CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN Security Target

Version 0.7
January 7, 2021

Prepared for:

CommScope Technologies LLC
130 Holger Way
San Jose, CA 95134

Prepared By:

Gossamer
Laboratories
www.gossamersec.com

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is the Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN provided by CommScope Technologies LLC. The TOE is being evaluated as a VPN Gateway device.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN Security Target

ST Version – Version 0.7

ST Date – January 7, 2021

1.2 TOE Reference

TOE Identification – CommScope Technologies LLC Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN, including the following ICX series and models: ICX 7450 (ICX 7450-24, ICX 7450-24P, ICX 7450-48, ICX 7450-48P, ICX 7450-48F) with the IPsec VPN module (FastIron Service Module FPGA version 2.09)

TOE Developer – CommScope Technologies LLC

Evaluation Sponsor – CommScope Technologies LLC

1.3 TOE Overview

The Target of Evaluation (TOE) is the CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN products including the following series and models: ICX 7450 (ICX 7450-24, ICX 7450-24P, ICX 7450-48, ICX 7450-48P, ICX 7450-48F) with the IPsec VPN module. The TOE is being evaluated as a VPN Gateway and provides IPsec services to its clients. The optional IPsec VPN Module must be included to be in the evaluated configuration. The IPsec VPN Module is a FPGA module that is embedded when the optional IPsec VPN Module is purchased.

The TOE is composed of a hardware appliance with embedded software installed on a management processor. The software controls the switching and routing network frames and packets among the connections available on the hardware appliances.

All TOE appliances are configured at the factory with default parameters to allow immediate use of the system's basic features through its Command Line Interface (CLI). However, the product should be configured in accordance with the evaluated configuration prior to being placed into operation. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using IPsec. This remote management interface is protected using encryption as explained later in this ST.

The hardware platforms that support the TOE have a number of common hardware characteristics:

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operations
- Flash memory, used to store the operating system image
- Non-volatile memory, which stores configuration parameters used to initialize the system at system startup
- Multiple physical network interfaces either fixed in configuration or removable as in a chassis-based product

1.4 TOE Description

The Target of Evaluation (TOE) is the CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN including the following ICX series and models: ICX 7450 (ICX 7450-24, ICX 7450-24P, ICX 7450-48, ICX 7450-48P, ICX 7450-48F) with the IPsec VPN module (FastIron Service Module FPGA version 2.09).

While there are different models in the series, they differ primarily in physical form factor, number and types of connections and slots, and relative performance. The ICX Series possesses between 24 and 48 10/100/1000 Mbps RJ-45 ports, and the presence of "F" in the model number indicates 100/1000 Mbps SFP ports instead of RJ-45 ports and the presence of "P" indicates that the RJ-45 ports are PoE+. While there are some functional differences among the families, they each provide the same security characteristics as claimed in this security target. The ICX 7450 Series utilizes a Quad-core ARM Cortex A9 1GHz (ARMv7-A architecture).

The ICX 7450 utilizes the Firmware crypto library referred to as the BRCD-IP-CRYPTO-VER-4.0 running on the A9, and the "FastIron Service Module FPGA" crypto library running within the IPsec VPN module.

1.4.1 TOE Architecture

The basic architecture of each TOE appliance begins with a hardware appliance with physical network connections. Within the hardware appliance the ICX is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions). ICX enforces applicable VPN Gateway security policies on network information flowing through the hardware appliance.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface.

1.4.1.1 Physical Boundaries

Each TOE appliance runs the 8.0.95 version of the Ruckus FastIron software and has physical network connections to its environment to facilitate routing and switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in an environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE can be configured to synchronize its internal clock using an NTP server in the operational environment.

The use of external authentication services such as RADIUS is supported with protection using IPsec.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by the Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Packet Filtering
- Protection of the TSF
- TOE access
- Trusted path/channels

1.4.1.2.1 Security audit

The TOE is able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using IPsec to protect the logs while in transit on the network.

1.4.1.2.2 Cryptographic support

The TOE contains a CAVP-tested cryptographic module that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher-level cryptographic protocols including IPsec.

1.4.1.2.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching/routing rules. It provides the ability to both assign attributes (user names, passwords and privilege levels) and to authenticate users against these attributes.

1.4.1.2.4 Security management

The TOE provides Command Line Interface (CLI) commands to access the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Super User can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management since the Super User allows for complete read-and-write access to the system.

1.4.1.2.5 Packet Filtering

The TOE provides extensive packet filtering capabilities for IPv4, IPv6, TCP, and UDP. The authorized administrator can define packet filtering rules that apply to most every field within the identified packet types. The authorized administrator can define each rule to permit, deny, and log each decision.

1.4.1.2.6 Protection of the TSF

The TOE implements a number of features to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability). The TOE can also be configured to work with an NTP server for reliable time.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

1.4.1.2.7 TOE access

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

1.4.1.2.8 Trusted path/channels

The TOE protects interactive communication with administrators using IPsec for CLI access to ensure both integrity and disclosure protection. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established.

The TOE protects communication with network peers, such as a log server, using IPsec connections to prevent unintended disclosure or modification of logs.

1.4.2 TOE Documentation

CommScope offers a series of documents that describe the installation of the FastIron Router products as well as guidance for subsequent use and administration of the applicable security features of the VPN Gateway. The following document was examined as part of the evaluation:

- Ruckus FastIron FIPS and Common Criteria Configuration Guide 08.0.95, 27 October 2020.

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
  - Part 3 Conformant
- Package Claims:

  PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways, 22 November 2019
  The PP-Configuration includes the following components:
  - collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (CPP_ND_V2.1)
  - PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 2019-09-17 (CFG_NDcPP-VPNGW_V1.0)
- Technical Decisions

TD	PP	Applied to FastIron VPN	Notes
TD0395	CPP_ND_V2.1	No	TOE does not claim protection from TLS
TD0396	CPP_ND_V2.1	No	TOE does not claim protection from TLS
TD0397	CPP_ND_V2.1	Yes	
TD0398	CPP_ND_V2.1	No	TOE does not claim protection from SSH
TD0399	CPP_ND_V2.1	Yes	
TD0400	CPP_ND_V2.1	Yes	
TD0401	CPP_ND_V2.1	Yes	
TD0402	CPP_ND_V2.1	Yes	
TD0407	CPP_ND_V2.1	Yes	
TD0408	CPP_ND_V2.1	Yes	
TD0409	CPP_ND_V2.1	Yes	
TD0410	CPP_ND_V2.1	Yes	
TD0411	CPP_ND_V2.1	No	TOE does not claim protection from SSH
TD0412	CPP_ND_V2.1	No	TOE does not claim protection from SSH
TD0423	CPP_ND_V2.1	Yes	
TD0424	CPP_ND_V2.1	No	TOE does not claim protection from SSH
TD0425	CPP_ND_V2.1	Yes	
TD0447	CPP_ND_V2.1	No	TOE does not claim protection from SSH
TD0450	CPP_ND_V2.1	No	TOE does not claim protection from TLS or DTLS
TD0451	CPP_ND_V2.1	No	TOE is not distributed

TD0453	CPP_ND_V2.1	No	TOE does not claim protection from SSH
TD0475	CPP_ND_V2.1	No	TOE does not claim protection from SSH
TD0477	CPP_ND_V2.1	yes	
TD0478	CPP_ND_V2.1	Yes	
TD0480	CPP_ND_V2.1	Yes	
TD0481	CPP_ND_V2.1	No	TOE does not claim protection from TLS or DTLS
TD0482	CPP_ND_V2.1	Yes	
TD0483	CPP_ND_V2.1	Yes	
TD0484	CPP_ND_V2.1	Yes	
TD0511	CFG_NDCPP-VPNGW_V1.0	No	Firewall not claimed
TD0520	CFG_NDCPP-VPNGW_V1.0	Yes	
TD0528	CPP_ND_V2.1	Yes	
TD0529	CPP_ND_V2.1	Yes	
TD0530	CPP_ND_V2.1	No	TOE does not claim protection from TLS
TD0531	CPP_ND_V2.1	No	TOE does not claim protection from SSH
TD0532	CPP_ND_V2.1	Yes	
TD0533	CPP_ND_V2.1	Yes	
TD0535	CPP_ND_V2.1	Yes	
TD0536	CPP_ND_V2.1	Yes	
TD0538	CPP_ND_V2.1	Yes	

2.1 Conformance Rationale

The ST conforms to the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 offers additional information about the identified security objectives, but that has not been reproduced here and the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 should be consulted if there is interest in that material.

