Cisco AnyConnect Secure Mobility Desktop Client

Security Target

Version 1.1

March 24, 2016

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

List of Tables

List of Figures

List of Acronyms

The following acronyms and abbreviations are common and may be used in this Security Target:

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
EC-DH	Elliptic Curve-Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
IT	Information Technology
NGE	Next Generation Encryption
OS	Operating System
PP	Protection Profile
PRF	Pseudo-Random Functions
RFC	Request For Comment
SHS	Secure Hash Standard
SPD	Security Policy Database
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
VPN	Virtual Private Network

DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco AnyConnect Desktop (TOE). This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document. The Common Criteria Functional Specification is met through the description of interfaces in this Security Target and the parameters described within the Common Criteria Guidance Documentation as well as the Cisco documentation for TOE.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- References [Section 7]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 2.

1.1 ST and TOE Reference

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

Table 2: ST and TOE Identification

Name	Description
ST Title	AnyConnect Secure Mobility Desktop Client
ST Version	1.1
Publication Date	March 24, 2016
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	AnyConnect Secure Mobility Desktop Client
TOE Software Version	4.1
Keywords	IPsec, VPN Client

1.2 TOE Overview

The TOE is the core VPN component of the Cisco AnyConnect Secure Mobility Desktop Client (herein after referred to as the VPN client, or the TOE). The Cisco AnyConnect Secure Mobility client is the next-generation VPN client, providing remote users with secure IPsec (IKEv2) VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA) VPN Gateway. The TOE is a software-only product running on Windows 8 or 8.1.

1.2.1 TOE Product Type

The TOE product type is a VPN client. A VPN client provides protection of data in transit across a public network. The VPN client implements IPsec to establish a cryptographic tunnel protecting the transmission of data between IPsec peers. The VPN client is intended to be located outside an organization's private network, protecting data flows between a host and the Cisco 5500 Series Adaptive Security Appliance (ASA) VPN Gateway.

1.2.2 Required non-TOE Hardware and Software

The TOE requires the following IT Environment Components when the TOE is configured in its evaluated configuration:

Table 3: Required IT Environment Components

Component	Usage/Purpose Description
Certificate Authority	A Certificate Authority is used to provide valid digital certificates.
OS Platform	The TOE relies on the Microsoft Windows 8 or 8.1 Operating System Platform.
VPN Gateway	The Cisco ASA 5500-X functions as the head-end VPN Gateway.

1.3 TOE DESCRIPTION

This section provides an overview of the Target of Evaluation (TOE). The TOE is software-only IPsec VPN client application that protects data in transit on both IPv4 and IPv6 networks.

The TOE provides IPsec to authenticate and encrypt network traffic travelling across an unprotected public network. The TOE includes Cisco NGE (Next Generation Encryption), providing support for Suite B algorithms. Additionally, the TOE provides for X.509 certificate-based-authentication of the VPN Gateway.

The TOE allows a remote user to establish an IPsec tunnel across the public network to protect an organization's network resources and application communication from unauthorized disclosure or modification.

The following figure provides a visual depiction of a TOE deployment. The TOE boundary is surrounded with a hashed red line.

