genuscreen 7.0
Security Target

genua GmbH — Kirchheim

2020-07-17

Version 7.0.15(8ef848c)

Contents

1 ST Introduction

1.1 ST Reference

	ST Reference
ST Title	genuscreen 7.0 Security Target
Version	Version 7.0.15
Developer	genua GmbH
Date	2020-07-17

1.2 TOE Reference

	TOE Reference
TOE Title	genuscreen 7.0
TOE Reference	genuscreen 7.0 software
Product Name	genuscreen 7.0p11 / genucenter 7.0p6

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

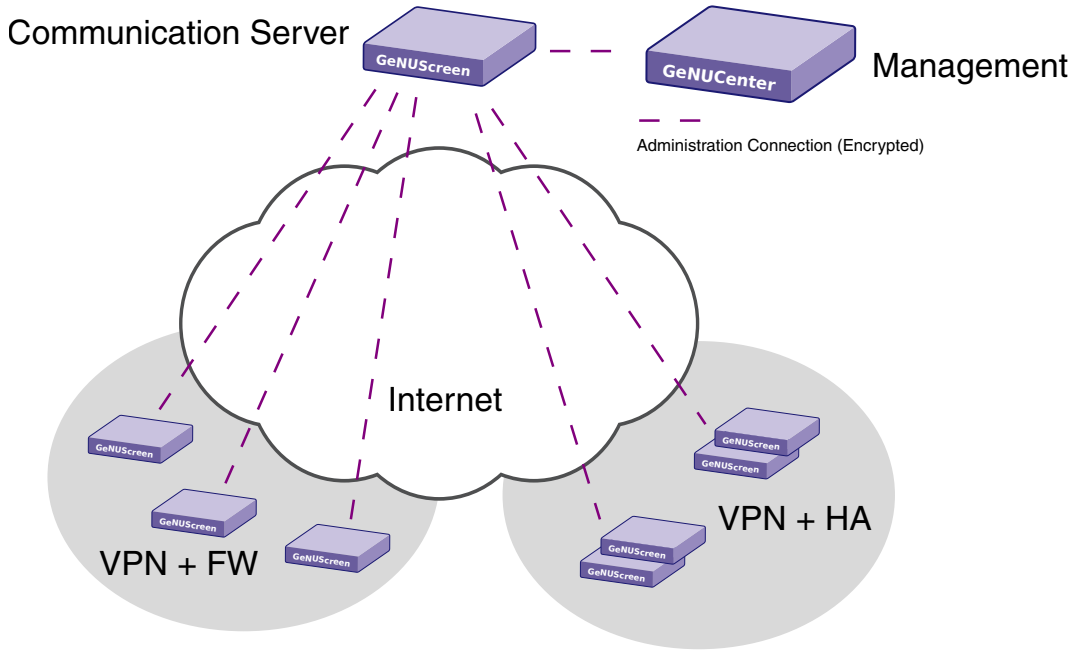
The TOE **genuscreen 7.0** makes VPN and firewall functionality available and easy to manage. It consists only of software and documentation. It protects networks at the border to the Internet by filtering incoming and outgoing data traffic. It also protects the data flowing between several protected networks against unauthorised inspection and modification.

One part of the TOE runs on a number (at least 2) of machines (**genuscreen** appliances) that work as network filters, hereafter called firewall components. The other part of the TOE runs on the machine to manage the network of firewall components. This machine, the **genucenter** management system, is a central component. The firewall components are initialised on a secure network from the management system. The TOE provides IPv4 and 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 he ISAKMP Internet standard RFC2409 [14], and is implemented in user space by OpenBSD's `isakmpd`.

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.



Optionally, a SIP module can be installed on the genuscreen components in order to integrate a Session Border Controller (SBC).

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 genubox, genucard, 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 1.3.1 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 by IPsec using IKEv1.

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, an optional CD ROM, an optional USB interface, and a hard drive as permanent storage for the configuration and log files.

  Currently[1], the supported hardware variants are genucenter S revision 2 and 3, genucenter M revision 2 and 3, and genucenter L revision 2 and 3.

- Software: OpenBSD Version 6.1, 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[1], the supported hardware variants are genuscreen XS revision 2, genuscreen S revision 2 and 3, genuscreen M revision 2 and 3, genuscreen L revision 2 and 3, genuscreen XL revision 2 and 3, and infodas SDoT Server V3.

- Software: OpenBSD Version 6.2, kernel and user space programs, HTTP/S server.

1.3.3.3 Legacy Hardware and Virtual genucenter There are also the legacy versions genuscreen and genucenter versions 200, 400, 600 and 800 in the field with hardware revision 6 and 7 which are out of scope for the current certification. The software genuscreen 7.0 runs on this hardware with the same functionality and security measures, but running the software on the legacy hardware has not been evaluated.

Also, operating the genucenter software on a virtual machine is out of scope for this certification. If the virtual genucenter is used, the end user has to ensure that all assumptions and objectives on the operational environment are met by the virtual machine.

