GoSilent Cube + GoSilent Server v25.01

Security Target

Version 1.18

December 2022

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
0.1	29 Apr 2022	G Nickel	Initial Draft
0.2	04 May 2022	G Nickel	Address IDTech comments
1.0	5 May 2022	T Condly	Addressed Evaluator ORs
1.1	27 Jun 2022	G Nickel	Address OR03 - Validator comments
1.2	28 Jun 2022	G Nickel	Address additional Validator Comments
1.3	27 Jul 2022	G Nickel	Address OR04
1.4	06 Sep 2022	G Nickel	Address IDTech comments, Added TD's, Address OR06, OR07, and OR08, update TOE version.
1.5	21 Sep 2022	G Nickel	Address OR09, Add new TD
1.6	07 Oct 2022	G Nickel	Address OR03v2
1.7	17 Oct 2022	G Nickel	Address OR03v3 / Updated TOE version
1.8	18 Oct 2022	G Nickel	Address OR05
1.9	08 Nov 2022	G Nickel	Address OR10
1.10	10 Nov 2022	G Nickel	Update TOE version, Update CAVP
1.10a	16 Nov 2022	G Nickel	Address OR05v2, OR10v2
1.11	18 Nov 2022	K Kaur	Update TOE version, Address OR10,OR11
1.12	24 Nov 2022	G Nickel	Address OR11-9, OR12
1.13	25 Nov 2022	G Nickel	Update document references
1.14	30 Nov 2022	G Nickel	Address updated OR05, OR10, OR11, OR12, OR13.
1.15	01 Dec 2022	G Nickel	Update document references
1.16	05 Dec 2022	G Nickel	Address QA Comments, Added TD0683
1.17	20 Dec 2022	G Nickel	Address ECR Comments
1.18	21 Dec 2022	G Nickel	Address ECR Comments

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the ID Technologies GoSilent Cube + GoSilent Server v25.01 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The GoSilent Cube + GoSilent Server v25.01 provides firewall and VPN services in a portable form factor to secure the connectivity and remote communications of one or more network devices.

1.2 Identification

Table 1: Evaluation identifiers

TOE Name	ID Technologies GoSilent Cube + GoSilent Server v25.01
TOE Version	Build: 25.01.4 (GoSilent Server) Build: 25.01.3 (GoSilent Cube)
Security Target	ID Technologies GoSilent Cube + GoSilent Server v25.01 Security Target, v1.18

1.3 Conformance Claims

3 This ST supports the following conformance claims:

- CC version 3.1 revision 5
- CC Part 2 extended
- CC Part 3 conformant
- PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 (CFG_NDcPP-FW-VPNGW_V1.2)
  This PP-Configuration includes the following components:
  - i) Base PP: collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
  - ii) PP-Module: PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e (MOD_CPP_FW_V1.4e)
  - iii) PP-Module: PP-Module for Virtual Private Network (VPN) Gateways, Version 1.2 (MOD_VPNGW_V1.2)
- NIAP Technical Decisions per Table 2

Table 2: NIAP Technical Decisions

TD #	Name	Source	Exclusion Rationale
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	CPP_ND_V2.2E	

TD #	Name	Source	Exclusion Rationale
TD0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	CPP_ND_V2.2E	FCS_NTP_EXT.1 not claimed.
TD0536	NIT Technical Decision for Update Verification Inconsistency	CPP_ND_V2.2E	
TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	CPP_ND_V2.2E	
TD0538	NIT Technical Decision for Outdated link to allowed-with list	CPP_ND_V2.2E	
TD0545	NIT Technical Decision for Conflicting FW rules cannot be configured (extension of Rfl#201837)	MOD_CPP_FW_v1.4e	
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	CPP_ND_V2.2E	FCS_DTLSC_EXT.1 not claimed.
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	CPP_ND_V2.2E	
TD0551	NIT Technical Decision for Incomplete Mappings of OEs in FW Module v1.4+Errata	MOD_CPP_FW_v1.4e	
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	CPP_ND_V2.2E	
TD0556	NIT Technical Decision for RFC 5077 question	CPP_ND_V2.2E	
TD0563	NiT Technical Decision for Clarification of audit date information	CPP_ND_V2.2E	
TD0564	NiT Technical Decision for Vulnerability Analysis Search Criteria	CPP_ND_V2.2E	
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	CPP_ND_V2.2E	

TD #	Name	Source	Exclusion Rationale
TD0570	NiT Technical Decision for Clarification about FIA_AFL.1	CPP_ND_V2.2E	
TD0571	NiT Technical Decision for Guidance on how to handle FIA_AFL.1	CPP_ND_V2.2E	
TD0572	NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	CPP_ND_V2.2E	
TD0580	NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	CPP_ND_V2.2E	
TD0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	CPP_ND_V2.2E	
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	CPP_ND_V2.2E	
TD0592	NIT Technical Decision for Local Storage of Audit Records	CPP_ND_V2.2E	
TD0631	NIT Technical Decision for Clarification of public key authentication for SSH Server	CPP_ND_V2.2E	FCS_SSHS_EXT.1 not claimed.
TD0632	NIT Technical Decision for Consistency with Time Data for vNDs	CPP_ND_V2.2E	
TD0633	NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	CPP_ND_V2.2E	
TD0634	NIT Technical Decision for Clarification required for testing IPv6	CPP_ND_V2.2E	
TD0635	NIT Technical Decision for TLS Server and Key Agreement Parameters	CPP_ND_V2.2E	
TD0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH	CPP_ND_V2.2E	FCS_SSHC_EXT.1 not claimed.
TD0638	NIT Technical Decision for Key Pair Generation for Authentication	CPP_ND_V2.2E	

TD #	Name	Source	Exclusion Rationale
TD0639	NIT Technical Decision for Clarification for NTP MAC Keys	CPP_ND_V2.2E	FCS_NTP_EXT.1 not claimed.
TD0656	Missing EAs for VPN GW Optional Headend SFRs	MOD_VPNGW_V1.2	FTA_SSL.3/VPN, FTA_TSE.1, FTA_VCM_EXT.1 not claimed.
TD0657	IPSEC_EXT.1.6 GCM support for VPN GW	MOD_VPNGW_V1.2	
TD0670	NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	CPP_ND_V2.2E	
TD0683	RFC 2460 to be replaced with RFC 8200	MOD_VPNGW_V1.2	

1.4 Terminology

Table 3: Terminology

Term	Definition
CC	Common Criteria
CDP	Certificate Distribution Point
CSfC	Commercial Solutions for Classified
cPP	Collaborative Protection Profile
GSS	ID Technologies GoSilent Server
GUI	Graphical User Interface
OCSP	Online Certificate Status Protocol
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VPN	Virtual Private Network

2 TOE Description

2.1 Type

4 The TOE is a distributed TOE which consists of the ID Technologies GoSilent Cube + GoSilent Server v25.01 operating together as a single solution to provide firewall and VPN capabilities for remote network devices to secure their communications. The GoSilent Cube is a hardware user device and the GoSilent Server is a virtualized appliance. The TOE conforms to distributed TOE Use Case 3 as defined in the NDcPP, whereby a network device requires a management component to satisfy all SFRs.

2.2 Usage

2.2.1 Overview

5 The GoSilent Server acts as the centralized management and external access system for the TOE integrated into one system. The GoSilent Server provides the management GUI for configuration of GoSilent Server as well as the GoSilent Cube user devices. Operationally, it acts as the central peer for all IPsec connections from the GoSilent Cube devices and provides gateway connectivity to external systems located behind a GoSilent Cube.

6 The GoSilent Cube is a portable enterprise-grade firewall and VPN, ideal for sensitive communications, secure remote network access, and IoT deployments. GoSilent Cube can be setup within minutes by non-technical users. Physical Ethernet connections are supported on both the user side and VPN side of GoSilent Cube.

7 Together, GoSilent Cube and GoSilent Server provide a secure communications path to one or more systems located “behind” each GoSilent Cube. These systems connect to GoSilent Cube via physical Ethernet. Each GoSilent Cube establishes an IPsec VPN to the GoSilent Server, and all traffic from the user systems is routed over that VPN. Physical Ethernet is supported on the VPN side of GoSilent Cube.

8 The TOE applies policies to restrict the traffic that is permitted to pass between the user systems and external networks.

9 Management of the system is performed via a GUI provided by GoSilent Server, accessed via a browser on remote PCs using TLS/HTTPS. Authorized administrators may configure GoSilent Server as well as the GoSilent Cubes.

10 GoSilent Cubes also provide a GUI accessed from a browser on a user system via a TLS/HTTPS connection. This GUI only provides authorized administrators with the ability to configure that specific GoSilent Cube with enough information to connect to GoSilent Server. All additional configuration information is downloaded from GoSilent Server once the IPsec VPN is established.

11 Both GoSilent Server and GoSilent Cube generate audit records that are stored locally as well as sent to a remote syslog server via a TLS connection.

2.2.2 Obtaining the TOE

12 The Cube devices are delivered to customers via trusted courier. The following checks should be performed upon receipt:

- Confirm that the correct device has been delivered per the packing slip and original order;

- Inspect all packaging to confirm there are no signs of tampering or damage incurred during transport.

13 The GSS software can be obtained digitally via URL provided to the customer directly by ID Technologies.

2.2.3 Deployment

14 The TOE is deployed in a distributed configuration with the GoSilent Server virtual appliance installed on a virtualization platform located at the enterprise destination and the GoSilent Cube at the user device side. The GoSilent Cube can be connected between a specific device and the LAN, or between an access switch with multiple user devices connected and the WAN. Figure 1 below shows the physical TOE deployment and the logical TOE boundary.