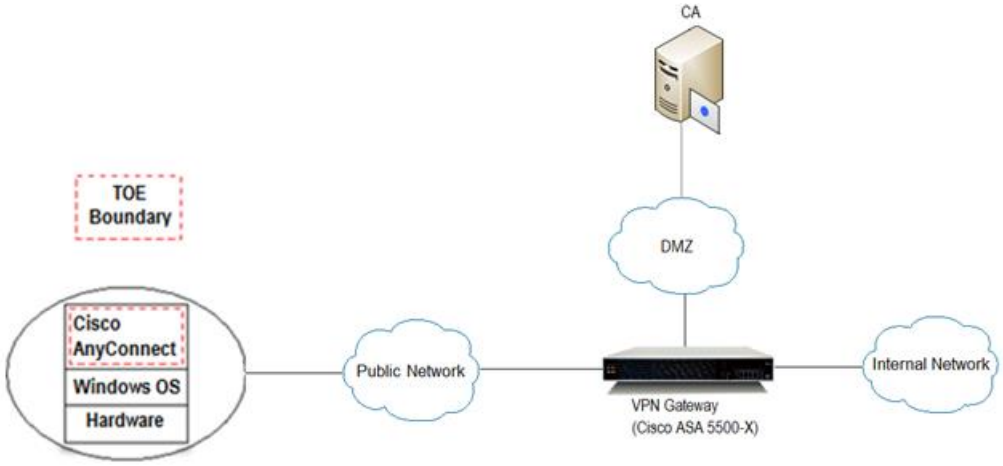

Figure 1 TOE Deployment

1.4 TOE Evaluated Configuration

The TOE is a VPN client application and requires the following to run:

- Windows 8, 8.1, & 8.1 Update 1, x86(32-bit) and x64(64-bit)
- 100 MB hard disk space.
- x86 Pentium class processor or greater

1.5 Physical Scope of the TOE

The TOE is a software-only VPN client application. The underlying platform on which the TOE resides is the Microsoft Windows operating system and is considered part of the IT environment.

The underlying platform provides some of the security functionality required in the VPNv1.4 Client PP, which is denoted with the phrase "TOE Platform" in this Security Target. The security functionality provided by the TOE platform is considered unevaluated.

1.6 Logical Scope of the TOE

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

1. Cryptographic Support
2. User Data Protection
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. Trusted Channels

These features are described in more detail in the subsections below.

1.6.1 Cryptographic support

The TOE authenticates and encrypts IPsec traffic using ESP symmetric cryptography for bulk AES encryption/decryption and SHA-2 algorithm for hashing. In addition the TOE provides the cryptography to support Diffie-Hellman key exchange and derivation function used in the IKEv2 protocol. The TOE incorporates the FIPS Object Module (FOM) v4.1 in accordance with the FIPS 140-2 standard. The Cisco FOM is a FIPS 140-2 validated cryptographic module, certificate #2100.

The TOE platform provides asymmetric cryptography, which is used by the TOE for IKE peer authentication using digital signature and hashing services. In addition the TOE platform provides a DRBG.

1.6.2 User Data Protection

The TOE and TOE platform ensures that residual information from previously sent network packets processed through the platform are protected from being passed into subsequent network packets.

1.6.3 Identification and Authentication

The TOE and TOE platform perform device-level X.509 certificate-based authentication of the VPN Gateway during IKE v2 key exchange. Device-level authentication allows the TOE to establish a secure channel with a trusted VPN Gateway. The secure channel is established only after each endpoint authenticates each other.

1.6.4 Security Management

The TOE, TOE platform, and VPN Gateway provide the management functions to configure the security functionality provided by the TOE.

1.6.5 Protection of the TSF

The TOE performs a suite of self-tests during initial start-up to verify correct operation of its FIPS 140-2 validated algorithms. Upon execution, the integrity of the TOEs software executables is also verified.

The TOE and TOE Platform provide for verification of TOE software updates prior installation.

1.6.6 Trusted Channels

The TOE's implementation of IPsec provides a trusted channel ensuring sensitive data is protected from unauthorized disclosure or modification when transmitted from the host to a VPN gateway.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 4: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation on the TOE	This mode of operation allows cryptographic operations that are not FIPS-approved.

These services will be disabled by configuration. The exclusion of this functionality does not affect conformance to the Protection Profile for IPsec Virtual Private Network (VPN) Clients.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The ST is compliant with the Common Criteria (CC) Version 3.1, Revision 4, September 2012. The ST is CC Part 2 extended and CC Part 3 conformant.

2.2 Protection Profile Conformance

This ST is conformant to the following NIAP-approved Common Criteria validated Protection Profile:

Table 5: Protection Profiles

Protection Profile	Version	Date
Protection Profile for IPsec Virtual Private Network (VPN) Clients	1.4	12 October 2013

2.3 Protection Profile Conformance Claim Rationale

2.3.1 Appropriateness

The ST provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profile:

- Protection Profile for IPsec Virtual Private Network (VPN) Clients v1.4, dated 12 October 2013 (VPNv1.4).

