ST Engineering
Electronics

NetCrypt Family Series

S20/R100/U1000/U2000

Security Target

V1.0

NetCrypt Family Series
S20/R100/U1000/U2000

Security Target
Contents

Chapter 1 – Security Target Introduction 1-1
1.1 Security Target Reference 1-1
1.2 TOE Reference Identification 1-1
1.3 TOE Overview 1-1
1.3.1 Non-TOE hardware/software/firmware required by the TOE 1-3
1.3.2 Physical Scope of the TOE 1-3
1.3.3 Logical Scope of the TOE 1-4
1.4 Terms and Acronyms 1-5
Chapter 2 – Conformance Claims 2-1
2.1 Common Criteria Conformance Claim 2-1
2.2 Protection Profile Conformance 2-1
Chapter 3 – Security Problem Definition 3-2
3.1 Assets 3-2
3.2 Threats 3-2
3.3 Assumptions 3-3
3.4 Organizational Security Policy 3-4
Chapter 4 Security Objectives 4-5
4.1 Security Objectives for the TOE 4-5
4.2 Security Objectives for the Operational Environment 4-6
4.3 Security Objectives Rationale 4-7
4.3.1 Threats 4-7
4.3.2 Assumptions 4-9
Chapter 5 Extended Requirements 5-11
5.1 Extended Components Definition 5-11
Chapter 6 - Security Requirements 6-13
6.1 Conventions 6-13

6.2 Security Functional Requirements (SFRs) 6-13
6.2.1 FAU_GEN.1 Audit data generation 6-13
6.2.2 FAU_STG.1 Protected Audit Trail Storage 6-13
6.2.3 FAU_SAR.1 Audit Review 6-14
6.2.4 FCS_CKM.1 Cryptographic Key Generation 6-14
6.2.5 FCS_CKM.4 Cryptographic Key Destruction 6-14
6.2.6 FCS_COP.1/Data Encryption/Decryption - Cryptographic operation 6-14
6.2.7 FCS_COP.1/Cryptographic Signature - Cryptographic operation 6-14
6.2.8 FCS_COP.1/Cryptographic Hashing - Cryptographic operation 6-14
6.2.9 FCS_COP.1/Keyed-hash Message Authentication - Cryptographic operation 6-15
6.2.10 FCS_IPSEC_EXT.1 – IPSEC Selected 6-15
6.2.11 FDP_IFC.1 Subset information flow control 6-16
6.2.12 FDP_IFF.1 Simple Security Attributes 6-16
6.2.13 FIA_USB.1 User-subject Binding 6-17
6.2.14 FIA_ATD.1 User attribute definition 6-17
6.2.15 FIA_UID.1 Timing of identification 6-17
6.2.16 FIA_UAU.1 Timing of authentication 6-17
6.2.17 FMT_MOF.1 Management of security functions behavior 6-18
6.2.18 FMT_MTD.1 Management of TSF Data 6-18
6.2.19 FMT_MSA.1 Management of security attributes 6-18
6.2.20 FMT_MSA.3 Static attribute initialization 6-19
6.2.21 FMT_SMF.1 Specification of Management Functions 6-19
6.2.22 FMT_SMR.1 Security Roles 6-19
6.2.23 FPT_FLS.1 Failure with Preservation of Secure State 6-19
6.2.24 FPT_TST.1 TSF Testing 6-20
6.2.25 FTA_SSL.4 User-initiated Termination 6-20
6.2.26 FTP_ITC.1 Inter-TSF trusted channels 6-20
6.3 Security Requirements Rationale 6-20
6.3.1 Security Objectives for the TOE 6-20
6.3.2 Dependencies 6-23
6.4 Security Assurance Requirements 6-25
6.4.1 Rational for Security Assurance Requirements 6-26
Chapter 7 TOE Summary Specification 7-27
7.1 Security Audit 7-27
7.1.1 Audit Selection and Generation 7-27
7.1.2 Preventing Audit Data Loss 7-27

7.2 Cryptographic Support 7-27
7.2.1 Cryptographic Operations 7-27
7.2.2 Cryptographic Keys Generation 7-28
7.2.3 Cryptographic Key Destruction by Zeroization 7-28
7.3 Identification and Authentication 7-29
7.4 Security Management 7-29
7.5 User Data Protection 7-30
7.6 Protection of the TSF 7-31
7.7 Trusted Channels 7-31
APPENDIX A 7-32

This page is left blank

Chapter 1 – Security Target Introduction

1.1Security Target Reference

Security Target Reference: NetCrypt Family Series S20/R100/U1000/U2000 Security Target

Version: 1.0

Security Target Publication Date: 19 June 2018

1.2TOE Reference Identification

TOE Reference: NetCrypt Family Series S20/R100/U1000/U2000

	NetCrypt S20	**NetCrypt R100**	**NetCrypt U1000**	**NetCrypt U2000**
HW Model	9910-8000-0723	9910-8000-1190	9910-8000-0733	9910-8000-1281
FW version	2.6.4	2.6.4	2.6.4	2.6.4

1.3TOE Overview

The TOE consists of both portable (NetCrypt S20) and rack mounted (NetCrypt R100/U1000/U2000) hardware IP encryptor that enables the user to leverage on public Ethernet/IP infrastructure to connect to multiple sites in a secure manner. It employs AES algorithms for data confidentiality, Secure Hash Algorithm (SHA) for integrity protection as well as Internet Key Exchange (IKE) protocols for keys derivations and authentications. All models provide similar security functionalities.

Figure 1: View of NetCrypt Series

The TOE comes with the following ports:

- 2 x Trusted Ports (T1 & T2, Gigabit NIC 10/100/1000Mbps Auto-sensing)
- 1 x External Port (Ext, Gigabit NIC 10/100/1000Mbps Auto-sensing) OR
- 1 x Management Port (Mgmt, Gigabit NIC 10/100/1000Mbps Auto-sensing)
- 1 x Console Port (RS232)

A total of 4 x network interface ports, of which two are dedicated for trusted (known as RED) network segments, one for the external and one for device management.

The two trusted (T1 & T2, known as RED) ports are connected to the internal network. All traffic within the trusted network segment is in clear.

The external port is connected to the public or untrusted network. All user traffic from Trusted (T1 and T2) network segment exiting from the external port is encrypted.

The management interface provides a physically controlled network segment where administrators could use to manage the TOE securely. Administrator account will require use of an external cryptographic token for 2-factor authentication.

The TOE has a built-in RS232 console port for the purpose of viewing port IP network verification and emergency erasure services as a last resort when access to device through network management is unsuccessful (e.g. loss of keys, misconfiguration that results in lockdown).

The TOE is interoperable with NetCrypt series of IP encryptor, allowing the TOE to form a secure VPN between itself and a peer TOE.

The TOE operates as a network layer encryption device. The evaluated configuration in this Security Target is a gateway-to-gateway configuration with only local management and KeyCrypt cryptographic token will be used for 2-factor authentication (no password-based authentication).

