Attila Security SilentEdge Enterprise Server and GoSilent Client Security Target

Acumen Security, LLC.

Document Version: 1.3

Table Of Contents

Revision History

Version	Date	Description
1.0	2/15/2019	Initial Release
1.1	4/22/2019	Addressed validator comments
1.2	9/30/2019	Updates during evaluation
1.3	10/25/2019	Addressed validator comments

1 Security Target Introduction

1.1 Security Target and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Category	Identifier
ST Title	Attila Security SilentEdge Enterprise Server and GoSilent Client Security Target
ST Version	1.3
ST Date	10/25/2019
ST Author	Acumen Security, LLC.
TOE Identifier	Attila Security SilentEdge Enterprise Server and GoSilent Client
TOE Software Version	19.07.3
TOE Developer	Attila Security
Key Words	Firewall VPN

Table 1 TOE/ST Identification

1.2 TOE Overview

The Target of Evaluation (TOE) is the Attila Security SilentEdge Enterprise Server and GoSilent Client v19.07. These products operate together as a single distributed TOE. Each component is a network appliance.

The SilentEdge Enterprise Server is a dedicated server that acts as the centralized management and external access system for all GoSilent platforms integrated into one system. This platform provides the management GUI for configuration of SilentEdge as well as the GoSilent platforms. Operationally, it acts as the central peer for all IPsec connections from the GoSilent devices and provides gateway connectivity to external systems from the platforms located behind a GoSilent Client.

The GoSilent Client is a portable enterprise-grade firewall and VPN, ideal for sensitive communications, secure remote network access, and IoT deployments. GoSilent can be setup within minutes by non-technical users.

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

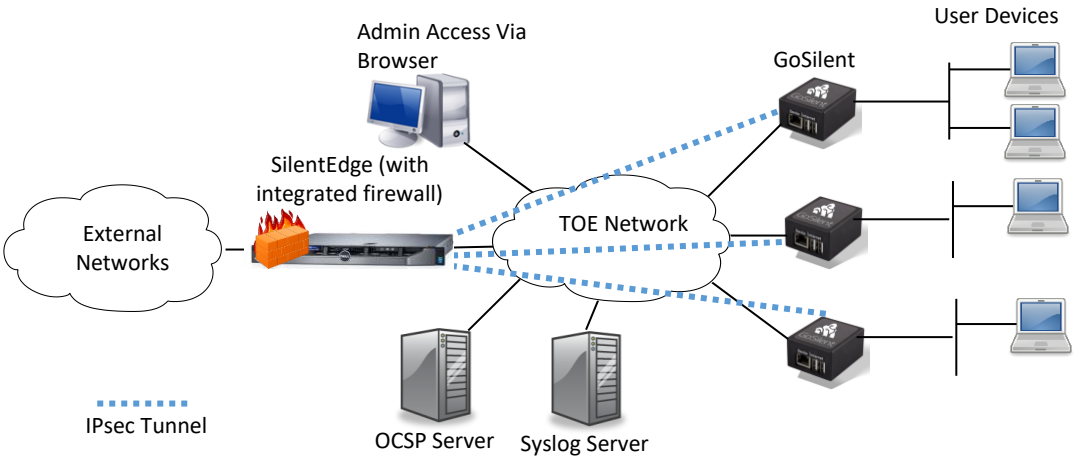
SilentEdge applies policies to restrict the traffic that is permitted to pass between the user systems and external networks.

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

GoSilent also provides 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 with enough information to connect to SilentEdge. All additional configuration information is downloaded from SilentEdge once the IPsec VPN is established.

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

Figure 1: Representative TOE Deployment

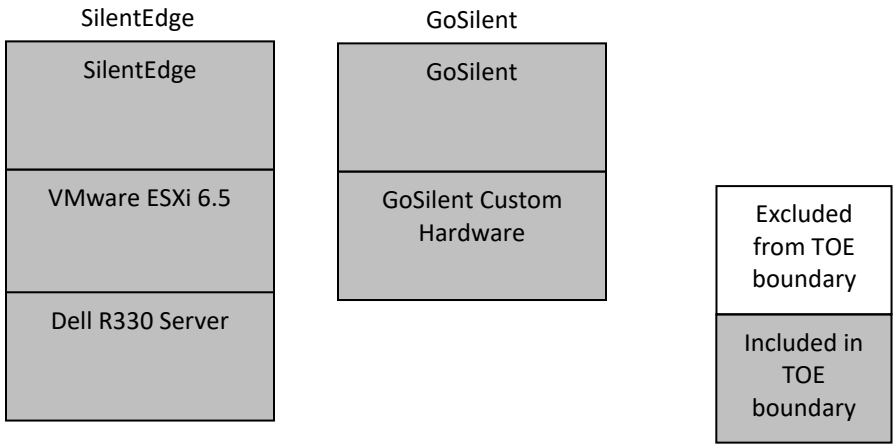


1.3 TOE Architecture

1.3.1 Physical Boundaries

The physical boundaries of the TOE are the physical boundaries of the Dell PowerEdge R330 Server used for the SilentEdge platform and the custom physical enclosure for GoSilent. The boundaries are illustrated in the following figure.

Figure 2: Physical Boundary



Details of the SilentEdge platform are:

Item	Description
Hardware Platform	Dell PowerEdge R330 Server
CPU	1 Intel Xeon E3-1270 v5
Memory	16GB UDIMM
Hard Drives	1 8GB SD card (used for hypervisor) 1 1TB 7.2K RPM SATA 6Gnps 3.5in HDD
Hypervisor	VMware ESXi 6.5
Network Interfaces	2 1Gb Ethernet

The Dell PowerEdge R330 Server comes factory-installed with an internal dual SD module. The SD module has no external access; the enclosure must be opened for access. The server has one 8GB SD card pre-populated that acts as a hard drive. This approach, as opposed to using a second traditional hard drive for the hypervisor, provides less accessibility, higher reliability, and lower power consumption compared to standard, hot swappable hard drive slots in the server.