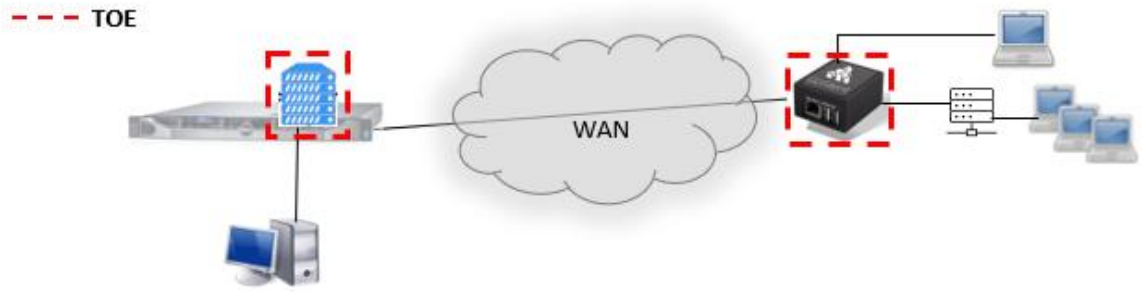

Figure 1: Example TOE deployment

2.2.4 Interfaces

15 The TOE management interfaces are depicted in Figure 2.

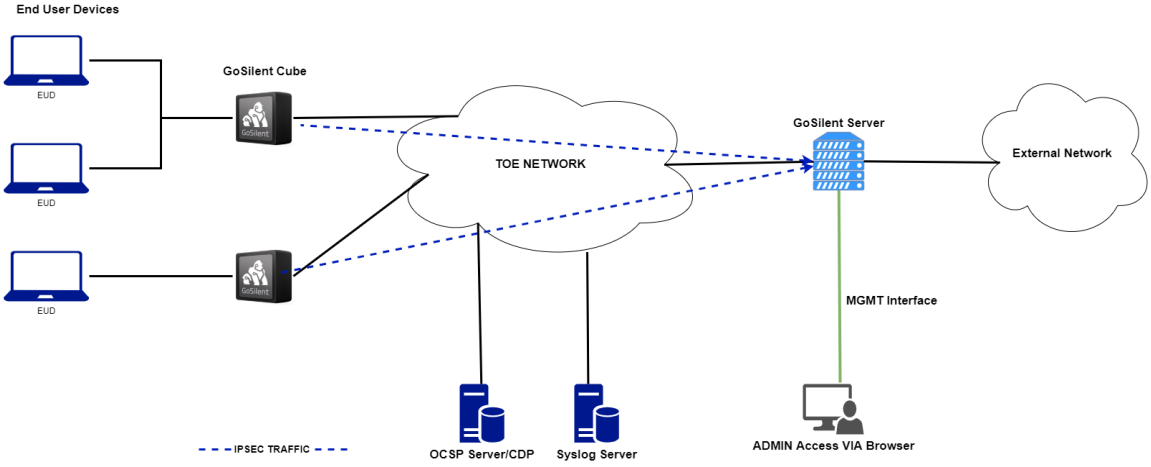

Figure 2: TOE interfaces

16 The TOE interfaces are as follows:

- **GUI (GoSilent Server).** Administrative GUI interface for managing GoSilent Server configurations and GoSilent Cubes. The GUI can be accessed via the GoSilent Server MGMT interface or from GoSilent Cube clients whose users are authorized administrators on GoSilent Server.

- **GUI (GoSilent Cube).** User GUI interface that provides limited functionality for initial cube configuration and authorized admin access to the GSS GUI.
- **Remote Logging.** Forwards TOE audit events to a syslog server for storage.
- **OCSP/CRL.** Certificate checking for IPSec connections are conducted by OCSP while CRLs are leveraged for syslog.
- **VPN Gateway.** VPN connections via IPSec.

2.3 Security Functions / Logical Scope

17 The TOE provides the following security functions:

- **Security Audit.** The TOE generates logs for auditable events. These logs are stored locally in protected storage and are also forwarded to an external audit server. When the maximum storage utilization has been reached, audit records are rotated as described in this ST.
- **Communication.** The TOE provides mechanisms for configuring, registering, and enabling components in order to establish secure communications with each other.
- **Cryptographic Support.** The TOE implements key generation and other cryptographic services to protect TOE communications including data in transit and at rest.
- **User Data Protection.** The TOE provides mechanisms to protect user data and prevent its persistence by overwriting storage space with zeros when memory is deallocated.
- **Firewall & Packet Filtering.** The TOE provides firewall functionality for all traffic passed through the TOE by enforcing stateful network traffic filtering based on examination of network packets and the application of information flow rules.
- **Identification and Authentication.** The TOE implements mechanisms to identify and authenticate all administrators to ensure only authorized access to TOE functionality or TSF data is granted.
- **Security Management.** The TOE provides a suite of management functionality for each TOE component, which is only configurable and accessible by authorized administrators.
- **Protection of the TSF.** The TOE implements a variety of protection mechanisms including authentication, self-tests, and trusted update functions to ensure the integrity of the TOE and that its TSF data is protected from unauthorized access.
- **TOE Access.** The TOE provides session monitoring and management functions for local and remote administrative sessions.
- **Trusted Path/Channels.** The TOE provides secure channels between itself and local/remote administrators, including logging channels to ensure data in transit is protected.

Table 4: CAVP Certificates

Algorithm	Description	Mode Supported	Cert (GoSilent Server)	Cert (GoSilent Cube)
AES	Used for symmetric encryption/decryption	CBC, GCM (128, 256)	C1159	C1104
SHS	Cryptographic hashing services	SHA-1, SHA-256, SHA-384,		
DRBG	Deterministic random bit generation	CTR_DRBG (AES)		
ECDSA (186)	Key Generation (SigGen/SigVer)	P-256, P-384		
HMAC	Keyed hashing services	SHA (1, 256, 384)		
KAS ECC	SP 800-56A	P-256, P-384		
KAS FFC SSC	SP 800-56Ar3		A2980	A2979
RSA	Key Generation	2048		
RSA	Key Establishment	n (2048)	Vendor Affirmed	Vendor Affirmed
RSA	SigGen (PKCS1_v1.5) SigVer (PKCS1_v1.5)	n = 2048 (SHA-256)	C1159	C1104

2.4 Physical Scope

18 The physical boundaries of the TOE are the physical boundaries of the GoSilent Server virtual appliance and the custom physical enclosure of the GoSilent Cube. Figure 3 below illustrates the boundaries of the TOE.

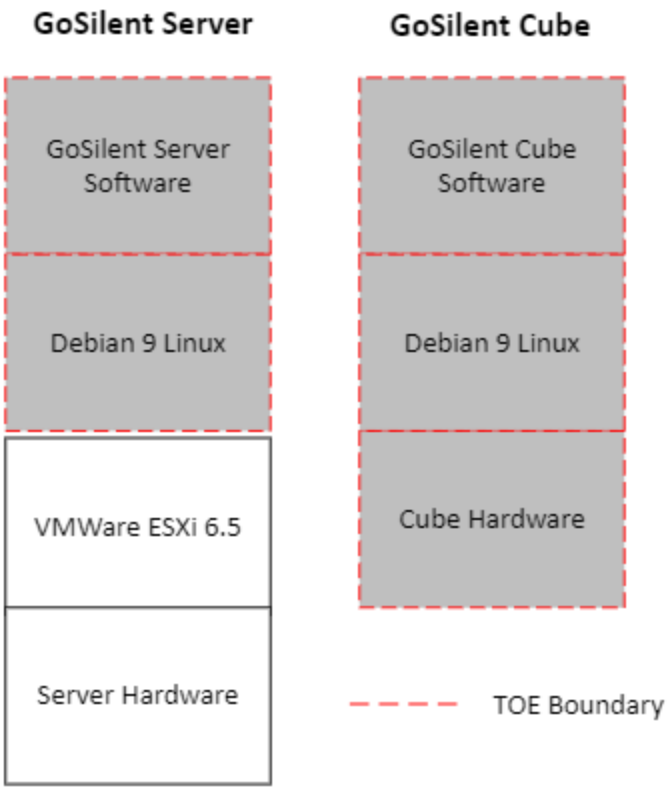

Figure 3: TOE Boundary

2.4.1 TOE Environment

19 The following components are required for the operation of the TOE in the evaluated configuration:

- Ethernet dongle for the WAN USB port of each GoSilent Cube for connection of the Cube to the WAN.
- TOE Network – Provides connectivity between the TOE components. Since IPsec tunnels are layered on top of this network, the network itself is not required to be trusted.
- External Network – GoSilent Server provides user systems with connectivity to systems on an External network, which may be limited to an Enterprise Network or provide much wider access.
- GoSilent Cube user networks – Physical Ethernet networks located on the user side of GoSilent Cube that provide connectivity between user systems and GoSilent Cube. In the simplest case, this is a direct connection using an Ethernet cable interconnecting the GoSilent Cube RJ45 Device port and a user system. To support multiple user systems, an Ethernet switch can be used.
- Management Workstation - Any computer that provides a supported browser may be used to access GoSilent Server or GoSilent Cube. The Management System can be connected to the GoSilent Cube for local management of the Cube and remote management of GoSilent Server.
- Syslog Server that supports syslog over TLS. The Syslog Server may be connected to the TOE Network or the External Network.

- OCSP Server accessed via OCSP to determine X.509 certificate revocation status for IPsec connections. The OCSP Server is connected to the TOE Network.
- Certificate Distribution Points (CDP) are accessed to determine X.509 certificate revocation status for syslog connections. The CDP may be connected to the TOE Network or the External Network.
- User systems – IT systems using GoSilent Cube as a secure path to external systems.

Table 5: TOE models

Type	Model	CPU	Memory	Storage
GoSilent Server	Virtual Appliance	Intel Xeon E3-1270 v5 (Skylake) w/ ESXi 6.5	16 GB UDIMM	8 GB SD Card (hypervisor)
				1 TB SATA HDD
GoSilent Cube	GSC-100	AllWinner H5/ Cortex A-53 (ARM v8-A)	1 GB DRAM	8 GB eMMC
	GSC-120		512 MB DRAM	

2.4.2 Guidance Documents

20 The TOE includes the following guidance documents (PDF):

- ID Technologies GoSilent Cube + GoSilent Server v25.01 Security Target, v1.18
- ID Technologies GoSilent Cube + GoSilent Server v25.01 Common Criteria Guide, v1.8

21 A pointer to the guidance documents is provided via an email sent to the TOE users during product delivery. Common Criteria Guide is available from the NIAP website.

2.4.3 Non-TOE Components

22 The TOE operates with the following components in the environment:

- **Audit Server.** The TOE makes use of a syslog server for remote logging.
- **OCSP Server/CDP.** The TOE communicates with an external OCSP Server and CDP for the purposes of certificate checking.

2.4.4 Functions not included in the TOE Evaluation

23 The following product functionality is not included in the Common Criteria evaluation:

- **Cloud instances of GoSilent Server**. GoSilent server is supported on virtual platforms and cloud instances; however, cloud deployments are not addressed by this evaluation.
- **WiFi connectivity**. The Cube is capable of accepting wireless connections from a client, however no security claims are made with respect to wireless connectivity and is therefore excluded from the evaluation.

3 Security Problem Definition

24 The Security Problem Definition is reproduced from Section 4 of the CPP_ND_V2.2E, Section 4 of the MOD_CPP_FW_v1.4e, and Section 3 of the MOD_VPNGW_v1.2.

