow the [**genucenter administrators and the genucenter root administrators**] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.17 FMT_SMF.1_(SSH) Specification of management functions

FMT_SMF.1.1_(SSH)

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

Application note: The key destruction is done on deletion of the associated firewall component.

6.1.6 SSHLD-SFP

This section identifies the SFRs associated with the flow control functions in relation to the SSH launch daemon communication between the firewall components. The SSHLD-SFP is the policy that models this aspect of information flow control. When cryptographic standards are referenced, the requirements only apply to the mandatory parts.

6.1.6.1 FDP_ITT.1_(SSHLD) Basic internal transfer protection

FDP_ITT.1.1_(SSHLD)

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

6.1.6.2 FDP_IFC.1_(SSHLD) Subset information flow control

FDP_IFC.1.1_(SSHLD)

The TSF shall enforce the [**SSHLD-SFP**] on [

- **subjects: firewall components;**
- **information: the data sent from one subject through the environment to another;**
- **operation: pass the data**].

6.1.6.3 FDP_IFF.1_(SSHLD) Simple security attributes

FDP_IFF.1.1_(SSHLD)

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

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

FDP_IFF.1.2_(SSHLD)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**subjects can cause information to flow through their respective components of the TOE if based on the subjects' host keys and user keys a secure connection can be negotiated between the subjects via the SSH protocol**].

FDP_IFF.1.3_(SSHLD)

The TSF shall enforce the [**none**].

FDP_IFF.1.4_(SSHLD)

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

FDP_IFF.1.5_(SSHLD)

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

6.1.6.4 FCS_CKM.1_(SSHLD-AES) Cryptographic key generation

FCS_CKM.1.1_(SSHLD-AES)

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

6.1.6.5 FCS_COP.1_(SSHLD-AES) Cryptographic operation

FCS_COP.1.1_(SSHLD-AES)

The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in CTR mode**] and cryptographic key sizes [**128 bit**] that meet the following: [**[FIPS-197] and [NIST-SP800-38A]**].

6.1.6.6 FCS_CKM.1_(SSHLD-ECDH) Cryptographic key generation

FCS_CKM.1.1_(SSHLD-ECDH)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**elliptic curve ecdh-sha2-brainpoolp256r1**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**[RFC5639] and [EBP]**].

Application note: The cryptographic algorithm elliptic curve ecdh-sha2-brainpoolp256r1 contains both the cryptographic key generation and the cryptographic operation. Therefore the respective SFR FCS_COP.1 is omitted.

6.1.6.7 FCS_CKM.1_(SSHLD-UMAC) Cryptographic key generation

FCS_CKM.1.1_(SSHLD-UMAC)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**authentication key generation**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**[RFC4253] with the ETM extension**].

6.1.6.8 FCS_COP.1_(SSHLD-UMAC) Cryptographic operation

FCS_COP.1.1_(SSHLD-UMAC)

The TSF shall perform [**generation and verification of message authentication code**] in accordance with a specified cryptographic algorithm [**UMAC-128-ETM**] and cryptographic key sizes [**256 bit**] that meet the following: [**[RFC4418]**].

6.1.6.9 FCS_CKM.1_(SSHLD-RSA) Cryptographic key generation

FCS_CKM.1.1_(SSHLD-RSA)

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

6.1.6.10 FCS_COP.1_(SSHLD-RSA) Cryptographic operation

FCS_COP.1.1_(SSHLD-RSA)

The TSF shall perform [**authentication**] in accordance with a specified cryptographic algorithm [**RSA signature generation and verification**] and cryptographic key sizes [**2048 bit**] that meet the following: [**[PKCS #1, v2.1] using RSASSA-PKCS1-v1_5**].

6.1.6.11 FCS_CKM.4_(SSHLD) Cryptographic key destruction

FCS_CKM.4.1_(SSHLD)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting with zeros**] that meets the following: [**none**].

Application note: The key destruction function is identical for FCS_CKM.1_(SSHLD-ECDH), FCS_CKM.1_(SSHLD-AES), FCS_CKM.1_(SSHLD-UMAC) and FCS_CKM.1_(SSHLD-RSA), so there is only one iteration of FCS_CKM.4 for all four SFRs.

6.1.6.12 FMT_MSA.1_(SSHLD-A) Management of security attributes

FMT_MSA.1.1_(SSHLD-A)

The TSF shall enforce the [**SSHLD-SFP**] to restrict the ability to [***modify***] the security attributes [**SSHLD configuration**] to [**the genucenter administrators, the genucenter root administrators, and the genuscreen administrator**].

6.1.6.13 FMT_MSA.1_(SSHLD-R) Management of security attributes

FMT_MSA.1.1_(SSHLD-R)

The TSF shall enforce the [**SSHLD-SFP**] to restrict the ability to [***query]*** the security attributes [**SSHLD configuration**] to [**the genucenter administrators, the genucenter root administrators, the genuscreen administrator, the genucenter service users, the genucenter revisors and the genuscreen revisor**].

6.1.6.14 FMT_MSA.2_(SSHLD) Secure security attributes

FMT_MSA.2.1_(SSHLD)

The TSF shall ensure that only secure values are accepted for [**the SSHLD configuration**].

6.1.6.15 FMT_MSA.3_(SSHLD) Static attribute initialisation

FMT_MSA.3.1_(SSHLD)

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

FMT_MSA.3.2_(SSHLD)

The TSF shall allow the [**genucenter administrators, the genucenter root administrators, and the genuscreen administrator**] to specify alternative initial values to override the default values when an object or information is created.

6.1.6.16 FMT_SMF.1_(SSHLD) Specification of management functions

FMT_SMF.1.1_(SSHLD)

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

6.1.7 Administration

These SFRs are related to the administration of the TOE.

6.1.7.1 FDP_IFC.1_(ADM) Subset information flow control

FDP_IFC.1.1_(ADM)

The TSF shall enforce the [**ADM-SFP**] on [

- **subjects: administrators from the administration network that interact with the administrative web server of the TOE;**
- **information: html form data for administration;**
- **operation: pass information**].

6.1.7.2 FDP_IFF.1_(ADM) Simple security attributes

FDP_IFF.1.1_(ADM)

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

- **the current domain (URL)**
- **the current administrator/service user/revisor (identified by cookie or basic-auth)**].

FDP_IFF.1.2_(ADM)

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

- **the cookie or basic-auth is still valid**
- **the administrator/service user/revisor is allowed to configure/review the domain**].

FDP_IFF.1.3_(ADM)

The TSF shall enforce the [**none**].

FDP_IFF.1.4_(ADM)

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

FDP_IFF.1.5_(ADM)

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

6.1.7.3 FMT_MSA.1_(ADM-A) Management of security attributes

FMT_MSA.1.1_(ADM-A)

The TSF shall enforce the [**ADM-SFP**] to restrict the ability to [***modify***] the security attributes [**TOE configuration**] to [**the genucenter administrators, the genucenter root administrators, and the genuscreen administrator**].

Application note: The term **TOE configuration** includes all configuration attributes besides those described in FMT_MSA.1.1_(ADM-ROOT).

6.1.7.4 FMT_MSA.1_(ADM-R) Management of security attributes

FMT_MSA.1.1_(ADM-R)

The TSF shall enforce the [**ADM-SFP**] to restrict the ability to [***query***] the security attributes [**TOE configuration**] to [**the genucenter administrators, the genucenter root administrators, the genuscreen administrator, the genucenter srevice users, the genucenter revisors, and the genuscreen revisor**].

Application note: The term **TOE configuration** includes all configuration attributes besides those described in FMT_MSA.1.1_(ADM-ROOT).

6.1.7.5 FMT_MSA.1_(ADM-O) Management of security attributes

FMT_MSA.1.1_(ADM-O)

The TSF shall enforce the [**ADM-SFP**] to restrict the ability to [***update***] the security attributes [**TOE data**] to [**the genucenter administrators, the genucenter service user, the genucenter root administrators, and the genuscreen administrator**].

Application note: The term **Update** includes the security management functions: transfer of configuration data onto the firewall components; collecting log data from the firewall components.

Application note: The term **TOE data** includes both the configuration and the log data of the respective appliance.