In general, the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 has defined Security Objectives appropriate for a VPN gateway and as such are applicable to the Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN TOE.

3.1 Security Objectives for the Operational Environment

OE.ADMIN_CREDENTIALS_SECURE The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.CONNECTIONS The TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

OE.NO_THRU_TRAFFIC_PROTECTION The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.RESIDUAL_INFORMATION The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

OE.UPDATES The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0. The CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 defines the following extended requirements and since they are not redefined in this ST the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- CPP_ND_V2.1:FAU_STG_EXT.1: Protected Audit Event Storage
- CPP_ND_V2.1:FCS_IPSEC_EXT.1: IPsec Protocol
- CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1: Internet Protocol Security (IPsec) Communications
- CPP_ND_V2.1:FCS_NTP_EXT.1: NTP Protocol
- CPP_ND_V2.1:FCS_RBG_EXT.1: Random Bit Generation
- CPP_ND_V2.1:FIA_PMG_EXT.1: Password Management
- CFG_NDCPP-VPNGW_V1.0:FIA_PSK_EXT.1: Pre-Shared Key Composition
- CPP_ND_V2.1:FIA_UAU_EXT.2: Password-based Authentication Mechanism
- CPP_ND_V2.1:FIA_UIA_EXT.1: User Identification and Authentication
- CPP_ND_V2.1:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
- CPP_ND_V2.1:FIA_X509_EXT.2: X.509 Certificate Authentication
- CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.2: X.509 Certificate Authentication
- CPP_ND_V2.1:FIA_X509_EXT.3: X.509 Certificate Requests
- CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.3: X.509 Certificate Requests
- CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1: Rules for Packet Filtering
- CPP_ND_V2.1:FPT_APW_EXT.1: Protection of Administrator Passwords
- CPP_ND_V2.1:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- CPP_ND_V2.1:FPT_STM_EXT.1: Reliable Time Stamps
- CPP_ND_V2.1:FPT_TST_EXT.1: TSF testing
- CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.1: TSF Testing
- CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.3: TSF Self-Test with Defined Methods
- CPP_ND_V2.1:FPT_TUD_EXT.1: Trusted update
- CFG_NDCPP-VPNGW_V1.0:FPT_TUD_EXT.1: Trusted Update
- CPP_ND_V2.1:FTA_SSL_EXT.1: TSF-initiated Session Locking

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0. The refinements and operations already performed in the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 are not identified (e.g., highlighted) here, rather the requirements have been copied from the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 and any residual operations have been completed herein. Of particular note, the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 which includes all the SARs for EAL 1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL 1 assurance requirements alone. The CPP_ND_V2.1/CFG_NDCPP-VPNGW_V1.0 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN TOE.

Requirement Class	Requirement Component
FAU: Security audit	CPP_ND_V2.1:FAU_GEN.1: Audit Data Generation
	CFG_NDCPP-VPNGW_V1.0:FAU_GEN.1: Audit Data Generation
	CPP_ND_V2.1:FAU_GEN.2: User identity association
	CPP_ND_V2.1:FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	CPP_ND_V2.1:FCS_CKM.1: Cryptographic Key Generation
	CFG_NDCPP-VPNGW_V1.0:FCS_CKM.1/IKE: Cryptographic Key Generation (for IKE Peer Authentication)
	CPP_ND_V2.1:FCS_CKM.2: Cryptographic Key Establishment
	CPP_ND_V2.1:FCS_CKM.4: Cryptographic Key Destruction
	CPP_ND_V2.1:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	CFG_NDCPP-VPNGW_V1.0:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	CPP_ND_V2.1:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	CPP_ND_V2.1:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	CPP_ND_V2.1:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	CPP_ND_V2.1:FCS_IPSEC_EXT.1: IPsec Protocol
	CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1: Internet Protocol Security (IPsec) Communications
	CPP_ND_V2.1:FCS_NTP_EXT.1: NTP Protocol
	CPP_ND_V2.1:FCS_RBG_EXT.1: Random Bit Generation
FIA: Identification and authentication	CPP_ND_V2.1:FIA_AFL.1: Authentication Failure Management
	CPP_ND_V2.1:FIA_PMG_EXT.1: Password Management
	CFG_NDCPP-VPNGW_V1.0:FIA_PSK_EXT.1: Pre-Shared Key Composition
	CPP_ND_V2.1:FIA_UAU.7: Protected Authentication Feedback

	CPP_ND_V2.1:FIA_UAU_EXT.2: Password-based Authentication Mechanism
	CPP_ND_V2.1:FIA_UIA_EXT.1: User Identification and Authentication
	CPP_ND_V2.1:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	CPP_ND_V2.1:FIA_X509_EXT.2: X.509 Certificate Authentication
	CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.2: X.509 Certificate Authentication
	CPP_ND_V2.1:FIA_X509_EXT.3: X.509 Certificate Requests
	CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	CPP_ND_V2.1:FMT_MOF.1/ManualUpdate: Management of security functions behavior
	CPP_ND_V2.1:FMT_MTD.1/CoreData: Management of TSF Data
	CPP_ND_V2.1:FMT_MTD.1/CryptoKeys: Management of TSF data
	CFG_NDCPP-VPNGW_V1.0:FMT_MTD.1/CryptoKeys: Management of TSF Data
	CPP_ND_V2.1:FMT_SMF.1: Specification of Management Functions
	CFG_NDCPP-VPNGW_V1.0:FMT_SMF.1: Specification of Management Functions
	CPP_ND_V2.1:FMT_SMR.2: Restrictions on Security Roles
FPF: Packet Filtering	CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1: Rules for Packet Filtering
FPT: Protection of the TSF	CPP_ND_V2.1:FPT_APW_EXT.1: Protection of Administrator Passwords
	CFG_NDCPP-VPNGW_V1.0:FPT_FLS.1/SelfTest: Fail Secure (Self-Test Failures)
	CPP_ND_V2.1:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	CPP_ND_V2.1:FPT_STM_EXT.1: Reliable Time Stamps
	CPP_ND_V2.1:FPT_TST_EXT.1: TSF testing
	CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.1: TSF Testing
	CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.3: TSF Self-Test with Defined Methods
	CPP_ND_V2.1:FPT_TUD_EXT.1: Trusted update
	CFG_NDCPP-VPNGW_V1.0:FPT_TUD_EXT.1: Trusted Update
FTA: TOE access	CPP_ND_V2.1:FTA_SSL.3: TSF-initiated Termination
	CPP_ND_V2.1:FTA_SSL.4: User-initiated Termination
	CPP_ND_V2.1:FTA_SSL_EXT.1: TSF-initiated Session Locking
	CPP_ND_V2.1:FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	CPP_ND_V2.1:FTP_ITC.1: Inter-TSF trusted channel
	CFG_NDCPP-VPNGW_V1.0:FTP_ITC.1/VPN: Inter-TSF Trusted Channel (VPN Communications)
	CPP_ND_V2.1:FTP_TRP.1/Admin: Trusted Path

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (CPP_ND_V2.1:FAU_GEN.1)

CPP_ND_V2.1:FAU_GEN.1.1

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

a) Start-up and shut-down of the audit functions;

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

c) All administrative actions comprising:

- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Resetting passwords (name of related user account shall be logged).
- [***no other actions***];

d) Specifically defined auditable events listed in Table 2.

Requirement	Auditable Events	Additional Content
CPP_ND_V2.1:FAU_GEN.1		
CFG_NDCPP-VPNGW_V1.0:FAU_GEN.1		
CPP_ND_V2.1:FAU_GEN.2		
CPP_ND_V2.1:FAU_STG_EXT.1		
CPP_ND_V2.1:FCS_CKM.1		
CFG_NDCPP-VPNGW_V1.0:FCS_CKM.1/IKE		
CPP_ND_V2.1:FCS_CKM.2		
CPP_ND_V2.1:FCS_CKM.4		
CPP_ND_V2.1:FCS_COP.1/DataEncryption		
CFG_NDCPP-VPNGW_V1.0:FCS_COP.1/DataEncryption		
CPP_ND_V2.1:FCS_COP.1/Hash		
CPP_ND_V2.1:FCS_COP.1/KeyedHash		
CPP_ND_V2.1:FCS_COP.1/SigGen		
CPP_ND_V2.1:FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1	Session Establishment with peer	Entire packet contents of packets transmitted/received during session establishment
CPP_ND_V2.1:FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server
CPP_ND_V2.1:FCS_RBG_EXT.1		
CPP_ND_V2.1:FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).
CPP_ND_V2.1:FIA_PMG_EXT.1		
CFG_NDCPP-VPNGW_V1.0:FIA_PSK_EXT.1		
CPP_ND_V2.1:FIA_UAU.7		
CPP_ND_V2.1:FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).