1.4 TOE Description

The TOE is a distributed stateful packet filter firewall system with VPN capabilities and central configuration. It provides IPv4 and basic IPv6 support.

[1] See section 1.4.11 and table 1 for the list of actually evaluated versions.

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.

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.

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 7.0 installation CD/USB stick 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 IPsec VPN functionality, 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 (security association) states are synced by two daemons. Thus a takeover can take place without interrupting connections and VPNs.

The genuscreen has two application layer proxies for FTP and SIP[2]. They are used to open dynamically negotiated ports for the respective protocols. This is done by inserting new rules into the packet filter *pf*, which is considered as the main security mechanism. Therefore this ST does not state SFRs for the proxies. The proxies themselves are not part of the TOE. However, they can be used in a certified configuration, because they have security advantages over the alternative of *a priori* allowing a large port range and do not interfere with the security properties 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.

[2]The SIP proxy should not be confounded with the SIP relay, see section 1.4.7.

The operational administrator is a restricted administrator which cannot change the cryptographic settings. Complementary the security administrator can only change the cryptographic settings. If not explicitly mentioned, both admin roles are subsumed under the general term genucenter administrators.

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.

As an alternative for appliances without connection to the genucenter, the update can also be performed using a USB stick. The configuration for one or several appliances is stored in an encrypted and signed form. Updates are only applied if the signature can be verified when the stick is inserted in a USB connector at the appliance.

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 7.0 installation CD/USB stick. This medium also contains all software to install the genuscreen appliances.

The authentication of administrators and revisors at the genucenter can be configured to use an external LDAP server. This allows to integrate the genucenter management roles in an existing infrastructure. However, the LDAP infrastructure must be secured against attacks. Note that the genucenter root administrator cannot be configured for LDAP usage.

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

The high availability option for genucenter is not part of the TOE.

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

1.4.3 Packet Filter 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 defragmentation 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. *pf* filter rules can be used to transfer packets between different routing domains.

The genucenter and genuscreen GUIs allow to mark interfaces to allow only encrypted traffic. This feature adds *pf* rules that allows only selected connections for cryptographic communications.

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 [24].
- Cryptographic key agreement: This operation uses the Diffie-Hellman exponent generation with a key size of 2048 bit, according to RFC2409 [14] and RFC3526 [17].
- Generation and verification of message authentication code: This operation uses the HMAC-SHA256 with a key size of 256 bit according to RFC2104 [18] and FIPS-180-4 [27].
- Authentication: This operation uses RSA signatures with a key size of 2048 bit according to PKCS#1, v2.1 using RSASSA-PKCS1-v1_5 and SHA-256.
- Key destruction: Expired keys are overwritten with zeros.

1.4.5 SSH Features

The TOE uses the following SSH features respective enhancements:

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 [24].
- Cryptographic key agreement: This operation uses the elliptic curve algorithm ecdh-sha2-brainpoolp256r1 with a key size of 256 bit, according to RFC5639 [20] and Brainpool curves [21].
- 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 [19].
- Authentication: This operation uses RSA signatures with a key size of 2048 bit according to PKCS#1, v2.1 using RSASSA-PKCS1-v1_5 and SHA-512.
- Key destruction: Expired keys are overwritten with zeros.

1.4.6 Basic IPv6 Support

The TOE can operate in IPv6 environments (see RFC2460 [11]). 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 SIP Relay as an Optional Module

The TOE includes a SIP relay to allow the usage of a Session Border Controller (SBC). The SIP relay is not included in the basic installation image but must be installed as an optional module at the genucenter. The SIP relay software is then installed on all appliances that use the relay. The SIP relay is the only module that is part of the TOE. The SIP relay is a user land process that controls the access to the SBC.

The SIP relay is more powerful than the SIP proxy because it can filter the SIP protocol and does not only open port ranges with *pf* states.

1.4.8 Network Separation using Routing Domains

The Kernel supports several different routing tables to which processes can be attached. This enables network separation through these routing domains. Selected packets can be transferred between the domains by explicitly configured *pf* rules. An example for this usage are different default routes.

1.4.9 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/USB stick. 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.

1.4.10 Excluded Features

The following features are excluded from the TOE.

1.4.10.1 No Cryptocard The firewall components can use a cryptocard to perform cryptographic operations for IPsec usage. However, usage of the cryptocard is out of scope for this TOE.

1.4.10.2 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.

1.4.10.3 No L2TP VPN Although the firewall components support the L2TP for VPN, it is excluded from the TOE and *must not be configured*.

1.4.10.4 No IKEv2/MOBIKE VPN The protocol IKEv2 is only used to connect to third party appliances such as mobile phones that use the MOBIKE VPN. IKEv2 is not intended to be a replacement for the IPsec using IKEv1.

1.4.10.5 No Dynamic Routing The dynamic routing feature which uses OSPF only works with IPv4 and is out of scope for this TOE.

