Commercial Solutions for Classified (CSfC) Selections for Internet Protocol Security (IPsec) Virtual Private Network (VPN) Gateways

Overview

IPsec VPN Gateway products used in Commercial Solutions for Classified (CSfC) solutions (as defined in the CSfC Capability Packages (CPs)) shall be validated by National Information Assurance Partnership (NIAP)/Common Criterial Evaluation and Validation Scheme (CCEVS) or Common Criteria Recognition Arrangement (CCRA) partnering schemes as complying with the current requirements of NIAP's:

1. Network Devices collaborative Protection Profile Version 2.2e (NDcPP); and
2. Protection Profile-Module for Virtual Private Network (VPN) Gateways Version 1.2 (MOD_VPNGW_v1.2)

This validated compliance shall include the selectable requirements contained in this document.

IPsec VPN Gateways are used to send encrypted traffic between one and/or many devices. The CSfC CPs generally refer to IPsec VPN Gateways as either Outer Encryption Component or Inner Encryption Component. IPsec VPN Gateways continue to evolve and threats continuously progress, which may cause the below selections to change or become obsolete. The objective of this document is to support the use of the Commercial National Security Algorithm (CNSA) Suite and NIAP-evaluated IPsec VPN Gateways within CSfC Solutions.

Please provide comments on usability, applicability, and/or shortcomings to the CSfC Program (csfc@nsa.gov).

Notes

Note 1: The following selections apply to CSfC IPsec VPN Gateway functionality. If needed, functionality and/or configurations outside the scope of a CSfC IPsec VPN Gateway that conflict with the CSfC selections could be NIAP validated without using a separate iteration of the Security Functional Requirement (SFR) (this is a change to previous guidance in Note 1). The Security Target (ST) author should document a specific CSfC IPsec VPN Gateway configuration in the product's Administrative Guide with a note that the configuration should be considered the NIAP-certified evaluated configuration for CSfC IPsec VPN Gateway Use Cases. The CSfC IPsec VPN Gateway configuration should be used to validate compliance with CSfC selections.

Note 2: See TD0591 for clarification on Physical Network Devices (pND) and Virtual Network Devices (vND).

Note 3: The below SFRs/Selections contain some mandatory SFRs without Selections or modifications. The exclusion of other mandatory SFRs in the below Selections do not indicate that mandatory SFRs are not required (i.e., Compliance with the Protection Profile (PP) requirements as prescribed by the PP and outlined in the Overview Section above is required). Some mandatory SFRs are included in the below Selections to highlight some SFRs relevant to CSfC IPsec VPN Gateways.

Note 4: The objective of the CSfC Selections for Pre-Shared Key (PSK) related SFRs is to support the use of Internet Engineering Task Force (IETF) Request for Comments (RFC) 8784-compliant implementations of Internet Key Exchange (IKE) v2 in compliance with the Symmetric Key Management (KM) Requirements Annex.

Document Conventions

The conventions used in descriptions of the document are as follows:

- Assignment completed within a selection in the PP: the completed assignment text is indicated with *italicized and underlined text* (i.e., CSfC mandatory completed assignments/selections unless otherwise indicated by the text “at least one of the following underlined selections”)
- Assignment partially completed in the PP: indicated with *italicized text*
- Refinement text is indicated with ~~strikethroughs~~
- Additional clarifying text or CSfC specific language is indicated with light blue Courier New Text
- Links to additional information and email addresses are indicated with blue underlined text.

Network Devices Collaborative Protection Profile Version 2.2e Selections

FCS_CKM.1.1
The TSF shall generate asymmetric cryptographic keys in accordance with specified cryptographic key generation algorithm with at least one of the following: [**Selection:**

- *RSA schemes using cryptographic key sizes of 2048-bit* and 3072-bits *or greater that meet the following FIPS PUB 186-4, "Digital Signature Standard (DSS), Appendix B.3";*
- *ECC schemes using NIST curves* [Selection: *~~P-256~~*, *P-384*, *~~P-521~~*] *that meet the following: FIPS PUB 186-4, “Digital Signature Standard(DSS)”, Appendix B.4*];
- ~~*FFC schemes using cryptographic key sizes of 2048-bit that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1*~~
- *FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and* [**Selection:** *RFC 3526, RFC 7919*].