3.1 Threats

Table 6: CPP_ND_V2.2E Threats

Identifier	Description
T.UNAUTHORIZED_ ADMINISTRATOR_ ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_ CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_ COMMUNICATION_ CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_ AUTHENTICATION_ ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_ COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

Identifier	Description
T.UNDETECTED_ ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_ FUNCTIONALITY_ COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_ CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_ FUNCTIONALITY_ FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

Table 7: MOD_CPP_FW_v1.4e Threats

Identifier	Description
T.NETWORK_ DISCLOSURE	An attacker may attempt to "map" a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported.
T.NETWORK_ ACCESS	With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services.
T.NETWORK_ MISUSE	An attacker may attempt to use services that are exported by machines in a way that is unintended by a site's security policies. For example, an attacker might be able to use a service to "anonymize" the attacker's machine as they mount attacks against others.
T.MALICIOUS_ TRAFFIC	An attacker may attempt to send malformed packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash.

Table 8: MOD_VPNGW_v1.2 Threats

Identifier	Description
T.DATA_INTEGRITY	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can communicate with those external devices then the data contained within the communications may be susceptible to a loss of integrity.
T.NETWORK_ ACCESS	Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network. From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network. From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled e-mail servers, or, that access to the mail server must be done over an encrypted link.
T.NETWORK_ DISCLOSURE	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information. From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or

Identifier	Description
	network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information. From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.
T.NETWORK_ MISUSE	Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network. From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services. From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.
T.REPLAY_ ATTACK	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions: - Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome. - No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these.

3.2 Assumptions

Table 9: CPP_ND_V2.2E Assumptions

Identifier	Description
A.PHYSICAL_ PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_ FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_ TRAFFIC_ PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

Identifier	Description
A.TRUSTED_ ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_ UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_ CREDENTIALS_ SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.COMPONENTS_ RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_ INFORMATION	The Administrator must ensure 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.
A.VS_TRUSTED_ ADMINISTRATOR (applies to vNDs only)	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_ UPDATES (applies to vNDs only)	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

Identifier	Description
A.VS_ISOLATON (applies to vNDs only)	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_ CONFIGURATION (applies to vNDs only)	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

Table 10: MOD_VPNGW_v1.2 Assumptions

Identifier	Description
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE's security policies will be enforced on all applicable network traffic flowing among the attached networks.

25 No additional Assumptions identified in MOD_CPP_FW_v1.4e.

3.3 Organizational Security Policies

Table 11: Organizational Security Policies

Identifier	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

26 No additional Organizational Security Policies identified in MOD_CPP_FW_v1.4e.

27 No additional Organizational Security Policies identified in MOD_VPNGW_v1.2.

4 Security Objectives

28 The following security objectives are reproduced from Section 5 of the CPP_ND_V2.2E, Section 5 of the MOD_CPP_FW_v1.4e, and Section 4 of the MOD_VPNGW_v1.2.

4.1 Security Objectives for the Operational Environment

Table 12: Security Objectives for the Operational Environment (CPP_ND_V2.2E)

Identifier	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
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.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. 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.
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.COMPONENTS_ RUNNING (applies to distributed TOEs only)	For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.

Identifier	Description
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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.VM_CONFIGURATION (applies to vNDs only)	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

Table 13: Security Objectives for the Operational Environment (MOD_VPNGW_v1.2)

Identifier	Description
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.

29 No additional Security Objectives for the Operational Environment identified in MOD_CPP_FW_v1.4e

4.2 Security Objectives for the TOE

Table 14: Security Objectives for the TOE (MOD_CPP_FW_v1.4e)

Identifier	Description
O.RESIDUAL_ INFORMATION	The TOE shall implement measures to ensure that any previous information content of network packets sent through the TOE is made unavailable either upon deallocation of the memory area containing the network packet or upon allocation of a memory area for a newly arriving network packet or both.
O.STATEFUL_ TRAFFIC_FILTERING	The TOE shall perform stateful traffic filtering on network packets that it processess. For this the TOE shall support the definition of stateful traffic filtering rules that allow to permit or drop network packets. The TOE shall support assignment of the stateful traffic filtering rules to each distinct network interface. The TOE shall support the processing of the applicable stateful traffic filtering rules in an administratively defined order. The TOE shall deny the flow of network packets if no matching stateful traffic filtering rule is identified. Depending on the implementation, the TOE might support the stateful traffic filtering of Dynamic Protocols (optional).

Table 15: Security Objectives for the TOE (MOD_VPNGW_v1.2)

Identifier	Description
O.ADDRESS_ FILTERING	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance, compliant TOE's will implement Packet Filtering capability. That capability will restrict the flow of network traffic between protected networks and other attached networks based on network addresses of the network nodes originating (source) or receiving (destination) applicable network traffic as well as on established connection information. Addressed by: FPF_RUL_EXT.1, FTA_VCM_EXT.1 (optional)

Identifier	Description
O.AUTHENTICATION	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (IPSec) will allow a VPN peer to establish VPN connectivity with another VPN peer and ensure that any such connection attempt is both authenticated and authorized. VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity. Addressed by: FCS_IPSEC_EXT.1 (refined from Base-PP), FIA_X509_EXT.1/Rev (from Base-PP), FIA_X509_EXT.2 (refined from Base-PP), FIA_X509_EXT.3 (from Base-PP), FTP_ITC.1/VPN, FPF_MFA_EXT.1 (optional), FTA_SSL.3/VPN (optional), FTA_TSE.1 (optional), FCS_EAP_EXT.1 (selection-based), FIA_HOTP_EXT.1 (selection-based), FIA_PSK_EXT.1 (selection-based), FIA_PSK_EXT.2 (selection-based), FIA_PSK_EXT.3 (selection-based), FIA_PSK_EXT.4 (selection-based), FIA_PSK_EXT.5 (selection-based), FIA_TOTP_EXT.1 (selection-based)
O.CRYPTOGRAPHIC_FUNCTIONS	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption of services, and network-based reconnaissance, compliant TOE's will implement a cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE. Addressed by: FCS_COP.1/DataEncryption (refined from Base-PP), FCS_IPSEC_EXT.1 (refined from Base-PP), FCS_CKM.1/IKE, FCS_EAP_EXT.1 (selection-based)
O.FAIL_SECURE	There may be instances where the TOE's hardware malfunctions or the integrity of the TOE's software is compromised, the latter being due to malicious or non-malicious intent. To address the concern of the TOE operating outside of its hardware or software specification, the TOE will shut down upon discovery of a problem reported via the self-test mechanism and provide signature-based validation of updates to the TSF. Addressed by: FPT_TST_EXT.1 (refined from Base-PP), FPT_TUD_EXT.1 (refined from Base-PP), FPT_FLS.1/SelfTest, FPT_TST_EXT.3
O.PORT_FILTERING	To further address the issues associated with unauthorized disclosure of information, etc., a compliant TOE's port filtering capability will restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) or receiving (destination) port (or service) identified in the network traffic as well as on established connection information. Addressed by: FPF_RUL_EXT.1

Identifier	Description
O.SYSTEM_ MONITORING	To address the issues of administrators being able to monitor the operations of the VPN gateway, it is necessary to provide a capability to monitor system activity. Compliant TOEs will implement the ability to log the flow of network traffic. Specifically, the TOE will provide the means for administrators to configure packet filtering rules to 'log' when network traffic is found to match the configured rule. As a result, matching a rule configured to 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security associations (SAs) is auditable, not only between peer VPN gateways, but also with certification authorities (CAs). Addressed by: FAU_GEN.1/VPN, FPF_RUL_EXT.1
O.TOE_ ADMINISTRATION	TOEs will provide the functions necessary for an administrator to configure the packet filtering rules, as well as the cryptographic aspects of the IPsec protocol that are enforced by the TOE. Addressed by: FMT_MTD.1/CryptoKeys (refined from Base-PP), FMT_SMF.1/VPN

30 No additional Security Objectives for the TOE identified in CPP_ND_V2.2E.

5 Security Requirements

5.1 Conventions

31 This document uses the following font conventions to identify the operations defined by the CC:

- **Assignment.** Indicated with italicized text.
- **Refinement.** Indicated with bold text and strikethroughs.
- **Selection.** Indicated with underlined text.
- **Assignment within a Selection:** Indicated with italicized and underlined text.
- **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

32 **Note:** Operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the NDcPP.

5.2 Extended Components Definition

33 Refer to Annex A: Extended Components Definition.

5.3 Functional Requirements

Table 16: Summary of SFRs

Requirement	Title	Source
FAU_GEN.1	Audit Data Generation	CPP_ND_V2.2E MOD_CPP_FW_v1.4e
FAU_GEN.1/VPN	Audit Data Generation	MOD_VPNGW_v1.2
FAU_GEN.2	User Identity Association	CPP_ND_V2.2E
FAU_GEN_EXT.1	Security Audit Generation	CPP_ND_V2.2E
FAU_STG_EXT.1	Protected Audit Event Storage	CPP_ND_V2.2E
FAU_STG_EXT.4	Protected Local Audit Event Storage for Distributed TOEs	CPP_ND_V2.2E
FCO_CPC_EXT.1	Component Registration Channel Definition	CPP_ND_V2.2E
FCS_CKM.1	Cryptographic Key Generation	CPP_ND_V2.2E
FCS_CKM.1/IKE	Cryptographic Key Generation (for IKE Peer Authentication)	MOD_VPNGW_v1.2
FCS_CKM.2	Cryptographic Key Establishment	CPP_ND_V2.2E

Requirement	Title	Source
FCS_CKM.4	Cryptographic Key Destruction	CPP_ND_V2.2E
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)	CPP_ND_V2.2E MOD_VPNGW_v1.2
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)	CPP_ND_V2.2E
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)	CPP_ND_V2.2E
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)	CPP_ND_V2.2E
FCS_RBG_EXT.1	Random Bit Generation	CPP_ND_V2.2E
FCS_HTTPS_EXT.1	HTTPS Protocol	CPP_ND_V2.2E
FCS_IPSEC_EXT.1	IPsec Protocol	CPP_ND_V2.2E MOD_VPNGW_v1.2
FCS_TLSC_EXT.1	TLS Client Protocol	CPP_ND_V2.2E
FCS_TLSS_EXT.1	TLS Server Protocol	CPP_ND_V2.2E
FDP_RIP.2	Full Residual Information Protection	MOD_CPP_FW_v1.4e
FFW_RUL_EXT.1	Stateful Traffic Filtering	MOD_CPP_FW_v1.4e
FIA_AFL.1	Authentication Failure Management	CPP_ND_V2.2E
FIA_PMG_EXT.1	Password Management	CPP_ND_V2.2E
FIA_UIA_EXT.1	User Identification and Authentication	CPP_ND_V2.2E
FIA_UAU_EXT.2	Password-based Authentication Mechanism	CPP_ND_V2.2E
FIA_UAU.7	Protected Authentication Feedback	CPP_ND_V2.2E
FIA_X509_EXT.1/ITT	X.509 Certificate Validation	CPP_ND_V2.2E
FIA_X509_EXT.1/Rev	X.509 Certificate Validation	CPP_ND_V2.2E MOD_VPNGW_v1.2