1.4.10.6 No genucenter HA While the HA setup for the genuscreens is part of the evaluation, the HA setup for genucenter is out of scope.

1.4.10.7 No Remote Maintenance The remote maintenance feature using a rendezvous genuscreen application is out of scope.

1.4.10.8 No genucenter Rest API The genucenter REST API is out of scope and must not be used.

1.4.11 Physical Scope

The physical scope of the 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.

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

The TOE runs on CPUs with a wide range of performance characteristics, depending on the customer's need. For revision 2 and 3 of the hardware, the CPUs are Intel CPUs running in 64 bit mode. The entry level hardware models use Intel Atom or Intel Celeron CPUs, the middle level hardware use a Intel Xeon-D CPU and the high performance hardeare use Intel Xeon E3 and Intel Xeon E5 CPUs. The TOE is compiled with compiler options that allow running the TOE on all CPUs. The network interfaces require on-board or PCI extension cards that are supported by the OpenBSD *em* or *ix* drivers.

Table 1: Scope of delivery

Type	Name	Release	Medium
Hardware genuscreen	genuscreen XS[3] [4], genuscreen S, genuscreen M, genuscreen L, genuscreen XL[5], infodas SDoT Server V3		
Hardware genucenter	genucenter S[6], genucenter M[7], genucenter L		
Software	genuscreen	7.0p11	CD-ROM / USB image
Software	genucenter	7.0p6	CD-ROM / USB image
Software	SIP module	7.0p11	TAR archive
Documentation	genuscreen	7.0	CD-ROM / USB image
Documentation	genucenter	7.0	CD-ROM / USB image

[3]the variant XS only exists in revision 2 [4]hardware only tested as communication server [5]hardware only tested as genucenter L
[6]hardware only tested as genuscreen M [7]hardware only tested as genuscreen L

Application Note: While the re-evaluation was performed only with genuscreen and genucenter hardware of revision 3, the software is expected to run with all security features also on older and newer hardware revisions, provided the hardware requirements of the preceding paragraph are met.

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

Application Note: Some CPUs allow the usage of hardware enhanced AES-NI. Please note that the evaluation was performed with disabled hardware enhancement. Users of the TOE have to judge by themselves if a hardware enhanced operation is acceptable.

1.4.12 Logical Scope

The following sections define the logical scope of the TOE.

1.4.12.1 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.

1.4.12.2 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).
- Interfaces can be configured into distinct routing domains with different routing tables.

1.4.12.3 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.

1.4.12.4 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.

1.4.12.5 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 [1]). If the system is supplied with an appropriate smartcard, the smartcard is used to regularly seed the random number generator from the smartcard. By this the random number generator can be upgraded to DRG.4. However, this Security Target only claims class DRG.3.

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 5 (April 2017).

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 2 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.[8]

The general term administrators describes the union of the genucenter administrators, the operational administrator, the security administrator, the genucenter root administrators, the genucenter root shell account, and the genuscreen administrator[9].

The general term service user describes the genucenter service users[10].

The general term revisors describes the union of the genucenter revisors and the genuscreen revisor[11].

[8] Note that the user operator for the genucenter and web operator for the genuscreen are used for the remote maintenance feature that is not part of the evaluation.

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

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

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

Table 2: 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.
operational 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, but they cannot change the cryptographic configuration.
security administrators	These are authenticated users at the management system that have administrative rights to change the firewall component's cryptographic 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 configuration on the firewall component. This user can also be used if the appliances are managed by a genucenter, either as a root user or as a configurable system user. The user also has a root shell account for administrative maintenance purposes.

	Users
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. This user can also be configured as a web revisor if the appliances are managed by a genucenter[12]

3.2 Threats

The two different components of the TOE (management system and firewall component) fulfil different purposes and therefore must confront different threats (see table 3).

Table 3: 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.

[12]The difference between the genuscreen revisor and the web revisor is that the genuscreen revisor is configured at the genuscreen GUI and the web revisor is configured at the genucenter GUI.

	Threats
T.MMODIFY	An anonymous user might modify the configuration or audit data 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 (see table 4).

Table 4: Policies

	Policies
P.AVAIL[13]	A high availability operation must be possible where peers can take over the services of a failing system. (This policy only applies if needed.)

[13] **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 (see table 5).

Table 5: 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 [13] and [12] (summarised in section 1.4.9).
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[14]	The environment provides a physical separate network for TSF data transfer for the optional high availability setup.

	Assumptions
A.REMOTE_AUTH[15]	The server for external LDAP authentication of genucenter administrators and revisors is located in a secure network.

[14]**Application Note**: This assumption only applies if the HA setup is used.
[15]**Application Note**: This assumption only applies if an external LDAP server is used for authentication.

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 objectives listed in table 6.