Deployment Use Case

The deployment scenario is as shown in Figure 2, where NetCrypt Family Series S20/R100/U1000/U2000 connects securely through the internet to reach the NetCrypt S20/R100/U1000/U2000 at the enterprise's backend network infrastructure. The internet/WAN network (black segment or untrusted network) is where all encrypted traffic traversed between NetCrypt Family Series S20/R100/U1000/U2000 and NetCrypt U1000/U2000, no clear traffic is allowed to pass through the black segment.

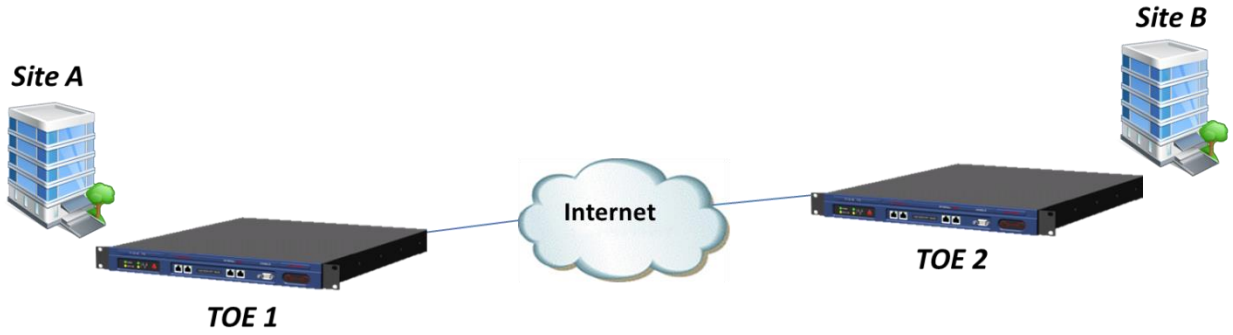


Figure 2: Deployment Scenario for NetCrypt Series

1.3.1 Non-TOE hardware/software/firmware required by the TOE

Items required by the TOE are as followed:

a. NetCrypt Administrative Management software (NetCrypt Admin), this is an application median where "Commands" are send to the TOE through input fields in Graphical User Interfaces

b. PKCS#11 Compliant USB Cryptographic token to be used for 2 factor authentication (KeyCrypt Cryptographic Token)

c. Another Peer TOE as described in this Security Target.

Please refer to Administrator Guide document for more details.

1.3.2 Physical Scope of the TOE

The physical scope of the TOE is defined by the hardware enclosure (mechanical housing) and internal circuitry (motherboard, daughterboard, flash storage) which provides the cryptographic functions for secure communication. The TOE is a hardware and software (firmware) solution. The TOE guidance documentation is also part of the TOE. The scope of delivery is as follow:

- TOE preparative and operative guidance (NETCRYPT FAMILY SERIES S20/R100/U1000/U2000 Administrator's Guide, Version 1.0.0 are provided in PDF format in CD delivered with TOE)
- The hardware appliance pre-installed with firmware version 2.6.4
  - ✓ NetCrypt S20
  - ✓ NetCrypt R100
  - ✓ NetCrypt U1000
  - ✓ NetCrypt U2000

The TOE shall be packaged in a sealed box and delivered via either:

- In-house delivery – for Local delivery (within Singapore)
- Trusted courier – for Overseas delivery

All software deliverables are burnt into a CD and delivered separately.

The TOE is shipped with a default factory configuration.

1.3.3 Logical Scope of the TOE

The TOE comprises of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. **Security Audit**

   The TOE is able to generate audit records of security-relevant events occurring on the TOE. Generated audit records include date and time stamp, event message. The TOE provides administrators with the ability to retrieve and view audit records stored within the TOE, where they are protected from unauthorised modification and deletion. The TOE has limited audit records storage capacity and it can only stores up to a maximum of 10,000 audit records, where the oldest audit records are then overwritten by new audit records.

2. **Cryptographic Support**

   The TOE implements cryptographic algorithms that provide key management, data encryption and decryption, RSA signature generation and verification, secure hashing and key-hashing features in support of higher level cryptographic protocols, including IKEv2 for keys derivations and authentications, and IPSec (ESP only) to provide confidentiality and integrity protections to data traffic.

3. **Identification and Authentication**

   The TOE requires administrators to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers a locally connected management interface (network port) for interactive administrative sessions.

   The TOE supports the local administration with 2-factor authentication (2FA) using an external cryptographic token (KeyCrypt).

4. **Security Management**

   TOE's security management functions are accessed using the TOE management application (NetCrypt Administrative Management software) via the Management port.

   An administrator may connect a workstation to the management port of the TOE and authenticate to it. Closing of the management software will terminate the interactive session.

   Access control of TOE's security management functions relies on assigned role for each user account.

   The TOE has a built-in RS232 console port which provides limited management functions.

5. **Protection of TOE**

   The TOE implements self-test (Cryptographic) is performed during initial startup to ensure its cryptographic functions are operating properly. The self-test may also be triggered by an authorised Administrator manually.

6. **Protection of User Data**

   User data sent from the trusted network segment within one TOE to the other TOE's trusted network segments is protected with confidentiality and integrity protections. The protection of user data is in accordance to the security policy defined within the TOE.

7. **Trusted Channels**

   The TOE provides secure IPSec communication channel between TOE and another peer TOE after successful device-to-device authentication through IKEv2 protocol.

1.4Terms and Acronyms

The following table describes the acronyms used in this document:

TERM	DEFINITION
2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSP	Critical Security Parameters
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
IPSEC	Internet Protocol Security
SA	Security Association
SP	Security Policy
SPI	Security Parameter Index
UDP	User Datagram Protocol
ESP	Encapsulating Security Payload
DH	Diffie-Hellman
ECP	Elliptic Curve Groups modulo a Prime (ECP Groups)
RSA	Rivest–Shamir–Adleman public-key cryptosystems

Chapter 2 – Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017. The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

The ST is package conformant to the package Evaluation Assurance Level EAL2.

2.2 Protection Profile Conformance

No Protection Profile claims.

Chapter 3 – Security Problem Definition

This chapter identifies the following:

- assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

3.1 Assets

AST.DATA
The primary asset is the data communications made between 2 parties (i.e. end points)

AST.TSF_DATA

Secondary assets are TOE configuration files and cryptographic keys used for authentication.

3.2 Threats

The following lists the threats addressed by the TOE and the IT Environment.

The TOE protects user data as primary asset by means of cryptographic functions. Thus, the cryptographic functions, their keys and CSP itself are also objects of attacks. These threats are defined here. In the following threat definition, the generic term "attacker" is used, which shall denote to either:

➢ An individual not being a user of the TOE trying to compromise AST.TSF_DATA and/or AST.DATA of any user of the TOE; or

➢ An authorised user of the TOE trying to compromise AST.TSF_DATA and/or AST.DATA of other users of the TOE, which this user is not authorised to access.

T.UNAUTHORISED_PEER

An unauthorised IT entity may impersonate as a legitimate communicating peer to establish a VPN communication channel with the TOE which leads to disclosure of AST.DATA.

T.EAVESDROP

An attacker eavesdrops on communication channel between parties over an untrusted network (e.g. Internet) which leads to unauthorised disclosure of AST.DATA.