Requirement	Title	Source
FIA_X509_EXT.2	X.509 Certificate Authentication	CPP_ND_V2.2E MOD_VPNGW_v1.2
FIA_X509_EXT.3	X.509 Certificate Requests	CPP_ND_V2.2E MOD_VPNGW_v1.2
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour	CPP_ND_V2.2E
FMT_MOF.1/Services	Management of Security Functions Behaviour	CPP_ND_V2.2E
FMT_MTD.1/CoreData	Management of TSF Data	CPP_ND_V2.2E
FMT_MTD.1/CryptoKeys	Management of TSF Data	CPP_ND_V2.2E MOD_VPNGW_v1.2
FMT_SMF.1	Specification of Management Functions	CPP_ND_V2.2E
FMT_SMF.1/FFW	Specification of Management Functions	MOD_CPP_FW_v1.4e
FMT_SMF.1/VPN	Specification of Management Functions (VPN Gateway)	MOD_VPNGW_v1.2
FMT_SMR.2	Restrictions on Security Roles	CPP_ND_V2.2E
FPF_RUL_EXT.1	Rules for Packet Filtering	MOD_VPNGW_v1.2
FPT_FLS.1/SelfTest	Failure with Preservation of Secure State (Self-Test Failures)	MOD_VPNGW_v1.2
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	CPP_ND_V2.2E
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)	CPP_ND_V2.2E
FPT_APW_EXT.1	Protection of Administrator Passwords	CPP_ND_V2.2E
FPT_TST_EXT.1	TSF Testing	CPP_ND_V2.2E MOD_VPNGW_v1.2
FPT_TST_EXT.3	TSF Self-Test with Defined Methods	MOD_VPNGW_v1.2

Requirement	Title	Source
FPT_TUD_EXT.1	Trusted Update	CPP_ND_V2.2E MOD_VPNGW_v1.2
FPT_STM_EXT.1	Reliable Time Stamps	CPP_ND_V2.2E
FTA_SSL_EXT.1	TSF-initiated Session Locking	CPP_ND_V2.2E
FTA_SSL.3	TSF-initiated Termination	CPP_ND_V2.2E
FTA_SSL.4	User-initiated Termination	CPP_ND_V2.2E
FTA_TAB.1	Default TOE Access Banners	CPP_ND_V2.2E
FTP_ITC.1	Inter-TSF trusted channel	CPP_ND_V2.2E
FTP_ITC.1/VPN	Inter-TSF Trusted Channel (VPN Communications)	MOD_VPNGW_v1.2
FTP_TRP.1/Admin	Trusted Path	CPP_ND_V2.2E

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

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

a) Start-up and shutdown of the audit functions;

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

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**~~ Table 17.*

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**~~ Table 17.*

Table 17: Audit Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_GEN_EXT.1	None.	None.
FAU_STG_EXT.1	None.	None.
FAU_STG_EXT.4	None.	None.
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Identities of the endpoint pairs enabled or disabled.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure

Requirement	Auditable Events	Additional Audit Record Contents
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FDP_RIP.2	None.	None.
FFW_RUL_EXT.1	Application of rules configured with the 'log' operation.	Source and destination address Source and destination ports Transport Layer Protocol TOE Interface
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/ITT	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.
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. Identification of certificates added, replaced, or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MOF.1/Services	None.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMF.1/FFW	All management activities of TSF data (including creation, modification, and deletion of firewall rules).	None.
FMT_SMR.2	None.	None.
FPT_ITT.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.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
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).
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the	None.

Requirement	Auditable Events	Additional Audit Record Contents
	session locking mechanism.	
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
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.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.

FAU_GEN.1/VPN Audit Data Generation (VPN Gateway)

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

a. Start-up and shutdown of the audit functions

b. Indication that TSF self-test was completed

c. Failure of self-test

d. All auditable events for the [*not specified*] level of audit; and

*e. [auditable events defined in the Auditable Events for Mandatory Requirements table]**.***

FAU_GEN.1.2/VPN The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*additional information defined in the Auditable Events for Mandatory Requirements table for each auditable event, where applicable*].

Table 18: Auditable Events for Mandatory Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1 /VPN	No events specified.	N/A
FCS_CKM.1/IKE	No events specified.	N/A
FMT_SMF.1/VPN	All administrative actions	No additional information.
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol
FPT_FLS.1/SelfTest	No events specified.	N/A
FPT_TST_EXT.3	No events specified.	N/A
FTP_ITC.1/VPN	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	No additional information. No additional information. Identification of the initiator and target of failed trusted channels establishment attempt.

FAU_GEN.2 User Identity Association

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.

FAU_GEN_EXT.1 Security Audit Generation

FAU_GEN_EXT.1.1 The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

FAU_STG_EXT.1 Protected Audit Event Storage

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.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition [

- The TOE shall be a distributed TOE that stores audit data on the following TOE components: [*GoSilent Server, GoSilent Cube*].

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule: [*the oldest of the audit files is discarded*]] when the local storage space for audit data is full.

FAU_STG_EXT.4 Protected Local Audit Event Storage for Distributed TOEs

FAU_STG_EXT.4.1 The TSF of each TOE component which stores security audit data locally shall perform the following actions when the local storage space for audit data is full:
[GoSilent Server, GoSilent Cube [overwrite previous audit records according to the following rule: *[the oldest audit files is discarded]]].*

5.3.2 Communication (FCO)

FCO_CPC_EXT.1 Component Registration Channel Definition

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [

- A channel that meets the secure channel requirements in [FPT_ITT.1]]

for at least *TSF data.*

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

5.3.3 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

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-384] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;

]~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]~~.

FCS_CKM.1/IKE Cryptographic Key Generation (for IKE Peer Authentication)

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.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*].

FCS_CKM.2 Cryptographic Key Establishment

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";
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- 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 [groups listed in RFC 3526];

] ~~that meets the following: [assignment: list of standards].~~

Application Note: This SFR has been modified by TD0580 and TD0581.

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- *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*.

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

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]**.

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

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, 384 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].

FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

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 cryptographic key sizes [assignment: cryptographic key sizes]~~ and **message digest sizes [160, 256, 384] bits** that meet the following: *ISO/IEC 10118-3:2004*.

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

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, implicit] and cryptographic key sizes

[160, 256, 384 bits] **and message digest sizes [160, 256, 384] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

FCS_RBG_EXT.1 Random Bit Generation

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)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*one*] software-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [not require client authentication] if the peer certificate is deemed invalid.

FCS_IPSEC_EXT.1 IPsec Protocol

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

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [tunnel mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms **[AES-CBC-128, AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-256 (specified in RFC 4106)] and [no other algorithm]** together with a Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, no HMAC algorithm].

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 [RFC 4868 for hash functions]

].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv2] protocol uses the cryptographic algorithms [AES-CBC-128, AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-256 (specified in RFC 5282)].

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 to 24*] hours.

  ]

].

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 to 8*] hours;

  ]

].

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 [*224/256/384*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [IKEv2] exchanges of length [

- according to the security strength associated with the negotiated DH group.

].

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) according to RFC 5114 and** [
- *[14 (2048-bit MODP)] according to RFC 3526*

].

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.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [ECDSA] that use X.509v3 certificates that conform to RFC 4945 and [no other method].

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)**, [no other reference identifier types].

FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication

FCS_TLSC_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

].

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 section 6 and no other attribute types].

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSC_EXT.1.4 The TSF shall [present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp384r1] and no other curves/groups] in the Client Hello.

FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

].

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [TLS 1.1].

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using [ECDHE curves [secp384r1] and no other curves].

FCS_TLSS_EXT.1.4 The TSF shall support [no session resumption or session tickets].

5.3.4 User Data Protection (FDP)

FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] all objects.

5.3.5 Firewall (FFW)

FFW_RUL_EXT.1 Stateful Traffic Filtering

FFW_RUL_EXT.1.1 The TSF shall perform stateful traffic filtering on network packets processed by the TOE.

FFW_RUL_EXT.1.2 The TSF shall allow the definition of stateful traffic filtering rules using the following network protocol fields:

- *ICMPv4*
  - *Type*
  - *Code*
- *ICMPv6*
  - *Type*
  - *Code*
- *IPv4*
  - *Source address*
  - *Destination Address*
  - *Transport Layer Protocol*
- *IPv6*
  - *Source address*
  - *Destination Address*
  - *Transport Layer Protocol*
  - *[*no other field*]*
- *TCP*
  - *Source Port*
  - *Destination Port*
- *UDP*
  - *Source Port*
  - *Destination Port*

and distinct interface.

FFW_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with stateful traffic filtering rules: permit or drop with the capability to log the operation.

FFW_RUL_EXT.1.4 The TSF shall allow the stateful traffic filtering rules to be assigned to each distinct network interface.

FFW_RUL_EXT.1.5 The TSF shall:

a) accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols: TCP, UDP, [no other protocols] based on the following *network packet attributes:*
    1. *TCP: source and destination addresses, source and destination ports, sequence number, Flags;*
    2. *UDP: source and destination addresses, source and destination ports;*
    3. [no other protocols].

b) Remove existing traffic flows from the set of established traffic flows based on the following: [session inactivity timeout].

FFW_RUL_EXT.1.6 The TSF shall enforce the following default stateful traffic filtering rules on all network traffic:

a) The TSF shall drop and be capable of [counting] packets which are invalid fragments;

b) The TSF shall drop and be capable of [counting] fragmented packets which cannot be re-assembled completely;

c) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a broadcast network;

d) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a multicast network;

e) The TSF shall drop and be capable of logging network packets where the source address of the network packet is defined as being a loopback address;

f) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address "reserved for future use" (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4;

g) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as an "unspecified address" or an address "reserved for future definition and use" (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6;

h) The TSF shall drop and be capable of logging network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified; and

i) [no other rules].