Table 6: Objectives

	Objectives
O.AUTH	The TOE must assure that only administrators can change the packet filter, VPN and SSH configuration.
O.MEDIAT	The TOE must mediate the flow of all data between all connected networks.
O.CONFID[16]	The TOE must assure that data transferred between the networks protected by firewall components is kept confidential unless explicitly configured otherwise.
O.INTEG[16]	The TOE must assure that data transferred between the networks protected by firewall components cannot be modified unnoticed unless explicitly configured otherwise.
O.NOREPLAY[16]	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.AVAIL[17]	The TOE must optionally provide a fail over solution where the services of a failing system are taken over by a peer machine.

[16] **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.
[17] **Application Note**: This objective only applies if the HA setup is used.

4.2 Security Objectives for the Operational Environment

The operational environment must ensure the security objectives from table 7.

Table 7: Objectives for the Operational 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 [13] and [12]. A summary of the procedure is given in section 1.4.9.
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[18]	The IT-environment must supply a physical network for transfer of TSF data between nodes for the optional high availability setup.
OE.REMOTE_AUTH[19]	The IT-environment must assure that the LDAP server for external authentication at the genucenter is located in a secure network.

[18] **Application Note**: This objective for the operational environment only applies if the HA setup is used.
[19] **Application Note**: This objective for the operational environment only applies if external LDAP authentication 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 8 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 8: TOE Rationale

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

4.3.1.8 A.REMOTE_AUTH The objective **OE.REMOTE_AUTH** assures that the LDAP server for external authentication is located in a secure 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 transforms.

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 he 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.

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.INTEG** and **O.NOREPLAY**. These assure that the firewall components' public keys are initialised over an authenticated network and that all data flowing between the firewall components is protected by IPsec transforms against unauthorised modification and re-injection of earlier data.

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.INTEG** and **O.NOREPLAY**. 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 Class FAU: Security audit

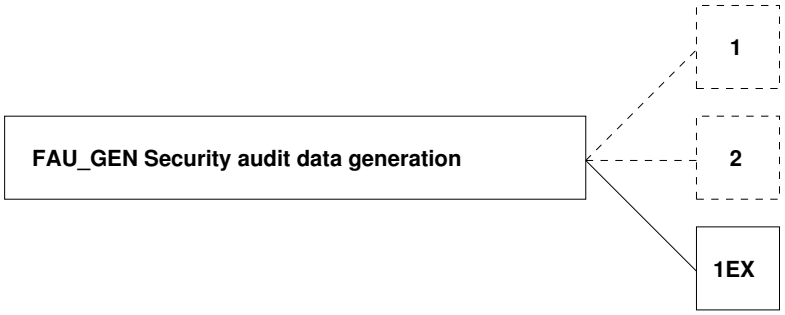
5.1.1 FAU_GEN: Security audit data generation

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 be used as a replacement for the dependencies on FAU_GEN.1, because all other audit events can be specified as in FAU_GEN.1.

Family behaviour

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

Component levelling



The components FAU_GEN.1 and FAU_GEN.2 are already described in [8]. 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]**.

The TSF are allowed to reduce audit data generation on the following conditions: **[assignment: conditions for reduction of audit data generation]**

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]**.

5.2 Class FCS: Cryptographic Support

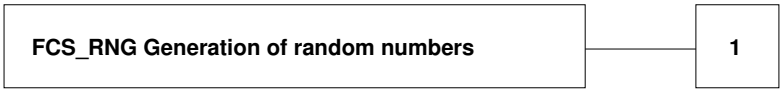
The following family has been defined in [16], a supporting document for AIS20 [1] and AIS31 [2]. For the rationale of the definition of this extended component, see [16].

5.2.1 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.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** (added text) and/or ~~crossed out~~ (removed text).
- 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 [8]. In the statement of the requirements, the abbreviation in parentheses defines the specific iteration of the associated Part 2 requirement.

6.1.1 Firewall 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: filter 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 re-assembled 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 operational 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 Network Separation SFP

This section identifies the SFRs associated with the network separation using routing domains.

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

FDP_IFC.2.1_(NS) The TSF shall enforce the [**NS-SFP**] on [

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

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

FDP_IFC.2.2_(NS) 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_(NS) Simple security attributes

FDP_IFF.1.1_(NS) The TSF shall enforce the [**NS-SFP**] based on the following types of subject and information security attributes: [

- **subject security attributes: none**
- **information security attributes:**
  - **the incoming interface and its routing table**].

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

- **the outgoing interface is selected using the routing table of the routing domain of the incoming interface**].

FDP_IFF.1.3_(NS) The TSF shall enforce the [**none**].

FDP_IFF.1.4_(NS) The TSF shall explicitly authorise an information flow based on the following rules: [

- **a packet filter rule changes the routing domain for the respective IP packet**].

FDP_IFF.1.5_(NS) The TSF shall explicitly deny an information flow based on the following rules: [**incoming and outgoing interface are in different routing domains (unless a pf rule exists).**].

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

FMT_MSA.1.1_(NS-A) The TSF shall enforce the [**NS-SFP**] to restrict the ability to [***modify***] the security attributes [**routing domain and *pf* routing domain changing rules**] to [**the genucenter administrators, the operational administrators, the genucenter root administrators, and the genuscreen administrator**].