T.UNAUTHORISED_UPDATE

An attacker installs or supplies to the Administrator an illegitimate firmware updated to the TOE The illegitimate firmware update of the TOE compromises the TSF allowing attackers to gain access to AST.DATA.

T.UNAUTHORISED_ADMINISTRATOR_ACCESS

An attacker may attempt to gain administrator access to the TOE by nefarious means such as masquerading as an administrator to the device, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session. Successfully gaining administrator rights allow access to AST.TSF_DATA and AST.DATA.

T.UNDETECTED_ACTIVITY

An attacker may attempt to access, change, and/or modify AST.TSF_DATA of the TOE without administrator awareness. These actions may remain undetected and thus their effects cannot be effectively mitigated.

T.MALFUNCTION

An attacker may use a malfunction of the TOE to deactivate, modify, or circumvent security functions of the TOE to enable attacks against the integrity or confidentiality of AST.DATA or AST.TSF_DATA.

3.3 Assumptions

This section describes the assumptions made in identification of the threats and security requirements for TOE.

A.TRUSTED_ADMIN

The Administrator(s) for the TOE are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation.

A.PHYSICAL_ENV

The provisioning and deployment of the TOE is at locations which are physically secured, and access controlled.

A.KEYCRYPT

KeyCrypt token provides appropriate protection for the 2-Factor Authentication keys.

A.TIME_STAMP

The environment in which the TOE operates in shall provide reliable time stamps

A.PEER_TOE

The TOE shall be configured only to communicate with another peer TOE.

3.4 Organizational Security Policy

There is no OSP.

Chapter 4 Security Objectives

This Chapter identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

4.1 Security Objectives for the TOE

The following subsections describe objectives for the TOE:

O.AUTHORISED_PEER

The TOE shall ensure it is communicating with an authorised peer TOE by authenticating the peer TOE before a VPN communication channel is established.

O.AUDIT

The TOE shall record a readable audit trail of security relevant events to assist in the detection of potential attacks on the TOE.

O.CORRECT_OPERATIONS

The TOE shall enter into a secure, non-operational state upon negative results of self-tests.

O.PROTECTED_COMMUNICATIONS

The TOE shall provide protected communication channel or path between TOE and peer TOE.

O.ACCESS_CONTROL

The TOE shall restrict the access of its management functions to Administrators only.

O.VERIFIABLE_UPDATES

The TOE shall ensure that any updates to the TOE can be verified by the Administrator to be unaltered and from a trusted source.

O.ADMIN_IDENT_AUTH

The TOE shall ensure that all Administrators are identified and authenticated before any administrative actions on the TOE can be performed.

4.2Security Objectives for the Operational Environment

The operational environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality. This part wise solution is called the security objectives for the operational environment and consists of a set of statements describing the goals that the operational environment should achieve.

This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures

OE.TRUSTED_ADMIN

The administrators are trusted, well trained and follow all administrator guidance.

OE.KEYCRYPT

The administrator uses a cryptographic token conforming to:

- JavaCard System Standard 2.2 Configuration Protection Profile, Version 1.0b EAL4+
- Secure Signature Creation device Protection Profile Type 2 v1.04 EAL4+
- Secure Signature Creation device Protection Profile Type 3 v1.05 EAL4+

OE.TIME_STAMP

The environment shall provide a reliable time stamp to the TOE.

OE.PHYSICAL_ENV

The physical environment of the provisioning and deployment site shall prevent unauthorised physical and logical access to the TOE.

OE.PEER_TOE

The administrator shall only configure the TOE to communicate with another peer TOE.

4.3Security Objectives Rationale

4.3.1 Threats

	T.UNAUTHORISED_PEER	T.EAVESDROP	T.UNAUTHORISED_UPDATE	T.UNATHORISED_ADMINISTRATOR_ACCESS	T.UNDETECTED_ACTIVITY	T.MALFUNCTION
O.AUTHORISED_PEER	✓					
O.AUDIT					✓	
O.CORRECT_OPERATIONS						✓
O.PROTECTED_COMMUNICATIONS		✓				
O.ACCESS_CONTROL				✓		
O.VERIFIABLE_UPDATES			✓			
O.ADMIN_IDENT_AUTH			✓	✓		
OE.TRUSTED_ADMIN				✓		
OE.KEYCRYPT				✓		
OE.TIME_STAMP					✓	
OE.PHYSICAL_ENV			✓	✓		

Figure 1 Mapping of Threats to Objectives

T.UNAUTHORISED_PEER

The threat T.UNAUTHORISED_PEER causes disclosure of user data when the TOE is unable to distinguish between a legitimate communicating peer and an illegitimate communicating peer. O.AUTHORISED_PEER requires that the TOE shall authenticate all peer TOE before setting up a VPN communication channel with the peer TOE upon which user data is transmitted to.

T.EAVESDROP

The threat T.EAVESDROP discloses user data communicated between parties by intercepting traffic transmitted over an untrusted network. The security objective O.PROTECTED_COMMUNICATIONS requires the TOE to establish a mutually authenticated secure channel prior to transmitting of user data traffic.

T.UNAUTHORISED_UPDATE

The threat T.UNAUTHORISED_UPDATE describes the replacement of legitimate TOE firmware with a malicious copy such that the TSFs which protect the user data is no longer effective. The security objective O.VERIFIABLE_UPDATES ensures that the installation package is from a trusted source and the package has not been tampered with. In addition, the environment objectives OE.PHYSICAL_ENV ensures the TOE is installed and operated in a secure physical environment such that no attackers are able to physically access the TOE to install the illegitimate firmware. O.ADMIN_IDENT_AUTH ensures that only identified and authenticated Administrators shall be able to perform the authorized update to the TOE.

T.UNAUTHORISED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain administrator access to the TOE by nefarious means such as masquerading as an administrator to the device or compromising the administrative session by performing man-in-the-middle attacks, which would provide access to the administrative session. O.ACCESS_CONTROL and O.ADMIN_IDENT_AUTH ensures that only identified and authenticated Administrators will be able to access the TOE and perform management functions.

In addition, the environment objectives OE.TRUSTED_ADMIN requires the authorised administrator to adhere to the guidance documents and not attempt to violate the security policies (e.g. configuring the TOE into the secure operating mode). OE.KEYCRYPT provides the protected platform on which the administrator's credentials resides on. OE.PHYSICAL_ENV ensures that the TOE is installed in a secure environment such that any unauthorized personnel shall be denied physical access to the TOE.

T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the TOE without administrator awareness. This could result in the TOE being compromised and the Administrator having no knowledge of it. The security objective O.AUDIT and OE.TIME_STAMP records a readable audit trail of security relevant events with accurate dates and times. Thus, assisting Administrators to be able to detect potential attacks on the TOE.

T.MALFUNCTION

A component of the TOE may fail during start-up or during operations causing a compromise or failure in the security functionality of the TOE, leaving the TOE susceptible to attackers. The security objective O.CORRECT_OPERATIONS prevents this by performing and verifying that the TOE's self-test has pass, indicating that TOE components are functional and operating correctly. Upon negative results of self-tests, the TOE shall enter a secure non-operational state.