6.1.7.6 FMT_MSA.1_(ADM-ROOT) Management of security attributes

FMT_MSA.1.1_(ADM-ROOT)

The TSF shall enforce the [**ADM-SFP**] to restrict the ability to [***modify***] the security attributes [**administrative role, password, administrative domain**] to [**the genucenter root administrators**].

6.1.7.7 FMT_MSA.3_(ADM) Static attribute initialisation

FMT_MSA.3.1_(ADM)

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

FMT_MSA.3.2_(ADM)

The TSF shall allow the [**genucenter root administrators**] to specify alternative initial values to override the default values when an object or information is created.

6.1.7.8 FMT_SMF.1_(ADM) Security management functions

FMT_SMF.1.1_(ADM)

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

- **assigning names and passwords for the administrators;**
- **assigning names and passwords for the service users;**
- **assigning names and passwords for the revisors;**
- **assigning genucenter administrators to domains;**
- **assigning genucenter service users to domains;**
- **assigning genucenter revisors to domains;**
- **initial configuration of the firewall components;**
- **transfer of configuration data onto the firewall components;**
- **collecting log data from the firewall components;**
- **switch administration mode for firewall components**].

6.1.8 Identification and Authentication

These SFRs are related to identification and authentication of administrators, service users and revisors.

6.1.8.1 FIA_ATD.1_(IA) User attribute definition

FIA_ATD.1.1_(IA)

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

- **administrator role: name, password, administrative domains**
- **service role: name, password, administrative domains**

- **revisor role: name, password, administrative domains**].

6.1.8.2 FIA_SOS.1_(IA) Verification of secrets

FIA_SOS.1.1_(IA)

The TSF shall provide a mechanism to verify that secrets meet [**the passwords for the genucenter administrators, the genucenter root administrators, the genucenter service users, the genucenter revisors, the genuscreen administrator and the genuscreen revisor must be at least 8 characters in length when changed in the administrative GUI**].

Application note: There is no such requirement for changing passwords at the console.

6.1.8.3 FIA_UAU.2_(IA) User authentication before any action

FIA_UAU.2.1_(IA)

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

6.1.8.4 FIA_UAU.6_(IA) Re-authenticating

FIA_UAU.6.1_(IA)

The TSF shall re-authenticate the ~~user~~**genucenter administrators, the genucenter root administrators, the genucenter service users and the genucenter revisors** under the conditions [**after 10 minutes idle time at the administrative GUI**].

6.1.8.5 FIA_UID.2_(IA) User identification before any action

FIA_UID.2.1_(IA)

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

6.1.9 Audit

This section provides SFRs relating to the audit capabilities of the TOE.

6.1.9.1 FAU_GEN.1EX_(AU) Audit data generation

FAU_GEN.1EX.1_(AU)

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

a) All auditable events for the [**not specified**] level of audit; and

b) [

1. **Starting of firewall components**
2. **IP datagrams matching log filters in firewall rules**].

FAU_GEN.1EX.2_(AU)

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, [**no other audit relevant information**].

6.1.9.2 FAU_SAR.1_(AU) Audit review

FAU_SAR.1.1_(AU)

The TSF shall provide [**the genucenter administrators, the genucenter root administrators, the genuscreen administrator, the genucenter service users, the genucenter revisors, and the genuscreen revisor**] with the capability to read [**the audit data from the administrator's/service user's domain/revisor's domain**] from the audit records.

FAU_SAR.1.2_(AU)

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

6.1.9.3 FAU_SAR.3_(AU) Selectable audit review

FAU_SAR.3.1_(AU)

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

- **range of time and date;**
- **the firewall component that produced the audit data;**
- **for log data of firewall rules: IP addresses and ports, where applicable**].

6.1.10 General Management Facilities

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

6.1.10.1 FMT_MOF.1_(GEN) Management of security functions behaviour

FMT_MOF.1.1_(GEN)

The TSF shall restrict the ability to [***modify the behaviour of***] the functions [**logging, reaction to failed random number generator test**] to [**the genucenter administrators, the genucenter root administrators, and the genuscreen administrator**].

6.1.10.2 FMT_SMF.1_(GEN) Specification of management functions

FMT_SMF.1.1_(GEN)

The TSF shall be capable of performing the following security management functions: [**configuration of the audit system; configuration of the reaction to failed random number generator test**].

6.1.10.3 FMT_SMR.1_(GEN) Security roles

FMT_SMR.1.1_(GEN)

The TSF shall maintain the roles [

- **administrator: genucenter administrators, genucenter root administrators, genucenter root shell account, genuscreen administrator;**
- **service: genucenter service users;**
- **revisor: genucenter revisors, genuscreen revisor**].

FMT_SMR.1.2_(GEN)

The TSF shall be able to associate users with roles.

6.1.10.4 FPT_TEE.1_(GEN) Testing of external entities

FPT_TEE.1.1_(GEN)

The TSF shall run a suite of tests [***during initial start-up***] to check the fulfilment of [**a minimum quality of random numbers generated**].

FPT_TEE.1.2_(GEN)

If the test fails, the TSF shall [**execute an administrator defined action (log the event and disable VPN functionality)**].

Application note: Remote access by SSH is not disabled in order to guarantee reachability.

6.1.10.5 FPT_TRC.1_(GEN) Internal TOE TSF data replication consistency

FPT_TRC.1.1

The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2

When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon ~~reconnection before processing any requests for~~**takeover for** [***pf* states and IPsec security associations**].

Application note: This SFR only applies if the HA setup is used. The refinement reflects the characteristic of the TOR to continuously synchronise the replicated TSF data so that consistency is maintained at takeover time.

6.1.11 Random Number Generation

This section describes the SFRs for the generated random numbers.

6.1.11.1 FCS_RNG.1 Random number generation (Class DRG.3)

FCS_RNG.1.1

The TSF shall provide a deterministic random number generator that implements:

(DRG.3.1) If initialized with a random seed ***[from a custom entropy pool]****, the internal state of the RNG shall [****have at least 64bit of entropy].***

(DRG.3.2) The RNG provides forward secrecy.

(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known.

FCS_RNG.1.2

The TSF shall provide random numbers that meet:

(DRG.3.4) The RNG, initialized with a random seed ***[with an entropy of 128 bit]****, generates output for which* **[k > 2^{26}]** *strings of bit length 128 are mutually different with probability* **[ε < 2^{-12}]**.

(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A ***[and the DieHarder[4] random number test suite]***.

6.2 Security Assurance Requirements

Table 6.1 shows the Security Assurance Requirements for the level EAL4. The augmented components ALC_FLR.2, ASE_TSS.2 and AVA_VAN.4 are set in a bold font. For the level EAL4, the SARs ADV_INT and ADV_SPM are not needed.

Table 6.1: SAR

Class	Family	Level	Name
Development	ADV_ARC	ADV_ARC.1	Security architecture description
	ADV_FSP	ADV_FSP.4	Complete functional specification
	ADV_IMP	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT		TSF internals
	ADV_SPM		Security policy modelling
	ADV_TDS	ADV_TDS.3	Basic modular design
Guidance	AGD_OPE	AGD_OPE.1	Operational user guidance
	AGD_PRE	AGD_PRE.1	Preparative procedures
Life-cycle	ALC_CMC	ALC_CMC.4	Production support, acceptance procedures and automation

[4] http://www.phy.duke.edu/~rgb/General/dieharder.php

Class	Family	Level	Name
	ALC_CMS	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL	ALC_DEL.1	Delivery procedures
	ALC_DVS	ALC_DVS.1	Identification of security measures
	ALC_FLR	**ALC_FLR.2**	Flaw reporting procedures
	ALC_LCD	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT	ALC_TAT.1	Well-defined development tools
Security Target	ASE_CCL	ASE_CCL.1	Conformance claims
	ASE_ECD	ASE_ECD.1	Extended components definition
	ASE_INT	ASE_INT.1	ST introduction
	ASE_OBJ	ASE_OBJ.2	Security objectives
	ASE_REQ	ASE_REQ.2	Derived security requirements
	ASE_SPD	ASE_SPD.1	Security problem definition
	ASE_TSS	**ASE_TSS.2**	TOE summary specification with architectural design summary
Tests	ATE_COV	ATE_COV.2	Analysis of coverage
	ATE_DPT	ATE_DPT.1	Testing: basic design
	ATE_FUN	ATE_FUN.1	Functional testing
	ATE_IND	ATE_IND.2	Independent testing - sample
Vulnerability	AVA_VAN	**AVA_VAN.4**	Methodical vulnerability analysis

6.3 Security Requirements Rationale

The table 6.2 lists the SFRs and their dependencies. The dependency on FIA_UID.1 is met by FIA_UID.2, which is hierarchical. The dependency on FDP_IFC.1_(RS) is met by FDP_IFC.2_(RS), which is hierarchical. The SFR FTP_STM.1 must be met by the environment.