Details of the GoSilent platform are:

Item	Description
Hardware Platform	Attila Security proprietary
CPU	Quad-core ARM v8 Cortex-A53
Memory	1GB DRAM
Hard Drives	8GB eMMC
Network Interfaces	RJ45 Ethernet for physical connection to user system(s) (Device) USB for user systems supporting (note the adapter is not part of the TOE): • Ethernet adapter (required in the evaluated configuration) • WiFi adapter providing Hotspot for user systems (note this option is not supported in the evaluated configuration)

1.3.2 Security Functions provided by the TOE

The TOE provides the security functionality required by [FWcPP] and [VPNGWEP].

1.3.2.1 Security Audit

Both SilentEdge and GoSilent generate audit records related to TOE operation and administration. These audit records are stored locally on SilentEdge and GoSilent and are also forwarded to an external audit server. When the audit storage reaches capacity, the oldest audit records are overwritten.

On SilentEdge, authenticated administrators can view audit records. GoSilent provides functionality for authorized administrators to export the audit records so that they can be viewed.

1.3.2.2 Cryptographic Support

The TOE provides the following cryptographic operations:

- Asymmetric key generation using ECC schemes (P-256, P-384) and Diffie-Hellman Group 14
- Asymmetric key establishment using RSA schemes (2048 bits), ECC schemes (P-256, P-384) and Diffie-Hellman Group 14
- AES data encryption in CBC and GCM mode with key sizes of 128 and 256 bits

- ECDSA digital signature generation and verification with key sizes of 256 bits and 384 bits
- RSA digital signature generation and verification with key size 2048 bit
- Hashing using SHA-1, SHA-256, SHA-384 and SHA-512
- Keyed hashing using HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-384
- DRBG functionality using CTR_DRBG (AES)

Storage space for cryptographic keys is overwritten with zeroes when the keys are deleted.

Communication protocols are provided for the following purposes:

- IPsec for intra-TOE communication between GoSilent and SilentEdge
- TLS/HTTPS for management GUI access on SilentEdge and GoSilent
- TLS for transmission of audit records to the syslog server

1.3.2.3 User Data Protection

When memory is deallocated, the storage space is overwritten with zeroes.

1.3.2.4 Firewall

The TOE provides stateful network traffic filtering based on examination of network packets and the application of information flow rules.

1.3.2.5 Identification and Authentication

Administrators connecting to the TOE are required to enter a valid username and password to authenticate the administrative connection prior to access being granted. If the configured number of authentication attempts is met for a configured remote administrator account, the account is locked for the configured amount of time.

SilentEdge and GoSilent authenticate to one another through X.509 certificates.

The syslog server is authenticated via X.509 certificates.

1.3.2.6 Security Management

An administrative GUI on SilentEdge and GoSilent can be accessed via TLS/HTTPS. These interfaces are used for administration of the TOE, including audit log configuration, upgrade of firmware and certificates, administration of users, configuration of IPsec and TLS connections. Only authorized administrators may access this management functionality.

1.3.2.7 Protection of the TSF

The TOE users must authenticate to the TOE before any administrative operations can be performed on the system. Passwords associated with administrator accounts are not stored in plaintext.

Self-tests are performed at component startup. If failures are detected in these self-tests, the component does not enter operational mode.

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

The TOE enables administrators to set the time on each component so that reliable timestamps can be inserted into audit records and to enable local validation of X.509 certificates.

The administrator can query the currently installed versions of software on the TOE components. Trusted update of the TOE software can be manually performed by authorized administrators using the management GUI.

1.3.2.8 TOE Access

The TOE monitors local and remote administrative sessions for inactivity and terminates the session when a threshold time is reached. An advisory notice is displayed at the start of each session.

1.3.2.9 Trusted Path/Channels

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

All communication with the syslog server uses TLS to protect the traffic.

All communication with remote administrators uses TLS/HTTPS to protect the traffic.

1.3.3 TOE Documentation

- Attila Security SilentEdge Enterprise Server and GoSilent Client Security Target
- Attila Security SilentEdge Enterprise Server and GoSilent Client Common Criteria Supplement

1.3.4 Other References

- collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0e+Errata 20180314 dated 14-March 2018 [FWcPP]
- Evaluation Activities for Stateful Traffic Filter Firewalls cPP, Version 2.0 dated October-2017
- Evaluation Activities for Network Device cPP, Version 2.0+Errata 20180314 dated March 2018
- Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, Version 2.1 dated 2017-03-08 [VPNGWEP]

1.4 TOE Environment

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

1. Ethernet USB adapter for the Network/VPN Ethernet interface of GoSilent
2. TOE Network – Provides communication between the TOE components. Since IPsec tunnels are layered on top of this network, the network itself is not required to be trusted.
3. External Network – SilentEdge provides user systems with connectivity to systems on an External network, which may be limited to an Enterprise Network or provide much wider access.
4. GoSilent user networks – Physical Ethernet network located on the user side of GoSilent that provide connectivity between user systems and GoSilent. In the simplest case, this is a direct connection using an Ethernet cable interconnecting the GoSilent RJ45 Device port and a user system. To support multiple user systems, an Ethernet switch can be used.
5. Local Management Workstation – Any computer using a web browser to access the management GUI via the dedicated Management Ethernet port of SilentEdge.
6. Management Workstation - Any computer that provides a supported browser may be used to access SilentEdge or GoSilent. The Management System can be connected via the TOE Network or the External Network.
7. Syslog Server that supports syslog over TLS. The Syslog Server may be connected to the TOE Network or the External Network. The Management System can be connected via the TOE Network or the External Network.