CPP_ND_V2.1:FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
CPP_ND_V2.1:FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
CPP_ND_V2.1:FIA_X509_EXT.2		
CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.2		
CPP_ND_V2.1:FIA_X509_EXT.3		
CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.3		
CPP_ND_V2.1:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	
CPP_ND_V2.1:FMT_MTD.1/CoreData		
CPP_ND_V2.1:FMT_MTD.1/CryptoKeys	Management of cryptographic keys.	
CFG_NDCPP-VPNGW_V1.0:FMT_MTD.1/CryptoKeys		
CPP_ND_V2.1:FMT_SMF.1	All management activities of TSF data.	
CFG_NDCPP-VPNGW_V1.0:FMT_SMF.1		
CPP_ND_V2.1:FMT_SMR.2		
CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol
CPP_ND_V2.1:FPT_APW_EXT.1		
CFG_NDCPP-VPNGW_V1.0:FPT_FLS.1/SelfTest		
CPP_ND_V2.1:FPT_SKP_EXT.1		
CPP_ND_V2.1:FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
CPP_ND_V2.1:FPT_TST_EXT.1		
CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.1		
CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.3		
CPP_ND_V2.1:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	
CFG_NDCPP-VPNGW_V1.0:FPT_TUD_EXT.1		
CPP_ND_V2.1:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	

CPP_ND_V2.1:FTA_SSL.4	The termination of an interactive session.	
CPP_ND_V2.1:FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism.	
CPP_ND_V2.1:FTA_TAB.1		
CPP_ND_V2.1:FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
CFG_NDCPP-VPNGW_V1.0:FTP_ITC.1/VPN		
CPP_ND_V2.1:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	

CPP_ND_V2.1: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, 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 cPP/ST, information specified in column three of Table 2.

5.1.1.2 Audit Data Generation (CFG_NDCPP-VPNGW_V1.0:FAU_GEN.1)

CFG_NDCPP-VPNGW_V1.0:FAU_GEN.1.1

See CPP_ND_V2.1:FAU_GEN.1 for audit events.

5.1.1.3 User identity association (CPP_ND_V2.1:FAU_GEN.2)

CPP_ND_V2.1:FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.4 Protected Audit Event Storage (CPP_ND_V2.1:FAU_STG_EXT.1)

CPP_ND_V2.1:FAU_STG_EXT.1.1

The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

CPP_ND_V2.1:FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself.

[***TOE shall consist of a single standalone component that stores audit data locally,***]

CPP_ND_V2.1:FAU_STG_EXT.1.3

The TSF shall [***overwrite previous audit records according to the following rule: [[audit is stored in a circular buffer and oldest records are overwritten first]***] when the local storage space for audit data is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (CPP_ND_V2.1:FCS_CKM.1)

CPP_ND_V2.1:FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [
- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3,
- ECC schemes using 'NIST curves' [P-256, P-384] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4,
- FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3].

5.1.2.2 Cryptographic Key Generation (for IKE Peer Authentication) (CFG_NDCPP-VPNGW_V1.0:FCS_CKM.1/IKE)

CFG_NDCPP-VPNGW_V1.0:FCS_CKM.1.1/IKE

The TSF shall generate asymmetric cryptographic keys used for IKE peer authentication in accordance with a specified cryptographic key generation algorithm: [
- FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3 for RSA schemes,
- FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4 for ECDSA schemes and implementing 'NIST curves' P-256, P-384 and [no other curves]] and [
- FFC Schemes using 'safe-prime' groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

Application Note: *The only FFC scheme that is supported for use with IPsec/IKE is one based upon key establishment using Diffie-Hellman group 14.*

5.1.2.3 Cryptographic Key Establishment (CPP_ND_V2.1:FCS_CKM.2)

CPP_ND_V2.1:FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [
- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications" Version 2.1 (TD0402 applied),
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography',
- Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3].

5.1.2.4 Cryptographic Key Destruction (CPP_ND_V2.1:FCS_CKM.4)

CPP_ND_V2.1:FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method
- For plaintext keys in volatile storage, the destruction shall be executed by a [***single overwrite consisting of [zeroes]***];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [***logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes]***]
that meets the following: No Standard.

5.1.2.5 Cryptographic Operation (AES Data Encryption/Decryption) (CPP_ND_V2.1:FCS_COP.1/DataEncryption)

CPP_ND_V2.1:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, GCM***] mode and cryptographic key sizes [***128 bits, 256 bits***] that meet the following: AES as specified in ISO 18033-3, [***CBC as specified in ISO 10116, GCM as specified in ISO 19772***].

5.1.2.6 Cryptographic Operation (AES Data Encryption/Decryption) (CFG_NDCPP-VPNGW_V1.0:FCS_COP.1/DataEncryption)

CFG_NDCPP-VPNGW_V1.0:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, GCM***] and [***no other***] mode and cryptographic key sizes [***128 bits, 256 bits***], and [***no other cryptographic key sizes***] that meet the following: AES as specified in ISO 18033-3, [***CBC as specified in ISO 10116, GCM as specified in ISO 19772***] and [***no other standards***].

5.1.2.7 Cryptographic Operation (Hash Algorithm) (CPP_ND_V2.1:FCS_COP.1/Hash)

CPP_ND_V2.1:FCS_COP.1.1/Hash

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256, SHA-384***] and message digest sizes [***160, 256, 384***] that meet the following: ISO/IEC 10118-3:2004.

5.1.2.8 Cryptographic Operation (Keyed Hash Algorithm) (CPP_ND_V2.1:FCS_COP.1/KeyedHash)

CPP_ND_V2.1:FCS_COP.1.1/KeyedHash

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384***] and cryptographic key sizes [***160, 256, 384***] and message digest sizes [***160, 256, 384***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

5.1.2.9 Cryptographic Operation (Signature Generation and Verification) (CPP_ND_V2.1:FCS_COP.1/SigGen)

CPP_ND_V2.1:FCS_COP.1.1/SigGen

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits],

- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits]]

that meet the following:

[***- For RSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,***

- For ECDSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 6 and Appendix D, Implementing 'NIST curves' [P-256, P-384]; ISO/IEC 14888-3, Section 6.4].

5.1.2.10 IPsec Protocol (CPP_ND_V2.1:FCS_IPSEC_EXT.1)

CPP_ND_V2.1:FCS_IPSEC_EXT.1.1

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

CPP_ND_V2.1:FCS_IPSEC_EXT.1.2

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

CPP_ND_V2.1:FCS_IPSEC_EXT.1.3

The TSF shall implement [***tunnel mode***].

CPP_ND_V2.1:FCS_IPSEC_EXT.1.4

The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [***no other algorithm***] together with a Secure Hash Algorithm (SHA)-based HMAC [***no other algorithm***] and [***AES-GCM-128, AES-GCM-256 (specified in RFC 4106)***].

CPP_ND_V2.1:FCS_IPSEC_EXT.1.5

The TSF shall implement the protocol: [***IKEv2 as defined in RFC 5996 and [with mandatory support for NAT traversal as specified in RFC 5996, section 2.23], and [no other RFCs for hash functions]***].

CPP_ND_V2.1:FCS_IPSEC_EXT.1.6

The TSF shall ensure the encrypted payload in the [***IKEv2***] protocol uses the cryptographic algorithms [***AES-CBC-128, AES-CBC-256 (specified in RFC 3602)***].

CPP_ND_V2.1:FCS_IPSEC_EXT.1.7

The TSF shall ensure that [***IKEv2 SA lifetimes can be configured by a Security Administrator based on [length of time, where the time values can be configured within [1-720] hours]***].

CPP_ND_V2.1:FCS_IPSEC_EXT.1.8

The TSF shall ensure that [***IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [length of time, where the time values can be configured within [1-8] hours]***].