4.3.2 Assumptions

	A.TRUSTED_ADMIN	A.PHYSICAL_ENV	A. KEYCRYPT	A.TIME_STAMP	A.PEER_TOE
OE.TRUSTED_ADMIN	✓				
OE.KEYCRYPT			✓		
OE.TIME_STAMP				✓	
OE.PHYSICAL_ENV		✓			
OE.PEER_TOE					✓

Figure 2 Mapping of Assumptions to Objectives for the Environment

A.TRUSTED_ADMIN

The assumption A.TRUSTED_ADMIN addresses the proficiency of the administrator such that they are appropriately trained, following policy, and adhering to guidance documentation. This assumption is directly and completely covered by the security objective for the environment OE.TRUSTED_ADMIN.

A.PHYSICAL_ENV

The assumption A.PHYSICAL_ENV addresses the physical security of the provisioning and deployment site. This assumption is directly and completely covered by the security objective for the environment OE.PHYSICAL_ENV where it assumes the deployment site is physically secured.

A.KEYCRYPT

The assumption A.KEYCRYPT refers to KeyCrypt cryptographic token that shall provide protection for the 2-factor authentication keys. OE.KEYCRYPT upheld this assumption that KeyCrypt Cryptographic token used to store the administrator's authentication keys is Common Criteria certified.

A.TIME_STAMP

The assumptions A.TIME_STAMP addresses the provision of reliable time stamp provided by the environment. OE.TIME_STAMP satisfies this assumption by ensuring that the environment where the TOE is installed in will provide reliable time stamp for the TOE.

A.PEER_TOE

The assumptions A.PEER_TOE addresses the setup of the TOE to communicate with another Peer TOE for IPSec communication. OE.PEER_TOE satisfies this assumption by ensuring that the administrator will configure the TOE to communicate only with another peer TOE.

Chapter 5 Extended Requirements

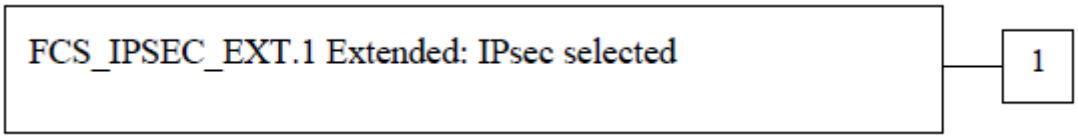
5.1Extended Components Definition

FCS_IPSEC_EXT Extended: IPsec selected

Family Behavior

This family addresses requirements for protecting communications using IPsec.

Component leveling



FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

Management:

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

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Failure to establish an IPsec SA

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to: No other components.

Dependencies:

FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)

FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)

FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

FCS_IPSEC_EXT.1 Extended: IPsec selected

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [*selection: tunnel mode, transport mode*].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithm [*selection: AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA2)-based HMAC (as specified by RFC 4868)*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection: IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [selection: no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers], and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 7296 (with mandatory support for NAT traversal as specified in section 2.23) and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: IKEv1, IKEv2] protocol uses the cryptographic algorithms AES-CBC-256 as specified in RFC 3602 and [selection: AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: IKEv2 SA lifetimes shall be established based on [selection: number of packets/number of bytes; length of time, where the time values shall not exceed: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]; IKEv1 SA lifetimes can be established based on [selection: number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: 24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP)), [assignment: other DH groups that are implemented by the TOE], no other DH groups].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: RSA, ECDSA] algorithm.

Chapter 6 - Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017 and all international interpretations.

6.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with ***bold italicized*** text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with *italicized* text;
- Iteration: Indicated by appending the iteration symbol.

  e.g. FCS_COP.1/AES, FCS_COP.1/RSA

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

6.2 Security Functional Requirements (SFRs)

6.2.1 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* level of audit; and

c) Refer to Appendix A for the list of all auditable events

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), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***no other audit relevant information***.

6.2.2 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

6.2.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide ***Administrators*** with the capability to read ***Device Management Logs, Key Exchange Logs and Packet Processing Logs*** 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.

6.2.4 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***RSA cryptographic key pair generation*** and specified cryptographic key sizes ***2048-bits and 4096-bits*** that meet the following: ***PKCS#1 standard (Version 1.5), SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms (Version 1.0), Chapter 4 Asymmetric Atomic Primitives***.

Application Note: The RSA key pair defined is used for signing purposes.

6.2.5 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*** that meets the following: ***none.***

6.2.6 FCS_COP.1/Data Encryption/Decryption - Cryptographic operation

FCS_COP.1.1/Data Encryption/Decryption
The TSF shall perform ***data encryption and decryption*** in accordance with a specified cryptographic algorithm ***AES used in CBC mode*** and cryptographic key sizes ***256 bits*** that meet the following: ***FIPS PUB 197 "Advanced Encryption Standard (AES)"***.

Application note: Used to protect device key within the non-volatile memory, IKEv2 and IPsec.

6.2.7 FCS_COP.1/Cryptographic Signature - Cryptographic operation

FCS_COP.1.1/Cryptographic Signature
The TSF shall perform ***cryptographic signature services (generation and verification)*** in accordance with a specified cryptographic algorithm ***RSA (digital signature)*** and cryptographic key sizes ***2048 bits and 4096 bits*** that meet the following: ***PKCS#1***.

Application note: Used to protect IKEv2 and NetCrypt management communication

6.2.8 FCS_COP.1/Cryptographic Hashing - Cryptographic operation

FCS_COP.1.1/Cryptographic Hashing
The TSF shall perform ***cryptographic hashing*** in accordance with a specified cryptographic algorithm ***SHA-2*** and message digest sizes ***256 and 512 bits*** that meet the following: ***FIPS PUB 180-4, "Secure Hash Standard".***

Application note: Used for signature algorithm for IKEv2 and NetCrypt management communication

6.2.9 FCS_COP.1/Keyed-hash Message Authentication - Cryptographic operation

FCS_COP.1.1/Keyed-hash Message Authentication
The TSF shall perform ***keyed-hash message authentication*** in accordance with a specified cryptographic algorithm ***HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512*** and cryptographic key size ***256, 384, 512 bits used in HMAC*** and message digest sizes ***256, 384, 512 bits*** that meet the following: ***FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code", and FIPS Pub 180-3, "Secure Hash Standard".***

Application note: Used for integrity/PRF algorithm for IKEv2 and NetCrypt management communication, IPsec (data integrity protection)

6.2.10 FCS_IPSEC_EXT.1 – IPSEC Selected

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement *tunnel mode*.

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using *the cryptographic algorithms AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA2)-based HMAC (as specified by RFC 4868).*

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: *IKEv2 as defined in RFCs7296 with mandatory support for NAT traversal as specified in section 2.23, and RFC 4868 for hash functions*.

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the *IKEv2* protocol uses the cryptographic algorithms *AES-CBC-256* as specified in RFC 3602 and *no other algorithm*.

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that *IKEv2 SA lifetimes shall be established based on number of packets/number of bytes; length of time, where the time values shall not exceed: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*.