8. OCSP Server accessed via OCSP to determine X.509 certificate revocation status. The OCSP Server is connected via the TOE Network.
9. User systems – IT systems using GoSilent as a secure path to external systems.

1.5 Product Functionality Not Included in the Evaluation

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

1. Cloud instances of SilentEdge. SilentEdge is supported on physical platforms and cloud instances. Only physical platforms are included in the evaluation.
2. WiFi support for the user or Network/VPN interfaces of GoSilent.

2 Conformance Claims

2.1 CC Conformance

This TOE is conformant to:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 4, September 2012: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 4, September 2012: Part 3 extended

2.2 Protection Profile Conformance

This TOE is conformant to:

- collaborative Protection Profile for Stateful Traffic Filter Firewall + Errata 20180314, Version 2.0e [FWcPP]
- Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, Version 2.1 dated 2017-03-08 [VPNGWEP]

2.3 Conformance Rationale

This Security Target provides exact conformance to [FWcPP] and [VPNGWEP]. The security problem definition, security objectives and security requirements in this Security Target are all taken from the Protection Profile and Extended Package performing only operations defined there.

2.3.1 Technical Decisions

All NIAP Technical Decisions (TDs) issued to date that are applicable to [FWcPP] and [VPNGWEP] have been addressed. The following table identifies all applicable TDs:

Identifier	Applicable	Exclusion Rationale (if applicable)
TD0451: NIT Technical Decision for ITT Comm UUID Reference Identifier	Yes	
TD0447: IT Technical Decision for Using 'diffie-hellman-group-exchange-sha256' in FCS_SSHC/S_EXT.1.7	No	SSH functionality is not included in this evaluation.
TD0436: IPsec protocol ESP algorithms	Yes	
TD0423: NIT Technical Decision for Clarification about application of RfI#201726rev2	Yes	
TD0412: NIT Technical Decision for FCS_SSHS_EXT.1.5 SFR and AA discrepancy	No	SSH functionality is not included in this evaluation.
TD0411: NIT Technical Decision for FCS_SSHC_EXT.1.5, Test 1 - Server and client side seem to be confused	No	SSH functionality is not included in this evaluation.
TD0410: NIT technical decision for Redundant assurance activities associated with FAU_GEN.1	Yes	
TD0409: NIT decision for Applicability of FIA_AFL.1 to key-based SSH authentication	Yes	
TD0408: NIT Technical Decision for local vs. remote administrator accounts	Yes	
TD0407: NIT Technical Decision for handling Certification of Cloud Deployments	Yes	
TD0402: NIT Technical Decision for RSA-based FCS_CKM.2 Selection	Yes	

Identifier	Applicable	Exclusion Rationale (if applicable)
TD0401: NIT Technical Decision for Reliance on external servers to meet SFRs	Yes	
TD0400: NIT Technical Decision for FCS_CKM.2 and elliptic curve-based key establishment	Yes	
TD0399: NIT Technical Decision for Manual installation of CRL (FIA_X509_EXT.2)	Yes	
TD0398: NIT Technical Decision for FCS_SSH*EXT.1.1 RFCs for AES-CTR	No	SSH functionality is not included in this evaluation.
TD0397: NIT Technical Decision for Fixing AES-CTR Mode Tests	Yes	
TD0396: NIT Technical Decision for FCS_TLSC_EXT.1.1, Test 2	Yes	
TD0395: NIT Technical Decision for Different Handling of TLS1.1 and TLS1.2	No	TLS with mutual authentication functionality is not included in this evaluation.
TD0394: NIT Technical Decision for Audit of Management Activities related to Cryptographic Keys	Yes	
TD0356: OE.CONNECTIONS added to VPN GW v2.1	Yes	
TD0343 – NIT Technical Decision for Updating FCS_IPSEC_EXT.1.14 Tests	Yes	
TD0342 – NIT Technical Decision for TLS and DTLS Server Tests	Yes	
TD0341 – NIT Technical Decision for TLS wildcard checking	Yes	
TD0340 – NIT Technical Decision for Handling of the basicConstraints extension in CA and leaf certificates	Yes	
TD0339 – NIT Technical Decision for Making password-based authentication optional in FCS_SSHS_EXT.1.2	No	SSH functionality is not included in this evaluation.
TD0338 – NIT Technical Decision for Access Banner Verification	Yes	
TD0337 – NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6	No	SSH functionality is not included in this evaluation.
TD0336 – NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8	No	SSH functionality is not included in this evaluation.
TD0335 – NIT Technical Decision for FCS_DTLS Mandatory Cipher Suites	Yes	
TD0334 – NIT Technical Decision for Testing SSH when password-based authentication is not supported	No	SSH functionality is not included in this evaluation.
TD0333 – NIT Technical Decision for Applicability of FIA_X509_EXT.3	Yes	
TD0329: IPSEC X.509 Authentication Requirements	Yes	
TD0324 – NIT Technical Decision for Correction of section numbers in SD Table 1	Yes	
TD0323 – NIT Technical Decision for DTLS server testing - Empty Certificate Authorities list	No	DTLS functionality is not included in this evaluation.
TD0322 – NIT Technical Decision for TLS server testing - Empty Certificate Authorities list	Yes	
TD0321 – Protection of NTP communications	Yes	
TD0319: Updates to FMT_SMF.1 in VPN Gateway EP	Yes	
TD0317: FMT_MOF.1/Services and FMT_MTD.1/CryptoKeys	Yes	
TD0316: Update to FPT_TST_EXT.2.1	Yes	
TD0307: Modification of FTP_ITC_EXT.1.1	Yes	
TD0291 – NIT technical decision for DH14 and FCS_CKM.1	Yes	