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

FCS_CKM.2.1
The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [**Selection**:

- ~~*RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”;*~~
- ~~*Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”*~~

- *Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"* (See TD0581)*;*
- ~~*Finite field-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";*~~
- *FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [**Selection**: groups listed in RFC 3526, groups listed in RFC 7919]* (See TD0580).

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

FCS_COP.1.1/DataEncryption
The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [**Selection:** *CBC*, *CTR*, *GCM*] mode and cryptographic key sizes [Selection: ~~*128 bits*~~, ~~*192 bits*~~, *256 bits*] that meet the following: AES as specified in ISO 18033-3, [**Selection:** *CBC as specified in ISO 10116*, *CTR as specified in ISO 10116*, *GCM as specified in ISO 19772*].

FCS_COP.1.1/SigGen
The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm in at least one of the following: [**Selection**:

- *RSA Digital Signature Algorithm using cryptographic key sizes (modulus) of [assignment*: *3072 bits or greater]*
- *Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [assignment*: *384 bits or greater]*

]
that meet at least one of the following that corresponds to the previous selection: [**Selection**:

- *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 RSASSAPKCS2v1_5; ISO/IEC 9796-2, Digital signature scheme2 or Digital Signature scheme 3,*
- *For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [*selection: ~~*P-256*~~, *P-384*, ~~*P-521*~~*]; ISO/IEC 14888-3, Section 6.4*]

]

FCS_COP.1.1/Hash
The TSF shall perform *cryptographic hashing* services in accordance with at least one of the following underlined specified cryptographic algorithm [**Selection**: ~~*SHA-1*~~, *SHA-256*, *SHA-384*, *SHA-512*] ~~and cryptographic key sizes [assignment: *cryptographic key sizes*]~~ and at least one of the following underlined message digest sizes [**Selection**: ~~*160*~~, *256*, *384*, *512*] bits that meet the following: ISO/IEC 10118-3:2004.

FCS_COP.1.1/KeyedHash
The TSF shall perform *keyed-hash message authentication* in accordance with ~~a~~ at least one of the following underlined specified cryptographic algorithm [**Selection**: ~~*HMAC-SHA-1*~~, ~~*HMAC-SHA-256*~~, *HMAC-SHA-384*, *HMAC-SHA-512*] and cryptographic key sizes [**Assignment**: *key size(s) in bits ≥ the message digest size(s)*] and at least one of the following underlined message

digest sizes [**Selection**: *~~160~~*, *~~256~~*, *384*, *512*] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.

FCS_RBG_EXT.1.1
The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using at least one of the following [**Selection:** *Hash_DRBG (*SHA-384, SHA-512*), HMAC_DRBG (*SHA-384, SHA-512*), CTR_DRBG (*AES-256*)*].

Application Note: The objective of the CSfC specific language for DRBG algorithms is to ensure compatibility with the CSfC CPs by selecting compliant algorithms that provide the required security strength.

FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [**Selection**: [***Assignment***: *number of software-based sources*] software-based noise source, [*assignment*: *at least one (1)] platform-based noise source*]] with a minimum of [Selection: ~~128 bit~~, ~~192 bits~~, 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.

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 [**Selection**: digital signature, hash comparison] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- [**Selection**:
    - *Ability to start and stop services;*
    - *Ability to configure audit behavior (e.g. changes to storage locations for audit; changes to behavior when local audit storage space is full);*
    - *Ability to modify the behavior of the transmission of audit data to an external IT entity;*
    - *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*
    - *Ability to manage the cryptographic keys;*
    - *Ability to configure the cryptographic functionality;*
    - *Ability to configure thresholds for SSH rekeying;*
    - *Ability to configure the lifetime for IPsec SAs;*
    - *Ability to configure the interaction between TOE components;*
    - *Ability to enable or disable automatic checking for updates or automatic updates;*
    - *Ability to re-enable an Administrator account;*
    - *Ability to set the time which is used for time-stamps;*
    - *Ability to configure NTP;*
    - *Ability to configure the reference identifier for the peer;*
    - *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;*
    - *Ability to import X.509v3 certificates to the TOE's trust store;*
    - *~~No other capabilities~~*].

