LANCOM
Systems

Security Target
for LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN

Version 1.15
Release

LANCOM Systems GmbH

Adenauer Str. 20/B2
52146 Würselen
Germany

Document History

Date	Version	Editor	Change
01.08.2011	0.1	RBurlaga	Document creation
03.08.2011	0.2	RBurlaga	No Tunnel-in-Tunnel Transport, no RIPv2, no VLAN in TOE
06.09.2011	0.3	TJansen	Rewrote Conformance Claim section, Wrote Security Assurance Requirements section
05.10.2011	0.4	TJansen	Filled out SFRs, Continued after SARs
10.10.2011	- 0.8	TJansen	Internal reviews, amendments & finalization
11.10.2011	0.8.1	CSchalle	Further details added to device overview and supported protocols; RIP propagation added
19.01.2012	0.9	TJansen	Software TOE, hardware cryptography moved to the environment
25.01.2012	0.9.1	TJansen	Added SHA-2 algorithms Added Diffie-Hellman-Groups with larger keys
03.02.2012	1.0	TJansen	Updated list of supported router models. Described how the hardware acceleration engine is used by the TOE. Further clarification of the TOE scope.
27.02.2012	1.1	TJansen	Removed SHA-2 algorithms not supported on all hardware platforms. Further clarification of the cryptographic operations. Updates formal aspects of the SFRs. More verbose explanation of the TOE summary specification.
02.03.2012	1.2	TJansen	Enhanced SFR dependencies.
14.03.2012	1.3	TJansen	Addressed evaluator comments.
21.03.2012	1.4	TJansen	Addressed further evaluator comments.
23.03.2012	1.5	TJansen	Addressed further evaluator comments.
27.03.2012	1.6	TJansen	Addressed further evaluator comments.
13.04.2012	1.7	TJansen	Addressed further comments.
10.05.2012	1.8	TJansen	Addressed consistency problem with ADV_ARC.
21.12.2012	1.9	TJansen	Additional SFRs for Cryptography acc. to BSI-Requirements.
16.01.2013	1.10	TJansen	Addressed further evaluator comments.
15.02.2013	1.11	TJansen	Addressed additional Crypto Kickoff requirements on SFRs, OE.
09.04.2013	1.12	TJansen	Addressed further BSI comments
18.04.2013	1.13	TJansen	Updated TOE identification
22.04.2013	1.14	TJansen	Marked as release version
08.05.2013	1.15	TJansen	Updated CC version

Table of Contents

Terminology

This Security Target refers to the terms and definitions of Section 4 of Part 1 of the CC. Additionally, the following terms and acronyms, most of them specific to LANCOM products, shall be defined

Term	Definition
DH	Diffie-Hellman key exchange
ESP	Encapsulating Security Payload, a packet format defined in RFC 2406. ESP is used by IPsec VPN to encapsulate encrypted traffic.
Internetworking Device	A device connecting two or more networks, usually a router. These devices are not necessarily LANCOM devices. The term 'router' is reserved for devices running the TOE.
LANCOM router	One of the devices (hardware running the TOE), not included in the TOE, like LANCOM VPN routers, central site VPN gateways, 3G/4G routers; in this ST the term 'LANCOM router' always refers to the hardware.
LCOS	LANCOM operating system; the operating system of LANCOM routers in common, within this ST the specific version as defined by TOE Identification in 1.2 TOE Reference is meant.
LCMS	LANCOM management system; a software package run on a standard personal computer with a Microsoft Windows operating system higher than or equal to Windows XP. LCMS is used to configure, monitor and maintain LANCOM devices, such as LANCOM routers. LCMS is not necessarily needed to manage a LANCOM device and out of scope within this ST; it may be used in a trusted environment to prepare configurations or commit changes to configurations, analyze output or obtain new software packages and documentation.
LANCOM AVC	LANCOM Advanced VPN Client; a remote access client (software) that terminates IPsec VPN connections and runs on third party hardware, e. g. a standard personal computer with Microsoft Windows operating system. Though the LANCOM AVC can be used to establish secured VPN connections to LANCOM routers it is not part of the TOE and outside the physical and logical boundaries of the TOE described in this ST; a LANCOM AVC may belong to the IT environment fulfilling the organizational security policies and being managed and maintained in a way that makes it equal to the TOE described with this ST, thus an IPsec connection from the TOE to that LANCOM AVC may be trustworthy.
Protected route	A route to a network that will be protected by an IPsec VPN connection.
Security Association	For each active IPsec VPN connection, the security association holds the state information for that connection, in particular the session keys.
Trusted network	Each network connected to the TOE can be untrusted or trusted: Public networks (e.g., the Internet) are untrusted. Local networks (e.g., networks under the control of the administrator) are trusted. Remote networks connected via IPsec VPN are trusted.
VPN peer	Each IPsec VPN connection is terminated by two hosts, the VPN peers. Since one of the hosts is the TOE itself, the VPN peer refers to the remote host terminating the IPsec VPN connection. The VPN peer may either be another instance of the TOE or another device implementing IPsec VPN.

1. ST Introduction

1.1. ST Reference

Title:	Security Target for LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN
Sponsor:	LANCOM Systems GmbH
Editor(s):	Roland Burlaga, LANCOM Systems GmbH
	Thomas Jansen, LANCOM Systems GmbH
Version Number:	1.15
Date:	08-May-2013
CC Version:	Version 3.1, Revision 4
Assurance Level:	EAL4+, that is here EAL4 augmented with ALC_FLR.1
Certification-ID:	BSI-DSZ-CC-0815
Keywords:	VPN, IPsec

1.2. TOE Reference

TOE Identification: LANCOM Operating System LCOS 8.70 CC

Router Model	Firmware
1781-4G (CC)	LC-1781-4G-8.70.0095-Rel.upx SHA-256: 95d8eed735be352de69366c688802eea33e576369b0a96bf9549b877b03c3d3e
1781A-3G (CC)	LC-1781A-3G-8.70.0095-Rel.upx SHA-256: d73a6536a07a0a504741443788adb7ddfbf91ae0aa1118bcc261e82961f86258
1781A-4G (CC)	LC-1781A-4G-8.70.0096-Rel.upx SHA-256: e27be5f81261b0ac8b58d23aee65e33b6e9cf8a94361ffc7995164a0f1dc5c72
1781A (CC)	LC-1781A-8.70.0095-Rel.upx SHA-256: 5cc9c34a058336e60bb91d77b0503e558b6d1dbdbc66921aa47146607f1eab39
1781EF (CC)	LC-1781EF-8.70.0095-Rel.upx SHA-256: 888075304feb3d29b284bb9e35ba31efabfa730833a57284ffd6cd41d421da90
7100+ VPN (CC)	LC-7100plus-8.70.0095-Rel.upx SHA-256: dbfd7c4c7045aaa14e572dfb500d19aa1aac67793435612ad59c662c702b1ce5
9100+ VPN (CC)	LC-9100plus-8.70.0095-Rel.upx SHA-256: dcb20236335a789abbacef93203f9244568a7c7ab002c6c0e7e8ebf47cf80ff5
	Documentation
	LCOS 8.70 – Preparative Procedures.pdf SHA-256: 1b82f43ad013ee1475479ae74db9cb6a14f72f19dfb2cfd3f998b603096bd5fa
	LCOS 8.70 – Operational User Guidance.pdf SHA-256: 96de218b8f3f09535e9cfecd109b41e3634cf7b57358a8cc4f27387eb9320a99

Further Reading
LCOS-REFMANUAL-800-EN.pdf – LCOS Reference Manual Version 8.00
LCOS-MENU-860-EN.pdf – LCOS Menu Reference Version 8.60

1.3. TOE Summary

The TOE consists of software used to construct virtual private networks (VPNs) between networks or a remote access client. The TOE is the operating system LCOS (software) for the LANCOM routers. The TOE provides all functions to manage a secure IPsec connection. Thus temporary or mobile sites of a company, home offices, branch offices or co-locations of an enterprise or public entity can be connected to each other or to a central site at the headquarters safely by the use of the TOE at each location. Also, the TOE can manage IPsec connections from mobile users facilitating LANCOM AVC software on their mobile devices. The LANCOM AVC is considered part of the IT environment.

The TOE also includes the two guidance documents: the preparative procedures and the operational guidance. The TOE must be operated in compliance with both guidance documents.

IPsec provides confidentiality, authenticity and integrity for IP data transmitted between trusted (private) networks or remote clients over untrusted (public) links or networks. The TOE uses a cryptographic acceleration engine in the hardware, which is not part of the TOE, to implement parts of IPsec.

The TOE implements the following security functions: IPsec, packet filtering, configuration management and key management.

1.4. TOE Description

This section provides context for the TOE evaluation by identifying the product type and describing the product and evaluated configuration.

1.4.1. Product Type

LCOS in a version as defined by 1.2 TOE Reference, TOE Identification is a software TOE which combines network data routing, virtual private network (VPN) connection and acceleration, and packet filtering. This product type makes use of public telecommunication infrastructure (most commonly the Internet) or untrusted network links in order to connect physically separate private or trusted network segments at different locations to one ‘virtually contiguous’ private network or trusted network. Also, LANCOM routers running the TOE can terminate VPN connections from remote VPN peers using LANCOM AVC on standard personal computers or mobile computers and thus make them appear as terminal devices in a local private or trusted network. The LANCOM AVC is considered part of the IT environment.

Privacy and security of corporate data transmitted from one location to the other is maintained through the use of the encrypted tunneling protocol IPsec for VPN connections that transit untrusted networks (e. g. the Internet) and the firewall (packet filter) that separates untrusted (e. g. the Internet) from trusted networks (e. g. the LAN).

1.4.2. Product Description

All LANCOM routers execute the same operating system LCOS (LANCOM Operating System) providing all functions for router operation, IPsec, packet filtering, configuration management and key management. For the TOE the version defined by 1.2 TOE Reference, TOE Identification is mandatory.

To configure a VPN in the TOE, a VPN connection to a remote site must be defined. The routing engine works with remote site definitions, which inherently define next router address and the possible interfaces which have a path to the next router. If a remote site is one defined by a VPN connection and a packet shall be routed to that site, the packet will be checked to conform to the source and

destination network definitions of the IPsec SA. If it conforms to the SA, it will be sent to the hardware for encryption due to the IPsec SA's encryption parameters and the result will then be forwarded by the TOE to the interface with a path to the destination address of the remote site. There it will be sent out as an IPsec encrypted packet.