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

FMT_MSA.1.1_(NS-R) The TSF shall enforce the [**NS-SFP**] to restrict the ability to [***query***] the security attributes [**routing domain**] 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_(NS) Static attribute initialisation

FMT_MSA.3.1_(NS) The TSF shall enforce the [**NS-SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2_(NS) 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_(NS) Specification of management functions

FMT_SMF.1.1_(NS) The TSF shall be capable of performing the following security management functions: [**changing the routing domain of an 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: encrypt/decrypt 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 [23] and NIST-SP800-38A [24]**].

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 [18] and FIPS-180-4 [27]**].

Application Note: RFC2104 [18] 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: negotiate keys for IPsec usage**].

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 [14]**].

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 [23] and NIST-SP800-38A [24]**].

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 [14] and RFC3526 [17]**].

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 [14] and RFC3526 [17]**].

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 [14]**].

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 [18] and FIPS-180-4 [27]**].

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 [15]**].

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 and SHA-256 [15]**].

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 security 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 security 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: encrypt/decrypt 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 [28] 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 [23] and NIST-SP800-38A [24]**].

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 [20] and [21]**].

Application Note: The cryptographic algorithm elliptic curve ecdh-sha2-brainpoolp256r1 contains both the cryptographic key generation and the cryptographic operation. Therefore the respective 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 [28] with the ETM extension [22]**].

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 [22]**] and cryptographic key sizes [**256 bit**] that meet the following: [**RFC4418 [19] 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 [15]**].

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 and SHA-512 [15]**].

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, the security 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, the security 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 SIP Relay

This section identifies the SFRs associated with the access control by the SIP relay.

6.1.6.1 FDP_IFC.1_(SIP) Complete information flow control

FDP_IFC.1.1_(SIP) The TSF shall enforce the [**SIP-SFP**] on [

- **subjects: users that send and receive information through the TOE to one another;**
- **information: traffic sent through the TOE from one subject to another;**
- **operation: perform access control**]

6.1.6.2 FDP_IFF.1_(SIP) Simple security attributes

FDP_IFF.1.1_(SIP) The TSF shall enforce the [**SIP-SFP**] based on the following types of subject and information security attributes: [

- **IP and TCP header;**
- **SIP protocol and application data**].

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

- **The SIP relay is installed and configured**].

FDP_IFF.1.3_(SIP) The TSF shall enforce the [**none**].

FDP_IFF.1.4_(SIP) The TSF shall explicitly authorise an information flow based on the following rules: [

- **The tests for the configured internal and external domains and RTP port ranges pass.**
- **The ACL and request method checks pass**].

FDP_IFF.1.5_(SIP) The TSF shall explicitly deny an information flow based on the following rules: [

- **The tests for the configured internal and external domains and RTP port ranges fail.**
- **The ACL and request method checks fail**].

6.1.6.3 FMT_MSA.1_(SIP-A) Management of security attributes

FMT_MSA.1.1_(SIP-A) The TSF shall enforce the [**SIP-SFP**] to restrict the ability to [***modify***] the security attributes [**SIP relay configuration**] to [**the genucenter administrators, the operational administrators, the genucenter root administrators, and the genuscreen administrator**].

6.1.6.4 FMT_MSA.1_(SIP-R) Management of security attributes

FMT_MSA.1.1_(SIP-R) The TSF shall enforce the [**SIP-SFP**] to restrict the ability to [***query***] the security attributes [**SIP relay configuration**] to [**the genucenter administrators, the genucenter root administrators, the genuscreen administrator, the genucenter service users, the genucenter revisors, and the genuscreen revisor**].

6.1.6.5 FMT_MSA.3_(SIP) Static attribute initialisation

FMT_MSA.3.1_(SIP) The TSF shall enforce the [**SIP-SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2_(SIP) The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.

6.1.6.6 FMT_SMF.1_(SIP) Specification of management functions

FMT_SMF.1.1_(SIP) The TSF shall be capable of performing the following security management functions: [**installation and configuration of the SIP relay**].

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: perform access control**].

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 operational 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 service 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 operational 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.

Application Note: This SFR does not apply if an external LDAP server is used for administrator and revisor authentication.

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**].

The TSF are allowed to reduce audit data generation on the following conditions: [**the log rate exceeds the threshold: 30000 log messages per second.**]

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 operational 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, operational administrators, security 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 TOE 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 64 bit 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 [$\mathbf{k} > \mathbf{2^{26}}$] strings of bit length 128 are mutually different with probability [$\epsilon < \mathbf{2^{-12}}$].*

*(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 DieHarder1[20] random number test suite**].*

6.2 Security Assurance Requirements

Table 9 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 9: Security Assurance Rationale

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
	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	Developer defined life-cycle model
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

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

Class	Family	Level	Name
	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 10 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_(NS) is met by FDP_IFC.2_(NS), which is hierarchical. The SFR FTP_STM.1 must be met by the environment.