FFW_RUL_EXT.1.7 The TSF shall be capable of dropping and logging according to the following rules:

a) The TSF shall drop and be capable of logging network packets where the source address of the network packet is equal to the address of the network interface where the network packet was received;

b) The TSF shall drop and be capable of logging network

packets where the source or destination address of the network packet is a link-local address;

c) *The TSF shall drop and be capable of logging network packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received.*

FFW_RUL_EXT.1.8 The TSF shall process the applicable stateful traffic filtering rules in an administratively defined order.

FFW_RUL_EXT.1.9 The TSF shall deny packet flow if a matching rule is not identified.

FFW_RUL_EXT.1.10 The TSF shall be capable of limiting an administratively defined number of *half-open TCP connections. In the event that the configured limit is reached, new connection attempts shall be dropped and the drop event shall be* [logged].

5.3.6 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*1-10*] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

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 a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

FIA_PMG_EXT.1 Password Management

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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”,*[no other characters]*];

b) Minimum password length shall be configurable to between [*8*] and [*40*] characters.

FIA_UIA_EXT.1 User Identification and Authentication

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;
- [[*reset GoSilent Cube to the factory default configuration*]]

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.

FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local [password-based] authentication mechanism to perform local administrative user authentication.

FIA_UAU.7 Protected Authentication Feedback

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**.

FIA_X509_EXT.1/ITT X.509 Certificate Validation

FIA_X509_EXT.1.1/ITT 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 two 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:
    - *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.*
    - *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.*
    - *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*.

FIA_X509_EXT.1.2/ITT The TSF shall only treat a certificate as a CA certificate if the basicContraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate 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 [a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *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.*
  - *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.*
  - *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.*
  - *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*.

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.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for **IPsec and [TLS],** and [no additional uses].

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, accept the certificate].

Application Note: “not accept the certificate” applies to OCSP for IPsec, while “accept the certificate” applies to CRLs for TLS.

FIA_X509_EXT.3 X.509 Certificate Requests

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].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.3.7 Security Management (FMT)

FMT_MOF.1/ManualUpdate Management of security functions behaviour

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual updates* to *Security Administrators*.

FMT_MOF.1/Services Management of security functions behaviour

FMT_MOF.1.1/Services The TSF shall restrict the ability to **start and stop** ~~the functions~~ **services** to *Security Administrators*.

FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1.1/CoreData The TSF shall restrict the ability to *manage* the *TSF data* to *Security Administrators*.

FMT_MTD.1/CryptoKeys Management of TSF data

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*].

FMT_SMF.1 Specification of Management Functions

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;*
- [
    - Ability to start and stop services;

- Ability to modify the behaviour of the transmission of audit data to an external IT entity;
- Ability to manage the cryptographic keys;
- Ability to configure the cryptographic functionality;
- Ability to configure the lifetime for IPsec SAs;
- Ability to configure the interaction between TOE components;
- Ability to set the time which is used for time-stamps;
- Ability to configure the reference identifier for the peer
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Ability to import X.509v3 certificates to the TOE's trust store].

FMT_SMF.1/FFW Specification of Management Functions

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

- *Ability to configure firewall rules*;

FMT_SMF.1/VPN Specification of Management Functions (VPN Gateway)

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

- *Definition of packet filtering rules;*
- *Association of packet filtering rules to network interfaces;*
- *Ordering of packet filtering rules by priority;*

[

- No other capabilities*]*].

FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator*.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

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.

5.3.8 Packet Filtering (FPF)

FPF_RUL_EXT.1 Rules for Packet Filtering

FPF_RUL_EXT.1.1 The TSF shall perform packet filtering on network packets processed by the TOE.

FPF_RUL_EXT.1.2 The TSF shall allow the definition of packet filtering rules by using the following network protocols and protocol fields: [

- *IPv4 (RFC 791)*
  - *source address*
  - *destination address*
  - *protocol*
- *IPv6 (RFC 8200)*
  - *source address*
  - *destination address*
  - *next header (protocol)*
- *TCP (RFC 793)*
  - *source port*
  - *destination port*
- *UDP (RFC 768)*
  - *source port*
  - *destination port*

].

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.

FPF_RUL_EXT.1.4 The TSF shall allow the packet filtering rules to be assigned to each distinct network interface.

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*].

FPF_RUL_EXT.1.6 The TSF shall drop traffic if a matching rule is not identified.

Application Note: This SFR has been modified by TD0683.

5.3.9 Protection of the TSF (FPT)

FPT_FLS.1/SelfTest Failure with Preservation of Secure State (Self-Test Failures)

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*].

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and **detect its** modification when it is transmitted between separate parts of the TOE **through the use of [IPsec]**.

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

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

FPT_TST_EXT.1 TSF Testing

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: **noise source health tests,** [*integrity of executable code, DRBG randomness test*].

FPT_TST_EXT.3 TSF Self-Test with Defined Methods

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*].

FPT_TST_EXT.3.2 The TSF shall execute the self-testing through [*a TSF-provided cryptographic service specified in FCS_COP.1/**SigGen***].

FPT_TUD_EXT.1 Trusted update

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 [no other TOE firmware/software version].

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].

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.

FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [allow the Security Administrator to set the time **(applies to GSS and Cube)**, obtain time from the underlying virtualization system **(applies to GSS only)**].

Application Note: This SFR has been modified by TD0632

5.3.10 TOE Access (FTA)

FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [

- terminate the session]

after a Security Administrator-specified time period of inactivity.

FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate **a remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

FTA_SSL.4 User-initiated Termination

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

FTA_TAB.1 Default TOE Access Banners

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.

5.3.11 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall **be capable of using [TLS] to provide** a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [no other capabilities]** 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**.

FTP_ITC.1.2 The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*transmission of audit records to the audit server*].

FTP_ITC.1/VPN Inter-TSF Trusted Channel (VPN Communications)

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**.
FTP_ITC.1.2/VPN	The TSF shall permit [*the authorized IT entities*] to initiate communication via the trusted channel.
FTP_ITC.1.3/VPN	The TSF shall initiate communication via the trusted channel for [remote VPN gateways or peers].

FTP_TRP.1 /Admin Trusted Path

FTP_TRP.1.1/Admin	The TSF shall **be capable of using [TLS, HTTPS] 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**.
FTP_TRP.1.2 /Admin	The TSF shall permit remote **Administrators** to initiate communication via the trusted path.
FTP_TRP.1.3 /Admin	The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

5.4 Assurance Requirements

34 The TOE security assurance requirements are summarized in Table 19.

Table 19: Assurance Requirements

Assurance Class	Assurance Components
Security Target (ASE)	Conformance Claims (ASE_CCL.1)
	Extended Components Definition (ASE_ECD.1)
	ST Introduction (ASE_INT.1)
	Security Objectives for the operational environment (ASE_OBJ.1)
	Stated Security Requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE Summary Specification (ASE_TSS.1)
Development (ADV)	Basic Functional Specification (ADV_FSP.1)
Guidance Documents (AGD)	Operational User Guidance (AGD_OPE.1)
	Preparative User Guidance (AGD_PRE.1)
Life Cycle Support (ALC)	Labelling of the TOE (ALC_CMC.1)
	TOE CM Coverage (ALC_CMS.1)
Tests (ATE)	Independent Testing – conformance (ATE_IND.1)
Vulnerability Assessment (AVA)	Vulnerability survey (AVA_VAN.1)

35 In accordance with section 7.1 of the NDcPP, the following refinement is made to ASE:

- **ASE_TSS.1.1C Refinement:** The TOE summary specification shall describe how the TOE meets each SFR. **In the case of entropy analysis, the TSS is used in conjunction with required supplementary information on Entropy.**

6 TOE Summary Specification

36 The following describes how the TOE fulfils each SFR included in section 5.3.

6.1 Security Audit

6.1.1 FAU_GEN.1, FAU_GEN.1/VPN, FAU_GEN.2 & FAU_GEN_EXT.1

37 The TOE generates the audit records specified at FAU_GEN.1 containing fields that include the timestamp, IP address (if applicable), action, user (if applicable) and a contextual message indicating success or failure of the action.

38 GoSilent Server and GoSilent Cube generate audit records specified at FAU_GEN.1, FAU_GEN.1/VPN, FAU_GEN.2, and FAU_GEN_EXT.1 for operation and administration of each component. The specific events audited on each component correspond to the SFRs applicable to each component and can be found in Table 17 and Table 18. Auditing is always enabled, and each audit record includes:

- Date and time of the event,
- Type (i.e., category and action) of event,
- Subject (i.e., user and domain) identity,
- Result (success or failure) of the event, and
- Description (where applicable access mode, target object, etc.).

39 The TOE includes the user identity in audit events resulting from actions of identified users.

40 For audit records involving the generating/import of, changing, or deleting of cryptographic keys, the record identifies the key via reference to the certificate or key identifier associated with the key.

41 The GoSilent Server and GoSilent Cube components generate audit records associated with the SFRs they implement as specified in Table 20: SFR Distribution Between Components.

6.1.2 FAU_STG_EXT.1 & FAU_STG_EXT.4

42 Each TOE component stores audit event records that are generated on that component. GSS can store up to 50MB of audit information and the Cube can store up to 1.5MB. When that space is exhausted, the oldest records are discarded so that new records can be saved. The records are stored in a series of 5 files, 10MB each on GSS and 300KB each on the Cube. The current file is always “messages”. When it fills, it is initially renamed messages1 and a new (empty) messages file is created. As additional files fill, the number appended to each of the existing files is incremented to make room for a new messages1. The name of the messages4 file is not incremented; instead, that file is deleted to limit the amount of saved data.

43 Each component also transmits a copy of each audit record to an external syslog server in real time; the syslog server is configured on GoSilent Server and communicated to all GoSilent Cubes. Each Cube transmits the syslog server traffic via TLS through the established IPsec tunnel. Once the IPsec header has been stripped by GSS, the syslog (TLS) traffic is then forwarded to the syslog server based on the IP destination address. If the connection to the syslog server is unavailable, audit records continue to be saved locally. Once the connection is re-established, audit logs saved locally but not previously transmitted to the syslog server and sent.

44 GoSilent Server provides a mechanism for authorized administrators to view local audit records via the management GUI. GoSilent provides the capability to export audit record files for external review.

45 Only authorized administrators may view audit records and no capability to modify the audit records is provided.

6.2 Communication (FCO)

6.2.1 FCO_CPC_EXT.1

46 GoSilent Cube registration (enablement) involves some manual configuration by an authorized administrator on GoSilent Server prior to the enablement process taking place. The X.509 certificate for GoSilent Server and the specific GoSilent Cube are communicated out of band and imported by an authorized administrator on that component. Guidance information instructs administrators to use a secure communication channel for communication of the certificates.