Identifier	Applicable	Exclusion Rationale (if applicable)
TD0290 – NIT technical decision for physical interruption of trusted path/channel.	Yes	
TD0289 – NIT technical decision for FCS_TLSC_EXT.x.1 Test 5e	Yes	
TD0281 – NIT Technical Decision for Testing both thresholds for SSH rekey	No	SSH functionality is not included in this evaluation.
TD0259 – NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187	No	SSH functionality is not included in this evaluation.
TD0257 – NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4	Yes	
TD0256 – NIT Technical Decision for Handling of TLS connections with and without mutual authentication	No	TLS mutual authentication functionality is not included in this evaluation.
TD0248: FAU_GEN.1 Guidance Activity	Yes	
TD0242: FPF_RUL_EXT.1.7, Test 3 - Logging Dropped Packets	Yes	
TD0228 – NIT Technical Decision for CA certificates - basicConstraints validation	Yes	
TD0209: Additional DH Group added as selection for IKE Protocols	Yes	
TD0179: Management Capabilities in VPN GW EP 2.1	Yes	

Table 2 Technical Decisions

3 Security Problem Definition

The security problem definition has been taken from [FWcPP] and [VPNGWEP] and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any organizational security policies that the TOE is expected to enforce. Threats from [VPNGWEP] only applicable to head-end VPN functionality are not included.

3.1 Threats

The following threats are drawn directly from the [FWcPP] and [VPNGWEP].

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the firewall by nefarious means such as masquerading as an administrator to the firewall, masquerading as the firewall 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 the firewall and a network device. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the firewall 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 firewalls 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 firewall 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 firewall 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.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the firewall 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 firewall data enabling continued access to the firewall 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 firewall 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 firewall. Having privileged access to the firewall 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.
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.
T.DATA_INTEGRITY/VPN	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 establish communications with those external devices then the data contained within the communications may be susceptible to a loss of integrity.
T.NETWORK_ACCESS/VPN	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/VPN	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 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 and/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/VPN	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/VPN	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 modifications.

Table 3 Threats

3.2 Assumptions

The following assumptions are drawn directly from the [FWcPP] and [VPNGWEP].

ID	Assumption
A.PHYSICAL_PROTECTION	The firewall device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the firewall's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the firewall and the data it contains. As a result, the

	cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the firewall that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the firewall.
A.LIMITED_FUNCTIONALITY	The firewall 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 firewall device should not provide a computing platform for general purpose applications (unrelated to networking/filtering functionality).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the firewall device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the firewall. The firewall 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.
A.REGULAR_UPDATES	The firewall 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 firewall device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING	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 firewall equipment when the equipment is discarded or removed from its operational environment.
A.CONNECTIONS	It is assumed that 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.

Table 4 Assumptions

3.3 Organizational Security Policies

The following Organizational Security Policies are drawn directly from the [FWcPP] and [VPNGWEP].

ID	OSP
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.

Table 5 OSPs

4 Security Objectives

The security objectives have been taken from [FWcPP] and [VPNGWEP] and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the TOE

The following security objectives apply to the TOE.

ID	Objective for the Operation Environment
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) and/or receiving (destination) applicable network traffic as well as on established connection information.
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. VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity.
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.
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 signaturebased validation of updates to the TSF.
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) and/or receiving (destination) port (or service) identified in the network traffic as well as on established connection information.
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).

ID	Objective for the Operation Environment
O. TOE_ADMINISTRATION	Compliant 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.

Table 6 Objectives for the Operational Environment

4.2 Security Objectives for the Operational Environment

The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track with the assumptions about the environment.

ID	Objective for the Operation Environment
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.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
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	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.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
OE.CONNECTIONS	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.

Table 7 Objectives for the Operational Environment

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012 and all international interpretations.

Requirement	Description
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_STG_EXT.1	Protected Audit Event Storage
FCO_CPC_EXT.1	Component Registration Channel Definition
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.1/IKE	Cryptographic Key Generation (for IKE Peer Authentication)
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_RBG_EXT.1	Random Bit Generation
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_IPSEC_EXT.1	IPsec Protocol
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSS_EXT.1	TLS Server Protocol
FDP_RIP.2	Full Residual Information Protection
FFW_RUL_EXT.1	Stateful Traffic Filtering
FIA_AFL.1	Authentication Failure Management
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Password-based Authentication Mechanism
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/ITT	X.509 Certificate Validation
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FMT_MOF.1/ManualUpdate	Management of security functions behaviour
FMT_MOF.1/Services	Management of security functions behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on security roles
FPF_RUL_EXT.1	Rules for Packet Filtering
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_FLS.1/SelfTest	Fail Secure (Self-test Failures)
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

FPT_TST_EXT.1	TSF Testing
FPT_TST_EXT.3	TSF Testing
FPT_TUD_EXT.1	Trusted Update
FPT_STM_EXT.1	Reliable Time Stamps
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	Default TOE Access Banner
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1/Admin	Trusted Path

Table 8 SFRs

5.1 Conventions

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

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Iteration to distinguish between SilentEdge and GoSilent functionality: Indicated by appending the iteration identifier "(SE)" or "(GS)".
- Where operations were completed in the PP itself, the formatting used in the PP has been retained.

Extended SFRs are identified by having a label 'EXT' after the requirement name. Formatting conventions outside of operations matches the formatting specified within the PP.