FTP_ITC.1.1
The TSF shall be capable of using [**Selection:** *IPsec, SSH, TLS, DTLS, HTTPS*] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [**Selection:** *authentication server*, [***Assignment***: *other capabilities*], *no other capabilities*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_TRP.1.1/Admin
The TSF shall be capable of using at least one of the following [**Selection:** *~~DTLS~~, IPsec, SSH, 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.

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 [**Selection**: *allow the Security Administrator to set the time, synchronize time with an NTP server*].

FIA_X509_EXT.1.1/ITT
If applicable due to a distributed TOE, the TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of two certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using at least one of the following [**Selection:** *the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3* and *Certificate Revocation List (CRL) as specified in RFC ~~5759~~* 8603 *Section ~~5~~*7]
- 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.

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

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

FPT_ITT.1.1
If applicable due to a distributed TOE, 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 [**Selection:** *IPsec, SSH, TLS, ~~DTLS~~, HTTPS*].

FCS_SSHS_EXT.1.1
If the TOE has an SSH Server, the TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [**Selection**: *4256, ~~4344~~, 5647, 5656, 6187, ~~6668~~, 8268, 8308 section 3.1, 8332*].

FCS_SSHS_EXT.1.2
If the TOE has an SSH Server, the TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [**Selection**: *password-based, no other method*].

FCS_SSHS_EXT.1.3
If the TOE has an SSH Server, the TSF shall ensure that, as described in RFC 4253, packets greater than [**Assignment**: *number of bytes*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4
If the TOE has an SSH Server, the TSF shall ensure that the SSH transport implementation uses at least one of the following encryption algorithms and rejects all other encryption algorithms: [**Selection***: ~~aes128-cbc~~, ~~aes256-cbc~~, ~~aes128-ctr~~, ~~aes256-ctr~~, ~~AEAD_AES_128_GCM~~, AEAD_AES_256_GCM, ~~aes128-gcm@openssh.com~~, aes256-gcm@openssh.com*].

FCS_SSHS_EXT.1.5
If the TOE has an SSH Server, the TSF shall ensure that the SSH public-key based authentication implementation uses at least one of the following underlined [**Selection**: *~~ssh-rsa, rsa-sha2-256~~, rsa-sha2-512, ~~ecdsa-sha2-nistp256~~, ~~x509v3-ssh-rsa~~, ecdsa-sha2-nistp384~~, ecdsa-sha2-nistp521~~, ~~x509v3-ecdsa-sha2-nistp256~~, x509v3-ecdsa-sha2-nistp384, ~~x509v3-ecdsa-sha2-nistp521~~, ~~x509v3-rsa2048-sha256~~*] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6
If the TOE has an SSH Server, the TSF shall ensure that the SSH transport implementation uses at least one of the following [**Selection**: *~~hmac-sha1~~, ~~hmac-sha1-96~~, ~~hmac-sha2-256, hmac-sha2-512~~, ~~AEAD_AES_128_GCM~~, AEAD_AES_256_GCM, implicit*] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7
If the TOE has an SSH Server, the TSF shall ensure that [**Selection**: *~~diffie-hellman-group14-sha1~~, diffie-hellman-group15-sha512, ~~ecdh-sha2-nistp256~~*] [**Selection**: *~~diffie-hellman-group14-sha256~~, diffie-hellman-group16-sha512, ~~diffie-hellman-group17-sha512~~, ~~diffie-hellman-group18-sha512~~, ecdh-*

sha2-nistp384, ~~*ecdh-sha2-nistp521*~~, ~~*no other methods*~~] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8

If the TOE has an SSH Server, the TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

FAU_STG_EXT.5.1

If applicable due to a distributed TOE and if the TOE component cannot forward logs to a Security Information and Event Management (SIEM) server, each TOE component which does not store security audit data locally shall be able to buffer security audit data locally until it has been transferred to another TOE component that stores or forwards it. All transfer of audit records between TOE components shall use a protected channel according to [**Selection**: *FPT_ITT.1*, *FTP_ITC.1*].