47 When the necessary steps have been taken by an administrator to prepare the Cube for enablement, the channel described in FCO_CPC_EXT.1 is used to execute and finalize the registration process which occurs during the first connection of a Cube to GSS.

48 Any attempt by a GoSilent Cube to establish an IPsec tunnel (connect) to GoSilent Server is rejected by the GoSilent Server if enablement has not been completed. Each GoSilent Cube only establishes an IPsec tunnel with GoSilent Server. Attempts to establish an IPsec tunnel from one GoSilent Cube to another are always rejected. Alternatively, a cube may also be suspended from within the GSS GUI, whereby subsequent connections from the cube are rejected.

6.3 Cryptographic Support

6.3.1 FCS_CKM.1, FCS_CKM.1/IKE, & FCS_CKM.2

49 As described in FCS_CKM.1, the TOE generates 2048-bit RSA keys and P-384 ECC keys in support of TLS client connections with the syslog server, and P-384 ECC keys in support of Administrative GUI TLS server sessions. When performing Elliptic Curve Diffie-Hellman, the TOE acts as a sender with the TLS client connections and a recipient with the TLS server connections.

50 These keys are also used to authenticate the TOE component to the administrator in TLS exchanges for the management GUI.

51 As described in FCS_CKM.1/IKE, the TOE generates ECDSA P-256 and P-384 Elliptic Curve keys as specified in FIPS Pub 186-4 “Digital Signature Standard (DSS)” Appendix B.4 and implements all “shall” and “should” statements and does not implement any “shall not” or “should not” statements. In addition, the TOE also generates keys with FFC schemes using safe-prime groups that meet NIST SP 800-56A Revision 3 and per RFC3526 for DH14.

These keys are used to perform Diffie-Hellman in IPsec and adhere to a size equivalent to or greater than a strength of 112 bits.

52 The TOE acts as a sender and a recipient when performing Diffie-Hellman.

53 The TOE supports key establishment as follows:

- TLS Client to syslog server – RSAES-PKCS1-v1_5 and Elliptic-curve (P-384)
- TLS Server for administrative GUI - Elliptic-curve (P-384)

- IKE/IPsec - Elliptic-curve (P-256, P-384) and FFC safe-primes (RFC 3526 DH14)

54 ECDSA key pairs for X509 certificates can also be generated through the TOE GUI where the option of keys using P-256 or P-384 curves can be selected.

6.3.2 FCS_CKM.4

55 The TOE leverages the underlying filesystem to facilitate the destruction of cryptographic keys. Cryptographic keys in volatile and non-volatile are overwritten with zeroes when a key is deleted. Keys in volatile memory are also destroyed when a component is powered down or rebooted. The following keys and other sensitive information are maintained on each component:

- ECDSA private key – stored on the hard drive and overwritten when a factory reset is performed
- IPsec session key – stored in volatile memory and overwritten when a session is terminated
- TLS session key - stored in volatile memory and overwritten when a session is terminated
- Administrator passwords – Plaintext value is stored in volatile memory when supplied by a user and overwritten after validation; configured administrator passwords are stored on the hard drive as hashed (SHA-256) values only

6.3.3 FCS_COP.1/DataEncryption

56 The TOE performs data encryption and decryption functions using AES 128 and 256 bit encryption in CBC and GCM modes as follows:

- TLS Client to syslog server – AES-GCM, 128 or 256 bit keys
- TLS Server for administrative GUI - AES-GCM, 256 bit keys
- IKE/IPsec – AES-CBC or AES-GCM, 128 or 256 bit keys

6.3.4 FCS_COP.1/SigGen

57 The TOE provides cryptographic signature generation and verification services using:

- ECDSA P-256 and P-384 SigGen to support IPsec and TLS functions.
- ECDSA P-256 and P-384 SigVer to support IPsec, TLS, X.509, trusted update functions including firmware integrity checking.
- RSA SigGen and SigVer with key sizes of 2048 bits to support TLS client connections

58 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.3.5 FCS_COP.1/Hash

59 The TOE provides cryptographic hashing services using SHA-1, SHA-256, and SHA-384.

60 These hashes are used for SigGen and SigVer operations; SHA-256 is used for hashing configured passwords. The hash algorithms are also used in the associated HMAC algorithms.

61 SHA-256 and SHA-384 are used with TLS client connections to the syslog server.

62 SHA-1, SHA-256, and SHA-384 are used with IKE/IPsec connections.

63 SHA-384 is used for TLS server connections for the administrative web GUI.

64 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.3.6 FCS_COP.1/KeyedHash

65 The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384.

66 The TOE uses HMAC-SHA-256 and HMAC-SHA-384 TLS KDF and TLS message authentication, and TLS client connections to the syslog server with key sizes [256, 384] bits, [512, 1024] bit block size, and [256, 384] bit message digest size. The administrative GUI uses HMAC-SHA-384 with a key size of 384 bits.

67 The TOE uses HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384 for IKE/IPsec, with key sizes [160, 256, 384] bits, [512, 512, 1024] bit block size, and [160, 256, 384] bit message digest size.

68 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.3.7 FCS_IPSEC_EXT.1

69 The TOE implements the IPsec architecture per RFC 4301 using tunnel mode. Only IKEv2 is supported. AES in CBC and GCM mode using 128- or 256-bit keys is supported for both IKEv2 and ESP. HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384 are used with CBC mode. IPsec support includes:

- NAT traversal
- SA lifetimes based on time, configurable between 1 and 24 hours
- Child SA lifetimes based on time, configurable between 1 and 8 hours
- DH groups 14, 19 and 20 (security strengths 112, 128 and 192 bits)[1]
- Size of the random secret value “x” and nonce used for key establishment, as generated by the DRBG, is at least twice the security strength of that associated with the negotiated DH group.
- Child SA key sizes must be the same or less than the IKEv2 SA key size. During the IKEv2 CHILD_SA process, the TOE performs checks to ensure that encryption strengths for the selected algorithm are less than or equal to that of the IKEv2 SA.
- Peer authentication using ECDSA certificates
- Distinguished Names as reference identifiers.

70 The GoSilent Server has a nominal SPD that denies all traffic. When an IPsec tunnel to GoSilent Server is established, an SPD entry is dynamically added that permits all traffic received from user systems with an IP source address that is consistent with the IP subnet address configured for the GoSilent Cube IPsec interface. No traffic from a user system is forwarded to the TOE Network other than through an IPsec tunnel (to GoSilent Server).

71 The GoSilent Server has a nominal SPD that denies all traffic to any GoSilent Cube. When an IPsec tunnel from each GoSilent Cube is established, an SPD entry is

[1] DH groups used in IPsec VPN configurations are selectable within GSS. The default selection is DH20.

dynamically added that permits all traffic destined for an IP address that is consistent with the IP subnet address configured for the GoSilent Cube IPsec interface.

6.3.8 FCS_TLSC_EXT.1

72 The TOE acts as a TLS client to provide a trusted channel to the syslog server. The TOE initiates this connection. This client supports TLSv1.2 with the following ciphersuites:

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

73 Any SSL/TLS version stated in the Server Hello other than TLS v1.2 causes the connection to be terminated.

74 The TOE always presents the Supported Elliptic Curves Extension indicating support for P-384 in the Client Hello.

75 The TOE automatically parses the reference identifier from the connection parameters, using the hostname or IP address as the reference identifier. When validating the server certificate, the TSF matches the reference identifier against the SAN:DNS or SAN:IP address field in the presented certificate (if present) per RFC 6125 section 6 and falls back to the CN if the SAN is not present. The TOE treats the CN as a string value and compares the configured syslog server string to that value. The TOE does not support wildcards.

6.3.9 FCS_TLSS_EXT.1, FCS_HTTPS_EXT.1

76 The TOE acts as a TLS/HTTPS server to provide a web GUI to administrators. This server supports TLSv1.2 with the following ciphersuites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

77 Any SSL/TLS version stated in the Client Hello other than TLS v1.2 causes the connection to be terminated.

78 Key Establishment is performed using Elliptic Curve Diffie-Hellman P-384 keys.

79 This connection is always initiated by the remote end.

80 Session resumption and session tickets are not supported.

6.3.10 FCS_RBG_EXT.1

81 The TOE implements a Counter DRBG (AES), compliant with SP800-90A to generate random bits needed for asymmetric key, symmetric key, nonce, and salt generation. The DRBG is seeded with 256 bits of entropy from one software-based noise source.

82 Additional detail is provided in the proprietary Entropy Description.

6.4 User Data Protection (FDP)

6.4.1 FDP_RIP.2

83 The only resource made available to information flowing through a TOE is the temporary storage of packet information when access is requested and when information is being routed. User data is not persistent when resources are released by one user/process and allocated to another user/process. Temporary storage (memory) used to build network packets is erased when the resource is released.

Therefore, no residual information from packets in a previous information stream can traverse through the TOE.

6.5 Firewall (FFW) & Packet Filtering (FPF)

6.5.1 FFW_RUL_EXT.1 & FPF_RUL_EXT.1

84 The TOE performs stateful packet filtering on all packets received from or being sent to the External Network, MGMT interface or WAN interface (excepting IPsec traffic) of the GoSilent Server.

85 The boot sequence of the TOE aids in establishing the secure domain and preventing tampering or bypass of security functionality. This includes ensuring the packet filtering rules cannot be bypassed during the boot sequence of the TOE. The following steps list the boot sequence for the TOE:

- BIOS hardware and memory checks
- Loading and initialization of the OS
- Self-tests including firmware integrity tests are executed
- The init utility is started (mounts file systems, sets up network cards, and generally starts all the processes that usually are run on the system at startup)
- Daemon programs such as Internet Service Daemon (INETD), Syslogd are started; Routing and forwarding tables are initialized
- Application daemons are loaded, enabling access to the GoSilent Server management GUI
- Physical interfaces are active

86 Once the interfaces are brought up, they will start to receive and send packets based on the current configuration (or not receive or send any packets if they have not been previously configured). Interfaces are brought up only after successful loading of the kernel and daemons, and these interfaces cannot send or receive packets unless previously configured by an administrator. Since the daemon for the management GUI is not loaded until after the kernel and INETD are initialized, no modification to the security attributes can be made by a user or process other than via the management process.

87 The TOE applies a uniform policy to the traffic flows to and from all GoSilent Cube users. By default, no traffic is allowed to flow from GoSilent Cube users to the External Network, no traffic is allowed to flow from the External Network to GoSilent Cube users, and no traffic is allowed to flow between GoSilent Server interfaces.