Table 6.2: SFR dependencies

ID	SFR	Dependency	Solution
		FW-SFP	
A01	FDP_IFC.1_(FW)	FDP_IFF.1	A02
A02	FDP_IFF.1_(FW)	FDP_IFC.1	A01
		FMT_MSA.3	A04
A03-A	FMT_MSA.1_(FW-A)	FDP_IFC.1	A01
		FMT_SMR.1	K03

ID	SFR	Dependency	Solution
		FMT_SMF.1	A05
A03-R	FMT_MSA.1_(FW-R)	FDP_IFC.1	A01
		FMT_SMR.1	K03
		FMT_SMF.1	A05
A04	FMT_MSA.3_(FW)	FMT_MSA.1	A03-A, A03-R
		FMT_SMR.1	K03
A05	FMT_SMF.1_(FW)	-	-
RS-SFP			
B01	FDP_IFC.2_(RS)	FDP_IFF.1	B02
B02	FDP_IFF.1_(RS)	FDP_IFC.1	B01 (hierarchical)
		FMT_MSA.3	B04
B03-A	FMT_MSA.1_(RS-A)	FDP_IFC.1	B01 (hierarchical)
		FMT_SMR.1	K03
		FMT_SMF.1	B05
B03-R	FMT_MSA.1_(RS-R)	FDP_IFC.1	B01 (hierarchical)
		FMT_SMR.1	K03
		FMT_SMF.1	B05
B04	FMT_MSA.3_(RS)	FMT_MSA.1	B03-A, B03-R
		FMT_SMR.1	K03
B05	FMT_SMF.1_(RS)	-	-
IPSEC			
D01	FDP_ITT.1_(IPSEC)	FDP_IFC.1	D02
D02	FDP_IFC.1_(IPSEC)	FDP_IFF.1	E03
D03	FCS_COP.1_(IPSEC-AES)	FCS_CKM.1	E06
		FCS_CKM.4	D05
D04	FCS_COP.1_(IPSEC-HMAC)	FCS_CKM.1	E06
		FCS_CKM.4	D05
D05	FCS_CKM.4_(IPSEC)	FCS_CKM.1	E06
IKE-SFP			
E01	FDP_ITT.1_(IKE)	FDP_IFC.1	E02
E02	FDP_IFC.1_(IKE)	FDP_IFF.1	E03

ID	SFR	Dependency	Solution
E03	FDP_IFF.1_(IKE)	FDP_IFC.1	E02
		FMT_MSA.3	E15
E04	FCS_CKM.1_(IKE-AES)	FCS_COP.1	E05
		FCS_CKM.4	E12
E05	FCS_COP.1_(IKE-AES)	FCS_CKM.1	E04
		FCS_CKM.4	E12
E06	FCS_CKM.1_(IKE-DH)	FCS_COP.1	E07, D03, D04
		FCS_CKM.4	E12, D05
E07	FCS_COP.1_(IKE-DH)	FCS_CKM.1	E06
		FCS_CKM.4	E12
E08	FCS_CKM.1_(IKE-HMAC)	FCS_COP.1	E09
		FCS_CKM.4	E12
E09	FCS_COP.1_(IKE_HMAC)	FCS_CKM.1	E08
		FCS_CKM.4	E12
E10	FCS_CKM.1_(IKE-RSA)	FCS_COP.1	E11
		FCS_CKM.4	E12
E11	FCS_COP.1_(IKE-RSA)	FCS_CKM.1	E10
		FCS_CKM.4	E12
E12	FCS_CKM.4_(IKE)	FCS_CKM.1	E04, E06, E08, E10
E13-A	FMT_MSA.1_(IKE-A)	FDP_IFC.1	E02
		FMT_SMR.1	K03
		FMT_SMF.1	E16
E13-R	FMT_MSA.1_(IKE-R)	FDP_IFC.1	E02
		FMT_SMR.1	K03
		FMT_SMF.1	E16
E14	FMT_MSA.2_(IKE)	FDP_IFC.1	E02
		FMT_MSA.1	E13-A, E13-R
		FMT_SMR.1	K03
E15	FMT_MSA.3_(IKE)	FMT_MSA.1	E13-A, E13-R
		FMT_SMR.1	K03
E16	FMT_SMF.1_(IKE)	-	-
SSH-SFP			

ID	**SFR**	**Dependency**	**Solution**
F01	FPT_ITT.1_(SSH)	-	-
F02	FDP_ITT.1_(SSH)	FDP_IFC.1	F03
F03	FDP_IFC.1_(SSH)	FDP_IFF.1	F04
F04	FDP_IFF.1_(SSH)	FDP_IFC.1	F03
		FMT_MSA.3	F16
F05	FCS_CKM.1_(SSH-AES)	FCS_COP.1	F06
		FCS_CKM.4	F13
F06	FCS_COP.1_(SSH-AES)	FCS_CKM.1	F05
		FCS_CKM.4	F13
F07	FCS_CKM.1_(SSH-ECDH)	FCS_COP.1	F07
		FCS_CKM.4	F13
F09	FCS_CKM.1_(SSH-UMAC)	FCS_COP.1	F10
		FCS_CKM.4	F13
F10	FCS_COP.1_(SSH-UMAC)	FCS_CKM.1	F09
		FCS_CKM.4	F13
F11	FCS_CKM.1_(SSH-RSA)	FCS_COP.1	F12
		FCS_CKM.4	F13
F12	FCS_COP.1_(SSH-RSA)	FCS_CKM.1	F11
		FCS_CKM.4	F13
F13	FCS_CKM.4_(SSH)	FCS_CKM.1	F05, F07, F09, F11
F14-A	FMT_MSA.1_(SSH-A)	FDP_IFC.1	F03
		FMT_SMR.1	K03
		FMT_SMF.1	F17
F14-R	FMT_MSA.1_(SSH-R)	FDP_IFC.1	F03
		FMT_SMR.1	K03
		FMT_SMF.1	F17
F15	FMT_MSA.2_(SSH)	FDP_IFC.1	F03
		FMT_MSA.1	F14-A, F14-R
		FMT_SMR.1	K03
F16	FMT_MSA.3_(SSH)	FMT_MSA.1	F14-A, F14-R
		FMT_SMR.1	K03
F17	FMT_SMF.1_(SSH)	-	-

ID	SFR	Dependency	Solution
SSHLD-SFP			
G01	FDP_ITT.1_(SSHLD)	FDP_IFC.1	G02
G02	FDP_IFC.1_(SSHLD)	FDP_IFF.1	G03
G03	FDP_IFF.1_(SSHLD)	FDP_IFC.1	G02
		FMT_MSA.3	G15
G04	FCS_CKM.1_(SSHLD-AES)	FCS_COP.1	G05
		FCS_CKM.4	G12
G05	FCS_COP.1_(SSHLD-AES)	FCS_CKM.1	G04
		FCS_CKM.4	G12
G06	FCS_CKM.1_(SSHLD-ECDH)	FCS_COP.1	G06
		FCS_CKM.4	G12
G08	FCS_CKM.1_(SSHLD-UMAC)	FCS_COP.1	G09
		FCS_CKM.4	G12
G09	FCS_COP.1_(SSHLD-UMAC)	FCS_CKM.1	G08
		FCS_CKM.4	G12
G10	FCS_CKM.1_(SSHLD-RSA)	FCS_COP.1	G11
		FCS_CKM.4	G12
G11	FCS_COP.1_(SSHLD-RSA)	FCS_CKM.1	G10
		FCS_CKM.4	G12
G12	FCS_CKM.4_(SSHLD)	FCS_CKM.1	G04, G06, G08, G10
G13-A	FMT_MSA.1_(SSHLD-A)	FDP_IFC.1	G02
		FMT_SMR.1	K03
		FMT_SMF.1	G16
G13-R	FMT_MSA.1_(SSHLD-R)	FDP_IFC.1	G02
		FMT_SMR.1	K03
		FMT_SMF.1	G16
G14	FMT_MSA.2_(SSHLD)	FDP_IFC.1	G02
		FMT_MSA.1	G13-A, G13-R
		FMT_SMR.1	K03
G15	FMT_MSA.3_(SSHLD)	FMT_MSA.1	G13-A, G13-R
		FMT_SMR.1	K03
G16	FMT_SMF.1_(SSHLD)	-	-