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the VPNv1.4 for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in the VPNv1.4 for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the VPNv1.4 for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in section 4.3 of the VPNv1.4.

3 SECURITY PROBLEM DEFINITION

This section identifies the following:

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

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 6 TOE Assumptions

Assumption	Assumption Definition
A.NO_TOE_BYPASS	Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

3.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 7 Threats

Threat	Threat Definition
T.TSF_CONFIGURATION	Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender because it is not rendered inaccessible after it is done being used.

4 SECURITY OBJECTIVES

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

- This document identifies objectives of the TOE as O.objective with objective specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with objective specifying a unique name.

4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 8 Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
O.VPN_TUNNEL	The TOE will provide a network communication channel protected by encryption that ensures that the VPN client communicates with an authenticated VPN gateway.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to allow administrators to be able to configure the TOE.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.

4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.NO_TOE_BYPASS	Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the operational environment.
OE.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

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.

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:

- Where operations were completed in the VPNv1.4 itself, the formatting used in the VPNv1.4 has been retained;
- Assignment: Indicated with *italicized* text, which may or may not be bracketed;
- Refinement made by PP author: Indicated with **bold** text; may have **Refinement:** at the beginning of the element for further clarification.
- Selection: Indicated with underlined text, which may or may not be bracketed;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

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

5.2 Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE/TOE platform. The Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 10 Security Functional Requirements

Class Name	Component Identification	Component Name
FCS: Cryptographic support	FCS_CKM.1(1)	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM.1(2)	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.2	Cryptographic Key Storage
	FCS_CKM_EXT.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic Operation (for keyed-hash message authentication)
	FCS_IPSEC_EXT.1	Explicit: IPSEC
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
FDP: User data protection	FDP_RIP.2	Full Residual Information Protection
FIA: Identification and authentication	FIA_X509_EXT.1	Extended: X.509 Certificates

Class Name	Component Identification	Component Name
FMT: Security management	FMT_SMF.1(1)	Specification of Management Functions
	FMT_SMF.1(2)	Specification of Management Functions
FPT: Protection of the TSF	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Extended: Trusted Update
FTP: Trusted path/channels	FTP_ITC.1	Trusted Channel

5.3 SFRs Drawn from VPNv1.4

5.3.1 Cryptographic Support (FCS)

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

FCS_CKM.1.1(1) Refinement: The TOE and TOE platform shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance with:

- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;*
- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [P-521] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*
- NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits. See NIST Special Publication 800-57, "Recommendation for Key Management" for information about equivalent key strengths.

5.3.1.2 FCS_CKM.1(2) Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.2(2) Refinement: The TOE platform shall generate **asymmetric** cryptographic keys **used for IKE peer authentication** in accordance with a:

[

- *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* [P-521]

]

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

5.3.1.3 FCS_CKM_EXT.2 Cryptographic Key Storage

FCS_CKM_EXT.2.1 The TOE and TOE platform shall store persistent secrets and private keys when not in use in platform-provided key storage.

5.3.1.4 FCS_CKM_EXT.4 Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TOE and TOE platform shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.3.1.5 FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1(1) Refinement: The TOE shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm *AES operating in* **GCM and CBC mode** with cryptographic key sizes 128-bits and 256-bits that meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **NIST SP 800-38D, NIST SP 800-38A.**

5.3.1.6 FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2) Refinement: The TOE platform shall perform **cryptographic signature services** in accordance with a specified cryptographic algorithm:

- **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 for RSA scheme**

- **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384 and P-521**

and cryptographic key sizes ***equivalent to, or greater than, a symmetric key strength of 112 bits*.**

5.3.1.7 FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1(3) Refinement: The TOE and TOE platform shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm **SHA-256, SHA-384] and message digest sizes 256, 384 bits** that meet the following: *FIPS Pub 180-4, "Secure Hash Standard."*

5.3.1.8 FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1(4) Refinement: The TOE shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm HMAC- **SHA-1, SHA-256, SHA-384, SHA-512, key size [*160, 256, 384, 512 bits*], and message digest size of 160, 256, 384, 512 bits** that meet the following: **FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code", and FIPS Pub 180-4, "Secure Hash Standard."**

5.3.1.9 FCS_IPSEC_EXT.1 Explicit: IPSEC

FCS_IPSEC_EXT.1.1 The TOE and TOE Platform shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TOE shall implement tunnel mode.