FCS_HTTPS_EXT.1.1

If the TOE uses HTTPS, the TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2

If the TOE uses HTTPS, the TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3

If the TOE uses HTTPS and if a peer certificate is presented, the TSF shall perform at least one of the following [**Selection**: ~~*not require client authentication*~~, *not establish the connection*, ~~*request authorization to establish the connection*~~, *[assignment: allow the Administrator to choose whether to establish the connection if the TSF fails to determine the revocation status]*] if the peer certificate is deemed invalid.

FCS_TLSS_EXT.1.1

If the TOE has a TLS server, the TSF shall implement [Selection: ~~*TLS 1.1 (RFC 4346)*~~, *TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support at least one of the following ciphersuites: [**Selection:**

- ~~*TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268*~~
- ~~*TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268*~~
- ~~*TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268*~~
- ~~*TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268*~~
- ~~*TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*~~
- ~~*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*~~
- ~~*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*~~
- ~~*TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*~~
- ~~*TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*~~
- ~~*TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246*~~
- ~~*TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246*~~
- ~~*TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246*~~
- ~~*TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*~~
- ~~*TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*~~

- ~~*TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*~~
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- ~~*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*~~
- ~~*TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*~~
- ~~*TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*~~
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- ~~*TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*~~
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- ~~*TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*~~
- ~~*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*~~

].

FCS_TLSS_EXT.1.2

If the TOE has a TLS server, the TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [Selection: *TLS 1.1*, ~~*TLS 1.2*~~, ~~*none*~~].

FCS_TLSS_EXT.1.3

If the TOE has a TLS server, the TSF shall perform key establishment for TLS using at least one of the following underlined selections [**Selection**: ~~*RSA with key size* [selection: *2048 bits*, *3072 bits*, *4096 bits*]~~, ~~*Diffie-Hellman parameters with size* [selection: *2048 bits*, *3072 bits*, *4096 bits*, *6144 bits*, *8192 bits*]~~, *Diffie-Hellman groups* [**Selection**: ~~*ffdhe2048*~~, *ffdhe3072*, *ffdhe4096*, ~~*ffdhe6144*~~, ~~*ffdhe8192*~~, *no other groups*], *ECDHE curves* [**Selection**: ~~*secp256r1*~~, *secp384r1*, ~~*secp521r1*~~*] and no other curves*]].

FCS_TLSS_EXT.1.4

If the TOE has a TLS server, the TSF shall support [Selection: *no session resumption or session tickets*, ~~*session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2)*, *session resumption based on session tickets according to RFC 5077*~~].

FIA_X509_EXT.1.1/Rev

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

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using at least one of the following [**Selection:** *the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3* and *Certificate Revocation List (CRL) as specified in RFC* ~~*5759*~~ 8603 *Section* ~~*5*~~7].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.

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

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

FIA_X509_EXT.2.1
The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for all of the following applicable underlined selections [**Selection:** *~~DTLS~~, HTTPS, IPsec, SSH, TLS*] and [**Selection:** *code signing for system software updates* [***Assignment***: *other uses*], *no additional uses*].

FIA_X509_EXT.2.2
When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [**Selection:** *allow the Administrator to choose whether to accept the certificate in these cases, ~~accept the certificate~~, not accept the certificate*].

FIA_X509_EXT.3.1
The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [**Selection:** *device-specific information, Common Name, Organization, Organizational Unit, Country*].

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

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

FCS_IPSEC_EXT.1.5
The TSF shall implement the protocol: [selection:

- ~~IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [selection: no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers], and [selection: no other RFCs for hash functions, RFC 4868 for hash functions];~~
- *IKEv2 as defined in RFC 5996 [selection: ~~with no support for NAT traversal~~, with mandatory support for NAT traversal as specified in RFC 5996, section 2.23)], and [selection: ~~no other RFCs for hash functions~~, RFC 4868 for hash functions]]*.

FCS_IPSEC_EXT.1.6
The TSF shall ensure the encrypted payload in the [selection: *~~IKEv1~~, IKEv2*] protocol uses the cryptographic algorithms [Selection**:** ~~AES-CBC-128~~, ~~AES_CBC-192~~ *AES-CBC-256 (specified in RFC 3602), ~~AES-GCM-128~~, ~~AES-GCM-192~~, AES-GCM-256 (specified in RFC 5282)*].