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP) *and* ***16 (4096-bit MODP) and 21 (521-bit Random ECP)***.

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the *RSA* algorithm.

6.2.11 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the ***VPN SFP*** on

Subjects:

- ***Source Subjects: TOE interface (Trusted ports) on which User information is received***
- ***Destination Subjects: TOE interface (External port) on which User information is destined***

Information: User data traffic sent through the TOE's Trusted and External interface port

Operations: Encrypt, decrypt, or deny information.

6.2.12 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the ***VPN SFP*** based on the following types of subject and information security attributes:

Subjects:

- ***Source Subjects: TOE interface (Trusted ports) on which User information is received***
- ***Destination Subjects: TOE interface (External port) on which User information is destined***

Information: User data traffic sent through the TOE's Trusted and External interface port
Information Security attributes: Source IP address, Destination IP address, IP protocol (only ESP), UDP destination port 4500, Security Policy of TOE

FDP_IFF.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:

Receiving from Source Subjects (on Trusted interface), Sending to Destination Subjects (through External interface):

- ***The IP packet contains an authorised source and destination IP addresses***
- ***The TSF can find an associated Security Association (SA) using the destination IP addresses of the IP packet***

Receiving from Destination Subjects (on External interface), Sending to Source Subjects (through Trusted interface):

- ***UDP 4500 for IPsec traffic***
- ***If the IPSec packet contains a SPI (within ESP header)***
  – The TSF can find an associated Security Association (SA) using the SPI within the IPSec packet
- ***The IP packet has been properly protected according to the SA referred by the associated SA***
- ***The decrypted IP packet contains an authorised source and destination IP addresses***

FDP_IFF.1.3 The TSF shall enforce the ***following additional rules: None.***

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: ***None***.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: ***None.***

6.2.13 FIA_USB.1 User-subject Binding

FIA_USB.1.1 the TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

(1) User Account ID

(2) User certificate subject distinguished name

(3) Issuer distinguished name (CA)

(4) Role

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on behalf of users: ***the initial role of the user is Unidentified user***.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on behalf of users:

(1) the subject attribute Role shall be changed from Unidentified user to Unauthenticated user after successful identification.

(2) after successful authentication the subject attribute Role shall be changed from Unauthenticated User to an administrator role.

6.2.14 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

(1) User Account ID

(2) User certificate subject distinguished name

(3) Role

6.2.15 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow ***none*** on behalf of the user to be performed before the **user** is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.16 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow:

1. Identification according to FIA_UID.1;

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.17 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1 The TSF shall restrict the ability to *determine the behavior of, and modify the behavior of* the functions:

- ***Add/Remove Administrator account***
- ***Import Administrator Public certificate***
- ***Synchronize the system date and time***
- ***Change Root Account password or Disable Root Account***
- ***Select the cryptographic suite employed***
- ***Configure port IP addresses***
- ***Configure device routing table***
- ***Delete, add, or modify communicating peers***
- ***Import Peer Public certificate***
- ***Import/generate/purge Device keys (for TOE-TOE authentication)***
- ***Import Root CA Public certificate***
- ***Export Device Public certificate***
- ***Configure audit behavior, view, or purge audit trail***
- ***View firmware information***
- ***Initiate cryptographic self-test***

to ***Administrators***

6.2.18 FMT_MTD.1 Management of TSF Data

FMT_MTD.1 The TSF shall restrict the ability to ***Import, Export, Add, synchronize, view,*** *delete, clear, change_default, modify* the ***TSF data (refer to the table below)*** to ***Administrators.***

Roles	***Operations***	***TSF Data***
Administrator	***Import,*** *delete*	***Device Key***
	Import, *delete*	***Peer Public certificate***
	Add*, delete*	***Administrator account ID***
	Import, *delete*	***Administrator Token Public certificate***
	Export, *delete*	***Device Public certificate***
	synchronize	***Date and time***
	View, *clear*	***Audit logs***
	change_default, modify, ***view***	***Configuration data (IP address, cryptographic suite, routing table)***

6.2.19 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the ***VPN SFP*** to restrict the ability to *change_default, modify, delete,* the security attributes: ***information flow rule defined in FDP_IFF.1*** to ***Administrators.***

6.2.20 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the ***VPN SFP*** to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***Administrator*** to specify alternative initial values to override the default values when an object or information is created.

6.2.21 FMT_SMF.1 Specification of Management Functions

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

- ***Add/Remove Administrator account***
- ***Import Administrator Public certificate***
- ***Update the TOE firmware***
- ***Synchronize the system date and time***
- ***Factory reset***
- ***Factory boot with firmware upgrade***
- ***Change Root Account password or Disable Root Account***
- ***Perform emergency erasure***
- ***Select the cryptographic suite employed***
- ***View and configure port IP addresses***
- ***Configure device routing table***
- ***Delete, add, or modify communicating peers***
- ***Import Peer Public certificate***
- ***Import/generate/purge Device keys (for TOE-TOE authentication)***
- ***Import Root CA Public certificate***
- ***Export Device Public certificate***
- ***Configure audit behavior, view, or purge audit trail***
- ***View firmware information***
- ***Initiate cryptographic self-test***

6.2.22 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles:

- ***Unidentified user***
- ***Unauthenticated user***
- ***Administrator***

Application Note:

1. ***Unidentified user – A user not being identified***
2. ***Unauthenticated user – An identified user not being authenticated***

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

6.2.23 FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: ***negative results of self-tests***.

Application note: In the secure state (TOE in non-operational mode), all input and output through the network interface ports are disabled. As an indicator of self-test failure, the alarm LED would be activated.

6.2.24 FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self-tests *during initial start-up and at the request of the authorised User* to demonstrate the correct operation of**:**

- ***Cryptographic operation (FCS_COP.1/Data Encryption/Decryption)***

FPT_TST.1.2
The TSF shall provide authorised users with the capability to verify the integrity of ***none.***

FPT_TST.1.3
The TSF shall provide the capability to verify the integrity of ***none***.
Application Note: Crypto test is performed on all symmetric encryption (FCS_COP.1/Encryption/Decryption) and HMAC (KAT according to FIPS 140-2).

6.2.25 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.26 FTP_ITC.1 Inter-TSF trusted channels

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and **peer TOE** 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 *the TSF***, peer TOE** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***peer TOE authentication functions and VPN connections.***

6.3 Security Requirements Rationale

6.3.1 Security Objectives for the TOE

O.AUTHORISED_PEER

The security objective O.AUTHORISED_PEER requires the TOE to provide the means to ensure it is communicating with an authorised peer TOE by authenticating the peer TOE before a VPN communication channel is established. This objective is provided by the SFRs:

- FCS_CKM.1 and FCS_IPSEC_EXT.1 ensures that cryptographic keys used for TOE-to-TOE authentication are generated and used for signing and verification purposes during Diffie-Hellman key exchange.