88 By default, the TOE allows administrators to define traffic filtering rules based on a distinct interface and the following network protocol fields:

- ICMPv4 (Type, Code)
- ICMPv6 (Type, Code)
- IPv4 (Source address, Destination address, Transport Layer Protocol)
- IPv6 (Source address, Destination address, Transport Layer Protocol)
- TCP (Source port, Destination port)
- UDP (Source port, Destination port)

89 The TOE maintains a session table which tracks all known TCP and UDP sessions based on the information in incoming packets. Specifically, the lookup is based on an exact match of the following network packet attributes:

- TCP
  - i) Source and Destination IP address
  - ii) Source and Destination Port
  - iii) Protocol Flags (e.g. SYN, ACK, RST, and FIN flags),
  - iv) Sequence numbers
- UDP
  - i) Source and Destination IP address
  - ii) Source and Destination Port

90 The TSF allows the definition of packet filtering rules by using the following network protocols and protocol fields:

- IPv4 (RFC 791)
  - i) Source address
  - ii) Destination address
  - iii) Protocol
- IPv6 (RFC 8200)
  - i) Source address
  - ii) Destination address
  - iii) Next header (protocol)
- TCP (RFC 793)
  - i) Source port
  - ii) Destination port
- UDP (RFC 768)
  - i) Source port
  - ii) Destination port

Conformance with the above listed RFC's has been determined through testing and development and as a requirement of this evaluation.

91 For TCP sessions, the TOE removes existing traffic flows from the list of established sessions based on the completion of the session. An exchange of FIN flags indicates the end of data transmission to finish a TCP connection, at which point the session is terminated and the session is removed from the table. TCP session are also removed after a configurable session inactivity timeout threshold. By default, this threshold is 432000 seconds. Once this timeout period has been reached, the TOE will then terminate the connection and remove it from the table. New packets that match the session will start a new session.

92 UDP sessions are removed after the session inactivity timeout threshold. Once this threshold has been reached, the TOE terminates the connection and removes it from the table. New packets that match the session will start a new session.

93 The default session timeout thresholds for TCP and UDP connections are indicated below.

94 Traffic for known sessions is permitted to flow. For traffic not associated with known sessions, rules within information flow policies are processed in an administrator-defined order to determine if the traffic should be forwarded. By default, the TOE behavior is to deny packets when there is no rule match. The TOE performs stateful network traffic filtering on network packets using the network traffic protocols and network fields specified in FFW_RUL_EXT.1.5 and FPF_RUL_EXT.1.3. The TOE allows permit, deny, and log operations to be associated with rules and these rules can be assigned to distinct network interfaces.

95 The TOE tracks the number of half-open TCP connections. When the configured limit for half-open TCP connections is exceeded, TCP SYN are discarded until the number drops below the configured limit. An audit record is generated if the firewall rule is configured to log these events. Half-open TCP connections are automatically discarded after a 60 second timeout period. The following default timeout parameters (in seconds) are configurable in GSS within the Networking tab:

- Generic IP Timeout: 600
- TCP Connection Timeout: 432000
- UDP Protocol Timeout: 30
- UDP Stream Timeout: 180

96 In situations where the TOE receives packets faster than they can be processed (flooding), the TOE silently discards the excess packets. An audit record is generated when flooding is detected, but not for each packet.

97 The TOE can enforce the following reject rules with logging on traffic:

- invalid fragments (counted by TSF);
- fragmented IP packets which cannot be re-assembled completely (counted by TSF);
- where the source address is equal to the address of the network interface where the network packet was received;
- where the source address does not belong to the networks associated with the network interface where the network packet was received;
- where the source address is defined as being on a broadcast network;
- where the source address is defined as being on a multicast network;
- where the source address is defined as being a loopback address;
- where the source address is a multicast;
- packets where the source or destination address is a link-local address;
- where the source or destination address is defined as being an address “reserved for future use” as specified in RFC 5735 for IPv4;
- where the source or destination address is defined as an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6;
- with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified;

- where the source address of the network packet is equal to the address of the network interface where the network packet was received;
- where the source or destination address of the network packet is a link-local address;
- where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received;
- when a new TCP connection attempt would exceed the configured limit of half-open TCP connections;
- packets are checked for validity. “Invalid fragments” are those that violate these rules:
    i) No overlap
    ii) The total fragments in one packet should not be more than 62 pieces
    iii) The total length of merged fragments should not larger than 64k
    iv) All fragments in one packet should arrive in 2 seconds
    v) The total queued fragments has limitation, depending on the platform
    vi) The total number of concurrent fragment processing for different packet has limitations depending on platform

98 The TOE logs the actions taken on packets when they are processed by the INPUT, OUTPUT, and FORWARD rulesets.

99 In the event of a component failure, such as the firewall failing to initialize, the TOE will not enter a state where network traffic is able to flow. If a component fails during operation, the TOE will enter into a non-operational state and reboot.

6.6 Identification and Authentication

6.6.1 FIA_AFL.1, FIA_PMG_EXT.1, FIA_UIA_EXT.1, FIA_UAU_EXT.2 & FIA_UAU.7

100 Management of the TOE is primarily performed locally or remotely through GoSilent Server. However, management of GoSilent Cube locally provides the initial configuration information for it to connect to GoSilent Server.

101 Identification and authentication are required for both local and remote administrator access. Management access to the TOE is via an HTTPS session.

102 The TOE supports local authentication where it looks up the username in its local configuration and compares the hash of the password to the saved value. If the credentials are valid, the user is successfully authenticated and is authorized to access the management interface.

103 Authentication of an administrator is through use of a username/password. The minimum password may be configured from 8 to 40 characters, that incorporate a combination of lowercase letters, uppercase letters, numbers and special characters (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”). During entry of the password, each character entered is masked with a “*” when progress is reflected on the screen. If an authentication attempt fails, (either the username is not recognized or the password is incorrect) the same “Login failed” error message is presented.

104 The TOE tracks the number of sequential failed authentication attempts for each user account. Upon meeting the configured limit for failed authentication attempts,

the TOE locks the account in question for an administrator configured period of time. During this time, entering the correct password for the locked account will still result in an authentication failure. Any successful authentication resets the counter to zero.

105 For both local and remote connections, the TOE only provides the warning banner as described in FTA_TAB.1 prior to authentication. For local connections only, the GoSilent Cube also provides a function to reset the Cube to factory default configuration via the GUI.

106 Local access to the GoSilent Server is via an HTTPS session through the MGMT interface. The source IP address must match the configured whitelist address. Administrator account lockout is not applicable to local access. Remote administrator access is via an HTTPS session from GoSilent Cube client systems.

107 Local access for GoSilent Cube is via the Ethernet interface labelled 'Device'. Remote configuration of some features on the GoSilent Cube can be achieved via GoSilent Server. Those configuration settings are downloaded by the GoSilent Cube when it establishes an IPsec tunnel to the GoSilent Server.

6.6.2 FIA_X509_EXT.1/ITT, FIA_X509_EXT.1/Rev, FIA_X509_EXT.2, FIA_X509_EXT.3

108 The TOE uses X.509 certificates to:

- provide IPsec connections between GSS and Cube devices
- verify the identity of the Syslog server

109 When a TOE component receives a certificate asserting the identity of a remote system during an IPsec connection, the TOE ensures the current time is within the validity time of the certificate, the certificate has not been revoked (verified via OCSP for IPsec or CRLs for TLS), contains the appropriate extendedKeyUsage purpose set (Server Authentication), and the certificate chain terminates with a trusted CA certificate. The certificate chain is validated by verifying each certificate (except for the end entity certificate) in the chain is currently valid, has not been revoked, contains the basic constraints extension with the CA flag set to TRUE, and is signed by a trusted CA or is explicitly configured as a trusted CA. If the TOE cannot establish a connection to the OCSP server, the TOE will reject the certificate. The certificate of the OCSP responder must include OCSP Signing in its EKU. If the TOE cannot establish a connection to the CDP, the TOE will accept the certificate.

110 Revocation checking for the entire certificate chain (to the Root) is performed when certificates are loaded into the TOE, when certificates are received from the remote side during TLS and IPsec connection establishment, and when OCSP responses are received.

111 The EKU checks for Code Signing and Client Authentication are not applicable to this TOE. Trusted updates are not verified using X.509 certificates, and TLS mutual authentication is not supported.

112 On GoSilent Server, distinct leaf certificates are supported for IPsec (VPN connections) and the administrator GUI. The same certificate can be used for both functions, or separate certificates can be used and are therefore determined during import when selecting the usage for the certificate. On GoSilent Cube, a distinct leaf certificate is supported for IPsec connections with each configured Server profile. The certificates used is determined by the certificate configured in the profile selected by the user. On the Cube, the client certificate to be used is chosen during the configuration of the server profile (Virtual Server setup). When receiving a certificate, GSS will verify it against its own trust store, and check the revocation status via OCSP (for IPsec) and CRL (for TLS).

6.7 Security Management

6.7.1 FMT_MOF.1/ManualUpdate, FMT_MOF.1/Services, FMT_MTD.1/CoreData, FMT_MTD.1/CryptoKeys, FMT_SMF.1, FMT_SMF.1/FFW, FMT_SMF.1/VPN, FMT_SMR.2

113 Management of the TOE is primarily performed through GoSilent Server. However, initial management of GoSilent Cube, providing enough configuration information for it to connect to GoSilent Server, is required. The TOE supports the role of Security Administrator. The TOE can be administered both locally and remotely.

114 The GoSilent Server provides the following management capabilities to authorized administrators both locally and remotely:

- Perform manual updates of GoSilent Server;
- Enable and disable audit logging (although note that the evaluated configuration requires auditing to be enabled at all times);
- Manage (import) cryptographic keys and certificates;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to configure firewall rules;
- Ability to configure the cryptographic functionality;
- Ability to configure the lifetime for IPsec SAs;
- Ability to configure the transmission of audit data;
- Ability to set the time which is used for time-stamps;
- Ability to configure the reference identifier for the peer
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;

115 GoSilent Cube provides the following management capabilities to authorized administrators locally:

- Perform manual updates of the GoSilent Cube the administrator is connected to;
- Manage (import) cryptographic keys and certificates;
- Ability to configure the cryptographic functionality;
- Ability to set the time which is used for time-stamps;
- Ability to configure the reference identifier for the peer

116 The Cube provides the ability to pull additional configuration information from the GSS it is registered with upon connection establishment and includes the following:

- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to configure the authentication failure parameters for FIA_AFL.1;

- Ability to configure the transmission of audit data;

6.8 Protection of the TSF (FPT)

6.8.1 FPT_APW_EXT.1 & FPT_SKP_EXT.1

117 The TOE does not provide access to the filesystem or any administrative interface, including those designed specifically for that purpose, that would allow a user or administrator to view plaintext administrative passwords, pre-shared keys, symmetric keys, or private keys and additionally prevents the reading of any plaintext administrative passwords by instead storing their SHA-256 hash values.