1.4.3. Physical Scope and Boundary

The TOE includes only the operating system, not the hardware on which the operating system is executed. In particular, the cryptographic acceleration engine in the CPU is not part of the TOE.

The TOE manages the hardware it is running on, in particular the various network interfaces available, and uses them to distinguish untrusted networks and trusted networks. When the TOE is in use, at least one of the network interfaces of the internetworking device will be attached to a trusted network, and at least one other interface will be attached to an untrusted network. The decision which network is trusted and which is untrusted is made by the administrator. The TOE configuration will determine how IP packets received on one interface will be transmitted on another. IP packets that are protected by the IPsec security function of the TOE are received on a trusted network interface and encrypted using IPsec before being sent out an untrusted interface.

1.4.4. Logical Scope and Boundary

TOE software

As defined the TOE consists of a LANCOM router specified under 1.4.3 and the TOE software specified by 1.2 TOE Reference, TOE Identification. The TOE software is a special version of the LANCOM operating system LCOS with the following security relevant features included in the evaluated configuration:

- Firewall
- Internet Key Exchange (IKE) for IPsec (the payload encryption is done by the hardware engine not belonging to the TOE)
- SSH v2 (server), including SCP
- VPN
- RIPv2 (route propagation)
- Syslog (internal logging)
- support for ADSL/VDSL modem (availability depends on the hardware model)
- support for 3G/4G modem (availability depends on the hardware model)

The following features are explicitly excluded from the evaluated configuration and must be disabled in the configuration:

- IEEE 802.11 standards/Wireless LAN
- ISDN
- LANCAPI
- external USB interfaces
- COM port server
- SIP, SIP ALG
- Content Filter option
- HTTP
- HTTPS
- IPsec-over-HTTPS
- DES, 3DES
- Dynamic VPN
- OCSP
- SCEP
- RIPv2 (route learning)
- TFTP
- SNMP
- Syslog (external logging)
- Telnet

The TOE supports the PPP protocol to establish a connection to an Internet provider via, e.g., DSL. The PPP protocol is not used to provide additional security and, therefore, is not within the scope of the security evaluation. Similarly, the TOE supports the use of VLAN-Tags for Ethernet network interfaces. The use of VLAN-Tags is not used to provide additional security and, therefore, is not within the scope of the security evaluation. The evaluated configuration only supports IPv4, not IPv6. The firmware update mechanism depends on the bootloader, which is outside the TOE scope as defined in section 1.5.

IPsec

IPsec is an Internet standard developed by the IETF and described in RFCs 2401-2404, 2406-2409 and 2451. It provides network data encryption at the IP packet level to guarantee the confidentiality, authenticity and integrity of IP packets. IPsec only supports IP packets - other network protocols must be encapsulated within IP to be encrypted with IPsec. Individual IP packets encrypted with IPsec can be detected during transmission, but the IP packet contents (payload) cannot be read. IPsec encrypted packets are forwarded through an IP network in exactly the same manner as normal IP packets, allowing IPsec encrypted packets to be transported across networks and internetworking devices that do not participate in IPsec. The actual encryption and decryption of IP packets therefore occurs only at devices that are capable of and configured for, IPsec. When an IP packet is transmitted or received by an IPsec-enabled device, it is encrypted or decrypted only if the packet meets criteria defined by the administrator. These criteria are typically described in the form of IPsec connection profiles. Internetworking devices such as routers are used to connect networks together to form larger networks. They are therefore logical places in which to implement IPsec to provide confidentiality, authenticity and integrity for IP packets passing from one network to another.

The TOE supports the following IPsec options, partly by using the cryptographic acceleration engine:

Function	Operation
Authentication between TOE and VPN Peer	IPsec Internet Key Exchange (IKE) with ■ Pre-Shared Keys, or ■ Digital Certificates
Confidentiality of Packets	IPsec Encapsulating Security Payload (ESP) with AES using IPsec Tunnel Mode (provided by the hardware, which is not part of the TOE)
Integrity and Authenticity of Packets	IPsec Encapsulating Security Payload (ESP) with HMAC Keyed Hash Algorithm, using SHA-1 or SHA-256 in IPsec Tunnel Mode (provided by the hardware, which is not part of the TOE)

Firewalling (Packet Filtering)

TOE internetworking devices are deployed at the edges of untrusted networks (such as the Internet) to provide controlled communications between two networks that are physically separated. When an IP packet reaches the TOE packet filtering mechanisms are applied to the traffic before forwarding it into the remote network. Packets arriving at a network interface of the TOE are checked to ensure that they conform to the configured firewall rules, this may include checking attributes such as the presumed source or destination IP address, the protocol used, the network interface the IP packet was received on, and source or destination UDP/TCP port numbers. Packets not matching the configured packet filter rules are dropped.

Configuration Management

Configuration, management and operation are performed directly from the command line interface of LCOS within the TOE, either by direct connection to the serial interface of the LANCOM router and a terminal emulator, or by remote connection with SSH. To ensure that only the authorized administrator can gain secure access to the TOE over a network, the security target specifies that remote management be conducted using SSH. Initial configuration of the TOE is performed via serial interface.

The command line interface also allows querying the device status and retrieving diagnostic information. External monitoring of the TOE via SNMP is not supported in the evaluated configuration.

Key Management

The key management for IPsec connections is part of the IPsec implementation (IKE) of the TOE offering authentication based on pre-shared keys or digital certificates. The TOE provides a secure digital certificate storage within its non-volatile memory. Imported certificates cannot be read out without physical access to the memory logic since there are no commands at the LCOS command line interface or procedures for management protocols allowing to copy or show imported certificate's private key portions.

If certificates are used to authenticate VPN peers, the administrator is responsible for manually uploading the certificates to the TOE via SSH. Automatic certificate generation and distribution via SCEP is not supported in the evaluated configuration.

1.5. Description of the non-TOE Hardware and Software

The TOE requires the appropriate hardware to operate on, i.e. a LANCOM router. The router hardware is outside the scope of the TOE. The LANCOM router hardware is a standalone, self-supporting device with its own power supply, a chassis enclosing a main board with central processing unit, memory and different physical interfaces to interconnect networks depending on the model. The different models of LANCOM router hardware that can be operated by the software covered by the TOE have these characteristics in common:

- Central processing unit (CPU) that supports all software operations of LCOS
- Security engine as hardware part of the CPU that accelerates cryptographic operations, such as AES, SHA-1, SHA-256
- Real-time clock to provide for accuracy of timestamps and certificate validation
- Dynamic memory (DRAM) used by the CPU for operations and non-persistent data
- Non-volatile memory (Flash) to store the operating system and the configuration data
- A serial communication port to configure and manage the device over a physical connection
- At least two or more Ethernet network interfaces to connect to different network segments

Depending on the specific model, some LANCOM routers do also have an integrated modem for ADSL, VDSL, 3G or 4G mobile networks. Additionally, the routers may have ISDN, external USB interfaces and/or wireless LAN adapters which must be deactivated in the evaluated configuration.

The cryptographic acceleration engine is used by the TOE as part of the environment to perform the encryption and decryption (AES) and for the calculation of cryptographic hashes (SHA-1 and SHA-256) of the IPsec ESP packets only. The cryptographic acceleration engine is integrated into the CPU. The manufacturer of the CPU claims to have performed thorough tests on the implementation of these algorithms showing for example their time invariance. Since the hardware is not within the scope of the TOE, these claims are not subject to this evaluation.

Series	Model	HW platform	WAN	LAN	Device Category
178x	1781-4G (CC)	A	4G	4-Port Switch	VPN Business Router
	1781A (CC)	A	ADSL	4-Port Switch	
	1781A-3G (CC)	A	ADSL, 3G	4-Port Switch	
	1781A-4G (CC)	A	ADSL, 4G	4-Port Switch	
	1781EF (CC)	A	Ethernet, SFP	4-Port Switch	
x100	7100+ VPN (CC)	B	Ethernet	Ethernet	Large VPN Concentrator
	9100+ VPN (CC)	C	Ethernet	Ethernet	

The CPU families used in the hardware required to run the TOE support additional microcode packages for an optional coprocessor. The specific processor models used in the hardware required to run the TOE do not include this coprocessor. Thus, the microcode packages are not used by the TOE.

2. Conformance Claims

2.1. CC Conformance Claim

This Security Target and the TOE claim conformance to part 2 and part 3 of CC version 3.1:

- CC part 2 extended,
- CC part 3 conformant.

Note: This ST conforms to part 2 extended, because it uses the component FCS_RNG.1. Since this component and its family FCS_RNG are defined in a publically available scheme document (see the application note in the corresponding section in chapter 5.1), no chapter for extended components definition was included in this document. All necessary information for the definition is available in the reference document.

2.2. PP Claim

This Security Target does not claim conformance to a Protection Profile.

2.3. Package Claim

This Security Target claims conformance to EAL4 augmented with ALC_FLR.1.

2.4. Conformance Rationale

As this Security Target does not claim conformance to a Protection Profile a conformance claim rationale is not necessary.

3. Security Problem Definition

3.1. Assets

The assets that should be protected are the TOE configuration, the IP packets transmitted/received over an untrusted network, and the IT resources of the trusted network.

3.2. Threats

The threat agents against the TOE are attackers with expertise, resources, and motivation that combine to be an enhanced-basic attack potential.

3.2.1. Threats Addressed by the TOE

The TOE addresses the following threats:

Name	Description
T.Attack	An attacker may gain access to the TOE and compromise its security functions by altering its configuration.
T.Untrusted-Path	An attacker may attempt to disclose, modify or insert data within IP packets transmitted/received by the TOE over an untrusted network. An attacker may attempt to replay ESP packets transmitted to the TOE over an untrusted network. If such an attack was successful, then the confidentiality, integrity and authenticity of IP packets transmitted/received over an untrusted path would be compromised.
T.Mediate	An attacker may send IP packets through the TOE which do not conform to the rules of the TOE and can then access resources on the trusted network.

3.3. Organisational Security Policies

The following table describes the organizational security policies relevant to the operation of the TOE.