- FCS_COP.1/Data Encryption/Decryption, FCS_COP.1/Cryptographic Signature, FCS_COP.1/Cryptographic Hashing, FCS_COP.1/Keyed-hash Message Authentication collectively implements the underlying cryptographic protection during key exchange (IKEv2).
- FMT_MTD.1 provides the functionality to import Device Key, Peer public certificate and Root CA public certificate, and export Device public certificate. All of which are used during TOE-to-TOE authentication during key exchange.

O.AUDIT

The security objective O.AUDIT requires the TOE to provide a readable audit trail of security relevant events to assist in the detection of potential attacks on the TOE. This objective is provided by the SFRs:

- FAU_GEN.1 ensures that the TOE shall generate audit logs (Device management, Key management and packet processing) for auditable events as according to Appendix A.
- FAU_SAR.1 ensures that the TOE shall provide Administrators with the capability to view the audit records.
- FAU_STG.1 ensures that the audit log shall be protected from unauthorised deletion.
- FMT_MOF.1 ensures that only authenticated Administrators shall have access to the audit logs

O.CORRECT_OPERATIONS

The security objective O.CORRECT_OPERATIONS requires the TOE to perform self-test and enter into a secure, non-operational state upon negative results of self-tests. This is provided by the SFRs:

- FPT_TST.1 ensures the TOE performs self-test on the cryptographic functions to ensure cryptographic operations of the TOE are sound and functional.
- FPT_FLS.1 requires the TSF to preserve a secure state when self-test fails.

O.PROTECTED_COMMUNICATIONS

The security objective O.PROTECTED_COMMUNICATIONS requires the TOE to provide protected communication channel between: TOE-to-TOE. This is provided by the following SFRs:

- FTP_ITC.1 enforces a trusted channel upon which user data traffic is exchanged between the communicating TOEs.
- FCS_COP.1/Data Encryption/Decryption and FCS_COP.1/Keyed-hash Message Authentication collectively implements the underlying cryptographic protection (confidentiality and integrity) providing a trusted communication channel between TOE and peer TOE.
- FDP_IFC.1 and FDP_IFF.1 enforces information flow control when subjects exchange data traffic between the TOEs based on the security attributes presented at each interface (Trusted, External). Information (user data) permitted shall be protected according to the SA and security policy defined within the TOE and sent to peer TOE via the secure communication channel (IPsec) established. All user data that traverse through this channel is protected with confidentiality and integrity protection. Information not permitted based on the security attributes defined shall be dropped/denied.
- FMT_MTD.1, FMT_MSA.1, FMT_MSA.3 ensure only authenticated administrator shall be able to access and modify, delete, add, change default, import, export,

synchronize the TSF data or security attributes of the TOE via the management functions provided under FMT_MOF.1 and FMT_SMF.1.

- FCS_CKM.4 ensures that all transient keys that were generated during the IKEv2 key exchange and IPSec are removed after the session is finished.

O. ACCESS_CONTROL

The objective O.ACCESS_CONTROL ensures that the TOE shall restrict the access of its management functions to Administrators only. This is provided by the following SFRs:

- FMT_SMR.1, FMT_MTD.1, FMT_MSA.1, FMT_MSA.3 ensure that only administrator is able to access and modify, delete, add, change default, import, export, synchronize the TSF data or security attributes of the TOE via the management functions provided under FMT_MOF.1 and FMT_SMF.1.
- FTA_SSL.4 ensures that Administrators are able to terminate their secure session with the TOE to prevent any potential attackers from exploiting an unclosed session and gaining access to the TOE management functions.

O.VERIFIABLE_UPDATES

The objective O.VERIFIABLE_UPDATES ensure that any updates to the TOE can be verified by the Administrator through the TOE to be unaltered and from a trusted source. This is provided by the following SFRs:

- FCS_COP.1/Cryptographic Signature ensures the package is signed by the trusted source and its integrity is not violated.

O. ADMIN_IDENT_AUTH

The security objective O.ADMIN_IDENT_AUTH requires that all Administrators are identified and authenticated before any administrative actions on the TOE can be performed. This security objective is provided by the following SFRs:

- FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1 ensure that only Administrators are able to add or create Administrator accounts.
- FIA_UID.1 and FIA_UAU.1 ensures that management functions of the TOE may be performed (via NetCrpyt Administrative Management application) only after successful identification and authentication.
- FIA_ATD.1 ensures security attributes to individual users including
  User certificate subject distinguished name and Role as prerequisite for identification and authentication of authorized users is maintained.
- FIA_USB.1 ensures the user certificate subject distinguished name, issuer distinguished name and the role are associated with the subjects acting for the authenticated user.

6.3.2 Dependencies

6.3.2.1 SFRs Dependencies

Requirements	Dependencies	Inclusion/Rational for non-inclusion
FAU_GEN.1 Audit Data Generation	FPT_STM.1 Reliable Time Stamps	The environment in which the TOE operates in shall provide reliable time stamps. This can be configured using an NTP server connected locally to the TOE trusted network.
FAU_ STG.1 Protected Audit Trail Storage	FAU_GEN.1 Audit Data Generation	FAU_GEN.1
FAU_SAR.1 Audit Review	FAU_GEN.1 Audit Data Generation	FAU_GEN.1
FCS_CKM.1 Cryptographic Key Generation	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/Cryptographic Signature, FCS_CKM.4
FCS_CKM.4 Cryptographic Key Destruction	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1, FCS_IPSEC_EXT.1.5 and FCS_IPSEC_EXT.1.9 explains the key derivation from IKEv2 based on diffie-hellman key exchange
FCS_COP.1 Data Encryption/Decryption	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4. FCS_IPSEC_EXT.1.5 and FCS_IPSEC_EXT.1.9 explains the key derivation from IKEv2 based on diffie-hellman key exchange and hence FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 are not relevant.
FCS_COP.1 Cryptographic Signature	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1, FCS_CKM.4
FCS_COP.1 Cryptographic Hashing	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key	FCS_CKM.4 FCS_CKM.1 not met – keys are not required for hashing.

	destruction	
FCS_COP.1 Keyed-hash Message Authentication	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4, FCS_IPSEC_EXT.1.5 and FCS_IPSEC_EXT.1.9 explains the key derivation from IKEv2 based on diffie-hellman key exchange and hence FDP_ITC.1, FDP_ITC.2 and FCS_CKM.1 are not relevant.
FCS_IPSEC_EXT.1 IPsec Selected	FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys) FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption) FCS_COP.1(b) Cryptographic Operation (for signature generation/verification) FCS_COP.1(c) Cryptographic Operation (Hash Algorithm) FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)	FCS_CKM.1, FCS_COP.1/Data Encryption/Decryption, FCS_COP.1/Cryptographic Signature, FCS_COP.1/Cryptographic Hashing, FCS_COP.1/Keyed-hash Message Authentication
FDP_IFF.1 Simple Security Attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.1 FMT_MSA.3
FDP_IFC.1 Subset information flow control	FDP_IFF.1 Simple security attributes	FDP_IFF.1
FIA_USB.1 User-subject Binding	FIA_ATD.1 User attribute definition	FIA_ATD.1
FIA_ATD.1 User attribute definition	No Dependencies	-
FIA_UID.1 Timing of Identification	No Dependencies	-
FIA_UAU.1 Timing of Authentication	FIA_UID.1 Timing of Identification	FIA_UID.1
FPT_FLS.1 Failure with preservation of secure state	No Dependencies	-
FMT_MOF.1 Management of security functions behaviour	FMT_SMF.1 Specification of Management Functions, FMT_SMR.1 Security roles	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1 Management of Security Attributes	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of	FDP_IFC.1, FMT_SMR.1, FMT_SMF.1

	Management Functions	
FMT_MSA.3 Static Attribute Initialisation	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1 Specification of Management Functions	No Dependencies	-
FMT_SMR.1 Security Roles	FIA_UID.1 Administrator Identification	FIA_UID.1
FPT_TST.1 TSF Testing	No Dependencies	-
FTA_SSL.4 User-initiated Termination	No Dependencies	-
FTP_ITC.1 Inter-TSF trusted channel	No Dependencies	-

Table 1 SFRs Dependencies

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2 components, as specified in (CC) part 3. No operations are applied to the assurance components.