Table 10: SFR dependencies

ID	Users	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
		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)	-	-
NS-SFP			
B01	FDP_IFC.2_(NS)	FDP_IFF.1	B02
B02	FDP_IFF.1_(NS)	FDP_IFC.1	B01 (hierarchical)
		FMT_MSA.3	B04
B03-A	FMT_MSA.1_(NS-A)	FDP_IFC.1	B01 (hierarchical)
		FMT_SMR.1	K03
		FMT_SMF.1	B05
B03-R	FMT_MSA.1_(NS-R)	FDP_IFC.1	B01 (hierarchical)
		FMT_SMR.1	K03
		FMT_SMF.1	B05
B04	FMT_MSA.3_(NS)	FMT_MSA.1	B03-A, B03-R
		FMT_SMR.1	K03
B05	FMT_SMF.1_(NS)	-	-
IPSEC			

ID	Users	Dependency	Solution
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
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

ID	Users	Dependency	Solution
E16	FMT_SMF.1_(IKE)	-	-
SSH-SFP			
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[21]	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)	-	-
SIP-SFP			
G01	FDP_IFC.1_(SIP)	FDP_IFF.1	G02
G02	FDP_IFF.1_(SIP)	FDP_IFC.1	G01
		FMT_MSA.3	G04
G03-A	FMT_MSA.1_(SIP-A)	FDP_IFC.1	G01 (hierarchical)
		FMT_SMR.1	K03

ID	Users	Dependency	Solution
		FMT_SMF.1	G05
G03-R	FMT_MSA.1_(SIP-R)	FDP_IFC.1	G01 (hierarchical)
		FMT_SMR.1	K03
		FMT_SMF.1	G05
G04	FMT_MSA.3_(SIP)	FMT_MSA.1	G03-A, G03-R
		FMT_SMR.1	K03
G05	FMT_SMF.1_(SIP)	-	-
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, 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
General Management Facilities			
K01	FMT_MOF.1_(GEN)	FMT_SMR.1	K03

ID	Users	Dependency	Solution
		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	-	-

[21] **Application Note**: The ID F08 is missing from the table. See rationale for the reason.

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 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 (and the ID F08 is missing in the table).

Table 11 shows how the SFRs can be traced back to the objectives.

Table 11: Objectives

		O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC	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_(NS)		X					
B02	FDP_IFF.1_(NS)		X					

		O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC	O.AVAIL
B03-A	FMT_MSA.1_(NS-A)		X					
B03-R	FMT_MSA.1_(NS-R)		X					
B04	FMT_MSA.3_(NS)		X					
B05	FMT_SMF.1_(NS)		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		
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[22]	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		

		O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC	O.AVAIL
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_IFC.1_(SIP)		X					
G02	FDP_IFF.1_(SIP)		X					
G03-A	FMT_MSA.1_(SIP-A)		X					
G03-R	FMT_MSA.1_(SIP-R)		X					
G04	FMT_MSA.3_(SIP)		X					
G05	FMT_SMF.1_(SIP)		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	
K04	FPT_TEE.1_(GEN)			X	X	X		
K05	FPT_TRC.1_(GEN)							X
L01	FCS_RNG.1			X	X	X		

[22] **Application Note**: The ID F08 is missing from the table.

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

FDP_IFC.1_(SIP), FDP_IFF.1_(SIP), FMT_MSA.1_(SIP-A), FMT_MSA.1_(SIP-R), FMT_MSA.3_(SIP), and FMT_SMF.1_(SIP) handle the SIP-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.

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.

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.

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

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

6.3.7 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 12 lists the SAR dependencies. The table shows that all dependencies are met.

Table 12: 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

ID	Requirement	Dependency	Solution
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
		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

7.1.1.1 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:

- address of source
- address of destination
- transport layer protocol
- interface on which traffic arrives and departs
- IP version (IPv4 or IPv6)
- differentiated services field

7.1.1.2 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.

7.1.1.3 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.

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

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

7.1.2 SF_NS Network Separation

7.1.2.1 SF_NS.1: The firewall components implement the network separation with routing domains. All interfaces that are tagged with the same routing table index are part of the same routing domain. Routes for that routing domain determine how IP packets are forwarded.

7.1.2.2 SF_NS.2: A change in the routing domain for specific IP packets can be achieved by adding explicit *pf* rules.

7.1.2.3 SF_NS.3: Daemons that are configured for network interfaces in routing domains are put into the respective routing domain at boot time and during reconfiguration.

This Security Functions addresses the SFRs FDP_IFC.2_(NS) and FDP_IFF.1_(NS).

7.1.3 SF_IPSEC: IPsec Filtering

7.1.3.1 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_SIP: SIP Relay

7.1.4.1 SF_SIP.1: The SIP relay module can be installed by a genucenter administrator. The software is transferred to all appliances that have the SIP relay configured. This requires a separate relay installation job.