CPP_ND_V2.1:FCS_IPSEC_EXT.1.9

The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ('x' in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [***224, 256, and 384***] bits.

CPP_ND_V2.1:FCS_IPSEC_EXT.1.10

The TSF shall generate nonces used in [***IKEv2***] exchanges of length [***at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash***].

CPP_ND_V2.1:FCS_IPSEC_EXT.1.11

The TSF shall ensure that all IKE protocols implement DH Group(s) [***14 (2048-bit MODP), 19 (256-bit Random ECP), 20 (384-bit Random ECP)***].

CPP_ND_V2.1:FCS_IPSEC_EXT.1.12

The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [***IKEv2 IKE_SA***] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [***IKEv2 CHILD_SA***] connection.

CPP_ND_V2.1:FCS_IPSEC_EXT.1.13

The TSF shall ensure that all IKE protocols perform peer authentication using [***RSA, ECDSA***] that use X.509v3 certificates that conform to RFC 4945 and [***Pre-shared Keys***].

CPP_ND_V2.1:FCS_IPSEC_EXT.1.14

The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [***Distinguished Name (DN)***] and [***no other reference identifier type***].

5.1.2.11 Internet Protocol Security (IPsec) Communications (CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1)

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.1

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.2

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.3

The TSF shall implement [***tunnel mode***].

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.4

The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [***AES-GCM-128, AES-GCM-256 (specified in RFC 4106)***] and [***no other algorithm***] together with a Secure Hash Algorithm (SHA)-based HMAC [***no other algorithm***]].

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.5

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.6

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.7

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.8

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.9

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.10

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.11

The TSF shall ensure that IKE protocols implement DH Groups 19 (256-bit Random ECP), 20 (384-bit Random ECP), and [***14 (2048-bit MODP)***].

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.12

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.13

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1.14

The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [***Distinguished Name (DN)***] and [***no other reference identifier type***]].

5.1.2.12 NTP Protocol (CPP_ND_V2.1:FCS_NTP_EXT.1)

CPP_ND_V2.1:FCS_NTP_EXT.1.1

The TSF shall use only the following NTP version(s) [***NTP v3 (RFC 1305), NTP v4 (RFC 5905)***].

CPP_ND_V2.1:FCS_NTP_EXT.1.2

The TSF shall update its system time using [***Authentication using [SHA1] as the message digest algorithm***].

CPP_ND_V2.1:FCS_NTP_EXT.1.3

The TSF shall not update NTP timestamp from broadcast and/or multicast addresses

CPP_ND_V2.1:FCS_NTP_EXT.1.4

The TSF shall support configuration of at least three (3) NTP time sources.

5.1.2.13 Random Bit Generation (CPP_ND_V2.1:FCS_RBG_EXT.1)

CPP_ND_V2.1:FCS_RBG_EXT.1.1

The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [***CTR_DRBG (AES)***].

CPP_ND_V2.1:FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[1] software-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011Table C.1 'Security Strength Table for Hash Functions', of the keys and hashes that it will generate.

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication Failure Management (CPP_ND_V2.1:FIA_AFL.1)

CPP_ND_V2.1:FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within [***3-100***] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password. (TD0408 applied)

CPP_ND_V2.1:FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed***]. (TD0408 applied)

5.1.3.2 Password Management (CPP_ND_V2.1:FIA_PMG_EXT.1)

CPP_ND_V2.1:FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***'!', '@', '#', '$', '%', '&', '*', '(', ')'***];

b) Minimum password length shall be configurable to between [***8***] and [***48***] characters.

5.1.3.3 Pre-Shared Key Composition (CFG_NDCPP-VPNGW_V1.0:FIA_PSK_EXT.1)

CFG_NDCPP-VPNGW_V1.0:FIA_PSK_EXT.1.1

The TSF shall be able to use pre-shared keys for IPsec and [***no other protocols***].

CFG_NDCPP-VPNGW_V1.0:FIA_PSK_EXT.1.2

The TSF shall be able to accept text-based pre-shared keys that: - Are 22 characters and [***[up to and including 100 characters]***] ; - composed of any combination of upper and lower case letters, numbers, and special characters (that include: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')').

CFG_NDCPP-VPNGW_V1.0:FIA_PSK_EXT.1.3

The TSF shall condition the text-based pre-shared keys by using [***[no conditioning]***].

CFG_NDCPP-VPNGW_V1.0:FIA_PSK_EXT.1.4

The TSF shall be able to [***accept***] bit-based pre-shared keys.

5.1.3.4 Protected Authentication Feedback (CPP_ND_V2.1:FIA_UAU.7)

CPP_ND_V2.1:FIA_UAU.7.1

The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.1.3.5 Password-based Authentication Mechanism (CPP_ND_V2.1:FIA_UAU_EXT.2)

CPP_ND_V2.1:FIA_UAU_EXT.2.1

The TSF shall provide a local [***password-based, [Radius]***] authentication mechanism to perform local administrative user authentication. (TD0408 applied)

5.1.3.6 User Identification and Authentication (CPP_ND_V2.1:FIA_UIA_EXT.1)

CPP_ND_V2.1:FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [***[network routing services]***].

CPP_ND_V2.1:FIA_UIA_EXT.1.2

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

5.1.3.7 X.509 Certificate Validation (CPP_ND_V2.1:FIA_X509_EXT.1/Rev)

CPP_ND_V2.1:FIA_X509_EXT.1.1/Rev

The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [***the Online Certificate Status Protocol (OCSP) as specified in RFC 6960***]
- The TSF shall validate the extendedKeyUsage field according to the following rules:

o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.

o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.

o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

CPP_ND_V2.1:FIA_X509_EXT.1.2/Rev

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.1.3.8 X.509 Certificate Authentication (CPP_ND_V2.1:FIA_X509_EXT.2)

CPP_ND_V2.1:FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***IPsec***], and [***no additional uses***].

CPP_ND_V2.1:FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [***not accept the certificate***].

5.1.3.9 X.509 Certificate Authentication (CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.2)

CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and [***no other protocols***], and [***no additional uses***].

5.1.3.10 X.509 Certificate Requests (CPP_ND_V2.1:FIA_X509_EXT.3)

CPP_ND_V2.1:FIA_X509_EXT.3.1

The TSF shall generate a Certification Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [***Common Name, Organization***].

CPP_ND_V2.1:FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.1.3.11 X.509 Certificate Requests (CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.3)

CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.3.1

The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [***Common Name, Organization***].

CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behavior (CPP_ND_V2.1:FMT_MOF.1/ManualUpdate)

CPP_ND_V2.1:FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions to perform manual update to Security Administrators.

5.1.4.2 Management of TSF Data (CPP_ND_V2.1:FMT_MTD.1/CoreData)

CPP_ND_V2.1:FMT_MTD.1.1/CoreData

The TSF shall restrict the ability to manage the TSF data to Security Administrators.

5.1.4.3 Management of TSF data (CPP_ND_V2.1:FMT_MTD.1/CryptoKeys)

CPP_ND_V2.1:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.1.4.4 Management of TSF Data (CFG_NDCPP-VPNGW_V1.0:FMT_MTD.1/CryptoKeys)

CFG_NDCPP-VPNGW_V1.0:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys and certificates used for VPN operation to Security Administrators.

5.1.4.5 Specification of Management Functions (CPP_ND_V2.1:FMT_SMF.1)

CPP_ND_V2.1:FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [***o Ability to configure audit behavior,***
o Ability to modify the behavior of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full,
o Ability to manage the cryptographic keys,
o Ability to configure the cryptographic functionality,
o Ability to configure the lifetime for IPsec SAs,
o Ability to set the time which is used for time-stamps;
o Ability to import X509v3 certificates to the TOE's trust store].

5.1.4.6 Specification of Management Functions (CFG_NDCPP-VPNGW_V1.0:FMT_SMF.1)

CFG_NDCPP-VPNGW_V1.0:FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using digital signature and [***no other***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to manage the cryptographic keys;
- Ability to configure the cryptographic functionality;
- Ability to configure the lifetime for IPsec SAs;

- Ability to import X.509v3 certificates to the TOE's trust store;
- Ability to enable, disable, determine and modify the behavior of all the security functions of the TOE identified in this PP-Module;
- Ability to configure all security management functions identified in other sections of this PP-Module;
[- ***Ability to configure audit behavior,***
- Ability to modify the behavior of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full,
- Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1,
- Ability to set the time which is used for time-stamps,
- Ability to configure NTP,
- Ability to manage the TOE's trust store and designate X.509v3 certificates as trust anchors].