ID	SFR	Dependency	Solution
Administration			
H01	FDP_IFC.1_(ADM)	FDP_IFF.1	H02
H02	FDP_IFF.1_(ADM)	FDP_IFC.1	H01
		FMT_MSA.3	H05
H03-A	FMT_MSA.1_(ADM-A)	FDP_IFC.1	H01
		FMT_SMR.1	K03
		FMT_SMF.1	H06
H03-R	FMT_MSA.1_(ADM-R)	FDP_IFC.1	H01
		FMT_SMR.1	K03
		FMT_SMF.1	H06
H03-O	FMT_MSA.1_(ADM-O)	FDP_IFC.1	H01
		FMT_SMR.1	K03
		FMT_SMF.1	H06
H04	FMT_MSA.1_(ADM-ROOT)	FDP_IFC.1	H01
		FMT_SMR.1	K03
		FMT_SMF.1	H06
H05	FMT_MSA.3_(ADM)	FMT_MSA.1	H03-A. H03-R, H03-O
		FMT_MSA.1	H04
		FMT_SMR.1	K03
H06	FMT_SMF.1_(ADM)	-	-
Identification and Authentication			
I01	FIA_ATD.1_(IA)	-	-
I02	FIA_SOS.1_(IA)	-	-
I03	FIA_UAU.2_(IA)	FIA_UID.1	I05 (hierarchical)
I04	FIA_UAU.6_(IA)	-	-
I05	FIA_UID.2_(IA)	-	-
Audit			
J01	FAU_GEN.1EX_(AU)	FPT_STM.1	environment (OE.TIMESTMP)
J02	FAU_SAR.1_(AU)	FAU_GEN.1	J01
J03	FAU_SAR.3_(AU)	FAU_SAR.1	J02

ID	SFR	Dependency	Solution
General Management Facilities			
K01	FMT_MOF.1_(GEN)	FMT_SMR.1	K03
		FMT_SMF.1	K02
K02	FMT_SMF.1_(GEN)	-	-
K03	FMT_SMR.1_(GEN)	FIA_UID.1	I05 (hierarchical)
K04	FPT_TEE.1_(GEN)	-	-
K05	FPT_TRC.1_(GEN)	FPT_ITT.1	Environment (OE.HANET)
Random Number Generation			
L01	FCS_RNG.1	-	-

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

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

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

The cryptographic algorithm elliptic curve ecdh-sha2-brainpoolp256r1 contains both the cryptographic key generation and the cryptographic operation. Therefore the dependence of FCS_CKM.1_(SSH-ECDH) on SFR FCS_COP.1 is fulfilled by itself.

The cryptographic algorithm elliptic curve ecdh-sha2-brainpoolp256r1 contains both the cryptographic key generation and the cryptographic operation. Therefore the dependence of FCS_CKM.1_(SSHLD_ECDH) on SFR FCS_COP.1 is fulfilled by itself.

Table 6.3 shows how the SFRs can be traced back to the objectives.

Table 6.3: Objectives

		O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC	O.RS	O.AVAIL
A01	FDP_IFC.1_(FW)		X						
A02	FDP_IFF.1_(FW)		X						
A03-A	FMT_MSA.1_(FW-A)		X						
A03-R	FMT_MSA.1_(FW-R)		X						
A04	FMT_MSA.3_(FW)		X						
A05	FMT_SMF.1_(FW)		X						
B01	FDP_IFC.2_(RS)		X					X	
B02	FDP_IFF.1_(RS)		X					X	
B03-A	FMT_MSA.1_(RS-A)		X					X	
B03-R	FMT_MSA.1_(RS-R)		X					X	
B04	FMT_MSA.3_(RS)		X					X	
B05	FMT_SMF.1_(RS)		X					X	
D01	FDP_ITT.1_(IPSEC)			X	X	X			
D02	FDP_IFC.1_(IPSEC)			X	X	X			
D03	FCS_COP.1_(IPSEC-AES)			X	X	X			
D04	FCS_COP.1_(IPSEC-HMAC)			X	X	X			
D05	FCS_CKM.4_(IPSEC)			X	X	X			
E01	FDP_ITT.1_(IKE)			X	X	X			
E02	FDP_IFC.1_(IKE)			X	X	X			
E03	FDP_IFF.1_(IKE)			X	X	X			
E04	FCS_CKM.1_(IKE-AES)			X	X	X			
E05	FCS_COP.1_(IKE-AES)			X	X	X			
E06	FCS_CKM.1_(IKE-DH)			X	X	X			
E07	FCS_COP.1_(IKE-DH)			X	X	X			
E08	FCS_CKM.1_(IKE-HMAC)			X	X	X			
E09	FCS_COP.1_(IKE_HMAC)			X	X	X			
E10	FCS_CKM.1_(IKE-RSA)			X	X	X			
E11	FCS_COP.1_(IKE-RSA)			X	X	X			
E12	FCS_CKM.4_(IKE)			X	X	X			
E13-A	FMT_MSA.1_(IKE-A)			X	X	X			

		O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC	O.RS	O.AVAIL
E13-R	FMT_MSA.1_(IKE-R)			X	X	X			
E14	FMT_MSA.2_(IKE)			X	X	X			
E15	FMT_MSA.3_(IKE)			X	X	X			
E16	FMT_SMF.1_(IKE)			X	X	X			
F01	FPT_ITT.1_(SSH)			X	X	X			
F02	FDP_ITT.1_(SSH)			X	X	X			
F03	FDP_IFC.1_(SSH)			X	X	X			
F04	FDP_IFF.1_(SSH)			X	X	X			
F05	FCS_CKM.1_(SSH-AES)			X	X	X			
F06	FCS_COP.1_(SSH-AES)			X	X	X			
F07	FCS_CKM.1_(SSH-ECDH)			X	X	X			
F09	FCS_CKM.1_(SSH-UMAC)			X	X	X			
F10	FCS_COP.1_(SSH-UMAC)			X	X	X			
F11	FCS_CKM.1_(SSH-RSA)			X	X	X			
F12	FCS_COP.1_(SSH-RSA)			X	X	X			
F13	FCS_CKM.4_(SSH)			X	X	X			
F14-A	FMT_MSA.1_(SSH-A)			X	X	X			
F14-R	FMT_MSA.1_(SSH-R)			X	X	X			
F15	FMT_MSA.2_(SSH)			X	X	X			
F16	FMT_MSA.3_(SSH)			X	X	X			
F17	FMT_SMF.1_(SSH)			X	X	X			
G01	FDP_ITT.1_(SSHLD)			X	X	X			
G02	FDP_IFC.1_(SSHLD)			X	X	X			
G03	FDP_IFF.1_(SSHLD)			X	X	X			
G04	FCS_CKM.1_(SSHLD-AES)			X	X	X			
G05	FCS_COP.1_(SSHLD-AES)			X	X	X			
G06	FCS_CKM.1_(SSHLD-ECDH)			X	X	X			
G08	FCS_CKM.1_(SSHLD-UMAC)			X	X	X			
G09	FCS_COP.1_(SSHLD-UMAC)			X	X	X			
G10	FCS_CKM.1_(SSHLD-RSA)			X	X	X			