7.1.4.2 SF_SIP.2: The SIP relay performs access control on the following parameters:

- internal and external SIP domain
- RTP port range
- IP ACL
- request method ACL

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

7.1.5 SF_IA: Identification and Authentication

7.1.5.1 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.

7.1.5.2 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.

7.1.5.3 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

7.1.6.1 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.

7.1.6.2 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.

7.1.6.3 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.

7.1.6.4 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.

7.1.6.5 SF_AU.5: The TSF is allowed to drop log messages to maintain a defined behaviour if the log rate is larger than the following threshold: 30000 log messages per second. The number of dropped messages is logged by the genucenter.

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

7.1.7.1 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 [23] and NIST-SP800-38A [24].

Cryptographic key agreement This operation uses the elliptic curve algorithm ecdh-sha2-brainpoolp256r1 with a key size of 256 bit, according to RFC5639 [20] and [21].

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 [19].

Authentication This operation uses RSA signatures with a key size of 2048 bit, according to PKCS#1, v2.1.

7.1.7.2 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

7.1.8.1 SF_ADM.1: The TOE allows the genucenter administrators, the security administrators and the genucenter root administrators to change the IKE/IPsec configuration and the SSH configuration at the management system within their respective domain.

The TOE allows the genucenter administrators, the operational administrators and the genucenter root administrators to change the packet filter configuration, the network separation (routing domain) configuration, and the SIP configuration at the management system within their respective domain.

The TOE allows the genuscreen administrator to change the IKE 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 packet filter configuration, the network separation (routing domain) configuration, and the SIP configuration at the management system within their respective domain.

The TOE allows the genuscreen revisor to view the IKE configuration, the packet filter configuration the network separation (routing domain) configuration, and the SIP configuration 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.

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

The network separation (routing domain) configuration has permissive defaults.

7.1.8.3 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.

7.1.8.4 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.

7.1.8.5 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.

7.1.8.6 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_(NS-A), FMT_MSA.1_(NS-R), FMT_MSA.3_(NS), and FMT_SMF.1_(NS).

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

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

7.1.9.1 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.

7.1.9.2 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.

7.1.9.3 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.

7.1.9.4 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.

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

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

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 ISAKMP 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 OpenBSD application use the `pledge` system call to minimize their usage of system calls.
- The genuscreen appliances implement the secure boot process with UEFI and coreboot.
- The OpenBSD application use LibreSSL instead of OpenSSL.

The measures together build up a multilayered 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 13.

Table 13: 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, RFC2409	Modulus length = 2048	yes
2	Key Agreement	DH with Diffie-Hellman group 14 using HMAC-SHA-256	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 SHA-512	PKCS#1, v2.1, FIPS180-4, RFC4432	Modulus length = 2048	yes
7	Key Agreement	ECDH with SHA-256	RFC5656, FIPS-180-4, FIPS-186-4	Key sizes corresponding to the used elliptic curve brainpoolp256r1	yes
8	Confidentiality	AES in CTR mode	FIPS-197, NIST-SP800-38A, RFC4344	|k| = 128	yes
9	Integrity	UMAC with AES using the ETM extension	RFC4418, FIPS-197	|k| = 256	yes
10	Trusted Channel	SSH v2.0	RFC4253 with the ETM extension		yes

8.1 Conformity to BSI TR-02102

This section describes the conformance of the cryptographic algorithms and parameters with the recommended values from TR-02102.

8.1.1 Conformity to BSI TR-02102-1

The used algorithms and parameters are not completely conformant to TR-02102-1 [3].

1. For RSA signature generation, TR-02102-1 [3] recommends EMSA-PSA (RSASSA-PSS) in section 5.4.1 (see table 5.4).

   The implementation uses EMSA-PKCS1-v-1_5 (RSASSA-PKCS1-v1_5).

8.1.2 Konformität zu BSI TR-02102-2 (TLS)

The used algorithms and parameters are conformant to the recommended values in TR-02102-2 [4].

8.1.3 Conformity to BSI TR-02102-3 (IPsec with IKEv2)

The specified algorithmen are not completely conformant to TR-02102-3 [5].

1. TR-02102-3 [5] recommends usage of IKEv2 for complexity reasons. It does not cover IKEv1.

   The implementation uses IKEv1 for VPN usage.

2. Section 2.1.5 generally recommends Perfect Forward Secrecy (PFS).

   The default configuration for IPsec phase 2 (quick mode) does not enable PFS for performance reasons. However, an administrator can explicitly activate PFS.

8.1.4 Konformität zu BSI TR-02102-4 (SSH)

The specified algorithmen are not completely conformant to TR-02102-4 [6].

1. In section 3.3.1 the guideline recommends a key exchange after one hour or after transfer of one gigabyte, depending on which event occurs first.

   The default configuration changes keys after transfer of four gigabytes. However, an administrator can explicitely configure other parameters.

2. In section 3.5, table 3, the guideline recommends three MAC schemes.

   The implementation uses `umac-128-etm@openssh.com`.