The assurance components are summarised in the table below.

Assurance Class	**Assurance components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.4.1 Rational for Security Assurance Requirements

The evaluation assurance package selected for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2). EAL2 was chosen to provide a low to moderate level of assurance that is consistent with commercial products of this sort. The chosen assurance level is appropriate with the threats defined for the environment (physical protection by the environment, limited interface and access to the TOE).

Chapter 7 TOE Summary Specification

7.1 Security Audit

7.1.1 Audit Selection and Generation

The TOE relies on the environment (NTP server connected to the Trusted network segment) to provide the reliable date & time for the audit logs stored the storage area. The logs provide an audit trail of all security relevant events with corresponding dates and time. Any potential attacks in the form of malicious administration of TOE may be traced.

The TOE maintains 3 separate audit logs classification:

- Device Management store
- Key Exchange store
- Packet Processing store

Each classification has limited audit records storage capacity which can only store up to a maximum of 10,000 audit records. The oldest audit records are then overwritten by new audit records. Only authenticated administrators may view the audit logs using NetCrypt Administrative Management application.

This TSF is mapped to the following SFRs: FAU_GEN.1, FAU_SAR.1, FMT_MOF.1

7.1.2 Preventing Audit Data Loss

The TSF shall provide listing of audit information from the stored audit logs in the audit trail to Administrators only. With defined access control to the TOE, the stored audit records in the audit trail are protected from unauthorised deletion. Any modification of Audit logs is not possible. Only authenticated Administrators may perform deletion of the audit logs.

This TSF is mapped to the following SFRs: FAU_STG.1, FMT_MOF.1

7.2 Cryptographic Support

The TOE provides cryptographic functions such as RSA digital signature and verification, symmetric data encryption/decryption and integrity verification using secure hashing. All defined cryptographic functions use algorithm and key sizes as specified in the security policy of the TOE (during TOE configuration). The cryptographic support provided by the TOE is defined as follow:

- Cryptographic Operations
- Cryptographic Keys Generation
- Cryptographic Keys Destruction by Zeroization

The table below summarizes the cryptographic operations and SFRs mapping.

7.2.1 Cryptographic Operations

IPSEC				
	Service	**Method**	**Standard**	**SFR**
ESP	Authentication and Encryption	AES-256 CBC	AES: FIPS 197	FCS_COP.1/Data Encryption/Decryption, FCS_IPSEC_EXT.1

IKEv2				
	Service	**Method**	**Standard**	**SFR**
Messages	Encryption	AES-256 CBC	AES: FIPS 197	FCS_COP.1/Data Encryption/Decryption
Messages	Authentication	HMAC-SHA-256, HMAC-SHA-382, HMAC-SHA- 512	HMAC: FIPS 198-1, 180-3	FCS_COP.1/Keyed-hash Message Authentication
Peer Authentication	Signature services (RSA)	RSA signing	PKCS#1	FCS_COP.1/Cryptographic Signature
Peer Authentication	Hash for signatures	SHA-256 bits, 512 bits	FIPS 180-4	FCS_COP.1/Cryptographic Hashing

7.2.2 Cryptographic Keys Generation

Key	**Used For**	**Key Size (Bit)**	**Key Generation Standard**	**SFR**
RSA	Device Authentication	2048 or 4096	PKCS#1	FCS_CKM.1/ Cryptographic Key Generation

7.2.3 Cryptographic Key Destruction by Zeroization

The TOE destroys cryptographic keys in the memory by overwriting the specific memory with zeroes. This happens in the following events: Expiration of IPsec sessions keys or purging of shared secret and derived keys after DH key exchange.
This TSF is mapped to the following SFRs: FCS_CKM.4

7.3 Identification and Authentication

The TOE requires administrators to be successfully identified and authenticated before they can access the security management functions within the TOE. The TOE offers a locally connected management interface (network port) for interactive administrative sessions.

The TOE supports the local administration of the TOE where Administrators are required to present an external Administrator cryptographic token (KeyCrypt) to access the TOE. No access to the TOE shall be granted until Administrators have been successfully identified using the User Account ID and authenticated using the Administrator cryptographic token.

The Administrator cryptographic token contains the administrator's certificate and is used to identified itself based on the user certificate subject distinguished name and issuer distinguished name, together with the User Account ID which were defined within TOE during the configuration phase. Once the User Account ID, user certificate subject distinguished name and issuer distinguished name are identified, the cryptographic token would then perform cryptographic signing operation over exchanged handshake with the TOE, allowing the TOE to verify the authenticity of the administrator.

This TSF is mapped to the following SFR: FIA_UID.1, FIA_UAU.1, FIA_USB.1, FIA_ATD.1, FCS_COP.1/Cryptographic Signature.

7.4 Security Management

The TOE provides the management functions to only authenticated Administrators as shown below:

- Add/Remove Administrator account
- Import Administrator Public certificate
- Update the TOE firmware
- Synchronize the system date and time
- Factory reset
- Factory boot with firmware upgrade
- Change Root Account password or Disable Root Account
- Perform emergency erasure
- Select the cryptographic suite employed
- View and configure port IP addresses
- Configure device routing table
- Delete, add or modify communicating peers
- Import Peer Public certificate
- Import/generate/purge Device keys (for TOE-TOE authentication)
- Import Root CA Public certificate
- Export Device Public certificate
- Configure audit behavior, view or purge audit trail
- View firmware information
- Initiate cryptographic self-test

These functions may be access using NetCrypt Administrative Management application where

an interactive session from NetCrypt Administrative Management application to the TOE is setup. Closing of the software application by the Administrator will terminate the interactive session.

Administrators who have physical access to the TOE may connect to the console port (RS232) and have access to the following functions:

- View port IP addresses
- Emergency erasure
- Factory reset
- Factory boot with firmware upgrade

This TSF is mapped to the following SFRs: FMT_MOF.1, FMT_SMF.1, FMT_MTD.1, FMT_SMR.2, FTA_SSL.4.