FCS_IPSEC_EXT.1.7
The TSF shall ensure that [selection:

- ~~IKEv1 Phase 1 SA lifetimes can be configured by a Security Administrator based on [selection:~~
  - ~~number of bytes;~~

   - ~~length of time, where the time values can be configured within [assignment: integer range including 24] hours;~~

   ];

- *IKEv2 SA lifetimes can be configured by a Security Administrator based on* [**Selection**:
   - *Number of bytes;*
   - *Length of time, where the time values can be configured within* [**Assignment**: *integer range including 24] hours;*

   ]

].

FCS_IPSEC_EXT.1.8

The TSF shall ensure that [selection:

- ~~IKEv1 Phase 2 SA lifetimes can be configured by a Security Administrator based on [selection:~~
   - ~~number of bytes;~~
   - ~~length of time, where the time values can be configured within [assignment: integer range including 8] hours~~;

   ];

- *IKEv2 Child SA lifetimes can be configured by a Security Administrator based on* [**Selection**:
   - *number of bytes;*
   - *length of time, where the time values can be configured within* [**Assignment**: *integer range including 8] hours;*

   ]

].

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 [selection: ~~*IKEv1 Phase 1,*~~ *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 [selection: ~~*IKEv1 Phase 2,*~~ *IKEv2 CHILD_SA*] connection.

FCS_IPSEC_EXT.1.13

The TSF shall ensure that all IKE protocols perform peer authentication using at least one of the following [**Selection:** *RSA, ECDSA*] that use X.509v3 certificates that conform to RFC 4945 and [Selection: *Pre-shared Keys*, ~~*no other method*~~].

Protection Profile-Module for Virtual Private Network (VPN) Gateways Version 1.2 Selections

FCS_IPSEC_EXT.1.3

The TSF shall implement [**Selection**: *transport mode, tunnel mode*].

FCS_IPSEC_EXT.1.4

The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [Selection: ~~*AES-CBC-128*~~, *AES-CBC-256 (specified in RFC 3602)*, ~~*AES-GCM-128*~~, *AES-GCM-256 (specified in RFC 4106)*] and [Selection: ~~*AESCBC-192 (RFC 3602)*~~, ~~*AES-GCM-192 (RFC*~~

~~4106)~~, *no other algorithm*] together with a Secure Hash Algorithm (SHA)-based HMAC [**Selection:** *~~HMAC-SHA-1~~*, *~~HMAC-SHA-256~~*, *HMAC-SHA-384*, *HMAC-SHA-512*, ~~no HMAC algorithm~~].

FCS_IPSEC_EXT.1.11
The TSF shall ensure that IKE protocols implement DH Group(s)

- **19 (256-bit Random ECP), 20 (384-bit Random ECP) according to RFC 5114 and** *[**Selection:***
- *[**Selection**:~~ 14 (2048-bit MODP), ~~15 (3072-bit MODP), 16 (4096-bit MODP)~~, 17 (6144-bit MODP), 18 (8192-bit MODP)]~~ according to RFC 3526,*
- *[Selection: ~~21 (521-bit Random ECP)~~, ~~24 (2048-bit MODP with 256-bit POS)~~, no other DH Groups] according to RFC 5114*

].

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)**, [**Selection:** *SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN, CN: IP address, CN: Fully Qualified Domain Name (FQDN), CN: user FQDN, no other reference identifier type*, [**Assignment:** *other supported reference identifier types*]].

FCS_CKM.1.1/IKE
The TSF shall generate asymmetric cryptographic keys used for IKE peer authentication in accordance with at least one of the following specified cryptographic key generation algorithm:
[***Selection***:

- *FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes;*
- *FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" ~~P-256~~, P-384 and [selection: ~~P-521~~, no other curves]]*

and [***Selection***:

- *FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [**Selection:** RFC 3526, RFC 7919]*
- *no other key generation algorithms]*

and specified cryptographic key sizes [*equivalent to, or greater than, a symmetric key strength of ~~112~~* 256 *bits*].