5.1.4.7 Restrictions on Security Roles (CPP_ND_V2.1:FMT_SMR.2)

CPP_ND_V2.1:FMT_SMR.2.1
The TSF shall maintain the roles: - Security Administrator.
CPP_ND_V2.1:FMT_SMR.2.2
The TSF shall be able to associate users with roles.
CPP_ND_V2.1:FMT_SMR.2.3
The TSF shall ensure that the conditions
- The Security Administrator role shall be able to administer the TOE locally;
- The Security Administrator role shall be able to administer the TOE remotely are satisfied.

5.1.5 Packet Filtering (FPF)

5.1.5.1 Rules for Packet Filtering (CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1)

CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1.1
The TSF shall perform Packet Filtering on network packets processed by the TOE.
CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1.2
The TSF shall allow the definition of Packet Filtering rules using the following network protocols and protocol fields:
- IPv4 (RFC 791)
  o Source address
  o Destination Address
  o Protocol
- IPv6 (RFC 2460)
  o Source address
  o Destination Address
  o Next Header (Protocol)
- TCP (RFC 793)
  o Source Port
  o Destination Port
- UDP (RFC 768)
  o Source Port
  o Destination Port.

CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1.3
The TSF shall allow the following operations to be associated with Packet Filtering rules: permit and drop with the capability to log the operation.
CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1.4
The TSF shall allow the Packet Filtering rules to be assigned to each distinct network interface.

CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1.5

The TSF shall process the applicable Packet Filtering rules (as determined in accordance with FPF_RUL_EXT.1.4) in the following order: Administrator-defined.

CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1.6

The TSF shall drop traffic if a matching rule is not identified.

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Protection of Administrator Passwords (CPP_ND_V2.1:FPT_APW_EXT.1)

CPP_ND_V2.1:FPT_APW_EXT.1.1

The TSF shall store administrative passwords in non-plaintext form.

CPP_ND_V2.1:FPT_APW_EXT.1.2

The TSF shall prevent the reading of plaintext administrative passwords. (TD0483 applied).

5.1.6.2 Fail Secure (Self-Test Failures) (CFG_NDCPP-VPNGW_V1.0:FPT_FLS.1/SelfTest)

CFG_NDCPP-VPNGW_V1.0:FPT_FLS.1.1/SelfTest

The TSF shall shut down when the following types of failures occur: failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests.

5.1.6.3 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (CPP_ND_V2.1:FPT_SKP_EXT.1)

CPP_ND_V2.1:FPT_SKP_EXT.1.1

The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.1.6.4 Reliable Time Stamps (CPP_ND_V2.1:FPT_STM_EXT.1)

CPP_ND_V2.1:FPT_STM_EXT.1.1

The TSF shall be able to provide reliable time stamps for its own use.

CPP_ND_V2.1:FPT_STM_EXT.1.2

The TSF shall [***allow the Security Administrator to set the time, synchronise time with an NTP server***].

5.1.6.5 TSF testing (CPP_ND_V2.1:FPT_TST_EXT.1)

CPP_ND_V2.1:FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [***during initial start-up (on power on)***] to demonstrate the correct operation of the TSF: [***cryptographic algorithm self-tests, firmware integrity tests***].

5.1.6.6 TSF Testing (CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.1)

CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [***during initial startup (on power on)***] to demonstrate the correct operation of the TSF: noise source health tests, [***cryptographic algorithm self-tests, firmware integrity tests***].

5.1.6.7 TSF Self-Test with Defined Methods (CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.3)

CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.3.1

The TSF shall run a suite of the following self-tests when loaded for execution to demonstrate the correct operation of the TSF: integrity verification of stored executable code.

CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.3.2

The TSF shall execute the self-testing through a TSF-provided cryptographic service specified in FCS_COP.1/SigGen.

5.1.6.8 Trusted update (CPP_ND_V2.1:FPT_TUD_EXT.1)

CPP_ND_V2.1:FPT_TUD_EXT.1.1

The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***the most recently installed version of the TOE firmware/software***].

CPP_ND_V2.1:FPT_TUD_EXT.1.2

The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***no other update mechanism***].

CPP_ND_V2.1:FPT_TUD_EXT.1.3

The TSF shall provide means to authenticate firmware/software updates to the TOE using a [***digital signature mechanism***] prior to installing those updates.

5.1.6.9 Trusted Update (CFG_NDCPP-VPNGW_V1.0:FPT_TUD_EXT.1)

CFG_NDCPP-VPNGW_V1.0:FPT_TUD_EXT.1.1

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FPT_TUD_EXT.1.2

No change from base PP

CFG_NDCPP-VPNGW_V1.0:FPT_TUD_EXT.1.3

The TSF shall provide means to authenticate firmware/software updates to the TOE using a digital signature mechanism and [***no other mechanisms***] prior to installing those updates.

5.1.7 TOE access (FTA)

5.1.7.1 TSF-initiated Termination (CPP_ND_V2.1:FTA_SSL.3)

CPP_ND_V2.1:FTA_SSL.3.1

The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.1.7.2 User-initiated Termination (CPP_ND_V2.1:FTA_SSL.4)

CPP_ND_V2.1:FTA_SSL.4.1

The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.1.7.3 TSF-initiated Session Locking (CPP_ND_V2.1:FTA_SSL_EXT.1)

CPP_ND_V2.1:FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, [- ***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.7.4 Default TOE Access Banners (CPP_ND_V2.1:FTA_TAB.1)

CPP_ND_V2.1:FTA_TAB.1.1

Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.1.8 Trusted path/channels (FTP)

5.1.8.1 Inter-TSF trusted channel (CPP_ND_V2.1:FTP_ITC.1)

CPP_ND_V2.1:FTP_ITC.1.1

The TSF shall be capable of using [***IPsec***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***authentication server***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

CPP_ND_V2.1:FTP_ITC.1.2

The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

CPP_ND_V2.1:FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [***transmitting audit records to an audit server, requests to authentication server***].

5.1.8.2 Inter-TSF Trusted Channel (VPN Communications) (CFG_NDCPP-VPNGW_V1.0:FTP_ITC.1/VPN)

CFG_NDCPP-VPNGW_V1.0:FTP_ITC.1.1/VPN

The TSF shall be capable of using IPsec to provide a communication channel between itself and authorized IT entities supporting VPN communications that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

CFG_NDCPP-VPNGW_V1.0:FTP_ITC.1.2/VPN:

The TSF shall permit the authorized IT entities to initiate communication via the trusted channel.

CFG_NDCPP-VPNGW_V1.0:FTP_ITC.1.3/VPN:

The TSF shall initiate communication via the trusted channel for [remote VPN gateways/peers].

5.1.8.3 Trusted Path (CPP_ND_V2.1:FTP_TRP.1/Admin)

CPP_ND_V2.1:FTP_TRP.1.1/Admin

The TSF shall be capable of using [***IPsec***] to provide a communication path between itself and authorized remote Administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.

CPP_ND_V2.1:FTP_TRP.1.2/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

CPP_ND_V2.1:FTP_TRP.1.3/Admin

The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 2 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d

The developer shall provide a functional specification.

ADV_FSP.1.2d

The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

The operational user guidance shall describe, for each user role, the user accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6c

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d

The developer shall provide the TOE, including its preparative procedures.

AGD_PRE.1.1c

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d

The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c

The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d

The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c

The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing – Conformance (ATE_IND.1)

ATE_IND.1.1d

The developer shall provide the TOE for testing.

ATE_IND.1.1c

The TOE shall be suitable for testing.

ATE_IND.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d

The developer shall provide the TOE for testing.

AVA_VAN.1.1c

The TOE shall be suitable for testing.

AVA_VAN.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence...

AVA_VAN.1.2e

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Packet Filtering
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE produces syslog conformant messages in a number of circumstances including warnings about the device itself (such as temperature, power failures, etc.) as well as security relevant events (the success and failure login of the user, regardless of the authentication mechanism; changing a user's password; and adding and deleting user accounts). In each case the audit record includes the time and date, identification of the responsible subject (e.g., by network address or user ID), the type of event, the outcome of the event, and other information depending on the event type. For cryptographic keys, the act of importing a key is audited and the associated administrator account is identified using the trust point name corresponding to the operation being performed.