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

FCS_IPSEC_EXT.1.4 The TOE shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-GCM-128, AES-GCM-256 as specified in RFC 4106, [AES-CBC-128, AES-CBC-256 (both specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC].

FCS_IPSEC_EXT.1.5 The TOE shall implement the protocol IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [no other RFCs for hash functions].

FCS_IPSEC_EXT.1.6 The TOE shall ensure the encrypted payload in the IKEv2 protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 6379 and [AES-GCM-128, AES-GCM-256 as specified in RFC 5282].

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

> ***Application Note:*** *The TOE implements IKEv2 and does not support IKEv1. This is permitted in [VPNv1.4].*

FCS_IPSEC_EXT.1.8 The TOE shall ensure that IKEv2 SA lifetimes can be configured by VPN Gateway based on length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

FCS_IPSEC_EXT.1.9 The TOE 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 *320 (for DH Group 14), 256 (for DH Group 19), 256 (for DH Group 24), 384 (for DH Group 20)* bits.

FCS_IPSEC_EXT.1.10 The TOE shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^[*256*].

FCS_IPSEC_EXT.1.11 The TOE shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), 19 (256-bit Random ECP), and 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP).

FCS_IPSEC_EXT.1.12 The TOE shall ensure that all IKE protocols perform peer authentication using a RSA, ECDSA that use X.509v3 certificates that conform to RFC 4945 and no other method.

FCS_IPSEC_EXT.1.13 The TOE shall not establish an SA if the distinguished name (DN) contained in a certificate does not match the expected DN for the entity attempting to establish a connection.

FCS_IPSEC_EXT.1.14 Refinement: The TOE **configured by VPN Gateway** 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.

5.3.1.10 FCS_RBG_(EXT).1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TOE platform shall perform all deterministic random bit generation (RBG) services in accordance with NIST Special Publication 800-90A using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based RBG with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

5.3.2 User data protection (FDP)

5.3.2.1 FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TOE platform shall enforce that any previous information content of a resource is made unavailable upon the *allocation of the resource to* all objects.

5.3.3 Identification and authentication (FIA)

5.3.3.1 FIA_X509_EXT.1 Extended: X.509 Certificates

FIA_X509_EXT.1.1 The TOE and TOE platform shall validate certificates in accordance with the following rules:

- Perform RFC 5280 certificate validation and certificate path validation.
- Validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759.
- Validate the certificate path by ensuring the basicConstraints extension is present and the cA flag is set to TRUE for all CA certificates.
- Validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates, integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3).

FIA_X509_EXT.1.2 The TOE shall only treat a certificate as a CA certificate if the following is met: the basicConstraints extension is present and the cA flag is set to TRUE.

5.3.3.2 FIA_X509_EXT.2 Extended: X.509 Certificate Use and Management

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec exchanges, and integrity checks for FPT_TST_EXT.1.2.

FIA_X509_EXT.2.2 When a connection to determine the validity of a certificate cannot be established, the TOE shall allow the administrator to choose whether to accept the certificate in these cases.

FIA_X509_EXT.2.3 The TOE shall not establish an SA if a certificate or certificate path is deemed invalid.

5.3.4 Security management (FMT)

5.3.4.1 FMT_SMF.1(1) Specification of Management Functions

FMT_SMF.1.1(1) The TOE shall be capable of performing the following management functions:

- Specify VPN gateways to use for connections,
- Specify client credentials to be used for connections,
- [*no additional management functions*].