		O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC	O.RS	O.AVAIL
G11	FCS_COP.1_(SSHLD-RSA)			X	X	X			
G12	FCS_CKM.4_(SSHLD)			X	X	X			
G13-A	FMT_MSA.1_(SSHLD-A)			X	X	X			
G13-R	FMT_MSA.1_(SSHLD-R)			X	X	X			
G14	FMT_MSA.2_(SSHLD)			X	X	X			
G15	FMT_MSA.3_(SSHLD)			X	X	X			
G16	FMT_SMF.1_(SSHLD)			X	X	X			
H01	FDP_IFC.1_(ADM)		X						
H02	FDP_IFF.1_(ADM)		X						
H03-A	FMT_MSA.1_(ADM-A)		X						
H03-R	FMT_MSA.1_(ADM-R)		X						
H03-O	FMT_MSA.1_(ADM-O)		X						
H04	FMT_MSA.1_(ADM-ROOT)		X						
H05	FMT_MSA.3_(ADM)		X						
H06	FMT_SMF.1_(ADM)		X						
I01	FIA_ATD.1_(IA)	X							
I02	FIA_SOS.1_(IA)	X							
I03	FIA_UAU.2_(IA)	X							
I04	FIA_UAU.6_(IA)	X							
I05	FIA_UID.2_(IA)	X							
J01	FAU_GEN.1EX_(AU)						X		
J02	FAU_SAR.1_(AU)						X		
J03	FAU_SAR.3_(AU)						X		
K01	FMT_MOF.1_(GEN)						X		
K02	FMT_SMF.1_(GEN)						X		
K03	FMT_SMR.1_(GEN)		X				X	X	
K04	FPT_TEE.1_(GEN)			X	X	X			
K05	FPT_TRC.1_(GEN)								X
L01	FCS_RNG.1			X	X	X			

6.3.1 O.AUTH

This objective is met by the SFRs FIA_ATD.1_(IA), FIA_SOS.1_(IA), FIA_UAU.2_(IA), FIA_UAU.6_(IA), and FIA_UID.2_(IA). They handle authentication failures, user attribute definition, the verification of secrets, user authentication, re-authentication and user identification.

6.3.2 O.MEDIAT

This objective is met by several groups of SFRs.

FDP_IFC.1_(FW), FDP_IFF.1_(FW), FMT_MSA.1_(FW-A), FMT_MSA.1_(FW-R), FMT_MSA.3_(FW), and FMT_SMF.1_(FW) handle the firewall security policy. They define the access methods, the security attributes and their management.

FDP_IFC.2_(RS), FDP_IFF.1_(RS), FMT_MSA.1_(RS-A), FMT_MSA.1_(RS-R), FMT_MSA.3_(RS), and FMT_SMF.1_(RS) handle the RS-policy. They define the access methods, the security attributes and their management.

FDP_IFC.1_(ADM), FDP_IFF.1_(ADM), FMT_MSA.1_(ADM-A), FMT_MSA.1_(ADM-R), FMT_MSA.1_(ADM-O), FMT_MSA.1_(ADM-ROOT), FMT_MSA.3_(ADM), and FMT_SMF.1_(ADM) handle the administrative interface. They define the access method, the security attributes, and their management.

FMT_SMR.1_(GEN) defines the roles that can change the configuration.

6.3.3 O.CONFID

This objective is met by several groups of SFRs.

FDP_ITT.1_(IPSEC), FDP_IFC.1_(IPSEC), FCS_COP.1_(IPSEC-AES), FCS_COP.1_(IPSEC-HMAC), and FCS_CKM.4_(IPSEC) handle the IPsec functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.

FDP_ITT.1_(IKE), FDP_IFC.1_(IKE), FDP_IFF.1_(IKE), FCS_CKM.1_(IKE-AES), FCS_COP.1_(IKE-AES), FCS_CKM.1_(IKE-DH), FCS_COP.1_(IKE-DH), FCS_CKM.1_(IKE-HMAC), FCS_COP.1_(IKE_HMAC), FCS_CKM.1_(IKE-RSA), FCS_COP.1_(IKE-RSA), FCS_CKM.4_(IKE), FMT_MSA.1_(IKE-A), FMT_MSA.1_(IKE-R), FMT_MSA.2_(IKE), FMT_MSA.3_(IKE), and FMT_SMF.1_(IKE) handle the IKE functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.

FPT_ITT.1_(SSH), FDP_ITT.1_(SSH), FDP_IFC.1_(SSH), FDP_IFF.1_(SSH), FCS_CKM.1_(SSH-AES), FCS_COP.1_(SSH-AES), FCS_CKM.1_(SSH-ECDH), FCS_CKM.1_(SSH-UMAC), FCS_COP.1_(SSH-UMAC), FCS_CKM.1_(SSH-RSA), FCS_COP.1_(SSH-RSA), FCS_CKM.4_(SSH), FMT_MSA.1_(SSH-A), FMT_MSA.1_(SSH-R), FMT_MSA.2_(SSH), FMT_MSA.3_(SSH), and FMT_SMF.1_(SSH) handle the administrative SSH connections between management system and firewall component. They define the access methods, the security attributes, their management and cryptographic behaviour.

FDP_ITT.1_(SSHLD), FDP_IFC.1_(SSHLD), FDP_IFF.1_(SSHLD), FCS_CKM.1_(SSHLD-AES), FCS_COP.1_(SSHLD-AES), FCS_CKM.1_(SSHLD-ECDH), FCS_CKM.1_(SSHLD-UMAC), FCS_COP.1_(SSHLD-UMAC), FCS_CKM.1_(SSHLD-RSA), FCS_COP.1_(SSHLD-RSA), FCS_CKM.4_(SSHLD), FMT_MSA.1_(SSHLD-A), FMT_MSA.1_(SSHLD-R), FMT_MSA.2_(SSHLD), FMT_MSA.3_(SSHLD), and FMT_SMF.1_(SSHLD) handle the application layer SSH tunnel between firewall components. They define the access methods, the security attributes, their management and cryptographic behaviour.

FPT_TEE.1_(GEN) checks if the random numbers have a sufficient quality for cryptographic operations.

FCS_RNG.1 provides random input for cryptographic operations.

6.3.4 O.INTEG

This objective is met by several groups of SFRs.

FDP_ITT.1_(IPSEC), FDP_IFC.1_(IPSEC), FCS_COP.1_(IPSEC-AES), FCS_COP.1_(IPSEC-HMAC), and FCS_CKM.4_(IPSEC) handle the IPsec functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.

FDP_ITT.1_(IKE), FDP_IFC.1_(IKE), FDP_IFF.1_(IKE), FCS_CKM.1_(IKE-AES), FCS_COP.1_(IKE-AES), FCS_CKM.1_(IKE-DH), FCS_COP.1_(IKE-DH), FCS_CKM.1_(IKE-HMAC), FCS_COP.1_(IKE_HMAC), FCS_CKM.1_(IKE-RSA), FCS_COP.1_(IKE-RSA), FCS_CKM.4_(IKE), FMT_MSA.1_(IKE-A), FMT_MSA.1_(IKE-R), FMT_MSA.2_(IKE), FMT_MSA.3_(IKE), and FMT_SMF.1_(IKE) handle the IKE functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.

FPT_ITT.1_(SSH), FDP_ITT.1_(SSH), FDP_IFC.1_(SSH), FDP_IFF.1_(SSH), FCS_CKM.1_(SSH-AES), FCS_COP.1_(SSH-AES), FCS_CKM.1_(SSH-ECDH), FCS_CKM.1_(SSH-UMAC), FCS_COP.1_(SSH-UMAC), FCS_CKM.1_(SSH-RSA), FCS_COP.1_(SSH-RSA), FCS_CKM.4_(SSH), FMT_MSA.1_(SSH-A), FMT_MSA.1_(SSH-R), FMT_MSA.2_(SSH), FMT_MSA.3_(SSH), and FMT_SMF.1_(SSH) handle the administrative SSH connections between management system and firewall component. They define the access methods, the security attributes, their management and cryptographic behaviour.

FDP_ITT.1_(SSHLD), FDP_IFC.1_(SSHLD), FDP_IFF.1_(SSHLD), FCS_CKM.1_(SSHLD-AES), FCS_COP.1_(SSHLD-AES), FCS_CKM.1_(SSHLD-ECDH), FCS_CKM.1_(SSHLD-UMAC), FCS_COP.1_(SSHLD-UMAC), FCS_CKM.1_(SSHLD-RSA), FCS_COP.1_(SSHLD-RSA), FCS_CKM.4_(SSHLD), FMT_MSA.1_(SSHLD-A), FMT_MSA.1_(SSHLD-R), FMT_MSA.2_(SSHLD), FMT_MSA.3_(SSHLD), and FMT_SMF.1_(SSHLD) handle the application layer SSH tunnel between firewall components. They define the access methods, the security attributes, their management and cryptographic behaviour.

FPT_TEE.1_(GEN) checks if the random numbers have a sufficient quality for cryptographic operations.

FCS_RNG.1 provides random input for cryptographic operations.