5.2 Security Functional requirements

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1

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

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) *All administrative actions comprising:*

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

d) *Specifically defined auditable events listed in Table 9*.

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 9*.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Identities of the endpoints pairs enabled or disabled.
FCS_CKM.1	None.	None.
FCS_CKM.1/IKE	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
	Session Establishment with peer	Entire packet contents of packets transmitted/ received during session establishment
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
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 addresses Source and destination ports Transport Layer Protocol TOE Interface

Requirement	Auditable Events	Additional Audit Record Contents
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets Identifier of rule causing packet drop
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	Reason for failure
	Session Establishment with CA	Entire packet contents of packets transmitted/ received during session establishment
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MOF.1/Services	Starting and stopping of services.	None.
FMT_MTD.1/CoreData	All management activities of TSF data.	None.
FMT_MTD.1/CryptoKeys	Management of cryptographic keys.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPF_RUL_EXT.1	Application of rules configured with the ‘log’ operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets
FPT_APW_EXT.1	None.	None.
FPT_FLS.1/SelfTest	None.	None.
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel.	Identification of the initiator and target of failed trusted channels establishment attempt.

Requirement	Auditable Events	Additional Audit Record Contents
	Failure of the trusted channel functions.	
FPT_SKP_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TST_EXT.3	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 "lock the session" is selected)	Any attempts at unlocking of an interactive session.	None.
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 session locking mechanism.	None.
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.

Table 9 Security Functional Requirements and Auditable Events

5.2.1.2 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.

5.2.1.3 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.

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.

5.2.2 Communication (FCO)

5.2.2.1 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 *[*

- No channel*]*

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.

5.2.3 Cryptographic Support (FCS)

5.2.3.1 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: *[*

- *ECC schemes using "NIST curves" [P-384] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;*
- *FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3*

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

5.2.3.2 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:

[

- **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 specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.
Application Note: The presentation of this SFR is per [VPNGWEP].

5.2.3.3 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 8017, "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 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*
- *Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3;*

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

5.2.3.4 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*.

5.2.3.5 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 operating in GCM, CBC mode* and cryptographic key sizes ***128 bits, 256 bits,*** **and [no other 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]*.

Application Note: The presentation of this SFR is per [VPNGWEP].

5.2.3.6 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]]* ~~and cryptographic key sizes [assignment: *cryptographic key sizes*]~~

that meet the following: *[*

- *For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,*
- *For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256, P-384]; ISO/IEC 14888-3, Section 6.4*

].

5.2.3.7 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, SHA-512]* ~~and cryptographic key sizes [*assignment: cryptographic key sizes*~~] and **message digest sizes [160, 256, 384, 512] bits** that meet the following: *ISO/IEC 10118-3:2004*.

5.2.3.8 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]* and cryptographic key sizes *[assignment: key size (in bits) used in HMAC]* **and message digest sizes [160, 256, 384] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

5.2.3.9 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 [[*1*] software-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

5.2.3.10 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.

5.2.3.11 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].

Application Note: The presentation of this SFR is per [VPNGWEP].

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].

Application Note: The presentation of this SFR is per [VPNGWEP] as updated by TD0436.

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 [*10 minutes 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 [*10 minutes to 24*] 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*] bits.

FCS_IPSEC_EXT.1.10

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

- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash
  ].

FCS_IPSEC_EXT.1.11

The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), 19 (256-bit Random ECP), 20 (384-bit Random ECP), and [no other DH groups].

Application Note: The presentation of this SFR is per [VPNGWEP].

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)] and [no other reference identifier type].

Application Note: The presentation of this SFR is from [FWcPP] but DN is selected so [VPNGWEP] requirements are also addressed.

5.2.3.12 FCS_TLSC_EXT.1 TLS Client Protocol

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.

FCS_TLSC_EXT.1.3

The TSF shall only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall [not establish the connection].

FCS_TLSC_EXT.1.4

The TSF shall [present the Supported Elliptic Curves Extension with the following NIST curves: [secp384r1] and no other curves] in the Client Hello.

5.2.3.13 FCS_TLSS_EXT.1 TLS Server Protocol

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 [generate EC Diffie-Hellman parameters over NIST curves [secp384r1] and no other curves].

5.2.4 User Data Protection (FDP)

5.2.4.1 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.

5.2.5 Firewall (FFW)

5.2.5.1 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 [logging] packets which are invalid fragments;
b) The TSF shall drop and be capable of [logging] 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]*.

5.2.6 Identification and Authentication (FIA)

5.2.6.1 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

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

5.2.6.2 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 [*8*] and [*40*].

5.2.6.3 FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1(SE)

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;
- [no other actions].

FIA_UIA_EXT.1.2(SE)

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_UIA_EXT.1.1(GS)

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 to the factory default configuration]*].

FIA_UIA_EXT.1.2(GS)

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

5.2.6.4 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.

5.2.6.5 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 management workstation**.

5.2.6.6 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 certificate path validation **supporting a minimum path length of three certificates.**
- The certificate path must terminate with a trusted CA certificate.
- 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 basicConstraints extension is present and the CA flag is set to TRUE.

5.2.6.7 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 certificate path must terminate with a trusted CA certificate.
- 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.

5.2.6.8 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, TLS*], and [no additional uses*].

FIA_X509_EXT.2.2

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

5.2.7 Security Management (FMT)

5.2.7.1 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*.

5.2.7.2 FMT_MOF.1/Services Management of security functions behaviour

FMT_MOF.1.1/Services

The TSF shall restrict the ability to enable and disable the functions **and services** to *Security Administrators*.

5.2.7.3 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*.