Name	Description
P.Connectivity	The organizational security policy will a) Specify whether networks connected to the TOE are trusted or untrusted (including subnets), b) Define which IP packets are to be protected by the TOE, and c) Associate each protected route for IP packets with a VPN peer that will decrypt/encrypt the IP packets. d) Specify that no unintended bridges between the trusted and untrusted network may exist.

The organizational security policy, P.Connectivity, is required because it determines how IP packets between trusted networks can be transmitted over an untrusted network. Each instance of the TOE

implements a portion of P.Connectivity, which must be matched to, and consistent with, other VPN peers for the TOE security functions to be effective.

3.4. Assumptions

The following assumptions are made in relation to the TOE:

Name	Description
A.NoEvil	As the security functions of the TOE can be compromised by an authorized administrator, administrators are assumed to be non-evil and can be trusted to perform their duties correctly.
A.PhySec	As the security functions of the TOE can be compromised by an attacker with physical access to the internetworking device containing the TOE, it is assumed that the internetworking device containing the TOE is located in a physically secure environment.
A.Training	As the security functions of the TOE can be compromised due to errors or omissions in the administration of the security features of the TOE, it is assumed that administrators of the TOE have been trained to enable them to securely configure the TOE.
A.Keys	Pre-shared keys, IKE certificates, and SSH host keys are assumed to be securely generated and communicated between disparate administrators.
A.Trusted-Remote	Remote administration is assumed to be only initiated from a management station connected to a trusted network (either locally or via VPN).
A.Hardware	The TOE is assumed to run on a LANCOM router of a model listed in section 1.5. In particular it is assumed that the following functionality is available to the TOE: a) cryptographic acceleration engine supporting AES, SHA-1, and SHA-256. Keys must be securely deleted by the cryptographic acceleration engine when they are no longer used. b) hardware real time clock c) a trustworthy bootloader including an software update mechanism

4. Security Objectives

The security objectives are a high-level statement of the intended response to the security problem. These objectives indicate how the security problem, as characterized in the “TOE Security Environment” section, is to be addressed.

4.1. Security Objectives for the TOE

The following security objectives are defined for the TOE:

Name	Description
O.Cryptography	The TOE must implement the cryptographic algorithms for session establishment of the Internet Key Exchange (IKE). The TOE must implement the cryptographic algorithms for session establishment and payload processing for remote administration. The TOE must implement a random number generator.
O.ESP	The TOE must support the use of a hardware cryptography engine for Encapsulating Security Payload to protect confidentiality, authenticity, and integrity using the hardware cryptography engine.
O.Key-Confidentiality	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt IP packets between instances of the TOE and when kept in short and long-term storage.
O.Mediate	All IP packets sent through the TOE from an untrusted network must be mediated by the TOE.
O.NoReplay	The TOE must provide a means to detect that an ESP packet transmitted to the TOE has not been copied by an eavesdropper and retransmitted to the TOE.
O.Secure-Operation	The TOE must prevent unauthorized changes to its configuration and provide audit capabilities.

4.2. Security Objectives for the Operational Environment

Name	Description
OE.Policy	Those responsible for the administration of the TOE must provide a policy that specifies a) Whether networks connected to the TOE are trusted or untrusted b) The IP packets that are to be protected by the TOE, and c) The VPN peer that will encrypt/decrypt each IP packet for a route. Traffic gathered through a VPN peer and sent encrypted to the TOE over an untrusted network is trusted. d) That no unintended bridges between the trusted and untrusted networks may exist.
OE.Secure-Management	Those responsible for the operation of the TOE must ensure that the TOE environment is physically secure, and management and configuration of the security functions of the TOE are: a) Initiated via the serial interface or from a management station connected to a trusted network (either locally or via VPN) and protected using the security functions of the TOE b) Undertaken by non-evil administrators trained in the secure operation of the TOE c) Pre-shared Keys, IKE certificates, and SSH host keys are securely generated and distributed amongst disparate administrators. d) The administrator must set the real time clock. e) During installation of the TOE the administrator needs to provide a seed for the random number generator of the TOE.
OE.VPN	The VPN external IT entity must be able to encrypt data transmitted to the TOE and decrypt data received from the TOE in accordance with the negotiated IKE/IPsec policy for the established VPN tunnel.
OE.Hardware	The TOE is assumed to run on a LANCOM router of a model listed in section 1.5. In particular it is assumed that the following functionality is available to the TOE: a) cryptographic acceleration engine supporting AES, SHA-1, and SHA-256. Keys must be securely deleted by the cryptographic acceleration engine when they are no longer used. b) hardware real time clock c) a trustworthy bootloader including an software update mechanism

4.3. Security Objective Rationale

The following table lists all objectives for the TOE and the Operational Environment to show which objectives are necessary to counter a threat, meet a policy or satisfy an assumption. The table also shows that no objective exists which does not trace back to a threat, policy, or assumption.

Objective / Threat, Policy, Assumption	O.Cryptography	O.ESP	O.Key-Confidentiality	O.Mediate	O.NoReplay	O.Secure-Operation	OE.Policy	OE.Secure-Management	OE.VPN	OE.Hardware
T.Attack						X		X		
T.Untrusted-Path	X	X	X		X			X	X	X
T.Mediate				X						
P.Connectivity							X			
A.NoEvil								X		
A.PhySec								X		
A.Training								X		
A.Keys								X		
A.Trusted-Remote							X	X		
A.Hardware										X

The following table shows why the chosen objectives are sufficient to counter a threat, meet a policy, or satisfy an assumption.

Threat, Policy, Assumption	Objectives
T.Attack	O.Secure-Operation requires that the configuration can only be modified by the administrator. O.Secure-Operation ensures that audit capabilities are available to detect attacks. OE.Secure-Management requires that the administrators are non-evil. OE.Secure-Management also requires the real time clock to be set by the administrator to ensure that audit information generated has correct time stamps.
T.Untrusted-Path	O.Cryptography ensures that IKE session establishment and remote administration is performed in cryptographically secure way. This ensures that attackers cannot bypass TSF using session establishment and remote administration. O.ESP ensures that IP packets received from trusted sources are authentic, provides integrity protection for transmitted IP packets and protects confidentiality of IP packets during transmission.

Threat, Policy, Assumption	Objectives
	O.Key-Confidentiality ensures that keys used to encrypt or decrypt IP packets cannot be captured. O.NoReplay ensures that an IP packet has not been captured and replayed by an eavesdropper. OE.VPN requires that the VPN peer protects the confidentiality and integrity of the IP packets by implementing the negotiated IPsec policy. OE.Hardware requires that the hardware supports cryptographic operations used by O.ESP. The externally generated seed provided by OE.Secure_Management facilitates creation of strong nonces and session keys.
T.Mediate	O.Mediate requires that all IP packets must be mediated by the TOE before allowing IP packets to pass through the TOE.
A.NoEvil	OE.Secure-Management requires that management and configuration of the TOE is undertaken by non-evil administrators trained in the secure operation of the TOE.
P.Connectivity	OE.Policy implements P.Connectivity directly.
A.PhySec	OE.Secure-Management requires the TOE to be placed in a physically secure location.
A.Training	OE.Secure-Management requires that the administrators are trained in the secure operation of the TOE.
A.Keys	OE.Secure-Management requires that pre-shared keys, IKE certificates, and SSH host keys are securely generated and distributed among administrators.
A.Trusted-Remote	OE.Policy defines which networks are trusted networks and which networks are connected via VPN. OE.Secure-Management states that remote configuration and management of the TOE is undertaken from a management station connected to a trusted network and protected by the security functions of the TOE.
A.Hardware	OE.Hardware implements A.Hardware directly.

5. Security Requirements

Although this ST claims to be CC Part 2 extended, no extended Security Functional Requirements are defined in this document, see section 2.1 for a rationale. No extended Security Assurance Requirements are defined and used, as this ST claims to be CC Part 3 conformant.

The notation, formatting and conventions used in this section are consistent with those used in Version 3.1 of the Common Criteria (CC). The CC allows several operations to be performed on functional requirements; refinement, selection, assignment and iteration are defined in Section 8.1 of Part 1 of the CC:

- Refinements are indicated by **bold** text and ~~strikethrough~~
- Selections are enclosed in [square brackets]
- Assignments are enclosed in [square brackets and underlined]
- Iterations are numbered in sequence as appropriate

The following SFPs are used in the SFRs:

Certificate and cryptographic key access control SFP

The SFP regulates the upload of IKE certificates and SSH host keys to the TOE. The upload of certificates for IPsec and cryptographic keys for SSH authentication is performed by the administrator. Thus, the subject for this SFP is the administrator. The objects are the certificates and cryptographic keys that are uploaded to the TOE. The upload causes the TOE to store the objects for further reference.

Subject	Administrator
Object	Certificates and cryptographic keys
Operation	store

The cryptographic keys used by SSH refer to the SSH server private key.

Subject Security Attributes	password
Information Security Attributes	None

An administrator can store certificates and cryptographic keys on the TOE after successfully authenticating with his password. Therefore, the following rule is enforced by the certificate and cryptographic key access control SFP to determine if the upload is allowed:

- The password provided during the upload must match the stored password for the administrator.

IPsec information flow control SFP

The IPsec information flow control SFP regulates the behavior of the IPsec subsystem. Subjects in this SFP are IP network devices, i.e. all devices capable sending and receiving IP packets. The IP packets are the objects exchanged between two IP network devices. Depending on the direction of the IP packet traversing the TOE, the IP packet must be encrypted if they are sent via a VPN tunnel, decrypted if they are received from a VPN tunnel or ignored by IPsec subsystem if they are not related to a VPN tunnel.

Subject	IP network devices
Information	IP packets

Operations	Encrypt, decrypt, ignore

The administrator can configure the SFP by adding an entry to the routing table pointing to a VPN peer. The individual options for the IPsec security association are configured in the VPN configuration attributes used by the VPN peer. If the route for an IP packet does not point to a VPN peer, the operation ignore is used to indicate that the IPsec information flow control SFP is not applied to this IP packet.

Subject Security Attributes	Type of network the IP network device is connected to: trusted or untrusted
Information Security Attributes	IPsec security association

The IPsec security association is defined through the source and destination IP address of the IP packets for packets that are not encrypted. For encrypted packets, the IPsec security association is defined by the source and destination IP address of the IP packets along with the security policy index field of the ESP header of the encrypted packet.