5.3.4.2 FMT_SMF.1(2) Specification of Management Functions

FMT_SMF.1.1(2) The TOE, TOE platform, and VPN Gateway shall be capable of performing the following management functions:

- Configuration of IKE protocol version(s) used,
- Configure IKE authentication techniques used,
- Configure the cryptoperiod for the established session keys. The unit of measure for configuring the cryptoperiod shall be no greater than an hour,
- Configure certificate revocation check,
- Specify the algorithm suites that may be proposed and accepted during the IPsec exchanges,
- load X.509v3 certificates used by the security functions in this PP,
- ability to update the TOE, and to verify the updates,
- ability to configure all security management functions identified in other sections of this PP,
- allow the administrator to choose whether to accept the certificate when a connection to determine the validity of a certificate cannot be established, no other actions.

5.3.5 Protection of the TSF (FPT)

5.3.5.1 FPT_TST_EXT.1: TSF Testing

FPT_TST_EXT.1.1 The TOE shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TOE platform shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the [*cryptographic signature verification*].

5.3.5.2 FPT_TUD_(EXT).1 Extended: Trusted Update

FPT_TUD_(EXT).1.1 The TOE shall provide the ability to query the current version of the TOE firmware/software.

FPT_TUD_(EXT).1.2 The TOE shall provide the ability to initiate updates to TOE firmware/software.

FPT_TUD_(EXT).1.3 The TOE platform shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [no other functions] prior to installing those updates.

5.3.6 Trusted Path/Channels (FTP)

5.3.6.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TOE shall **use IPsec** to provide a **trusted** communication channel between itself and **a VPN Gateway** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data **from disclosure and detection of modification of the channel data.**

FTP_ITC.1.2 The TOE shall permit *the TSF* to initiate communication via the trusted channel.

FTP_ ITC.1.3 The TOE shall initiate communication via the trusted channel *for all traffic traversing that connection.*

5.4 TOE SFR Dependencies Rationale for SFRs Found in VPNv1.4

The VPNv1.4 contains all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PP itself has been approved.

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 11: Assurance Measures

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
	ALC_CMS.1	TOE CM coverage
Test	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability analysis

5.5.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the VPNv1.4 PP. As such, the VPNv1.4 SAR rationale is deemed acceptable since the PP itself has been validated.

5.5.3 Assurance Measures

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

Table 12: Assurance Measures

Component	How requirement will be met
ADV_FSP.1	The functional specification is comprised of the information contained in the AGD_OPR and AGD_PRE documentation, coupled with the information provided in the TSS of the ST.
AGD_OPE.1	The Administrative Guide provides operational user guidance.
AGD_PRE.1	The preparative procedures describes all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
ALC_CMC.1 ALC_CMS.1	Cisco will provide the TOE and a reference for the TOE.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

Table 13 identifies and describes how the Security Functional Requirements identified in section 5 of this ST are met.

Table 13 How TOE SFRs Measures

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><th colspan="2">Security Functional Requirements Drawn from VPNv1.4</th></tr>
<tr><td>FCS_CKM.1 (1)
FCS_CKM.1 (2)</td><td>The TOE incorporates a FIPS 140-2 validated cryptographic module, CMVP #2100, that provides public-private key establishment for Diffie-Hellman and Diffie-Hellman Elliptic Curve key exchange conformant to NIST SP 800-56A.

The TOE platform incorporates Cryptographic Service Providers (CSPs) which generate the public/private key pairs below:

• Elliptic Curve DSA (ECDSA) key establishment scheme with P-256, P-384, and P-521 prime curves;

• RSA key establishment scheme with 4096 bit key size.