6.3.5 O.NOREPLAY

This objective is met by several groups of SFRs.

FDP_ITT.1_(IPSEC), FDP_IFC.1_(IPSEC), FCS_COP.1_(IPSEC-AES), FCS_COP.1_(IPSEC-HMAC), and FCS_CKM.4_(IPSEC) handle the IPsec functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.

FDP_ITT.1_(IKE), FDP_IFC.1_(IKE), FDP_IFF.1_(IKE), FCS_CKM.1_(IKE-AES), FCS_COP.1_(IKE-AES), FCS_CKM.1_(IKE-DH), FCS_COP.1_(IKE-DH), FCS_CKM.1_(IKE-HMAC), FCS_COP.1_(IKE_HMAC), FCS_CKM.1_(IKE-RSA), FCS_COP.1_(IKE-RSA), FCS_CKM.4_(IKE), FMT_MSA.1_(IKE-A), FMT_MSA.1_(IKE-R), FMT_MSA.2_(IKE), FMT_MSA.3_(IKE), and FMT_SMF.1_(IKE) handle the IKE functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.

FPT_ITT.1_(SSH), FDP_ITT.1_(SSH), FDP_IFC.1_(SSH), FDP_IFF.1_(SSH), FCS_CKM.1_(SSH-AES), FCS_COP.1_(SSH-AES), FCS_CKM.1_(SSH-ECDH), FCS_CKM.1_(SSH-UMAC), FCS_COP.1_(SSH-UMAC), FCS_CKM.1_(SSH-RSA), FCS_COP.1_(SSH-RSA), FCS_CKM.4_(SSH), FMT_MSA.1_(SSH-A), FMT_MSA.1_(SSH-R), FMT_MSA.2_(SSH), FMT_MSA.3_(SSH), and FMT_SMF.1_(SSH) handle the administrative SSH connections between management system and firewall component. They define the access methods, the security attributes, their management and cryptographic behaviour.

FDP_ITT.1_(SSHLD), FDP_IFC.1_(SSHLD), FDP_IFF.1_(SSHLD), FCS_CKM.1_(SSHLD-AES), FCS_COP.1_(SSHLD-AES), FCS_CKM.1_(SSHLD-ECDH), FCS_CKM.1_(SSHLD-UMAC), FCS_COP.1_(SSHLD-UMAC), FCS_CKM.1_(SSHLD-RSA), FCS_COP.1_(SSHLD-RSA), FCS_CKM.4_(SSHLD), FMT_MSA.1_(SSHLD-A), FMT_MSA.1_(SSHLD-R), FMT_MSA.2_(SSHLD), FMT_MSA.3_(SSHLD), and FMT_SMF.1_(SSHLD) handle the application layer SSH tunnel between firewall components. They define the access methods, the security attributes, their management and cryptographic behaviour.

FPT_TEE.1_(GEN) checks if the random numbers have a sufficient quality for cryptographic operations.

FCS_RNG.1 provides random input for cryptographic operations.

6.3.6 O.AUDREC

FAU_GEN.1EX_(AU), FAU_SAR.1_(AU), and FAU_SAR.3_(AU) handle the audit data generation and its review.

FMT_SMR.1_(GEN) defines the roles that can change the configuration.

FMT_MOF.1_(GEN) and FMT_SMF.1_(GEN) define the security functions that can be configured by the administrators.

6.3.7 O.RS

FDP_IFC.2_(RS), FDP_IFF.1_(RS), FMT_MSA.1_(RS-A), FMT_MSA.1_(RS-R), FMT_MSA.3_(RS), and FMT_SMF.1_(RS) handle the RS-policy. They define the access methods, the security attributes and their management.

FMT_SMR.1_(GEN) defines the roles that can change the configuration.

6.3.8 O.AVAIL

FPT_TRC.1_(GEN) requires the synchronisation of *pf* states and IPsec security associations between HA peers. The synchronisation fulfils the availability requirements.

6.4 Security Assurance Requirements

Table 6.4 lists the SAR dependencies. The table shows that all dependencies are met.

Table 6.4: SAR dependencies

ID	Requirement	Dependency	Solution
R01	ADV_ARC.1	ADV_FSP.1	R02
		ADV_TDS.1	R04
R02	ADV_FSP.4	ADV_TDS.1	R04
R03	ADV_IMP.1	ADV_TDS.3	R04
		ADV_TAT.1	R13
R04	ADV_TDS.3	ADV_FSP.4	R02
R05	AGD_OPE.1	ADV_FSP.1	R02
R06	AGD_PRE.1	-	-
R07	ALC_CMC.4	ALC_CMS.1	R08
		ALC_DVS.1	R10
		ALC_LCD.1	R12
R08	ALC_CMS.4	-	-
R09	ALC_DEL.1	-	-
R10	ALC_DVS.1	-	-
R11	**ALC_FLR.2**	-	-
R12	ALC_LCD.1	-	-
R13	ALC_TAT.1	ADV_IMP.1	R03
R14	ASE_CCL.1	ASE_INT.1	R16
		ASE_ECD.1	R15
		ASE_REQ.1	R18
R15	ASE_ECD.1	-	-
R16	ASE_INT.1	-	-
R17	ASE_OBJ.2	ASE_SPD.1	R19
R18	ASE_REQ.2	ASE_OBJ.2	R17
		ASE_ECD.1	R15
R19	ASE_SPD.1	-	-
R20	**ASE_TSS.2**	ASE_INT.1	R16
		ASE_REQ.1	R18
		ADV_ARC.1	R01
R21	ATE_COV.2	ADV_FSP.2	R02
		ATE_FUN.1	R23
R22	ATE_DPT.1	ADV_ARC.1	R01

ID	Requirement	Dependency	Solution
		ADV_TDS.2	R04
		ATE_FUN.1	R23
R23	ATE_FUN.1	ATE_COV.1	R21
R24	ATE_IND.2	ADV_FSP.2	R02
		AGD_OPE.1	R05
		AGD_PRE.1	R06
		ATE_COV.1	R21
		ATE_FUN.1	R23
R25	**AVA_VAN.4**	ADV_ARC.1	R01
		ADV_FSP.4	R02
		ADV_TDS.3	R04
		ADV_IMP.1	R03
		AGD_OPE.1	R05
		AGD_PRE.1	R06
		ATE_DPT.1	R22

6.4.1 Security Assurance Rationale

The overall security claim of this Security Target is aimed at EAL4.

The attack potential of the anonymous users is moderate. It must be noted, however, that the firewall components are exposed to unrestricted attackers, simply because they are exposed to the Internet. Therefore the vulnerability analysis has been augmented to AVA_VAN.4 in order to match the resistance to attackers with a moderate attack potential.

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

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

7 TOE Summary Specification

7.1 TOE Summary Specification

7.1.1 SF_PF: Packet Filter

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

The filter rules allow to filter by the criteria:

1. address of source

2. address of destination
3. transport layer protocol
4. interface on which traffic arrives and departs
5. IP version (IPv4 or IPv6)
6. differentiated services field

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

SF_PF.3: Packets with presumed spoofed source- or destination-IP addresses are dropped if the option is activated and spoofing recognition is possible. Packets with source routing options are dropped. No spoofing check is possible when the firewall components operate as bridges.

SF_PF.4: The firewall components can modify headers to make the information flows less susceptible to hijacking attacks.

This Security Function addresses the SFRs FDP_IFC.1_(FW) and FDP_IFF.1_(FW).

7.1.2 SF_RS: Classification

SF_RS.1: The administrators can classify selected interfaces as level low or high. Then only encrypted traffic is allowed for low classified interfaces. All traffic send by the component will be encrypted. The default is not to classify any interface at level low. This allows unencrypted traffic.

This Security Function addresses the SFRs FDP_IFC.2_(RS) and FDP_IFF.1_(RS).

7.1.3 SF_IPSEC: IPsec Filtering

SF_IPSEC.1: Connections between networks protected by different firewall components can be protected by IPsec transforms against eavesdropping, modification and replay attacks. The transforms use the following probabilistic or permutational functions according to FIPS-197 and NIST-SP800-38A: AES block cipher in CBC mode with a key size of 128 bit, 192 bit (default), or 256 bit for confidentiality, the HMAC-SHA256 with a key size of 256 bit for integrity, Diffie-Hellman exponent generation with a key size of 2048 bit for cryptographic key agreement, and RSA signatures with a key size of 2048 bit for authentication. Expired keys are overwritten with zeros.