The following rules are enforced by the IPsec information flow control SFP:

- Incoming ESP-encapsulated IP packets shall be decrypted and processed according to RFC 2406, section 3.4 using the cryptographic acceleration engine with the keys stored in the IPsec security association.
- Outgoing IP packets that must be ESP-encapsulated according to the IPsec security association shall be encrypted and processed according to RFC 2406, section 3.3 using the cryptographic acceleration engine with the keys stored in the IPsec security association and then forwarded to the VPN peer's destination address.
- Incoming unencrypted IP packets shall only be accepted from IP network devices on the trusted network.
- IP packets that have been decrypted shall be forwarded unencrypted only to IP network devices on a trusted network.
- IP packets that are not routed to a VPN peer shall be ignored by the IPsec information flow control SFP.

Packet filter information flow control SFP

The packet filter information flow control SFP regulates the behavior of the packet filter subsystem. Subjects in this SFP are IP network devices, i.e. all devices capable of sending and receiving IP packets. The IP packets are the objects exchanged between two IP network devices. The IP packets can either be permitted or denied.

Subject	IP network devices
Information	IP packets
Operations	Accept, drop, reject

The following security attributes are used in the firewall rules:

Subject Security Attributes	Type of network the IP network device is connected to: trusted or untrusted
Information Security Attributes	IP header fields: source and destination IP address, protocol UDP and TCP header fields: source and destination port

The administrator can configure the SFP by modifying the firewall rules list. The firewall rules depend on the definitions made by the administrator in the actions table and the objects table. The packet filter

information flow control SFP applies to all packets that are routed by the TOE, not those packets addressed to the TOE itself.

Packets reaching the TOE from a trusted or untrusted network are checked against the firewall rules. The TOE generates an ordered list from the firewall rules. The first matching firewall rule according to this list is used to reach the decision. The verdict of a firewall rule can be

- Accept: The packet is forwarded to its destination by the router.
- Drop: The packet is discarded by the router.
- Reject: The packet is discarded by the router. Additionally, an ICMP error message is sent to the source IP address of the IP packet.

The following rules are used to explicitly deny an information flow:

- IP packets arriving on untrusted networks having a source IP address belonging to a trusted network shall be dropped.
- IP packets arriving on trusted networks having a source IP address belonging to a untrusted network shall be dropped.
- IP packets arriving on trusted or untrusted networks having a loopback source IP address shall be dropped.

Access control lists for SSH

The access control lists for SSH are used to restrict the establishment of a remote configuration connection via SSH. The access control list is applied only when a new remote configuration connection is established, not for each packet of an already established connection.

Two types of restrictions can be applied:

- The source IP address of an IP packet that tries to establish a new remote configuration connection must be from an IP network in the access control list. If the list is empty, any source IP address is accepted.
- The establishment of a new remote configuration connection can be restricted to hosts on local trusted networks, trusted networks connected via VPN, or untrusted networks.

Order of IPsec, packet filtering and access control lists for SSH

The IPsec information flow control SFP and the packet filter information flow control SFP both deal with IP packets. This section clarifies the order in which both SFPs are applied. The order depends on the direction in which the packet is sent. The packet filter information flow control is only applied to packets that are not addressed to the TOE itself but that are routed by the TOE.

In particular this implies that ESP encrypted packets are not subject to the packet filter, since these packets are addressed to the TOE itself. Incoming ESP packets are thus first decrypted by the IPsec and then routed towards the inner IP header's destination. At this point, the decrypted packet is subject to the packet filter.

For outgoing encrypted ESP packets, the order is reversed. The packet that will later on be encrypted arrives at the TOE with a destination address which is not an address of the TOE itself. Therefore, it is first subject to the packet filter. The IPsec then determines whether the packet must be encrypted or not.

IP packets addressed to the TOE that try to establish a remote configuration connection via SSH are not subject to packet filtering, since they are addressed to the TOE. They are not subject to IPsec since they are addressed to the TOE and the check if the packet is addressed to the TOE is performed before IPsec is processed.

5.1. Security Functional Requirements

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions

b) All auditable events for the [not specified][1] level of audit; and

c) [the events in the following table

Auditable Event
Start-up and shutdown of audit functions
Modification to the TSF data
Reading of information from the audit records
All modifications to the audit configuration that occur while the audit collection functions are operating
All use of the user identification and authentication mechanism
Modifications to the role allocation of users
User creation
All modifications in the behaviour of the functions of the TSF

][2]

FAU_GEN.1.2 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), 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, [none][3].

FAU_SAR.1 Security audit review

FAU_SAR.1.1 The TSF shall provide [administrators][4] with the capability to read [all audit trail data][5] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FCS_CKM.1 Cryptographic key generation - IKE

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [IKE Session Key Generation][6] and specified cryptographic key sizes [DH: 2048; AES: 128, 192, and 256; HMAC: 160, 256][7] that meet the following: [IPsec IKE v1 that meets the following standards:

[1] [selection, choose one of: *minimum, basic, detailed, not specified*]
[2] [assignment: *other specifically defined auditable events*]
[3] [assignment: *other audit relevant information*]
[4] [assignment: *authorised users*]
[5] [assignment: *list of audit information*]
[6] [assignment: *cryptographic key generation algorithm*]
[7] [assignment: *cryptographic key sizes]*

RFC 2409 sections 5.1 (Phase 1 - Authenticated With Signatures), 5.4 (Phase 1 - Authenticated With a Pre-Shared Key), 5.5 (Phase 2 - Quick Mode), and 5.7 (ISAKMP Informational Exchanges); Diffie-Hellman group 14 from RFC 3526; HMAC-SHA1 from RFC 2104; HMAC-SHA-256 from RFC 4868][8].

Application Note: This SFR focuses on key generation in IKE phase 1 and 2, which protects confidentiality, authenticity, and integrity of ESP data.

- The ISAKMP informational exchange (RFC 2409, sec 5.7) manages security associations, e.g. renewal of ESP session key.
- Key derivation (RFC 2409, section 5 and appendix B) relies on HMAC-SHA-1 and HMAC-SHA-256.

FCS_CKM.2(1) Cryptographic key distribution - IKE

FCS_CKM.2(1).1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [IKE Key Exchange][9] that meets the following: [IPsec IKE v1 that meets the following standard: RFC 2409 sections 5.1 (Phase 1 - Authenticated With Signatures) using RSA keys of 2048 bits length, 5.4 (Phase 1 - Authenticated With a Pre-Shared Key), 5.5 (Phase 2 - Quick Mode), and 5.7 (ISAKMP Informational Exchanges); Diffie-Hellman group 14 from RFC 3526; aes128-CBC, aes192-CBC, aes256-CBC from RFC 3602 and NIST 800-38A, sec. 6.2; HMAC-SHA1 from RFC 2104; HMAC-SHA-256 from RFC 4868] [10].

Application Note: In detail the TSF implements the following algorithms and functions:

- The TOE authenticates either using RSA signatures (RFC 2409, sec 5.1) or pre-shared keys (RFC 2409, sec 5.4). The TOE itself does not support RSA key generation. Authenticated RSA keys are imported via the remote administration interface.
- Encryption and decryption in accordance to AES-CBC meeting NIST 800-38A, sec. 6.2 and cryptographic key sizes 128, 192, and 256 bit meeting FIPS 197, section 6.1 and 6.2
- Digital signing and signature verification in accordance to HMAC-SHA-1-96 and cryptographic key sizes 160 bit meeting FIPS 198a, section 5. The 160 bit digests are truncated to 96 bit to conform to RFC 2404 in accordance with FIPS 198a appendix B.
- Digital signing and signature verification in accordance to HMAC-SHA-256-128 and cryptographic key sizes 256 bit meeting FIPS 198a, section 5. The 256 bit digests are truncated to 128 bit to conform to RFC 4868 in accordance with FIPS 198a appendix B.
- The TSF shall perform digital signing and signature verification in accordance to RSA and cryptographic key sizes 2048 bit meeting RFC 2313.
- The random number generator shall be used to generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Diffie-Hellman key agreement and specified cryptographic key sizes 2048 bit that meet the following: RFC 2631 and 3526.

FCS_CKM.2(2) Cryptographic key distribution - SSH

FCS_CKM.2(2).1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [Diffie-Hellmann for SSH Key Exchange][11] that meets the following: [SSH protocol according to RFC 4251 (sections 4.1 and

[8] [assignment: *list of standards*]
[9] [assignment: *cryptographic key distribution algorithm*]
[10] [assignment: *list of standards*]
[11] [assignment: *cryptographic key distribution algorithm*]

9.4.6) and RFC 4253 (ssh-rsa from section 6.6; section 8 and diffie-hellman-group14-sha1 from section 8.2)][12].

Application Note: In detail the TSF implements the following algorithms and functions:

- The TOE authenticates itself using a SSH host key. The TOE itself does not support RSA key generation. The SSH host key is imported via the remote administration interface.
- The TSF shall perform digital signing and signature verification in accordance to RSA and cryptographic key sizes 2048 bit meeting RFC 3447.
- The random number generator creates ephemeral keys that shall be used to generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Diffie-Hellman key agreement and specified cryptographic key sizes 2048 bit that meet the following: RFC 2631 and 3526.
- Key derivation (RFC 4253, section 7.2) relies on SHA-1.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite with zeroes][13] that meets the following: [none][14].

FCS_COP.1 Cryptographic operation - SSH

FCS_COP.1.1 The TSF shall perform [SSH protection][15] in accordance with a specified cryptographic algorithm [SSH protocol][16] and cryptographic key sizes [AES: 128, 192, and 256; HMAC: 160][17] that meet the following: [SSH protocol according to RFC 4251, 4252 (section 8, Password Authentication Method), RFC 4253: aes128-cbc, aes192-cbc, aes256-cbc from section 6.3; hmac-sha1 and hmac-sha1-96 from section 6.4] [18].

Application Note: In detail the TSF implements the following algorithms and functions for this SFR:

- Encryption and decryption in accordance to AES-CBC and cryptographic key sizes 128, 192, and 256 bit meeting FIPS 197, section 6.1 and 6.2
- Digital signing and signature verification in accordance to hmac-sha1 and hmac-sha1-96 and cryptographic key sizes 160 bit meeting FIPS 198a, section 5. The 160 bit digests are truncated to 96 bit in case of hmac-sha1-96 to conform to RFC 4253, section 6.4 in accordance with FIPS 198a appendix B. Note that SHA-2 is not used here for conformance with RFC 4253.
- The TOE enforces usage of 'no compression' (RFC 4253, section 6.2).