118 All administrative password hashes, pre-shared keys, symmetric keys, and private keys are stored in non-volatile memory at non-fixed locations that are otherwise not accessible by administrative users.

6.8.2 FPT_FLS.1/SelfTest, FPT_TST_EXT.1, FPT_TST_EXT.3

119 At power-on tests are performed on each component to confirm the integrity of the firmware and a statistical assessment of the entropy source. The integrity of the firmware is tested using the cryptographic services described in FCS_COP.1/SigGen, which covers all of the executable code. The noise source health test performs a statistical assessment of 1000 samples. DRBG randomness test compares the current and previously generated blocks to see if they are the same. Identical blocks indicate a failure of the generation function and produce an error and an error return value.

120 If any test fails, that component does not enter an operational state and the network interfaces are not activated. For GoSilent Server, an error is displayed on the local console accessible via ESXi). For GoSilent Cube, the LEDs indicate the system is not operational.

121 These tests are sufficient to demonstrate the TSF is operating correctly, as they confirm the integrity of all firmware modules prior to their execution, thereby confirming the modules have not been modified or replaced in any unauthorized manner, and they ensure the DRBG continues to operate successfully providing sufficient entropy in response to any requests.

6.8.3 FPT_ITT.1

122 All communication between the TOE components uses IPsec to protect the traffic.

123 IPsec connections are always initiated by GoSilent Cube; GoSilent Server only receives incoming connections from GoSilent Cube devices.

6.8.4 FPT_TUD_EXT.1

124 Authorized administrators can query the current version of the TOE software via the administration GUI. The administrator can initiate a manual update of the TOE component that they are connected to. Updates are downloaded from a specified URI using HTTPS. Administrators can manually load the update file on the GoSilent Server. An option is provided for administrators to download GoSilent Cube updates to itself from the ID Technologies update server. The updates are signed with an ID Technologies Security key. Once the image has been downloaded, the TOE checks the signature of the image (against the ID Technologies Security public key) before the image is applied.

125 When an update is successfully verified and installed, GSS will reboot automatically and the software update takes effect. If the update is unsuccessful or otherwise fails,

GSS will not proceed with the installation and continue to execute the current software version without interruption.

126 Prior to the installation of a software update, the Cube will tear down any active tunnels to ensure the integrity of the Cube and update process. Once the update is successfully verified and installed on the Cube, it will reestablish the tunnel with GSS. Should the verification of the update fail or is otherwise unsuccessful, the Cube will not proceed with the installation and continue executing the currently installed software version without interruption.

6.8.5 FPT_STM_EXT.1

127 GoSilent Server and GoSilent Cube each maintain a system clock used to provide date and time information for TOE operations, including reliable timestamping for audit logs, and validation of certificate expiration dates. The time can be manually set by authorized administrators only.

128 GoSilent Server receives time information from the virtualization platform to maintain the time across system reboots. When a VM is started, ESXi provides the VM with the ESXi's internal time value. Upon startup, the GSS sets its internal clock to that time from ESXi. Subsequently, the GSS internal clock is used and subsequent synchronization with the ESXi clock is not performed. There is a delay in updating the clock until the next GoSilent Server restart. Time information obtained from the underlying virtualization platform is considered to be reliable because access to the virtualization platform, including the time setting function, is restricted to authorized administrators of the platform only. When setting the time manually on GSS, only authorized administrators have access to and can modify that function.

129 For GoSilent Cube, guidance directs the administrator to manually set the clock on each reboot since it does not include a real-time clock.

6.9 TOE Access (FTA)

6.9.1 FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4

130 Following an administrator configured period of inactivity (of both local and remote interactive sessions) the session will be automatically terminated, requiring re-authentication by the administrator before the access to TOE functionality can be gained.

131 The administrator is able to terminate their GUI session by using the logout button.

6.9.2 FTA_TAB.1

132 The TOE displays an administrator configurable message prior to local and remote login via the GSS GUI. The Cube also displays an administrator configurable message prior to local login via the Cube GUI.

133 Prior to local and remote login to GSS and local login to the Cube, the GUI displays a consent banner to the administrator warning that proceeding with authentication is consenting to the terms of use of the TOE. The user is then prompted to enter their username and password.

6.10 Trusted Path/Channels (FTP)

6.10.1 FTP_ITC.1, FTP_ITC.1/VPN

134 Trusted channels are used for connections between GoSilent Cube and GoSilent Server as well as with the syslog server. TLS syslog server connections are always initiated by GoSilent Server and GoSilent Cube. IPsec connections between TOE components are always initiated by the GoSilent Cube.

6.10.2 FTP_TRP.1/Admin

135 The TOE provides a trusted path for remote administration of the GoSilent Server and GoSilent Cube. These logically distinct communications paths use TLS and HTTP to protect any transmitted data from unauthorized disclosure and leverage the ciphersuites listed in FCS_TLSS_EXT.1.

136

7 Rationale

7.1 Conformance Claim Rationale

137 The following rationale is presented with regard to the PP conformance claims:

- **TOE type.** As identified in section 2.1, the TOE is a network device, Firewall, and VPN Gateway consistent with the claimed protection profiles and PP Module.
- **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the CPP_ND_V2.2E, MOD_CPP_FWv1.4e, and MOD_VPNGW_v1.2.
- **Security objectives.** As shown in section 4, the security objectives are reproduced directly from the CPP_ND_V2.2E, MOD_CPP_FWv1.4e, and MOD_VPNGW_v1.2.
- **Security requirements.** As shown in section 5, the security requirements are reproduced directly from the CPP_ND_V2.2E, MOD_CPP_FWv1.4e, and MOD_VPNGW_v1.2. Some SFR selections were chosen to ensure compliance with CSfC requirements. No additional requirements have been specified.

7.2 Security Objectives Rationale

138 All security objectives are drawn directly from the claimed Protection Profiles and PP-Modules.

7.3 Security Requirements Rationale

139 All security requirements are drawn directly from the claimed PP and PP-Modules in accordance with exact conformance. Refer to the Rationale sections of the PP and PP-Modules as follows:

- CPP_ND_V2.2e – Appendix ‘E’
- MOD_CPP_FW_V1.4e – Appendix ‘E’
- MOD_VPNGW_V1.2 – Section 5.3 and Section 6

7.4 SFR Distribution Between Components

140 The following table addresses the SFR distribution requirements between TOE components, as required in Section 3.1 of MOD_CPP_FW_v1.4e. Since SFRs drawn from MOD_VPNGW_v1.2 are not addressed by the distribution requirements in MOD_CPP_FW_v1.4e, their distribution requirements in the following table have been specified to be consistent with the requirements for similar SFRs.

Table 20: SFR Distribution Between Components

SFR	Dist. Requirement	GoSilent Server	GoSilent Cube
FAU_GEN.1	All	X	X
FAU_GEN.1/VPN	All	X	X

SFR	Dist. Requirement	GoSilent Server	GoSilent Cube
FAU_GEN.2	All	X	X
FAU_GEN_EXT.1	All	X	X
FAU_STG_EXT.1	All	X	X
FAU_STG_EXT.4	Feature Dependent	X	X
FCO_CPC_EXT.1	All	X	X
FCS_CKM.1	One	X	X
FCS_CKM.1/IKE	One	X	X
FCS_CKM.2	All	X	X
FCS_CKM.4	All	X	X
FCS_COP.1 /DataEncryption	All	X	X
FCS_COP.1 /SigGen	All	X	X
FCS_COP.1 /Hash	All	X	X
FCS_COP.1 /KeyedHash	All	X	X
FCS_RBG_EXT.1	All	X	X
FCS_HTTPS_EXT.1	Feature Dependent	X	X
FCS_IPSEC_EXT.1	Feature Dependent	X	X
FCS_TLSC_EXT.1	Feature Dependent	X	X
FCS_TLSS_EXT.1	Feature Dependent	X	X
FDP_RIP.2	Feature Dependent	X	X
FFW_RUL_EXT.1	One	X	
FIA_AFL.1	One	X	X
FIA_PMG_EXT.1	One	X	X
FIA_UIA_EXT.1	One	X	X
FIA_UAU_EXT.2	One	X	X

SFR	Dist. Requirement	GoSilent Server	GoSilent Cube
FIA_UAU.7	Feature Dependent	X	X
FIA_X509_EXT.1 /ITT	Feature Dependent	X	X
FIA_X509_EXT.1 /Rev	Feature Dependent	X	X
FIA_X509_EXT.2	Feature Dependent	X	X
FIA_X509_EXT.3	Feature Dependent	X	X
FMT_MOF.1 /ManualUpdate	All	X	X
FMT_MOF.1 /Services	Feature Dependent	X	X
FMT_MTD.1 /CoreData	All	X	X
FMT_MTD.1 /CryptoKeys	Feature Dependent	X	X
FMT_SMF.1	Feature Dependent	X	X
FMT_SMF.1 /FFW	Feature Dependent	X	
FMT_SMF.1 /VPN	Feature Dependent	X	
FMT_SMR.2	One	X	X
FPF_RUL_EXT.1	Feature Dependent	X	
FPT_FLS.1 /SelfTest	All	X	X
FPT_ITT.1	Feature Dependent	X	X
FPT_SKP_EXT.1	All	X	X
FPT_APW_EXT.1	Feature Dependent	X	X
FPT_TST_EXT.1	All	X	X
FPT_TST_EXT.3	All	X	X
FPT_TUD_EXT.1	All	X	X

SFR	Dist. Requirement	GoSilent Server	GoSilent Cube
FPT_STM_EXT.1	All	X	X
FTA_SSL_EXT.1	Feature Dependent	X	X
FTA_SSL.3	Feature Dependent	X	X
FTA_SSL.4	Feature Dependent	X	X
FTA_TAB.1	One	X	X
FTP_ITC.1	One	X	X
FTP_ITC.1 /VPN	One	X	X
FTP_TRP.1 /Admin	One	X	X

Annex A: Extended Components Definition

141 Refer to the Extended Components Definitions sections of the PP and PP-Module as follows:

- CPP_ND_V2.2 – Appendix ‘C’
- MOD_CPP_FW_v1.4e – Appendix ‘C’
- MOD_VPNGW_v1.2 – Appendix ‘C’