5.2.7.4 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*.

Application Note: The presentation of this SFR is per [VPNGWEP].

5.2.7.5 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 and [no other]*** *capability prior to installing those updates;*
- ***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 import X.509v3 certificates;***
- ***Ability to enable, disable, determine and modify the behavior of all the security functions of the TOE identified in this EP to the Administrator;***
- ***Ability to configure all security management functions identified in other sections of this EP;***
- *[*
    - *Ability to configure audit behaviour;*
    - *Ability to set the time which is used for time-stamps;*
    - *Ability to configure the reference identifier for the peer]*

].

Application Note: The presentation of this SFR is per [VPNGWEP].

5.2.7.6 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.

5.2.8 Packet Filtering (FPF)

5.2.8.1 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 process the following network traffic protocols:

- Internet Protocol (IPv4)
- Internet Protocol version 6 (IPv6)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

and be capable of inspecting network packet header fields defined by the following RFCs to the extent mandated in the other elements of this SFR

- RFC 791 (IPv4)
- RFC 2460 (IPv6)
- RFC 793 (TCP)
- RFC 768 (UDP).

FPF_RUL_EXT.1.3

The TSF shall allow the definition of Packet Filtering rules using the following network protocol fields:

- IPv4
  - Source address
  - Destination Address
  - Protocol
- IPv6
  - Source address
  - Destination Address
  - Next Header (Protocol)
- TCP
  - Source Port
  - Destination Port
- UDP
  - Source Port
  - Destination Port

FPF_RUL_EXT.1.4

The TSF shall allow the following operations to be associated with Packet Filtering rules: permit, ~~deny~~, discard, and log.

FPF_RUL_EXT.1.5

The TSF shall allow the Packet Filtering rules to be assigned to each distinct network interface.

FPF_RUL_EXT.1.6

The TSF shall process the applicable Packet Filtering rules (as determined in accordance with FPF_RUL_EXT.1.5) in the following order: Administrator defined.

FPF_RUL_EXT.1.7

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

Application Note: The presentation of this SFR is per [VPNGWEP].

5.2.9 Protection of the TSF (FPT)

5.2.9.1 FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1

The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2

The TSF shall prevent the reading of plaintext passwords.

5.2.9.2 FPT_FLS.1/SelfTest Fail Secure (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.*]

Application Note: The presentation of this SFR is per [VPNGWEP].

5.2.9.3 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]**.

5.2.9.4 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.

5.2.9.5 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: [*integrity of executable code, DRBG randomness test*].

5.2.9.6 FPT_TST_EXT.3 Extended: TSF Testing

FPT_TST_EXT.3.1

The TSF shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF provided cryptographic service specified in FCS_COP.1/SigGen.

Application Note: The presentation of this SFR is per [VPNGWEP].

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

Application Note: The presentation of this SFR is per [VPNGWEP].

5.2.9.8 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].

5.2.10 TOE Access (FTA)

5.2.10.1 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.

5.2.10.2 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*.

5.2.10.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1

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

5.2.10.4 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.

5.2.11 Trusted path/channels (FTP)

5.2.11.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1

Refinement: The TSF shall use **IPsec, and [TLS]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, VPN communications, [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.

Application Note: The presentation of this SFR is per [VPNGWEP].

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 audit server]*.

5.2.11.2 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*.

5.3 TOE SFR Dependencies Rationale for SFRs

[FWcPP] and [VPNGWEP] contain all the requirements claimed in this Security Target. As such, the dependencies are not applicable since the PP has been approved.

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from [FWcPP] and [VPNGWEP] which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Assurance Class	Components	Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE

Assurance Class	Components	Components Description
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

Table 10 Security Assurance Requirements

5.5 Rationale for Security Assurance Requirements

The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.

5.6 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by [Vendor] to satisfy the assurance requirements. The table below lists the details.

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	
ATE_IND.1	[Vendor] will provide the TOE for testing.
AVA_VAN.1	[Vendor] will provide the TOE for testing. [Vendor] will provide a document identifying the list of software and hardware components.

Table 11 TOE Security Assurance Measures

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

TOR SFR	Rationale
FAU_GEN.1, FAU_GEN.2	SilentEdge and GoSilent generate audit records for operation and administration of each component. The specific events audited on each component correspond to the SFRs applicable to each component (see section 6.2); the audit aggregated audit event types and their content is provided in section 5.2.1.1. 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.). Audit records related to the generating/import of, changing, or deleting of long-term (non-ephemeral) cryptographic keys include a unique key name or other unique identifier to associate the audit record with a specific key.
FAU_STG_EXT.1	Each TOE component stores audit event records that are generated on that component. Each component can store up to 50MB of audit information. 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, each of 10MB. 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 to 50MB. Each component also transmits a copy of each audit record to an external syslog server in real time; the syslog server is configured on SilentEdge and communicated to all GoSilent instances. Each component opens a connection to the server using TLS. If the connection to the syslog server is unavailable, audit records continue to be saved locally; however, any records generated while the syslog server is unavailable will not be transmitted to it. SilentEdge 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.
FCO_CPC_EXT.1	GoSilent instances are manually registered (enablement) by an authorized administrator on SilentEdge, and the X.509 certificate for SilentEdge and the specific GoSilent are communicated out of band to the GoSilent and imported by an authorized administrator on that component. Guidance information instructs administrators to use a secure communication channel for communication of the certificates. Any attempt by an unregistered system to establish an IPsec tunnel (connect) to SilentEdge is rejected by SilentEdge. Each GoSilent only establishes an IPsec tunnel with SilentEdge. Attempts to establish an IPsec tunnel from one GoSilent to another are always rejected.
FCS_CKM.1, FCS_CKM.1/IKE, FCS_CKM.2	The TOE generates ECDSA P-256 and P-384 Elliptic Curve keys as specified in FIPS Pub 186-4. These keys are used to perform Elliptic Curve Diffie-Hellman in IPsec and TLS. The TOE acts as a sender and a recipient when performing Elliptic Curve Diffie-Hellman. These keys are also used to authenticate the TOE component to the administrator in TLS exchanges for the management GUI. The TOE performs key establishment per RSAES-PKCS1-v1_5 for TLS connections with the syslog server.