[12] [assignment: *list of standards*]
[13] [assignment: *cryptographic key destruction method*]
[14] [assignment: *list of standards*]
[15] [assignment: *list of cryptographic operations*]
[16] [assignment: *cryptographic key generation algorithm*]
[17] [assignment: *cryptographic key sizes]*
[18] [assignment: *list of standards*]

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

FCS_RNG.1.1 The TSF shall provide a [deterministic][19] random number generator that implements:

(DRG.3.1) If initialized with a random seed [using external input, which shall contain at least 100 bit of entropy][20], the internal state of the RNG shall [have an amount of entropy of at least 100 bit][21].
(DRG.3.2) The RNG provides forward secrecy.
(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known.[22]

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.3.4) The RNG, initialized with a random seed [using external input][23], generates output for which [2^{20}][24] strings of bit length 128 are mutually different with probability [$1-2^{-11}$][25].
(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.[26]

Application Note: The component FCS_RNG.1 is an extended component. The definition of the family FCS_RNG and its components can be found in the following document, which is part of the BSI scheme document AIS 20/31:

> W. Killmann, W. Schindler, „A proposal for: Functionality classes for random number generators“, Version 2.0, September 18, 2011.

FDP_ACC.1 Subset access control – Certificates and Cryptographic Keys

FDP_ACC.1.1 The TSF shall enforce the [certificate and cryptographic key access control SFP][27] on [the subjects, objects, and operations defined in the certificate and cryptographic key access control SFP][28].

FDP_ACF.1 Security attribute based access control – Certificates and Cryptographic Keys

FDP_ACF.1.1 The TSF shall enforce the [certificate and cryptographic key access control SFP][29] to objects based on the following: [subject and object security attributes defined in the cryptographic key access control SFP][30].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [rule defined in the cryptographic key access control SFP][31].

---

[19] [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]
[20] [selection: using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source, using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]]
[21] [selection: *have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]*]
[22] [assignment: *list of security capabilities*]
[23] [assignment: *requirements forseeding*]
[24] [assignment: *number of strings*]
[25] [assignment: *probability*]
[26] [assignment: *a defined quality metric*]
[27] [assignment: *access control SFP*]
[28] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[29] [assignment: *access control SFP*]
[30] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[31] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none][32].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none][33].

FDP_ITC.1 Import of user data without security attributes – Certificates, Cryptographic Keys

FDP_ITC.1.1 The TSF shall enforce the [certificate and cryptographic key access control SFP][34] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [none][35].

FDP_IFC.1(1) Subset information flow control – IPsec

FDP_IFC.1(1).1 The TSF shall enforce the [IPsec information flow control SFP][36] on [the subjects, information, and operations defined in the IPsec information flow control SFP][37]

FDP_IFF.1(1) Simple security attributes – IPsec

FDP_IFF.1(1).1 The TSF shall enforce the [IPsec information flow control SFP][38] based on the following types of subject and information security attributes: [subject and information security attributes defined in the IPsec information flow control SFP][39]

FDP_IFF.1(1).2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [rules defined in the IPsec information flow control SFP][40].

FDP_IFF.1(1).3 The TSF shall enforce the [none][41].

FDP_IFF.1(1).4 The TSF shall explicitly authorize an information flow based on the following rules: [none][42].

FDP_IFF.1(1).5 The TSF shall explicitly deny an information flow based on the following rules: [none][43].

FDP_IFC.1(2) Subset information flow control – Packet Filter

FDP_IFC.1(2).1 The TSF shall enforce the [packet filter information flow control SFP][44] on [the subjects, information, and operations defined in the packet filter information flow control SFP][45]

---

[32] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[33] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[34] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[35] [assignment: *additional importation control rules*]
[36] [assignment: *information flow control SFP*]
[37] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]
[38] [assignment: *information flow control SFP*]
[39] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[40] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[41] [assignment: *additional information flow control SFP rules*]
[42] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[43] [assignment: *rules, based on security attributes, that explicitly deny information flows*]
[44] [assignment: *information flow control SFP*]

FDP_IFF.1(2) Simple security attributes – Packet Filter

FDP_IFF.1(2).1 The TSF shall enforce the [packet filter information flow control SFP][46] based on the following types of subject and information security attributes: [subject and information security attributes defined in the packet filter information flow control SFP][47]

FDP_IFF.1(2).2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [rules defined in the packet filter information flow control SFP][48].

FDP_IFF.1(2).3 The TSF shall enforce the [none][49].

FDP_IFF.1(2).4 The TSF shall explicitly authorize an information flow based on the following rules: [none][50].

FDP_IFF.1(2).5 The TSF shall explicitly deny an information flow based on the following rules: [rules for denying an information flow in the packet filter information flow control SFP.][51]

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5(1) Multiple authentication mechanisms - IKE

FIA_UAU.5(1).1 The TSF shall provide [pre-shared key and signature based mechanisms][52] to support user authentication.

FIA_UAU.5(1).2 The TSF shall authenticate any user's claimed identity according to the [following rules:

- Authentication using pre-shared key (IKEv1: RFC 2409 section 5.4 (Phase 1 - Authenticated With a Pre-Shared Key)) based on a PRF (HMAC-SHA1 from RFC 2104; HMAC-SHA-256 from RFC 4868)
- Authentication using RSA signature generation and verification (IKEv1: RFC 2409 section 5.1 (Phase 1 - Authenticated With Signatures), PKCS #1 v1.5: RFC 2313) using RSA keys of 2048 bits length and based on a PRF (HMAC-SHA1 from RFC 2104; HMAC-SHA-256 from RFC 4868)][53].

FIA_UAU.5(2) Multiple authentication mechanisms – remote administration

FIA_UAU.5(2).1 The TSF shall provide [password based mechanism][54] to support user authentication.

FIA_UAU.5(2).2 The TSF shall authenticate any user's claimed identity according to the [password (RFC 4252, sections 5 and 8)][55].

---

[45] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]
[46] [assignment: *information flow control SFP*]
[47] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[48] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[49] [assignment: *additional information flow control SFP rules*]
[50] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[51] [assignment: *rules, based on security attributes, that explicitly deny information flows*]
[52] [assignment: *list of multiple authentication mechanisms*]
[53] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[54] [assignment: *list of multiple authentication mechanisms*]
[55] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

FIA_UID.2 User identification before any action

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

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of][56] the functions [

- IPsec
- packet filter

][57] to [administrators][58].

FMT_MSA.1(1) Management of security attributes - IPsec

FMT_MSA.1(1).1 The TSF shall enforce the [IPsec information flow SFP][59] to restrict the ability to [query, modify, delete][60] the security attributes [IPsec related configuration][61] to [administrators][62].

FMT_MSA.1(2) Management of security attributes – Packet Filter

FMT_MSA.1(2).1 The TSF shall enforce the [packet filter information flow control SFP][63] to restrict the ability to [query, modify, delete][64] the security attributes [packet filter configuration][65] to [administrators][66].

FMT_MSA.1(3) Management of security attributes – Certificates and Cryptographic Keys

FMT_MSA.1(3).1 The TSF shall enforce the [certificate and cryptographic key access control SFP] to restrict the ability to [modify][67] the security attributes [password][68] to [administrators][69].

FMT_MSA.3(1) Static attribute initialisation - IPsec

FMT_MSA.3(1).1 The TSF shall enforce the [IPsec information flow SFP][70] to provide [restrictive][71] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3(1).2 The TSF shall allow the [administrator][72] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(2) Static attribute initialisation – Packet Filter

FMT_MSA.3(2).1 The TSF shall enforce the [packet filter information flow control SFP][73] to provide [restrictive][74] default values for security attributes that are used to enforce the SFP.

---

[56] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
[57] [assignment: *list of functions*]
[58] [assignment: *the authorised identified roles*]
[59] [assignment: *access control SFP(s), information flow control SFP(s)*]
[60] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[61] [assignment: *list of security attributes*]
[62] [assignment: *the authorised identified roles*]
[63] [assignment: *access control SFP(s), information flow control SFP(s)*]
[64] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[65] [assignment: *list of security attributes*]
[66] [assignment: *the authorised identified roles*]
[67] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[68] [assignment: *list of security attributes*]
[69] [assignment: *the authorised identified roles*]
[70] [assignment: *access control SFP(s), information flow control SFP(s)*]
[71] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
[72] [assignment: *the authorised identified roles*]

FMT_MSA.3(2).2 The TSF shall allow the [administrator][75] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(3) Static attribute initialisation – Certificates and Cryptographic Keys

FMT_MSA.3(3).1 The TSF shall enforce the [certificate and cryptographic key access control SFP][76] to provide [permissive][77] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3(3).2 The TSF shall allow the [administrator][78] to specify alternative initial values to override the default values when an object or information is created.

Application Note: The security attribute used in the SFP is the password of the administrator. After the configuration of the TOE has been resetted during the installation of the TOE on the hardware, the password is initially empty, hence the permissive default. However, the guidance documentation requires a password to be set before the TOE is operated in a live network.

FMT_MTD.1(1) Management of TSF data – TSF configuration

FMT_MTD.1(1).1 The TSF shall restrict the ability to [query, modify, delete, clear][79] the [TSF configuration][80] to [administrators][81].

FMT_MTD.1(2) Management of TSF data – IPsec Pre-shared Keys

FMT_MTD.1(2).1 The TSF shall restrict the ability to [query, modify, delete][82] the [IPsec pre-shared keys][83] to [administrators][84].

FMT_MTD.1(3) Management of TSF data – SSH Host Keys

FMT_MTD.1(3).1 The TSF shall restrict the ability to [modify, delete][85] the [SSH host key][86] to [administrators][87].