7.5 User Data Protection

User data sent from the trusted network segment within one TOE to the other TOE's trusted network segments is protected with confidentiality (AES 256 CBC mode encryption) and integrity protections (HMAC SHA256, HMAC SHA384 or HMAC SHA512). The protection (IPsec) of user data is in accordance to the security policy (SP) defined within the TOE. This includes the security policy that defines the security attributes such as source IP address, destination IP address and cryptographic suite employed.

When receiving user data (on Trusted interface) to be sent to destination subjects (through External interface), the TOE shall ensure the following:

- The IP packet contains an authorised source and destination IP addresses
- The TSF can find an associated Security Association (SA) using the destination IP addresses of the IP packet

The TOE shall proceed to protect the received user data as according to the SP before sending to peer TOE.

When the encrypted user data is received by the peer TOE, the peer TOE shall ensure the following:

- Received data is using UDP port 4500 or IP Protocol 50 (ESP) for IPsec traffic
- If the IPSec packet contains a SPI (within ESP header)
  – The TSF can find an associated Security Association (SA) using the SPI within the IPSec packet
- The IP packet has been properly protected according to the SA referred by the associated SA
- The decrypted IP packet contains an authorised source and destination IP addresses

All received user data that does not fulfil the above mentioned requirement shall be dropped/denied.

Within the TOE, all processes are allocated separate memory locations within the RAM. Whenever memory is deallocated it is flushed of data. The TOE accounts for all packets (user data traffic) traversing the TOE in relation to the associated information stream. Therefore, no residual information relating to other packets will be reused on that stream.

This TSF is mapped to the following SFR: FCS_COP.1/Data Encryption/Decryption, FCS_COP.1/Keyed-hash Message Authentication, FDP_IFF.1, FDP_IFC.1, FCS_IPSEC_EXT.1.

7.6 Protection of the TSF

The TOE performs a cryptographic self-test during initial start-up or at request of authorised Administrator to ensure that this critical security function is functional. The self-test performed includes cryptographic algorithms Known Answer Test for AES256, SHA2 and HMAC.

In the event of self-tests failure, the TOE will enter a secure state (TOE in non-operational mode), all input and output through the network interface ports are disabled. As an indicator of self-test failure, the alarm LED would be activated. TOE may recover only after self-test passes.

Trusted firmware update is verified by the TOE through the digital signature verification. In the event of negative result of the digital signature verification, the firmware will be discarded and not installed by the TOE.

This TSF is mapped to the following SFR: FPT_TST.1, FPT_FLS.1, FCS_COP.1/Cryptographic Signature.

7.7 Trusted Channels

The TOE provides provide secure IPSec (AES 256 CBC together with SHA2 based HMAC cryptographic algorithms). communication between TOE and another peer TOE after successful device-to-device authentication using IKEv2 protocol.

During TOE provisioning, a RSA cryptographic key (2048 bits or 4096 bits) is generated within the TOE for signing purposes during TOE-to-TOE authentication. The Key exchange protocol used is IKEv2 as according to RFC7296. During the initial phase of key exchange, Diffie-Hellman key exchange with 4096 bits or ECP P521 bits may be used to generate the shared secret on both TOE. After which, it will be sent through a key expansion function to derive multiple keys for different purposes (encryption, integrity protection, authentication, signing and derivation of further key materials). Using this set of derived keys, the TOE performs data encryption/decryption (AES 256 CBC), data integrity protection (HMAC) of key exchange data. During key exchange, the cryptographic hash (SHA 2 256 or 512 bits) is used in conjuncture with the RSA key for signing and authentication purposes. Also, the keyed hash message authentication (HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) is used to protect the integrity of the data (as according the PRF algorithm defined in RFC7296) during key exchange. Upon successful key exchange, an IPsec tunnel between TOEs is created and the generated IPsec session keys shall be used for encryption/decryption (AES 256 CBC) of user data. The maximum IKEv2 SA lifetime is limited to 24 hours for phase 1 SAs and 8 hours for phase 2 SAs.

This TSF is mapped to the following SFR: FTP_ITC.1, FCS_COP.1/Data Encryption/Decryption, FCS_COP.1/Cryptographic Signature, FCS_COP.1/Cryptographic hashing, FCS_COP.1/Keyed-hash Message Authentication, FCS_IPSEC_EXT.1

APPENDIX A

1. List of Audit Logs

Log Types	Status/Errors	Meaning
Key Management	Initiating IKE SA to x.x.x.x	Starting of the key exchange protocol with another trusted IT device
Key Management	SA Init Established (I)	Initiator successfully completed the key exchange protocol with another trusted IT device
Key Management	SA Init Established (R)	Responder successfully completed the key exchange protocol with another trusted IT device
Key Management	Child SA (I) Established	Initiator successfully completed the traffic key exchange protocol with another trusted IT device
Key Management	Child SA (R) Established	Responder successfully completed the traffic key exchange protocol with another trusted IT device
Key Management	Receiving DPD request from x.x.x.x and sending acknowledgement	Device receiving dead peer detection heartbeat from another trusted IT device.
Key Management	Sending DPD request to x.x.x.x	Device receiving dead peer detection heartbeat from another trusted IT device.
Key Management	Passed CRL retrieval from Directory server	Device successfully retrieve CRL from Directory server
Key Management	Failed to retrieve CRL from Directory server	Device failed to retrieve CRL from Directory server
Key Management	Peer ID certificate criteria don't match	Certificate credentials of peer device does not match with current device's configuration
Key Management	Unsupported Authentication method 1	This error is mostly related to the above error "Peer ID certificate criteria don't match"

Key Management	Failed to public decrypt Auth data	Likely to be caused by non-matching RSA key pair
Key Management	Packet failed Authentication verification	This error is mostly related to the above error “Packet failed Authentication verification”
Key Management	Failed to allocate/decode payload	Unable to decipher IKE payloads
Key Management	Unsupported exchange type xx in message. Is transport key used?	1. Unknown or unsupported exchange type 2. Check if is Group Transport Key is used
Key Management	No proposal chosen	Maybe caused by unsupported encryption/ integrity algorithm or group key type
Device Management	Administrative user (xxx) denied access as userid is not defined as administrative account	Correct token , user account is undefined.
Device Management	Administrative user (xxx) denied access as authentication failed, account tentatively locked until (Date/time) (consecutive failure attempts = 1) Specified extended authentication user identity or password is incorrect.	Correct token and PIN, correct user account but wrong account password.
Device Management	The specified PIN is incorrect (i.e. does not match the PIN stored in token) attempt to authenticate user failed	Correct token, correct user account but wrong PIN. Note that this message will not be logged as it only appear as a temporary message box.
Device Management	Admin account (xxx) from (xxx.xxx.xxx.xxx) passed extended authentication	For successful login to TOE via its management port. Where xxx.xxx.xxx.xxx is the IP address and xxx is the account user
Device Management	Received request to load policy from admin1 (xxx.xxx.xxx.xxx)	Committing configuration changes to TOE. Where xxx.xxx.xxx.xxx is the IP address.
Packet Processing	Eth(x) : link up	When port eth(x) is connected
Packet	Eth(x) : link down	When port eth(x) is disconnected

Processing		
Packet Processing	System start-up	System boot-up
Packet Processing	System shutdown	System is shutting down.