The audit records are stored in a log (internal to the TOE appliance) that is protected so that only an authorized TOE User can read (for which tools accessible via the CLI are provided). The protection results from the fact that the logs can be accessed only after a user logs in (see section 6.3 below).

The log stores up to 4,000 entries after which the audit entries will be overwritten, oldest first. The administrator (with Super User privilege) can (and should) choose to configure one or more external syslog servers where the TOE will simultaneously send a copy of the audit records. The TOE can be configured to use IPsec (using any of the supported ciphersuites) to protect audit logs exported to an external server.

The TOE includes a hardware clock that is used to provide reliable time information for the audit records it generates.

The Security audit function satisfies the following security functional requirements:

- CPP_ND_V2.1:FAU_GEN.1: The TOE can generate audit records for events including starting and stopping the audit function, administrator commands, and all other events identified in Table 2 (in Section 5). Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in Table 2 (in Section 5).
- CFG_NDCPP-VPNGW_V1.0:FAU_GEN.1: VPN related audit events are included in CPP_ND_V2.1:FAU_GEN.1.
- CPP_ND_V2.1:FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.
- CPP_ND_V2.1:FAU_STG_EXT.1: The TOE can be configured to export audit records to an external SYSLOG server. This communication is protected with the use of IPsec.

6.2 Cryptographic support

The TOE supports a range of cryptographic services when configured in CC mode as required. On the ICX 7450 the TOE utilizes the Firmware crypto library referred to as the BRCD-IP-CRYPTO-VER-4.0 running on the A9, and the "FastIron Service Module FPGA" crypto library running within the IPsec VPN module. The IPsec VPN module crypto library performs the encryption and decryption supporting ESP only. All other cryptography supporting IPsec is performed by the BRCD-IP-CRYPTO-VER-4.0 crypto library.

The following functions have been CAVP tested.

Functions	Requirement	ICX 7450 & FPGA Cert #
Encryption/Decryption		
• AES CBC (128 and 256 bits) • AES GCM (128 and 256 bits)	FCS_COP.1/ DataEncryption	5022, 5074
Cryptographic signature services		
• RSA Digital Signature Algorithm (rDSA) (modulus 2048) • Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater	FCS_COP.1/ SigGen	2707 (RSA) 1282 (ECDSA)
Cryptographic hashing		
• SHA-1, SHA-256, SHA-384 (digest sizes 160, 256, 384)	FCS_COP.1/Hash	4081
Keyed-hash message authentication		
• HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 (digest sizes 160, 256, 384)	FCS_COP.1/ KeyedHash	3336
Random bit generation		
• CTR_DRBG with sw based noise sources with a minimum of 256 bits of non-determinism	FCS_RBC_EXT.1	1837
Key Generation		
• RSA Key Generation • ECDSA Key Generation	FCS_CKM.1 FCS_CKM.1/IKE	2707 (RSA) 1282 (ECDSA)
Key Establishment		
• ECC KAS	FCS_CKM.2	1566 (Component)

Table 3 Cryptographic Functions

The TOE supports NIST Special Publication 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, and P-384 (as defined in FIPS PUB 186-4, "Digital Signature Standard", Appendix B.4), specifically B.4.2 "Key Pair Generation by Testing Candidates". For elliptic curve based key establishment, the TOE implements the following sections of SP 800-56A: 5.6 and all subsections. The TOE does not implement any CommScope-specific extensions. These key establishment schemes are used by the IPsec protocol to support all trusted channels.

The TOE uses a software-based random bit generator that complies with Special Publication 800-90 using CTR_DRBG when operating in the FIPS mode (which is a subset of CC mode). AES-256 is used in conjunction with a minimum of 256 bits of entropy.

The TOE implements the IPsec architecture as specified in RFC 4301. SPD rules can be configured using access control List (ACL) entries. ACL entries are used to distinguish between DROP actions and permit (PROTECT) actions. BYPASS rules are defined using ACL entries as well. The authorized administrator defines a final discard entry so that any packet not matching another entry will be discarded. ACL entries are processed in the order specified by the administrator, and the first matching rule is applied. Packets received on an interface are compared against the ACL entries defined for interface upon which the packet was received, and then if the packet is to be forwarded, the packet is processed again against the ACL entries defined for the interface upon which the packet is to be transmitted.

Packets destined for an IP address that is part of an IPsec SA are always encrypted, as the IPsec SA is also analyzed alongside the ACL entries for encryption.

The TOE supports IKEv2 in tunnel mode. The TOE supports RFC 3602 conformant AES-CBC-128 and AES-CBC-256 encryption algorithms for IKEv2. The TOE also implements HMAC-SHA-256 and HMAC-SHA-384 as integrity/authentication algorithms as well as Diffie-Hellman Groups 14, 19, and 20. The authorized administrator assigns the default Diffie-Hellman Group. The encrypted payload for ESP uses AES-GCM-128, AES-GCM-256 as specified in RFC 5282. The authorized administrator can configure the TOE to support lifetimes based on time limits. The phase 1 limit can be set between 1-720 hours and the phase 2 limit can be set 1-8 hours. The TOE verifies that the default the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the IKEv1/2 Phase 1/IKE_SA connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the IKEv1/2 Phase 2/CHILD_SA connection, preventing configuration of a too-large Phase 2/Child algorithm strength.

For HMAC-SHA-256, the TOE uses key sizes of up to a length of 64 bytes, with a block size of 64 bytes and output MAC length of 32 bytes. For HMAC-SHA-384, the TOE uses key sizes of up to a length of 128 bytes, with a block size of 128 bytes and output MAC length of 48 bytes.

The TOE generates the secret value x used in the IKEv2 Diffie-Hellman key exchange ('x' in g^x mod p) using the CAVP tested RBG specified in FCS_RBG_EXT.1 and having possible lengths of 224, 256, or 384 bits. When a random number is needed for a nonce, the probability that a specific nonce value will be repeated during the life of a specific IPsec SA is less than 1 in 2^{112}, 2^{128}, or 2^{192}.

The IPsec implementation supports RSA and ECDSA certificates. The TOE generates RSA keys based on FIPS PUB 186-4, “Digital Signature Standard” Appendix B.3.3 and ECDSA keys based on FIPS PUB 186-4, “Digital Signature Standard” Appendix B.4.2. The TOE allows certificates to be stored in flash by importing them via SCEP (Simple Certificate Enrollment Protocol) or by copying them to the TOE’s flash. Local flash files cannot be modified, but an operator can view the local flash drive. Before the TOE can use any certificates loaded into the store, the operator must associate each certificate with a trustpoint. The trustpoint contains the local certificate as well as the issuing certificate authority. The trustpoint must also be authenticated before it can be used in an IPsec configuration. The TOE will check to ensure that the certificate is a valid certificate with the right public/private keypair.

The TOE also supports pre-shared keys. Pre-shared keys can include any letter from a-z, A-Z, the numbers 0 – 9, and any special character located above the numbers on the keyboard. Pre-shared keys up to 100 characters are supported. The TOE does not perform any processing on pre-shared keys. The TOE simply uses the pre-shared key that was entered by the administrator (either text-based or bit-based).

The TOE allows configuring only a DN as the reference identifier for IPsec authentication. Both a local and remote identifier must be configured. The local identifier is used to compare the local cert with the expected DN in the certificate, which ensures that the correct local certificate is used. The remote identifier is compared against the peer’s certificate, which ensures that only the peer’s certificate can be used in the IPsec connection. If either one of the local or remote identifier does not match the local or peer certificate, then the TOE will not complete the IPsec connection.