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- disable, enable, and modify the behavior of the functions that implement IPsec and packet filtering
- management of the IPsec-related configuration
- management of the packet filtering configuration
- management of the TSF configuration
- generate and review audit information
- upload and delete certificates and cryptographic keys][88]

---

[73] [assignment: *access control SFP, information flow control SFP*]
[74] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
[75] [assignment: *the authorised identified roles*]
[76] [assignment: *access control SFP, information flow control SFP*]
[77] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
[78] [assignment: *the authorised identified roles*]
[79] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[80] [assignment: *list of TSF data*]
[81] [assignment: *the authorised identified roles*]
[82] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[83] [assignment: *list of TSF data*]
[84] [assignment: *the authorised identified roles*]
[85] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[86] [assignment: *list of TSF data*]
[87] [assignment: *the authorised identified roles*]

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles~~s~~ [administrator][89].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FPT_TDC.1(1) Inter-TSF basic TSF data consistency – IKE certificate

FPT_TDC.1(1).1 The TSF shall provide the capability to consistently interpret [IKE certificates][90] when shared between the TSF and another trusted IT product.

FPT_TDC.1(1).2 The TSF shall use [PKCS#12 Personal Information Exchange Syntax Standard, version 1.1][91] when interpreting the TSF data from another trusted IT product.

Application Note: The TOE requires the IKE certificate of the partner site for authentication.

FPT_TDC.1(2) Inter-TSF basic TSF data consistency - SSH host key

FPT_TDC.1(2).1 The TSF shall provide the capability to consistently interpret [SSH host key][92] when shared between the TSF and another trusted IT product.

FPT_TDC.1(2).2 The TSF shall use [PKCS#1 RSA private key syntax in PEM format][93] when interpreting the TSF data from another trusted IT product.

FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [access control lists][94].

Application Note: The TSF restricts the access to the TOE for remote configuration via SSH. The access to the local configuration via serial console is not restricted by the access control lists. The administrator cannot lock himself out permanently even if the access control lists are misconfigured, since local configuration would still be possible. Via local configuration the administrator can change the access control lists and access the management functions described in FMT_SMF.1.

FTP_ITC.1 Inter-TSF trusted channel – Remote Management via SSH

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [another trusted IT product][95] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [remote administration][96].

Application Note: The TSF uses the algorithms and functions as defined in FCS_CKM.2(2) and FCS_COP.1 to implement this trusted channel.

---

[88] [assignment: *list of management functions to be provided by the TSF*]
[89] [assignment: *the authorised identified roles*]
[90] [assignment: *list of TSF data types*]
[91] [assignment: *list of interpretation rules to be applied by the TSF*]
[92] [assignment: *list of TSF data types*]
[93] [assignment: *list of interpretation rules to be applied by the TSF*]
[94] [assignment: *attributes*]
[95] [selection: *the TSF, another trusted IT product*]
[96] [assignment: *list of functions for which a trusted channel is required*]

5.2. Security Assurance Requirements

The TOE conforms to all security assurance requirements in EAL4 as defined in CC part 3 augmented with ALC_FLR.1. The following table lists all SARs. A **bold** typeface is used to indicate that ALC_FLR.1 is an augmentation to EAL4.

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, **ALC_FLR.1**, ALC_LCD.1, ALC_TAT.1
ASE	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.3

5.3. Security Functional Requirements Rationale

The following table maps security objectives to security functional requirements, showing that each security objective is covered by at least one security functional requirement and that no security functional requirement exists that is not needed by any security objective.

Objective / Requirement	O.Cryptography	O.ESP	O.Key-Confidentiality	O.Mediate	O.NoReplay	O.Secure-Operation
FAU_GEN.1						X
FAU_SAR.1						X
FCS_CKM.1	X	X				
FCS_CKM.2(1)	X	X				
FCS_CKM.2(2)	X					X
FCS_CKM.4	X		X			
FCS_COP.1	X					X
FCS_RNG.1	X					X
FDP_ACC.1						X

Objective / Requirement	O.Cryptography	O.ESP	O.Key-Confidentiality	O.Mediate	O.NoReplay	O.Secure-Operation
FDP_ACF.1						X
FDP_IFC.1(1)	X	X			X	
FDP_IFC.1(2)				X		
FDP_IFF.1(1)	X	X			X	
FDP_IFF.1(2)				X		
FDP_ITC.1						X
FIA_UAU.2						X
FIA_UAU.5(1)						X
FIA_UAU.5(2)						X
FIA_UID.2	X					X
FMT_MOF.1						X
FMT_MSA.1(1)						X
FMT_MSA.1(2)						X
FMT_MSA.1(3)						X
FMT_MSA.3(1)						X
FMT_MSA.3(2)						X
FMT_MSA.3(3)						X
FMT_MTD.1(1)						X
FMT_MTD.1(2)			X			X
FMT_MTD.1(3)			X			X
FMT_SMF.1						X
FMT_SMR.1						X
FPT_TDC.1(1)						X
FPT_TDC.1(2)						X

Objective / Requirement	O.Cryptography	O.ESP	O.Key-Confidentiality	O.Mediate	O.NoReplay	O.Secure-Operation
FTA_TSE.1						X
FTP_ITC.1						X

The following table shows what the individual security functional requirements contribute to the objective and that the requirements are sufficient to satisfy the objective.

Objective	Requirements
O.Cryptography	The TOE performs the cryptographic algorithms and protocols needed for the the confidentiality and integrity of the IKE protocol establishment and for remote administration as follows. FDP_IFF.1(1) allows the TOE to identify which VPN peer is authenticating which IP packets and which IP packets will be authenticated for transmission to a remote VPN peer, thus providing the correct keys for the HMAC. FDP_IFC.1(1) defines the IPsec information flow SFP and thus supports FDP_IFF.1(1). FIA_UID.2 guarantees that the IP packets are associated to a remote trusted IT product. FCS_CKM.1 and FCS_CKM.2(1) together provide the key agreement protocol needed for IKE. FCS_CKM.2(2) and FCS_COP.1 perform the cryptographic protocol for remote administration including the SSH session. FCS_CKM.4 ensures that keys are destroyed in a safe way. In particular, session keys negotiated via SSH and IKE are destroyed after they are no longer needed. FCS_RNG.1 provides the random numbers needed for key generation in both protocols mentioned above.
O.ESP	The TOE defers the confidentiality, authenticity, and integrity protection of ESP packets to the cryptographic acceleration engine. The following SFRs support that functionality within the TOE: FCS_CKM.1 authenticates the VPN peer during session key establishment. FCS_CKM.2(1) provides secure keys for the cryptographic protection of ESP packets. FDP_IFF.1(1) allows the TOE to identify which VPN peer is providing cryptographic protection for which IP packets and which IP packets will be protected when transmitted to a remote VPN peer, thus providing the correct keys for encryption, decryption, and authentication. FDP_IFC.1(1) defines the IPsec information flow SFP and thus supports

Objective	Requirements
	FDP_IFF.1(1).
O.Key-Confidentiality	FCS_CKM.4 ensures that keys are destroyed in a safe way. In particular, session keys negotiated via SSH and IKE are destroyed after they are no longer needed. For keys kept in system memory, the TOE is responsible for destroying the keys. The cryptographic acceleration engine destroys keys used in the hardware. FMT_MTD.1(2) ensures that only the administrator can query, modify and delete pre-shared keys. FMT_MTD.1(3) ensures that only the administrator can modify and delete the SSH host key.
O.Mediate	FDP_IFF.1(2) identifies which IP packets are to be mediated and that the packet filter rules can allow or deny IP packets to pass through the TOE. FDP_IFC.1(2) defines the information flow SFP and thus supports FDP_IFF.1(2).
O.NoReplay	The TOE can detect and drop replayed ESP packets by inspecting the sequence number in the ESP header. The following SFRs contribute to checking the sequence number: FDP_IFF.1(1) allows the TOE to identify which VPN peer has sent the ESP packet and thus which sequence numbers are valid. The list of seen sequence numbers is updated for each received ESP packet. FDP_IFC.1(1) defines the IPsec information flow SFP and thus supports FDP_IFF.1(1).
O.Secure-Operation	FDP_ACF.1 specifies that the password must be checked before an administrator can upload a certificate or cryptographic key. FDP_ACC.1 defines the certificate and cryptographic key access control SFP and thus supports FDP_ACF.1. FTP_ITC.1 is used to provide a trusted channel that protects integrity and confidentiality of remote administration sessions via SSH. FCS_CKM.2(2), FCS_COP.1, and FCS_RNG.1 support the generation of good keys and the cryptographic operations needed for the SSH protocol. FIA_UAU.2 requires user authentication before allowing any other TSF-mediated actions. FIA_UAU.5(1) and FIA_UAU.5(2) specify which methods of user authentication are supported for IKE and remote administration. FIA_UID.2 requires user identification before allowing any other TSF-mediated actions. FMT_MOF.1 restricts the configuration of security functions to administrators. FMT_MSA.1(1) restricts the configuration of IPsec security attributes to administrators. FMT_MSA.1(2) restricts the configuration of packet filter security attributes to administrators. FMT_MSA.1(3) restricts the modification of the password to administrators. FMT_MSA.3(1) specifies the default values for the IPsec information flow SFP and that only the administrator can specify alternative initial values. FMT_MSA.3(2) specifies the default values for the packet filter information

Objective	Requirements
	flow SFP and that only the administrator can specify alternative initial values. FMT_MSA.3(3) specifies the default values for the certificate and cryptographic key access control SFP. FMT_MTD.1(1) allows only administrators to query, modify, delete and clear the TSF configuration. FMT_MTD.1(2) ensures that only administrators can query, modify and delete pre-shared keys. FMT_MTD.1(3) ensures that only the administrator can modify and delete the SSH host key. FMT_SMF.1 describes the security functions the administrators can use to ensure the secure operation of the TOE. FMT_SMR.1 allows to associate users with the security role administrator. FDP_ITC.1 allows the upload of certificates and cryptographic keys. The SSH server private key is necessary for an administrator to establish the identity of the TOE for remote administration. FPT_TDC.1(1) and FPT_TDC.1(2) require the use of standardized formats for the upload of certificates and cryptographic keys and thus supports FDP_ITC.1. FTA_TSE.1 allows the TOE to reject unauthorized session establishment based on access control lists. SSH connection establishment can be limited to hosts from a specific IP range. SSH connection establishment can also be limited to hosts on a trusted network or hosts connected via VPN. The TOE shall provide audit capabilities. FAU_GEN.1 enforces the generation of audit records. FAU_SAR.1 allows administrators to review the audit records.

5.3.1. Security Functional Requirements Dependencies

The table lists the dependencies for each Security Functional Requirement (SFR) and shows by which SFRs they are met. The dependency for FAU_GEN.1 is not met by SFRs but by OE.Hardware. A more detailed rationale for this dependency is given in the following paragraph.