FMT_SMF.1/VPN
The TSF shall be capable of performing the following management functions [

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

[**Selection**:

- *Configuration of remote VPN client session timeout,*
- *Configuration of attributes used to deny establishment of remote VPN client sessions,*
- *Generation of bit-based pre-shared key,*

- *No other capabilities*

]].

FPF_RUL_EXT.1.1
The TSF shall perform Packet Filtering on network packets processed by the TOE.

FPF_RUL_EXT.1.2
The TSF shall allow the definition of Packet Filtering rules using the following network protocols and protocol fields:

- *IPv4 (RFC 791)*
    - *Source address*
    - *Destination Address*
    - *Protocol*
- *IPv6 (RFC 2460)*
    - *Source address*
    - *Destination Address*
    - *Next Header (Protocol)*
- *TCP (RFC 793)*
    - *Source Port*
    - *Destination Port*
- *UDP (RFC 768)*
    - *Source Port*
    - *Destination Port*

FPF_RUL_EXT.1.3
The TSF shall allow the following operations to be associated with Packet Filtering rules: permit and drop with the capability to log the operation

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

FPF_RUL_EXT.1.5
The TSF shall process the applicable Packet Filtering rules (as determined in accordance with FPF_RUL_EXT.1.4) in the following order: [*Administrator-defined*].

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

FTP_ITC.1.1/VPN
The TSF shall **be capable of using IPsec to** provide a communication channel between itself and **authorized IT entities supporting VPN communications** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data.**

FTP_ITC.1.2/VPN
The TSF shall permit [*the authorized IT entities*] to initiate communication via the trusted channel.

FTP_ITC.1.3/VPN
The TSF shall initiate communication via the trusted channel for [selection, choose one of: *remote VPN gateways or peers*, ~~*no functions*~~].

FTA_SSL.3.1/VPN
The TSF shall terminate a remote VPN client session after [*an Administrator-configurable time interval of session inactivity*].

FTA_TSE.1.1
The TSF shall be able to deny establishment of a **remote VPN client** session based on [*location, time, day, [**Selection**: no other attributes, [**Assignment:** other attributes]]*.

FTA_VCM_EXT.1.1
The TSF shall assign a private IP address to a VPN client upon successful establishment of a security session.

FIA_PSK_EXT.1.1
The TSF shall be able to use pre-shared keys for IPsec and [***Selection***: *no other protocols, [**Assignment:** other protocols that use pre-shared keys*]].

FIA_PSK_EXT.1.2
The TSF shall be able to accept at least one of the following underlined selections as pre-shared keys: [**Selection**: *generated bit-based*, *password-based*, *HMAC-based one-time password, time-based one-time password, combination of a generated bit-based and HMAC-based one-time password, combination of a generated bit-based and time-based one-time password, combination of a password-based and HMAC-based one-time password, Combination of a password-based and time-based one-time password*] keys.

FIA_PSK_EXT.2.1
The TSF shall be able to perform at least one of the following [**Selection**:

- *accept externally generated pre-shared keys,*
- *generate [selection: ~~128~~, 256] bit-based pre-shared keys via FCS_RBG_EXT.1.*

]

FIA_PSK_EXT.3.1
The TSF shall support a PSK of up to [***Assignment***: *positive integer of 64 or more*] characters.

FIA_PSK_EXT.3.2
The TSF shall allow PSKs to be composed of any combination of upper case characters, lower case characters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")", and [**Selection**: [***Assignment***: *other supported special characters], no other characters*]

FIA_PSK_EXT.3.3
The TSF shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm HMAC- [**Selection**: *SHA-256, SHA-384, SHA-512*], with [**Assignment**: *positive integer of 4096 or more*] iterations, and output cryptographic key sizes [Selection: *~~128~~, 256*] that meet the following: [NIST SP 800-132].

FIA_PSK_EXT.3.4
The TSF shall not accept PSKs less than [**Selection**: *a value settable by the administrator* of ≥ 32 characters, *[**Assignment**: minimum PSK length accepted by the TOE, must be >= 32 characters]*] and greater than the maximum PSK length defined in FIA_PSK_EXT.3.1.