TOR SFR	Rationale
FCS_CKM.4	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 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 values only
FCS_COP.1/DataEncryption	The TOE performs AES 128 and 256 bit encryption in CBC and GCM modes to secure TLS and IPsec communication channels.
FCS_COP.1/SigGen	The TOE performs ECDSA (P-256 and P-384) and RSA (2048 bit) SigGen to support IPsec and TLS functions. The TOE performs ECDSA (P-256 and P-384) and RSA (2048 bit) SigVer to support IPsec, TLS, X.509, and trusted update functions.
FCS_COP.1/Hash	The TOE performs SHA-1, SHA-256, SHA-384 and SHA-512 hashing. 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.
FCS_COP.1/KeyedHash	The TOE uses HMAC-SHA-384 TLS KDF and TLS message authentication. HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-384 are used with IPsec.
FCS_RBG_EXT.1	The TOE implements Block Cipher (CTR) DRBGs, compliant with SP800-90A to generate random bits needed for asymmetric key, symmetric key, nonce, and salt generation. The DRBGs are seeded with 512 bytes of data from one hardware-based noise source. The 512 bytes of data contain at least 256-bit of entropy.
FCS_HTTPS_EXT.1, FCS_TLSS_EXT.1, FTP_TRP.1/Admin	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 Key Establishment is performed using Elliptic Curve Diffie-Hellman P-384 keys. This connection is always initiated by the remote end.
FCS_IPSEC_EXT.1, FPT_ITT.1	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. IPsec support includes: • NAT traversal • SA and Child SA lifetimes based on time, configurable between 10 minutes and 24 hours • DH groups 14, 19 and 20 • Peer authentication using ECDSA certificates • Distinguished Names as reference identifiers GoSilent has a nominal SPD that denies all traffic. When an IPsec tunnel to SilentEdge is established, an SPD entry is dynamically added that permits all traffic received from user systems with an IP source address is consistent with the IP subnet address configured for the GoSilent user-side interface. No traffic from a user system is forwarded to the TOE Network other than through an IPsec tunnel (to SilentEdge). SilentEdge has a nominal SPD for each GoSilent that denies all traffic. When an IPsec tunnel from each GoSilent is established, an SPD entry is dynamically added that permits all traffic destined for an IP address that is consistent with the IP subnet address configured for the GoSilent user-side interface. If the IP destination address for a packet from the External Network does not map to any current GoSilent

TOR SFR	Rationale
	connection, the packet is dropped. No traffic from the External Network is forwarded to the TOE Network other than through an IPsec tunnel. IPsec connections are always initiated by GoSilent; SilentEdge only receives incoming connections from GoSilent instances.
FCS_TLSC_EXT.1	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_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 The TOE presents the Supported Elliptic Curves Extension indicating support for P-384 in the Client Hello. The TOE automatically parses the reference identifier from the connection parameters, using the FQDN as the reference identifier. When validating the server certificate, the TSF matches the reference identifier against the DNS SAN field in the presented certificate (if present) and falls back to the CN if the SAN is not present. The TOE does not support wildcards.
FDP_RIP.2	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.
FFW_RUL_EXT.1, FPF_RUL_EXT.1	SilentEdge performs stateful packet filtering on all packet received from or being sent to the External Network. The boot sequence of SilentEdge 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 SilentEdge management GUI • Physical interfaces are active 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. SilentEdge applies a uniform policy to the traffic flows to and from all GoSilent users. By default, no traffic is allowed to flow from GoSilent users to the External Network, and no traffic is allowed to flow from the External Network to GoSilent users.

TOR SFR	Rationale
	The TOE maintains a session table which tracks all known sessions based on the information in incoming packets. Specifically, the lookup is based on the exact match of source IP address and port, destination IP address and port, protocol attributes (e.g., SYN, ACK, RST, and FIN), and incoming interface. The TOE removes existing traffic flows due to session inactivity timeout, or completion of the session. 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. SilentEdge can enforce the following reject rules with logging on traffic: • invalid fragments; • fragmented IP packets which cannot be re-assembled completely; • 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: o No overlap o The total fragments in one packet should not be more than 62 pieces o The total length of merged fragments should not larger than 64k o All fragments in one packet should arrive in 2 seconds o The total queued fragments has limitation, depending on the platform o The total number of concurrent fragment processing for different packet has limitations depending on platform