FAU_GEN.1 requires timestamps to be added to audit data. Since the TOE is a software-only TOE, an accurate system time cannot be maintained when the system is powered down. Therefore, the TOE relies on a real time clock in the hardware. The availability of the real time clock in the hardware running the TOE is guaranteed by OE.Hardware. Since the TOE is in a protected environment (A.PhySec) the time cannot be tampered with. The real time clock is battery buffered.

SFR	Required Dependencies	Met/fullfilled by
FAU_GEN.1	FPT_STM.1	not met by a SFR but OE.Hardware
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.2(1) FCS_CKM.4
FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or	FDP_ITC.1

SFR	Required Dependencies	Met/fullfilled by
	FCS_CKM.1], FCS_CKM.4	FCS_CKM.4
FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FDP_ITC.1 FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1 FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	The first dependency refers to the question, how the TOE gets the cryptographic keys for the cryptographic operation. This is in part fulfilled by FTP_ITC.1 (for imported keys), however some session keys may also be generated during the SSH protocol, this is contained in FCS_COP.1 itself. Second dependency: FCS_CKM.4.
FCS_RNG.1	none	none
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3(3)
FDP_IFC.1(1)	FDP_IFF.1	FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1	FDP_IFF.1(2)
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1(1) FMT_MSA.3(1)
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1(2) FMT_MSA.3(2)
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1 FMT_MSA.3(3)
FIA_UAU.2	FIA_UID.1	FIA_UID.2 hierarchical to FIA_UID.1
FIA_UAU.5(1)	none	none
FIA_UAU.5(2)	none	none
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1(1)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1(1) FMT_SMR.1 FMT_SMF.1

SFR	Required Dependencies	Met/fullfilled by
FMT_MSA.1(2)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1(2) FMT_SMR.1 FMT_SMF.1
FMT_MSA.1(3)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3(1)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(1) FMT_SMR.1
FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(2) FMT_SMR.1
FMT_MSA.3(3)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(3) FMT_SMR.1
FMT_MTD.1(1)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1(2)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1(3)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2 hierarchical to FIA_UID.1
FPT_TDC.1(1)	none	none
FPT_TDC.1(2)	none	none
FTA_TSE.1	none	none
FTP_ITC.1	none	none

5.4. Security Assurance Requirements Rationale

EAL4 has been chosen to establish a sufficient level of confidence in the security offered by the TOE. It has been augmented with ALC_FLR.1 to ensure that customers can report flaws and that those flaws can be corrected according to flaw remediation procedures.

Since ALC_FLR.1 does not have dependencies and EAL4 satisfies its own dependencies, EAL4 augmented with ALC_FLR.1 is consistent with regard to its dependencies.

6. TOE Summary Specification

This section shows which Security Functions are implemented in the TOE and maps them to the Security Functional Requirements.

6.1. TOE Summary Specification

The Security Functions implemented by the TOE are described in the following text. This section shows which Security Functions are implemented in the TOE and maps them to the Security Functional Requirements.

6.1.1. IPsec

The TOE in conjunction with the cryptographic acceleration engine implements the IPsec protocols as described in RFCs 2401, 2402, 2406-2409. Confidentiality, authenticity, and integrity are provided for IP packets protected by IPsec. The implementation of IPsec in the TOE is split up into several components. The following sections describe which parts of IPsec are implemented in the TOE itself and which parts are delegated to the cryptographic acceleration engine.

The administrator defines which traffic must be protected by IPsec by configuring routes with a VPN peer as the gateway. For each VPN peer a set of acceptable authentication methods can be defined. For IP packets to be forwarded to a VPN peer, an established security association (SA) is required. An IP packet that does not have an established SA triggers IKE to negotiate a new SA to protect the IP packet. Once the SA is established, it is applied to the IP packet.

IPSEC.1 – IPsec Internet Key Exchange (IKE)

The Internet Key Exchange (IKE) is a key management protocol used to automatically negotiate IPsec security associations (SAs). Thus, IKE allows dynamic authentication of VPN peers, changing keys once their lifetime has expired.

IKE uses two phases for key negotiation. Phase 1 negotiates a SA between two IKE peers, providing a key that is used to encrypt the negotiations in phase 2. In phase 2, the actual keys and parameters for the IP packets are negotiated. During the negotiation, each IKE peer has a list of acceptable parameters, which is exchanged between the peers by using proposals.

The temporary keys negotiated via IKE are destroyed by overwriting them with zeroes when they are no longer needed.

The TOE implements the following operations in the IKE protocol:

- AES-CBC
- SHA-1 and SHA-256 in HMAC
- RSA
- Diffie-Hellman
- Random number generator

IPSEC.2 – IPsec Encapsulating Security Payload (ESP)

IP Packets are encrypted on their way through untrusted networks (e.g., the Internet) according to a policy defined by the administrator. The hardware cryptographic acceleration engine supports the TOE by encapsulating IP packets using the AES cipher with the encryption key previously negotiated by IKE to provide confidentiality for the IP packets. Furthermore, ESP provides integrity and authenticity for the IP packets by using the SHA-1 or SHA-256 algorithm of the hardware cryptographic acceleration engine in a HMAC in combination with the authentication key negotiated by IKE. The TOE uses ESP related information to detect replayed packets. Details regarding the use of the cryptographic hardware acceleration engine by IPsec can be found in Appendix A.

IPSEC.3 – IPsec Security Associations, Security Policies and Routing

The encryption key and the authentication key for an IPsec association are stored in a Security association (SA), reflecting the current state of an IPsec association. Since a SA is unidirectional, a bidirectional exchange of IP packets between VPN peer A and VPN peer B requires two SAs. The first SA protects the IP packets from A to B and the second SA protects the IP packets from B to A. The parameters of the SAs such as the keys are negotiated via IKE (IPSEC.1). Each SA and, thus, each encryption and authentication key has a lifetime. Expiring the lifetime causes IKE to negotiate new encryption and authentication keys, effectively replacing the old SA with a newly negotiated one. Encryption and authentication keys that are no longer used are deleted by overwriting them.

The SAs are accompanied by the Security Policies (SP), reflecting the requirements a packet must fulfill to be allowed for IPsec transfer. In contrast to the more dynamic SAs, which hold the state of an active IPsec association, SPs are more static in nature and define, which packets are to be protected by IPsec based on IP addresses.

SPs are automatically generated based on the information in the routing table. The TOE uses named peers to identify routes. Such a peer could be a WAN connection (e.g., ADSL, VDSL, 3G/4G) or a VPN peer. For VPN peers the SPs are generated to match the configured route to that VPN peer. IP packets that would be routed via a SP that does not have an active SA will trigger IKE to negotiate and set up a new SA. Therefore, the IPsec Information Flow SFP is modeled by the routing table in conjunction with the SAs and SPs.

6.1.2. Packet Filtering

PACKETFILTER.1 – Packet Filtering

The TOE performs packet filtering as a part of the IP router by applying the firewall rules to IP packets traversing the IP router. The administrator defined firewall rules can either allow an IP packet to be routed, dropped or rejected. The rules can be based on the source and destination IP address, the source and destination port number, and the IP protocol. The packet filter information flow policy models the firewall rules.

The TOE rejects packets that arrive on a network interface where the presumed address of the source is an IT entity on a different network. Thus, traffic from spoofed addresses and loopback addresses is blocked. This policy enforcement allows the TOE to ensure that the security policy cannot be bypassed provided that the TOE is correctly configured.

6.1.3. Configuration and Management

CONFIG.1 – System Messages

The TOE generates audit records to provide a log of security relevant events during TOE operation. A detailed list of logged events and relevant information for each type of event is given in FAU_GEN.1. Logged messages for these events are stored in an internal buffer within the TOE or be sent to an external logging server via the SYSLOG protocol. The evaluated configuration does not support the use of a SYSLOG server. Therefore, the logged messages are sent to the internal buffer and can be retrieved by accessing the log table via the CLI. Thus, administrators can review the audit records either locally via the serial console or remotely via SSH.

Timestamps used in audit records are based on the system time provided by the real time clock in the hardware as described in OE.Hardware. The administrator must set the real time clock when the TOE is initially deployed and verify the system time on a regular basis.

CONFIG.2 – Management

Management and configuration of the TOE are performed on a command line interface (CLI) which can be accessed either locally via a serial configuration port, or remotely via a SSH network connection. Other remote management options available in regular LCOS versions such as telnet, HTTP, HTTPS, or SNMP are not allowed in the evaluated configuration. Access to the CLI requires valid authentication. For the serial console, the administrator must log in with username and password. If only one user account exists, the username is implicitly assumed to be the name of the only user. In that case, only the password must be provided by the administrator for login.

The TOE maintains an administrator role. The CLI provides the means for the administrator to read, modify, and use all TOE status information, configuration data, and management functions. The CLI allows the administrator to delete uploaded certificates and cryptographic keys by overwriting them with zeroes. The default configuration is restrictive. The various implemented cryptographic functions and RFCs ensure that only secure values for cryptographic functions can be set.

6.1.4. Remote Management

REMOTE.1

Secure Shell (SSH) is used for remote management of the TOE by the administrator. Remote management via SSH provides full access to the command line interface as it would be available via the serial console. Remote administration via SSH provides confidentiality and integrity of the management session, which is completely ensured by TOE components without use of the cryptographic acceleration engine. SSH also provides protection against replay attacks by using a unique session identifier that is bound to the key exchange process in the transport protocol. The temporary session keys are destroyed by overwriting them with zeroes when the session is closed. SSH is described in detail in RFCs 4251-4254.

For cryptographic operations such as AES encryption and decryption, SHA-1 hashes used in HMACs or integer modulo arithmetic used by RSA and Diffie-Hellman, SSH uses the cryptographic functions provided by the TOE.

SSH authenticates users trying to establish a connection by requiring a username and password to be specified during connection establishment.

VPN peers can be authenticated via pre-shared keys or via public key cryptography. For the authentication via public key cryptography, the administrator can upload the certificate to the TOE via SSH. The certificate must be uploaded in the PKCS12 format. The TOE also uses a RSA key as the SSH server private key, which shall be uploaded to the TOE in PEM format. Acquiring the certificate and the cryptographic key is out of the scope of this ST. The certificate and cryptographic key access control SFP is implemented by this TSF by requiring user authentication.