This Security Function addresses the SFRs FDP_ITT.1_(IPSEC), FDP_IFC.1_(IPSEC), FCS_COP.1_(IPSEC-AES), FCS_COP.1_(IPSEC-HMAC), FCS_CKM.4_(IPSEC), FDP_ITT.1_(IKE), FDP_IFC.1_(IKE), FDP_IFF.1_(IKE), FCS_CKM.1_(IKE-AES), FCS_COP.1_(IKE-AES), FCS_CKM.1_(IKE-DH), FCS_COP.1_(IKE-DH), FCS_CKM.1_(IKE-HMAC), FCS_COP.1_(IKE-HMAC), FCS_CKM.1_(IKE-RSA), FCS_COP.1_(IKE-RSA), FCS_CKM.4_(IKE), and FCS_RNG.1.

7.1.4 SF_SSHLD: SSH Launch Daemon

SF_SSHLD.1: Connections between different firewall components can be protected by SSH transforms against eavesdropping, modification and replay attacks. The transforms use the following probabilistic or permutational functions.

- Data encryption and decryption: This operation uses an AES block cipher in CTRmode with a cryptographic key size of 128 bit according to FIPS-197 and NIST-SP800-38A.
- Cryptographic key agreement: This operation uses the elliptic curve algorithm ecdh-sha2-brainpoolp256r1 with a key size of 256 bit, according to RFC5639 and [EBP].
- Generation and verification of message authentication code: This operation uses the UMAC-128-ETM algorithm with a key size of 256 bit, according to RFC4418.
- Authentication: This operation uses RSA signatures with a key size of 2048 bit, according to PKCS#1, v2.1.

SF_SSHLD.2: Expired keys are overwritten with zeros.

This Security Function addresses the SFRs FDP_ITT.1_(SSHLD), FDP_IFC.1_(SSHLD), FDP_IFF.1_(SSHLD), FCS_CKM.1_(SSHLD-AES), FCS_COP.1_(SSHLD-AES), FCS_CKM.1_(SSHLD-ECDH), FCS_CKM.1_(SSHLD-UMAC), FCS_COP.1_(SSHLD-UMAC), FCS_CKM.1_(SSHLD-RSA), FCS_COP.1_(SSHLD-RSA), FCS_CKM.4_(SSHLD), and FCS_RNG.1.

7.1.5 SF_IA: Identification and Authentication

SF_IA.1: The TOE guarantees that the administrators, service users and revisors have to identify and authenticate to the management system GUI and the standalone GUI with a user name and password.

SF_IA.2: The genucenter and genuscreen administrative GUIs check the password quality of the genucenter administrators, the genucenter root administrators, the genucenter service users, the genucenter revisors, the genuscreen administrator and the genuscreen revisor: it must be at least 8 characters in length.

SF_IA.3: After 10 minutes of inactivity at the genucenter GUI, the administrators, service users and revisors must re-authenticate themselves.

This Security Function addresses the SFRs FDP_IFC.1_(ADM), FDP_IFF.1_(ADM), FIA_ATD.1_(IA), FIA_SOS.1_(IA), FIA_UAU.2_(IA), FIA_UAU.6_(IA), and FIA_UID.2_(IA).

7.1.6 SF_AU: Audit

SF_AU.1: The TOE shall generate audit records for

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

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

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

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

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

SF_AU.3: The TOE shall provide the genucenter administrators, genucenter root administrators, the genucenter service users and the genucenter revisors with a display of audit data on the management server within their administrative domain. The audit data shall be searchable by

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

SF_AU.4: The TOE shall provide the genuscreen administrator, the genuscreen revisor and the genuscreen service user with a display of audit data on the firewall components. The audit data shall be searchable by

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

This Security Function addresses the SFRs FAU_GEN.1EX_(AU), FAU_SAR.1_(AU), FAU_SAR.3_(AU).

7.1.7 SF_SSH: SSH Channel

SF_SSH.1: Connections between the firewall components and the management systems are protected by SSH transforms against eavesdropping, modification and replay attacks. The transforms use the following probabilistic or permutational functions.

- Data encryption and decryption: This operation uses an AES block cipher in CTR mode with a cryptographic key size of 128 bit, according to FIPS-197 and NIST-SP800-38A.
- Cryptographic key agreement: This operation uses the elliptic curve algorithm ecdh-sha2-brainpoolp256r1 with a key size of 256 bit, according to RFC5639 and [EBP].
- Generation and verification of message authentication code: This operation uses the UMAC-128-ETM algorithm with a key size of 256 bit, according to RFC4418.
- Authentication: This operation uses RSA signatures with a key size of 2048 bit, according to PKCS#1, v2.1.

SF_SSH.2: Expired keys are overwritten with zeros.

This Security Function addresses the SFRs FPT_ITT.1_(SSH), FDP_ITT.1_(SSH), FDP_IFC.1_(SSH), FDP_IFF.1_(SSH), FCS_CKM.1_(SSH-AES), FCS_COP.1_(SSH-AES), FCS_CKM.1_(SSH-ECDH), FCS_CKM.1_(SSH-UMAC), FCS_COP.1_(SSH-

UMAC), FCS_CKM.1_(SSH-RSA), FCS_COP.1_(SSH-RSA), FCS_CKM.4_(SSH), and FCS_RNG.1.

7.1.8 SF_ADM: Administration

SF_ADM.1: The TOE allows the genucenter administrators and the genucenter root administrators to change the IKE configuration, the SSHLD configuration, the packet filter configuration, and the network interface classification at the management system within their respective domain.

The TOE allows the genuscreen administrator to change the IKE configuration, the SSHLD configuration, the packet filter configuration, and the network interface classification at the firewall component.

The TOE allows the genucenter administrators and the genucenter root administrators to change the SSH configuration at the management system within their respective domain.

The TOE allows the genucenter service users and revisors to view the IKE configuration, the SSHLD configuration, the packet filter configuration, and the network interface classification at the management system within their respective domain.

The TOE allows the genuscreen revisor to view the IKE configuration, the SSHLD configuration, the packet filter configuration, and the network interface classification at the firewall component.

The TOE allows the genucenter service users and revisors to view the SSH configuration at the management system within their respective domain.

SF_ADM.2: The IKE configuration, the SSHLD configuration, the SSH configuration, and the packet filter configuration have restrictive defaults.

The network interface classification has permissive defaults.

SF_ADM.3: The TOE allows the genucenter administrators, the genucenter service users and the genucenter root administrator to transfer the configuration data to the firewall components and to update software on the firewall components within their administrative domain.

SF_ADM.4: The TOE allows the genucenter administrators, the genucenter service users, the genucenter root administrator, and the genucenter revisors to view the configuration and log data on the management system within their administrative domain.

The TOE allows the genuscreen administrator and the genuscreen revisor to view the configuration and log data on the firewall component.

SF_ADM.5: The TOE allows the genucenter root administrators to alter the passwords for the genucenter administrators, the genucenter administrators, the genucenter service users, the genucenter revisors, the genuscreen administrator, and the genuscreen revisor at the management system.

SF_ADM.6: The TOE allows the genuscreen administrator to alter the passwords for the genuscreen administrator and the genuscreen revisor at the firewall component.

This Security Function addresses the SFRs FMT_MSA.1_(FW-A), FMT_MSA.1_(FW-R), FMT_MSA.3_(FW), and FMT_SMF.1_(FW).

This Security Function addresses the SFRs FMT_MSA.1_(RS-A), FMT_MSA.1_(RS-R), FMT_MSA.3_(RS), and FMT_SMF.1_(RS).

This Security Function addresses the SFRs FMT_MSA.1_(IKE-A), FMT_MSA.1_(IKE-R), FMT_MSA.2_(IKE), FMT_MSA.3_(IKE), and FMT_SMF.1_(IKE).

This Security Function addresses the SFRs FMT_MSA.1_(SSH-A), FMT_MSA.1_(SSH-R), FMT_MSA.2_(SSH), FMT_MSA.3_(SSH), and FMT_SMF.1_(SSH).

This Security Function addresses the SFRs FMT_MSA.1_(SSHLD-A), FMT_MSA.1_(SSHLD-R), FMT_MSA.2_(SSHLD), FMT_MSA.3_(SSHLD), and FMT_SMF.1_(SSHLD).