TOR SFR	Rationale
FIA_AFL.1, FIA_PMG_EXT.1, FIA_UIA_EXT.1, FIA_UAU_EXT.2, FIA_UAU.7, FTA_TAB.1	Management of the TOE is primarily performed through SilentEdge. However, initial management of GoSilent, providing enough configuration information for it to connect to SilentEdge, is provided by GoSilent. Identification and authentication are required for both local and remote administrator access. Remote access to the TOE for both SilentEdge and GoSilent is via an HTTPS session with SE, and local access to the TOE is via HTTPS sessions using the dedicated Management Ethernet port for SilentEdge or the Device Ethernet interface for GoSilent. For SilentEdge, the IP address of a local administrator must be included in the configured white list for HTTPS access. Prior to logon via the web GUI, a consent banner is displayed to the administrator warning that proceeding with authentication is consenting to the terms of use of the TOE. The user is prompted to enter their username and password. 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. 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. 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. Failed logins are not counted when using the dedicated Management Ethernet port.
FIA_X509_EXT.1/ITT, FIA_X509_EXT.1/Rev, FIA_X509_EXT.2	The TOE uses X.509 certificates to: • provide mutual authentication between TOE components • verify the identify of the Syslog server When a TOE component receives a certificate asserting the identity of a remote system, the TOE ensures the current time is in the validity time of the certificate, the certificate has not been revoked (verified via OCSP for audit servers, and via CRLs (RFC5280) for IPsec), 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 or CRL Distribution Point, the TOE will reject the certificate.
FMT_MOF.1/ManualUpdate, FMT_MOF.1/Services, FMT_MTD.1/CoreData, FMT_MTD.1/CryptoKeys, FMT_SMF.1, FMT_SMR.2	Management of the TOE is primarily performed through SilentEdge. However, initial management of GoSilent, providing enough configuration information for it to connect to SilentEdge, is provided by GoSilent. Both local and remote administration is supported. SilentEdge provides the following management capabilities to authorized administrators: • Perform manual updates of SilentEdge; • Enable and disable functions and services; • Manage (import) cryptographic keys and certificates;

TOR SFR	Rationale
	• 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 audit behaviour; • Ability to set the time which is used for time-stamps; • Ability to configure the reference identifier for the peer GoSilent provides the following management capabilities to authorized administrators: • Perform manual updates of the GoSilent 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
FPT_APW_EXT.1, FPT_SKP_EXT.1	There is no filesystem access or administrative interface that allows any administrative users to read plaintext secret or private keys. The TOE stores hashed values of passwords.
FPT_FLS.1/SelfTest, FPT_TST_EXT.1, FPT_TST_EXT.3	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 a stored signature that covers all of the executable code. The entropy test performs a statistical assessment of 1000 samples. If any test fails, that component does not enter an operational state. For SilentEdge, an error is displayed on the console and the system stops. For GoSilent, the system enters a state where an administrator can connect to the management GUI and receive an error message. 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. These states do not permit any user traffic to flow through the component.
FPT_TUD_EXT.1	Authorized administrators can query the current version of the TOE software on the platform they are connected to; on SilentEdge, the administrator can also query the TOE version of all registered GoSilent instances. The administrator can initiate a manual update of the TOE component that they are connected to. The updates are signed with an Attila Security key. Once the image has been downloaded, the TOE checks the signature of the image (against the Attila Security public key) before the image is applied.
FPT_STM_EXT.1	SilentEdge and GoSilent each maintain a system clock used to provide date/time details for use by the TOE, and the time may be manually set by authorized administrators. SilentEdge includes a real-time clock to maintain the time across system reboots. For GoSilent, guidance directs the administrator to manually set the clock on each reboot since it does not include a real-time clock.
FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4	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. The administrator is able to terminate their GUI session.

TOR SFR	Rationale
FTP_ITC.1	Trusted channels are used for connections between GoSilent and SilentEdge as well as with the syslog server. TLS syslog server connections are always initiated by SilentEdge and GoSilent. IPsec connections are always initiated by GoSilent and received by SilentEdge.

Table 12 TOE Summary Specification SFR Description

6.1 CAVP Algorithm Certificate Details

Each of these cryptographic algorithms have been validated as identified below.

Algorithm	Description	Mode Supported	SilentEdge CAVP Cert. #	GoSilent CAVP Cert. #
AES	Used for symmetric encryption/decryption	CBC, GCM (128, 256)	C1159	C1104
SHS	Cryptographic hashing services	SHA-1, SHA-256, SHA-384, SHA-512	C1159	C1104
DRBG	Deterministic random bit generation	CTR_DRBG (AES 256)	C1159	C1104
ECDSA (186)	Key Generation SigGen SigVer	P-256, P-384	C1159	C1104
HMAC	Keyed hashing services	SHA (1, 256, 384)	C1159	C1104
KAS ECC	SP 800-56A	P-256, P-384	C1159	C1104
RSA	Key Establishment	n (2048)	Vendor Affirmed	Vendor Affirmed
RSA	SigGen (PKCS1_v1.5) SigVer (PKCS1_v1.5)	n = 2048 (SHA-256)	C1159	C1104

Table 13 CAVP Algorithm Certificate References

6.2 SFR Distribution Between Components

The following table addresses the SFR distribution requirements between TOE components, as required in section 3.4 of [FWcPP]. Since SFRs drawn from [VPNGWEP] are not addressed by the distribution requirements in [FWcPP], their distribution requirements in the following table have been specified to be consistent with the requirements for similar SFRs.

SFR	Dist. Rqmt	SilentEdge	GoSilent
FAU_GEN.1	All	X	X
FAU_GEN.2	All	X	X
FAU_STG_EXT.1	All	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

SFR	Dist. Rqmt	SilentEdge	GoSilent
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
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
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_SMR.2	One	X	X
FPF_RUL_EXT.1	One	X	
FPT_APW_EXT.1	Feature Dependent	X	X
FPT_FLS.1/SelfTest	All	X	X
FPT_ITT.1	All	X	X

SFR	Dist. Rqmt	SilentEdge	GoSilent
FPT_SKP_EXT.1	All	X	X
FPT_TST_EXT.1	All	X	X
FPT_TST_EXT.3	All	X	X
FPT_TUD_EXT.1	All	X	X
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_TRP.1/Admin	One	X	X

Table 14 SFR Distribution Between Components

End Of Document