The access control lists can limit establishing a remote configuration connection via SSH to specific IP addresses and subnetworks. The administrator can also specify from which type of connection (i.e., trusted local network, trusted network connected via VPN or untrusted network) a SSH connection attempt is accepted.

6.2. TOE Summary Specification Rationale

The following table shows the correspondence between the TOE Security Functions and the Security Functional Requirements.

SFR	IPSEC.1	IPSEC.2	IPSEC.3	PACKETFILTER.1	CONFIG.1	CONFIG.2	REMOTE.1
FAU_GEN.1					X		
FAU_SAR.1					X		
FCS_CKM.1	X						
FCS_CKM.2(1)	X						

SFR	IPSEC.1	IPSEC.2	IPSEC.3	PACKETFILTER.1	CONFIG.1	CONFIG.2	REMOTE.1
FCS_CKM.2(2)							X
FCS_CKM.4	X					X	X
FCS_COP.1							X
FCS_RNG.1	X						X
FDP_ACC.1							X
FDP_ACF.1							X
FDP_IFC.1(1)			X				
FDP_IFC.1(2)				X			
FDP_IFF.1(1)			X				
FDP_IFF.1(2)				X			
FDP_ITC.1							X
FIA_UAU.2	X					X	
FIA_UAU.5(1)	X						
FIA_UAU.5(2)						X	X
FIA_UID.2	X					X	X
FMT_MOF.1						X	
FMT_MSA.1(1)	X	X	X			X	
FMT_MSA.1(2)				X		X	
FMT_MSA.1(3)							X
FMT_MSA.3(1)						X	
FMT_MSA.3(2)						X	
FMT_MSA.3(3)							X
FMT_MTD.1(1)						X	
FMT_MTD.1(2)	X					X	
FMT_MTD.1(3)						X	X

SFR	IPSEC.1	IPSEC.2	IPSEC.3	PACKETFILTER.1	CONFIG.1	CONFIG.2	REMOTE.1
FMT_SMF.1					X	X	
FMT_SMR.1						X	
FPT_TDC.1(1)							X
FPT_TDC.1(2)							X
FTA_TSE.1							X
FTP_ITC.1							X

FAU_GEN.1

The TSF CONFIG.1 satisfies this SFR by generating audit logs according to the requirement.

FAU_SAR.1

The TSF CONFIG.1 satisfies this SFR by allowing the administrator to review the audit logs.

FCS_CKM.1 and FCS_CKM.2(1)

The TSF IPSEC.1 satisfies these SFRs by implementing the IKE protocol, which generates and exchanges keys in the key negotiation and authenticates the VPN peer.

FCS_CKM.2(2)

The TSF REMOTE.1 satisfies this SFR by implementing the SSH key establishment.

FCS_CKM.4

The TSF IPSEC.1 satisfies this SFR by zeroing cryptographic keys used for AES and HMAC when they are no longer used. This includes overwriting keys used in the cryptographic acceleration engine.

The TSF CONFIG.2 satisfies this SFR by zeroing cryptographic keys and certificates imported via SSH.

The TSF REMOTE.1 satisfies this SFR by zeroing cryptographic keys used for AES and HMAC when they are no longer used. This includes overwriting keys used in the cryptographic acceleration engine.

FCS_COP.1

The TSF REMOTE.1 implements this SFR by implementing all cryptographic aspects of the SSH protocol.

FCS_RNG.1

A deterministic random number generator is implemented by the TSF for all random numbers needed for key generation during REMOTE.1 and IPSEC.1.

FDP_ACC.1

The TSF REMOTE.1 satisfies this SFR by enforcing the certificate and cryptographic key access control SFP. The TSF allows uploading certificates and cryptographic keys to the TOE.

FDP_ACF.1

The TSF REMOTE.1 satisfies this SFR by enforcing the certificate and cryptographic key access control SFP. The decision if the upload of a certificate or cryptographic key is allowed is based on the password provided by the administrator.

FDP_IFC.1(1)

The TSF IPSEC.3 satisfies this SFR by applying the IPsec information flow control policy to each IP packet. The routing table and the IPsec security policies derived from the routing table identify IP packets that must be encrypted and decrypted.

FDP_IFC.1(2)

The TSF PACKETFILTER.1 satisfies this SFR by applying the packet filter information flow control policy to each IP packet going through the TOE.

FDP_IFF.1(1)

The TSF IPSEC.3 satisfies this SFR by implementing the IPsec information flow control policy to decide if an IP packet must be encrypted, decrypted or ignored.

FDP_IFF.1(2)

The TSF PACKETFILTER.1 satisfies this SFR by allowing or denying IP packets going through the TOE based on the information in the packet header and applying the packet filter information flow control SFP.

FDP_ITC.1

The TSF REMOTE.1 satisfies this SFR by allowing the administrator to upload certificates and cryptographic keys to the TOE. The TSF also ensures that the password was checked during connection establishment.

FIA_UAU.2

The TSF CONFIG.2 satisfies this SFR by requiring users to authenticate themselves before allowing access to the management interface.

The TSF IPSEC.1 satisfies this SFR by requiring device authentication prior to establishing a VPN connection.

FIA_UAU.5(1)

The TSF IPSEC.1 satisfies this SFR by requiring SA peer authentication as a part of the IKE protocol prior to establishing a VPN connection.

FIA_UAU.5(2)

The TSF CONFIG.2 together with TSF REMOTE.1 satisfy this SFR by requiring a username and a password for authentication purposes resp. password authentication in the SSH protocol.

FIA_UID.2

The TSF CONFIG.2 satisfies this SFR by requiring users to identify themselves before allowing access to the management interface.

The TSF REMOTE.1 satisfies this SFR by requiring the remote administrators to identify themselves in the SSH protocol.

The TSF IPSEC.1 satisfies this SFR by requiring SA peer identification as a part of the authentication process in IKE.

FMT_MOF.1

The TSF CONFIG.2 satisfies this SFR by only granting administrators the right to manage the functions implementing the IPsec and packet filtering information flow SFPs.

FMT_MSA.1(1)

The TSF CONFIG.2 satisfies this SFR by only granting administrators the right to manage the configuration that implements the IPsec information flow control SFP. The TSFs IPSEC.1, IPSEC.2, and IPSEC.3 implement the IPsec information flow control SFP.

FMT_MSA.1(2)

The TSF CONFIG.2 satisfies this SFR by only granting administrators the right to manage the configuration that implements the packet filter information flow SFP. The TSF PACKETFILTER.1 implements the packet filter information flow SFP.

FMT_MSA.1(3)

The TSF REMOTE.1 satisfies this SFR by only granting administrators the right to manage the configuration that implements the certificate and cryptographic key access control SFP.

FMT_MSA.3(1)

The TSF CONFIG.2 satisfies this SFR by ensuring that restrictive default values are used for the IPsec information flow control SFP and that the administrator can change the initial values.

FMT_MSA.3(2)

The TSF CONFIG.2 satisfies this SFR by ensuring that restrictive default values are used for the packet filter information flow control and that the administrator can change the initial values.

FMT_MSA.3(3)

The TSF REMOTE.1 satisfies this SFR by ensuring that restrictive default values are used for the certificate and cryptographic key access control SFP and that the administrator can change the initial values.

FMT_MTD.1(1)

The TSF CONFIG.2 satisfies this SFR by only allowing administrators to query, modify, delete, and clear the TSF configuration.

FMT_MTD.1(2)

The TSF CONFIG.2 satisfies this SFR by only allowing administrators to query, modify, and delete the IPsec pre-shared keys. The TSF IPSEC.1 uses the pre-shared keys during the IKE negotiation, being allowed to read the pre-shared keys but not to alter them.

FMT_MTD.1(3)

The TSF CONFIG.2 satisfies this SFR by only allowing administrators to modify and delete the SSH host key. The TSF REMOTE.1 uses the SSH host key for authentication during SSH connection establishment, being allowed to read the SSH host key but not to alter them.

FMT_SMF.1

The TSF CONFIG.1 satisfies this SFR by generating audit information and giving access to generated audit information for review.

The TSF CONFIG.2 satisfies this SFR by allowing an authenticated administrator to configure the TOE.

FMT_SMR.1

The TSF CONFIG.2 satisfies this SFR by maintaining the administrator role.

FPT_TDC.1(1)

The TSF REMOTE.1 satisfies this SFR by using the standardized format PKCS12 to upload IKE certificates.

FPT_TDC.1(2)

The TSF REMOTE.1 satisfies this SFR by using the standardized format PEM to upload cryptographic keys for server identity.

FTA_TSE.1

The TSF REMOTE.1 satisfies this SFR by applying the access control lists before a connection via SSH is established.

FTP_ITC.1

The TSF REMOTE.1 satisfies this SFR by providing a trusted channel via SSH for remote administration.

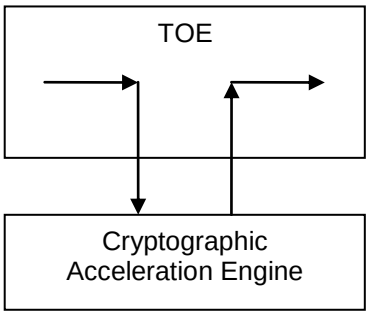
7. Appendix A: Hardware Cryptography

As described in section 1.5, the TOE must be installed on special hardware to be functional. The hardware includes a cryptographic acceleration engine implemented as a part of the CPU. The CPU model used depends on the LANCOM router model used. The algorithms used by the TOE are available in all LANCOM router models mentioned in section 1.5 to be consistent.

The following cryptographic operations are implemented in the cryptographic acceleration engine and used for TOE support:

- AES (128, 192, 256) CBC
- SHA-1
- SHA-256

The cryptographic operations are used by the TOE for the payload part of IPsec. The following figure illustrates on an abstract level how the control flow for ESP cryptographic operations works:



In the first step, the TOE performs some kind of preparative operations, e.g. determining to which connection the packet belongs. With this information, the TOE knows which keys and cryptographic algorithms must be used. The TOE fills a descriptor accordingly and triggers the cryptographic acceleration engine in the CPU to process that descriptor. When the cryptographic operation is complete, the TOE is notified and can continue to operate on the result of the cryptographic operation, e.g. forward the packet to its destination.