The TOE supports the following secret keys, private keys and CSPs:

Key or CSP:	Zeroized upon:	Stored in:	Zeroized by:
VPN IKE_SA Keys (Auth initiator and responder, Encryption initiator and responder)	Expiration	Memory	Overwriting with zeros
VPN CHILD/IPSEC_SA Keys (initiator and responder)	Expiration	Memory	Overwriting with zeros
User IPsec X.509v3 Certs (ECDSA) (public)		N/A – Public information	N/A – Public information
User IPsec X.509v3 Certs (ECDSA) (private)	Command	Memory	Overwriting with zeros
Appliance IPsec X.509v3 Certs (ECDSA) (public)		N/A – Public information	N/A – Public information
Appliance IPsec X.509v3 Certs (ECDSA) (private)	Command	Flash	Overwriting with zeros

Key or CSP:	Zeroized upon:	Stored in:	Zeroized by:
VPN PSK	Command	Memory	Overwriting with zeros
Administrator Password	Command	Flash	Overwriting with zeros

Table 4 Keys and CSPs

Table 5 Service, Protocol and Key Establishment Scheme Mapping

Scheme	Protocol	Service
RSA key establishment, FFC key establishment, DH group 14 establishment	IPsec	Remote Administration (Responder)
	IPsec	Syslog and RADUS (Initiator)
	IPsec	VPN Gateway (Initiator or Responder)

The Cryptographic support function satisfies the following security functional requirements:

- CPP_ND_V2.1:FCS_CKM.1: The TOE supports asymmetric key generation using RSA key establishment (key size 2048) and FCC key establishment (curves P-256 and P-384) as part of IPsec as described in the section above. The TOE acts as a server. The TOE supports DH group 14 key establishment scheme that meets standard RFC 3526, section 3 for interoperability
- CFG_NDCPP-VPNGW_V1.0:FCS_CKM.1/IKE: See CPP_ND_V2.1:FCS_CKM.1
- CPP_ND_V2.1:FCS_CKM.2: See CPP_ND_V2.1:FCS_CKM.1
- CPP_ND_V2.1:FCS_CKM.4: Keys are zeroized when they are no longer needed by the TOE.
- CPP_ND_V2.1:FCS_COP.1/DataEncryption: The TOE performs encryption and decryption using AES in CBC and GCM mode with key sizes of either 128 or 256. The corresponding CAVP certificate is identified in the table above
- CFG_NDCPP-VPNGW_V1.0:FCS_COP.1/DataEncryption: See CPP_ND_V2.1: FCS_COP.1/DataEncryption
- CPP_ND_V2.1:FCS_COP.1/Hash: The TOE supports cryptographic hashing services using SHA-1, SHA-256, SHA-384 with digest sizes 160, 256, and 384. The corresponding CAVP certificate is identified in the table above.
- CPP_ND_V2.1:FCS_COP.1/KeyedHash: The TOE supports keyed-hash message authentication using HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384 using SHA-1/256/384 with 160/256/384 bit keys to produce a 160/256/384 output MAC. The corresponding CAVP certificate is identified in the table above.
- CPP_ND_V2.1:FCS_COP.1/SigGen: The TOE supports the use of RSA with 2048 bit key sizes and ECDSA with P-256 and P384 for cryptographic signatures. The corresponding CAVP certificate is identified in the table above
- CPP_ND_V2.1:FCS_IPSEC_EXT.1: The TOE supports IPsec when exporting audit logs to an external server, when communicating with Radius authentication servers, when communicating with NTP servers, and when performing remote administration
- CFG_NDCPP-VPNGW_V1.0:FCS_IPSEC_EXT.1: See CPP_ND_V2.1:FCS_IPSEC_EXT.1.
- CPP_ND_V2.1:FCS_NTP_EXT.1: The TOE supports NTP v3 and v4. All communication with NTP servers is authenticated using a SHA1 message digest. The TOE allows a maximum of eight NTP servers can be configured.
- CPP_ND_V2.1:FCS_RBG_EXT.1: The TOE uses one software-based entropy source to seed for a software-based DRBG that complies with Special Publication 800-90 using CTR_DRBG when operating in the FIPS mode. AES-256 is used in conjunction with a minimum of 256 bits of entropy for the seed.

6.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, except to display a message of the day banner and to permit network routing services without identification or authentication. The TOE allows unauthenticated network routing services to route network traffic through the TOE as well as unauthenticated network routing protocol traffic destined to the TOE (including DNS, ARP, ICMP, BootP, DHCP, RIP, OSPF, BGP, VRRP, VRRP-E, Multi-VRF) but does not include any management configuration of the TOE's network routing services. The TOE authenticates TOE Users against their user name, password and privilege level.

The Authorized Administrator with Super User privilege represents the "administrator" referred to in the security requirements of the protection profile. Other accounts with privileges other than Super User were not tested during the evaluation. The available mechanisms include the Local Password for the Super User Privilege level and RADIUS authentication., The Authorized Administrator with Super User privilege defines local user (or TOE User) accounts and assigns passwords and privilege levels to the accounts. Each user account has a user name, password, and a privilege level associated with it. There is a default privilege level account associated with each privilege level and each has its own password. It is up to the Authorized Administrator with Super User privilege to decide whether or how to use these legacy accounts. Note however, that each has an identity, password, and privilege level. The Authorized Administrator logs on the TOE through either locally using the console or remotely using SSHv2 over IPsec. A successful authentication is determined by a successful username and password combination. An incorrect password will result in a failed authentication attempt.

While the Authorized Administrator with Super User privilege can create or otherwise modify accounts freely, other users cannot change their own (or any other) security attributes. Note that the TOE supports a password enforcement configuration where the minimum password length can be set by an administrator up to 48 characters. Passwords can be created using any alphabetic, numeric, and a wide range of special characters (identified in FIA_PMG_EXT.1).

The Authorized Administrator can set a lockout failure count for remote login attempts (the default is 3). If the count is exceeded, the targeted account is locked for an administrator-configurable time limit. The local console interface is not subject to the lockout failure enforcement.

The Identification and authentication function satisfies the following security functional requirements:

- CPP_ND_V2.1:FIA_AFL.1: Remote administrator accounts can be locked for an administrator configured period of time if the failed login threshold is surpassed.
- CPP_ND_V2.1:FIA_PMG_EXT.1: The TOE implements a rich set of password composition constraints as described above.
- CFG_NDCPP-VPNGW_V1.0:FIA_PSK_EXT.1: The TOE allows pre-shared keys for IPsec composed of between 8 and 100 characters. The pre-shared keys can be composed of uppercase alpha characters, lowercase alpha characters, numeric characters, and non-alpha ASCII characters. The TOE also supports 22 character pre-shared keys. The TOE supports bit-based keys by inputting '0x' in front of the hex value entered into the TOE. No conditioning of the character-based key or bit-based keys are performed by the TOE.
- CPP_ND_V2.1:FIA_UAU.7: The TOE does not echo passwords as they are entered; rather '*' characters are echoed when entering passwords.
- CPP_ND_V2.1:FIA_UAU_EXT.2: The TOE uses local password-based authentication and RADIUS server authentication.
- CPP_ND_V2.1:FIA_UIA_EXT.1: The TOE does not offer any services or access to its functions, except for the switching/routing of network traffic and displaying a message of the day banner, without requiring a user to be identified and authenticated.
- CPP_ND_V2.1:FIA_X509_EXT.1/Rev: OCSP is supported for X509v3 certificate validation. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE.
- CPP_ND_V2.1:FIA_X509_EXT.2: Certificates are checked and if found not valid are not accepted or if the OCSP server cannot be contacted for validity checks, then the certificate is not accepted. Certificates are

checked in the following order: chain validation, SAN checks, CN checks, revocation status, and lastly expiration status.

- CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.2: See CPP_ND_V2.1:FIA_X509_EXT.2.
- CPP_ND_V2.1:FIA_X509_EXT.3: The TOE generates certificate requests and validates the CA used to sign the certificates.
- CFG_NDCPP-VPNGW_V1.0:FIA_X509_EXT.3: See CPP_ND_V2.1:FIA_X509_EXT.3.

6.4 Security management

The TOE associates each defined user account with a privilege level. The most privileged level is Super User (with regards to the requirements in this Security Target users with lesser privilege levels are referred to collectively simply as TOE users since such users do not have complete read-and-write access to the system). Other accounts with privileges other than Super User were not tested during the evaluation. The TOE implements an internal access control mechanism that bases decisions about the use of functions and access to TOE data on those privilege levels. In this manner, the TOE is able to ensure that only the Authorized Administrator with Super User privilege can access audit configuration data, information flow policy ACLs, user and administrator security attributes (including passwords and privilege levels), authentication method lists, the logon failure threshold, the remote access user list; and cryptographic support settings.

Other than the Super User level, the TOE implements a Read Only level where only basic commands can be issued and no changes can be made and a Port Configuration level where non-security device parameters can be managed. Collectively, this ST refers to all users of the TOE as “TOE Users”, where TOE Users privileges are a subset of the broader role of “Authorized Administrator with Super User” privileges.