A 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

PFS Perfect Forward Secrecy

PXE Preboot eXecution Environment

RDR Redirect rule

RFC Request for comment

RSA Rivest Shamir Adleman

SA Security Association

SBC Session Border Controller

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

B References

[1] Bundesamt für Sicherheit in der Informationstechnik. Anwendungshinweise und Interpretationen zum Schema (AIS) AIS 20. Anwendungshinweise und Interpretationen zum Schema AIS 20, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, 15 Mai 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.html.

[2] Bundesamt für Sicherheit in der Informationstechnik. Anwendungshinweise und Interpretationen zum Schema (AIS) AIS 31. Anwendungshinweise und Interpretationen zum Schema AIS 31, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, 15 Mai 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.html.

[3] Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie TR-02102-1 – Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Technical report, 2019.

[4] Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie TR-02102-2 – Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS). Technical report, 2019.

[5] Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie TR-02102-3 – Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2). Technical report, 2019.

[6] Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie TR-02102-4 – Kryptographische Verfahren: Verwendung von Secure Shell (SSH). Technical report, 2019.

[7] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1 Revision 5. Technical report, Common Criteria, April 2017. CCMB-2017-04-001.

[8] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1 Revision 5. Technical report, Common Criteria, April 2017. CCMB-2017-04-002.

[9] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1 Revision 5. Technical report, Common Criteria, April 2017. CCMB-2012-04-003.

[10] Common Criteria. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5. Technical report, Common Criteria, April 2017. CCMB-2012-04-004.

[11] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460, Internet Engineering Task Force, December 1998. Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946, 7045, 7112. http://www.ietf.org/rfc/rfc2460.txt.

[12] genua GmbH. genucenter Installations- und Konfigurationshandbuch, Version 7.0, 19. Februar 2020.

[13] genua GmbH. genuscreen Installations- und Konfigurationshandbuch, Version 7.0, 19. Februar 2020.

[14] D. Harkins and D. Carrel. The Internet Key Exchange (IKE). RFC 2409, Internet Engineering Task Force, November 1998. Obsoleted by RFC 4306, updated by RFC 4109. http://www.ietf.org/rfc/rfc2409.txt.

[15] J. Jonsson and B. Kaliski. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. RFC 3447, Internet Engineering Task Force, February 2003. http://www.ietf.org/rfc/rfc3447.txt.

[16] Wolfgang Killmann and Werner Schindler. A proposal for: Functionality classes for random number generators. Anwendungshinweise und Interpretationen zum Schema AIS 20/AIS 31, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, 18 September 2011. Version 2.0. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile.

[17] T. Kivinen and M. Kojo. More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). RFC 3526, Internet Engineering Task Force, May 2003. http://www.ietf.org/rfc/rfc3526.txt.

[18] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, Internet Engineering Task Force, February 1997. Updated by RFC 6151. http://www.ietf.org/rfc/rfc2104.txt.

[19] T. Krovetz. UMAC: Message Authentication Code using Universal Hashing. RFC 4418, Internet Engineering Task Force, March 2006. http://www.ietf.org/rfc/rfc4418.txt.

[20] M. Lochter and J. Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. RFC 5639, Internet Engineering Task Force, March 2010. http://www.ietf.org/rfc/rfc5639.txt.

[21] Manfred Lochter. ECC Brainpool - ECC Brainpool Standard Curves and Curve Generation, Oktober 2005. http://www.ecc-brainpool.org/download/Domain-parameters.pdf.

[22] D. Miller and P. Valchev. The use of UMAC in the SSH Transport Layer Protocol. Internet draft, Network Working Group, September 3 2007. https://tools.ietf.org/html/draft-miller-secsh-umac-01.

[23] NIST. Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards 197, U.S. Department of Commerce / National Institute of Standards and Technology, 26 November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[24] NIST. Recommendation for Block Cipher Modes of Operation – Modes and Techniques. Special Publication 800-38A, U.S. Department of Commerce / National Institute of Standards and Technology, 2001. http://dx.doi.org/10.6028/NIST.SP.800-38A.

[25] NIST. Digital Signature Standard (DSS). Federal Information Processing Standards 186-3, U.S. Department of Commerce / National Institute of Standards and Technology, Juny 2009.

[26] NIST. Digital Signature Standard (DSS). Federal Information Processing Standards 186-4, U.S. Department of Commerce / National Institute of Standards and Technology, July 2013. doi:10.6028/NIST.FIPS.186-4.

[27] NIST. Secure Hash Standard (SHS). Federal Information Processing Standards 180-4, U.S. Department of Commerce / National Institute of Standards and Technology, August 2015. doi:10.6028/NIST.FIPS.180-4.

[28] T. Ylonen and C. Lonvick. The Secure Shell (SSH) Transport Layer Protocol. RFC 4253, Internet Engineering Task Force, January 2006. Updated by RFC 6668. http://www.ietf.org/rfc/rfc4253.txt.