This Security Function addresses the SFRs FMT_MSA.1_(ADM-A), FMT_MSA.1_(ADM-R), FMT_MSA.1_(ADM-O), FMT_MSA.1_(ADM-ROOT), FMT_MSA.3_(ADM), and FMT_SMF.1_(ADM).

7.1.9 SF_GEN: General Management Facilities

SF_GEN.1: The TOE allows the genucenter administrators, the genucenter root administrators, and the genuscreen administrator to change the logging configuration and the reaction to the failed random number generator test.

SF_GEN.2: The TOE knows the following roles:

- administrator: Depending on the administrated system and/or administrative domain, this role is filled by the genucenter administrators, the genucenter root administrators, the genucenter root shell account, or the genuscreen administrator.
- service: This role is filled by the genucenter service users.
- revisor: Depending on the administrated system and/or the administrative domain, this role is filled by the genucenter revisors or the genuscreen revisor.

SF_GEN.3: The TOE runs a random number generator test at start-up. If the quality of the random numbers generated is not sufficient, it takes an action. The action contains two parts:

- create a log entry,
- and disable VPN operation.

SF_GEN.4: The program `sasyncd` synchronises the IPsec security associations between HA peers. The pf uses the `pfsync` interface to synchronize the pf states between HA peers. The granularity of this synchronisation are single pf states and single SAs. The data is transferred as clear text.

This Security Function addresses the SFRs FMT_MOF.1_(GEN), FMT_SMF.1_(GEN), FMT_SMR.1_(GEN), FPT_TRC.1_(GEN), and FPT_TEE.1_(GEN).

Application note: **SF_GEN.4** only applies if the HA setup is used.

7.2 Self-protection against interference and logical tampering

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

- The configuration of the firewall components from the management system uses SSH as a cryptographic measure. The SSH configuration inhibits eavesdropping, man-in-the-middle, and reply attacks.
- The collection of the log data from the firewall components uses an SSH channel as a cryptographic measure. The SSH configuration inhibits eavesdropping, man-in-the-middle, and reply attacks.
- The ISAKMPD daemon uses cryptographic measures for key exchange and data transmission. The IKE configuration inhibits eavesdropping, man-in-the-middle, and reply attacks.

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

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

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

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

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

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

7.3 Self-protection against bypass

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

8 Use of Cryptographic Functions

The use of cryptographic functions is summarised in table 8.1.

Table 8.1: Cryptographic functions

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
IKEv1 IPsec					
1	Authentication	RSA signature generation and verification for mutual authentication (RSASSA-PKCS1-v1_5) using SHA-256	PKCS#1, v2.1, FIPS180-4, RFC2409e	Modulus length = 2048	yes
2	Key Agreement	DH with Diffie-Hellman group 14 using HMAC-SHA256	RFC2409, RFC3526, RFC2104, FIPS-180-4	P length = 2048	yes
3	Confidentiality	AES in CBC mode	FIPS-197, NIST-SP800-38A RFC3502	|k| = 128, 192 (default) or 256	yes
4	Integrity	HMAC with SHA-256	RFC2104, FIPS-180-4	|k| = 256	yes
5	Trusted Channel	IKEv1 and IPsec	RFC2409, RFC4301		yes
SSH-2					
6	Authentication	RSA signature generation and verification for mutual authentication (RSASSA-PKCS1-v1_5) using SHA1	PKCS#1, v2.1, FIPS180-4, RFC4432	Modulus length = 2048	no
7	Key Agreement	ECDH with SHA-256	RFC5656, FIPS-180-4, FIPS-186-3,	Key sizes corresponding to the used	yes

				elliptic curve brainpoolp 256r1	
8	Confidenti ality	AES in CTR mode	FIPS-197, NIST-SP800-38A, RFC4344	|k| = 128	yes
9	Integrity	UMAC with AES	RFC4418, FIPS-197	|k| = 256	yes
10	Trusted Channel	SSH v2.0	RFC4253 with the ETM extension		no[5]

9 Glossary

Administrator/s: This term is used both as a role and as users possessing that role. The singular administrator is used for the role, and the plural administrators is used for the users (unless a singular form is grammatically needed).

The meaning of role only applies when the role is explicitly mentioned in the context, otherwise the user is described by the term administrator(s).

Basic-auth: The basic authentication is a simple authentication method defined by the HTTP protocol, see RFC2617. It is used by the genuscreen administrative GUI.

Cookie: Cookies are part of the HTTP protocol, see RFC2965. They are used as an authentication method by the genucenter administrative GUI.

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

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

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

Isakmpd: The name of the OpenBSD ISAKMP daemon implementation.

genucrypt: The IPsec crypto appliance from genua.

genugate: The two-tiered (packet filter/application level gateway) highly secure firewall from genua.

Service: This term is used as a role. Users possessing that role are named service users.

Pf: The name of the OpenBSD packet filter.

[5] This follows from No 6.

Privilege revocation: A security measure where the process gives up all privileges no longer needed in an irreversible way after startup. Only then the process interacts with external entities. An attacker may only gain low privileges.

Privilege separation: A security measure that separates a task in two processes. One of the processes runs with low privileges and interacts with external entities. The other process runs with higher privileges and performs tasks on behalf of the first process. If the first process is corrupted, an attacker has only gained low privileges.

Revisor/s: This term is used both as a role and as users possessing that role. The singular revisor is used for the role, and the plural revisors is used for the users (unless a singular form is grammatically needed).

The meaning of role only applies when the role is explicitly mentioned in the context, otherwise the user is described by the term revisor(s).

10 Abbreviations

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
CTR	Counter (a block cipher mode of operation)
DH	Diffie-Hellman
ESP	Encapsulated Security Payload
ETM	Encrypt Then MAC
FTP	File Transfer Protocol.
GUI	Graphical User Interface
HA	High Availability
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security protocol suite
ISAKMP	Internet Security Association Key Management Protocol
L2TP	Layer 2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
NAT	Network address translation
OSPF	Open Shortest Path First
PXE	Preboot eXecution Environment
RDR	Redirect rule
RFC	Request for comment
RSA	Rivest Shamir Adleman
SA	Security Association
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SSH	Secure Shell
TCP	Transmission Control protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol
UMAC	Universal Hashing Message Authentication Code

11 Bibliography

[CC_1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1

[CC_2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1

[CC_3] Common criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1

[AIS20] Anwendungshinweise und Interpretationen zum Schema (AIS) https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/AnwendungshinweiseundInterpretationen/AISCC/aiscc_node.html

[AIS31] Anwendungshinweise und Interpretationen zum Schema (AIS) https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/AnwendungshinweiseundInterpretationen/AISCC/aiscc_node.html

[KS2011] W. Killmann, W. Schindler, “A proposal for: Functionality classes for random number generators”, Version 2.0, September 18, 2011

[DOC-GS] genuscreen Installations- und Konfigurationshandbuch Version 5.0 Z

[DOC-GZ] genucenter Installations- und Konfigurationshandbuch Version 5.0 Z

[PF] OpenBSD pf.conf Manual http://www.openbsd.org/cgi-bin/man.cgi?query=pf.conf&apropos=0&sektion=0&manpath=OpenBSD+5.5&arch=i386&format=html

[PKCS #1, v2.1] RSA Cryptography Standards Version 2.1 http://www.ietf.org/rfc/rfc3447.txt

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

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

[RFC2460] Internet Protocol, Version 6 (IPv6) Specification http://www.ietf.org/rfc/rfc2460.txt

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

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

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

[RFC4418] UMAC: Message Authentication Code using Universal Hashing http://www.ietf.org/rfc/rfc4418.txt

[RFC5639] Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation
http://www.ietf.org/rfc/rfc5639.txt

[RFC5656] Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer
http://www.ietf.org/rfc/rfc5656.txt

[FIPS-180-4] Secure Hash Standard
http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[FIPS-186-3] Digital Signature Standard (DSS)
http://csrc.nist.gov/publications/fips/fips186-3/fips186-3.pdf

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

[NIST-SP800-38A] Recommendation for Block Cipher Modes of Operation: Methods and Techniques
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

[EBP] ECC Brainpool, "ECC Brainpool Standard Curves and Curve Generation", October 2005,
http://www.ecc-brainpool.org/download/Domain-parameters.pdf