The TOE offers command line functions which are accessible via the CLI. The CLI is a password-protected text based interface which can be accessed from a directly connected terminal or via a remote terminal using SSH over IPsec. These command line functions can be used to effectively manage every security policy, as well as the non-security relevant aspects of the TOE.

Once authenticated (none of these functions is available to any user before being identified and authenticated), authorized administrators have access to the security functions listed in Sections 5.1.4.5 and 5.1.4.6.

The Security management function satisfies the following security functional requirements:

- CPP_ND_V2.1:FMT_MOF.1/ManualUpdate: Only the authorized administrator can update the TOE.
- CPP_ND_V2.1:FMT_MTD.1/CoreData: Only the authorized administrator can configure TSF-related functions.
- CPP_ND_V2.1:FMT_MTD.1/CryptoKeys: Only the authorized administrator can configure cryptographic keys.
- CFG_NDCPP-VPNGW_V1.0:FMT_MTD.1/CryptoKeys: See CPP_ND_V2.1:FMT_MTD.1/CryptoKeys.
- CPP_ND_V2.1:FMT_SMF.1: The TOE provides administrative interfaces to perform the functions identified in the requirement.
- CFG_NDCPP-VPNGW_V1.0:FMT_SMF.1: The TOE provides administrative interfaces to perform the functions identified in the requirement.
- CPP_ND_V2.1:FMT_SMR.2: The TOE maintains administrative user roles.

6.5 Packet Filtering

The TOE has a rich packet filtering interface implemented through the use of access control lists (ACLs). ACLS can be applied to both inbound and outbound interfaces. ACLs can be applied to any interface for either 'inbound' traffic or 'outbound traffic'. The ACL interface has options for filtering on IPv4, IPv6, TCP, and UDP as well as source and destination address. The TOE processes traffic that ACLs filter in hardware.

To prevent the layer 2 network from being flooded with excessive amount of broadcast, unknown-unicast, and multicast traffic, the TOE supports a rate-limiting policy. When the received traffic exceeds the pre-defined rate limit, the physical port can be configured to be automatically shutdown or disable using the shutdown option of the rate-limit command.

The default action when no ACL is applied on an outbound TOE interface is to permit all traffic. The CC Guide states a final deny ACL needs to be set on each outbound interface since the requirement is to deny all traffic not matching a rule. For inbound traffic to the device, traffic needs to be routed to a drop interface.

During initial boot, before the network interface becomes fully functional, the network interface drops all packets until the TOE is fully functional.

The Packet Filtering function satisfies the following security functional requirements:

- CFG_NDCPP-VPNGW_V1.0:FPF_RUL_EXT.1: The TOE supports all of the required protocols, ipv4 (RFC 791), ipv6 (RFC 2460), tcp (RFC 793), and udp (RFC 768) as well as source and destination address. The ALC entries implement permit and deny possibilities. Each ACL entry can be configured to log status of packets pertaining to the entry.

6.6 Protection of the TSF

The TOE is an appliance. The TOE is does not provide access to locally stored passwords (which can be administratively configured to be protected by SHA-1, or SHA-256) and also, while cryptographic keys can be entered, the TOE does not disclose any cryptographic keys stored in the TOE. The TOE is a hardware appliance that includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes administrator clock-related functions. The TOE can be configured to periodically synchronize its clock with a time server, but the TOE can only ensure its own reliability and not that of an external time mechanism. The TOE also implements the timing elements through timeout functionality due to inactivity for terminating both local and remote sessions. Note that the clock is used primarily to provide timestamp for audit records, but is also used to supporting timing elements of cryptographic functions.

The TOE includes a number of built in diagnostic tests that are run during start-up to determine whether the TOE is operating properly. An administrator can configure the TOE to reboot or to stop, with errors displayed, when an error is encountered. When operating in FIPS mode, the power-on self-tests comply with the FIPS 140-2 requirements for self-testing. The module performs Cryptographic algorithm known answer tests, firmware integrity tests using RSA signature verification and conditional self-tests for DRBG, Hardware RNG, Pair-wise consistency tests on generation of RSA keys, and a Firmware load test (RSA signature verification). Upon failing any of its FIPS mode power-on self-tests, the TOE will refuse to boot. The tests are sufficient to ensure the correct operation of the security features as they address firmware integrity and cryptographic operations.

The TOE supports loading a new software image manually by the administrator using CLI commands. From the CLI, an administrator can use SCP in order to download a software image, and the TOE, prior to actually installing and using the new software image, will verify its digital signature using a pre-installed vendor key. An unverified image cannot be installed.

The Protection of the TSF function satisfies the following security functional requirements:

- CPP_ND_V2.1:FPT_APW_EXT.1: The TOE does not offer any functions that will disclose to any user a plain text password. Furthermore, locally defined passwords are not stored in plaintext form.
- CFG_NDCPP-VPNGW_V1.0:FPT_FLS.1/SelfTest: Upon failing any of its FIPS mode power-on self-tests, the TOE will refuse to boot.
- CPP_ND_V2.1:FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key. Keys are stored as identified in Table 4 when they are created
- CPP_ND_V2.1:FPT_STM_EXT.1: The TOE includes its own hardware clock and can synchronize its time with an external NTP server.

- CPP_ND_V2.1:FPT_TST_EXT.1: The TOE performs a suite of self-tests to verify its integrity and proper cryptographic functionality.
- CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.1: See CPP_ND_V2.1:FPT_TST_EXT.1.
- CFG_NDCPP-VPNGW_V1.0:FPT_TST_EXT.3: The TOE performs a suite of self-tests to verify its integrity
- CPP_ND_V2.1:FPT_TUD_EXT.1: The TOE provides function to query the version and upgrade the software embedded in the TOE appliance. When installing updated software, digital signatures are used to authenticate the update to ensure it is the update intended and originated by the vendor.
- CFG_NDCPP-VPNGW_V1.0:FPT_TUD_EXT.1: See CPP_ND_V2.1:FPT_TUD_EXT.1.

6.7 TOE access

The TOE can be configured to display an administrator-configured message of the day banner that will be displayed before authentication is completed (before the user enters his password). The banner will be displayed when accessing the TOE via the console or SSH over IPsec interfaces.

The TOE can be configured by an administrator to set a session timeout value (any value up to 240 minutes, with 0 disabling the timeout) – the default timeout is disabled. A session (local or remote) that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. Upon exceeding the session timeout (if set), the TOE logs the user off.

The user will be required to login in after any session has been terminated due to inactivity or after voluntary termination. Of course, administrators can logout of local or remote sessions at any time.

The TOE access function satisfies the following security functional requirements:

- CPP_ND_V2.1:FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- CPP_ND_V2.1:FTA_SSL.4: The TOE provides the function to logout (or terminate) both local and remote user sessions as directed by the user.
- CPP_ND_V2.1:FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- CPP_ND_V2.1:FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners when administrators successfully establish interactive sessions with the TOE, allowing administrators to terminate their session prior to performing any functions.

6.8 Trusted path/channels

The TOE provides a trusted path for its remote administrative users accessing the TOE via the Ethernet ports provided on the TOE using either the command line interface using SSH over IPsec. Note that local administrator access via the serial port is also allowed for command line access. However this access is protected by physical protection of the serial interface along with the TOE itself.

When an administrator attempts to connect to the TOE remotely, the TOE attempts to negotiate a session. If the session cannot be negotiated, the connection is dropped.

Remote connections to third-party SYSLOG servers are supported for exporting audit records to an external audit server and for external user authentication using a RADIUS server. Communication with those external servers is protected using IPsec (as specified earlier). The TOE is the initiating part in both SYSLOG and RADIUS IPsec connections.

In all cases, the endpoints are assured by virtue of the certificates installed, trusted, and reviewable when connecting and by virtue of user authentication.

The Trusted path/channels function satisfies the following security functional requirements:

- CPP_ND_V2.1:FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use IPsec to ensure that any exported audit records are sent only to the configured server so they are not subject to inappropriate disclosure or modification. Likewise, communication with a configured RADIUS server must be configured to be protected by IPsec.
- CFG_NDCPP-VPNGW_V1.0:FTP_ITC.1/VPN: When making connections with remote VPN peers the TOE initiates the IPsec communication between the peers.
- CPP_ND_V2.1:FTP_TRP.1/Admin: The TOE uses IPsec to provide a trusted path for remote management interfaces to protect the communication from disclosure and modification.