A CSP is invoked on the TOE platform by an Application Programming Interface - Cryptography API: Next Generation (CNG). The CSPs provided by the TOE platform are FIPS 140 validated. The relevant FIPS certificate numbers are listed below:

<table>
<tr><th>TOE Platform</th><th>Certificate Numbers</th></tr>
<tr><td>Windows 8</td><td>CMVP# 1892, 1893, 1894</td></tr>
<tr><td>Windows 8.1</td><td>CMVP# 2355, 2356, 2357</td></tr>
</table>
</td></tr>
<tr><td>FCS_CKM_EXT.2</td><td>Persistent key, secret, or credentials manipulated by the TOE are stored when not in use on TOE platform-provided storage as follows:

<table>
<tr><th>Key, Secret, or Credential</th><th>Purpose</th><th>Stored In</th></tr>
<tr><td>Device identity certificates</td><td>IPsec peer authentication</td><td>Windows Certificate Store</td></tr>
<tr><td>CA certificate</td><td>IPsec peer authentication</td><td>Windows Certificate Store</td></tr>
</table>

The TOE does not use pre-shared keys for IPsec, making any possibility of storing it unencrypted on the TOE platform non-existent.

Persistent key, secret, or credentials manipulated by the TOE platform are stored when not in use on the TOE platform as follows:

<table>
<tr><th>Key, Secret, or Credential</th><th>Purpose</th><th>Stored In</th></tr>
<tr><td>Asymmetric ECDSA Private Key</td><td>ECDSA digital signature generation</td><td>Windows Key Storage Provider (KSP)</td></tr>
<tr><td>Asymmetric RSA Private Key</td><td>RSA digital signature generation</td><td>Windows Key Storage Provider (KSP)</td></tr>
<tr><td>Asymmetric ECDSA Public Key</td><td>ECDSA digital signature verification</td><td>Windows Key Storage Provider (KSP)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<table>
<tr><td>Asymmetric RSA Public Key</td><td>RSA digital signature verification</td><td>Windows Key Storage Provider (KSP)</td></tr>
</table>
</td></tr>
<tr><td>FCS_CKM_EXT.4</td><td>
The TOE ensures volatile memory areas containing plaintext private keys, secrets, and critical security parameters it manipulates are cleared by invoking a function on the TOE platform to perform zeroization as follows:
<table>
<tr><th>Key, Secret, or CSP</th><th>Purpose</th><th>Zeroization Method</th></tr>
<tr><td>Diffie-Hellman Shared Secret</td><td>IKE v2 SA setup</td><td>Overwritten with zeros when no longer in use by the IPsec VPN trusted channel.</td></tr>
<tr><td>SKEYID_d</td><td>IKEv2 SA key from which child IPsec keys are derived.</td><td>Overwritten with zeros when no longer in use by the IPsec VPN trusted channel.</td></tr>
<tr><td><u>IPsec child SA keys:</u>

o Initiator encryption and integrity key

o Responder encryption and integrity key</td><td>

ESP SA - encrypts and authenticates outgoing traffic

ESP SA - decrypts and authenticates incoming traffic</td><td>

Overwritten with zeros when no longer in use by the IPsec VPN trusted channel.</td></tr>
</table>
The TOE platform zeroizes private keys it manipulates and stores on the TOE platform:
<table>
<tr><th>Key, Secret, or CSP</th><th>Purpose</th><th>Zeroization Method</th></tr>
<tr><td>Asymmetric ECDSA Private Key stored on the TOE platform</td><td>ECDSA digital signature generation</td><td>Performed exclusively by the TOE Platform.</td></tr>
<tr><td>Asymmetric RSA Private Key stored on the TOE platform</td><td>RSA digital signature generation</td><td>Performed exclusively by the TOE Platform.</td></tr>
</table>
</td></tr>
<tr><td>FCS_COP.1(1)</td><td>
The TOE provides symmetric encryption and decryption capabilities using AES in CBC and GCM mode (128, 256 bits) as described in NIST SP 800-38A and NIST SP 800-38D.

The relevant FIPS certificate numbers are listed below:
<table>
<tr><th>Cryptographic Operation</th><th>Mode</th><th>NIST CAVP Cert #</th></tr>
<tr><td>AES</td><td>CBC (128, 256)
GCM (128, 256)</td><td>2685, 2678</td></tr>
</table>
</td></tr>
<tr><td>FCS_COP.1(2)</td><td>The TOE platform provides cryptographic signature services for the TOE to verify the VPN Gateway X.509 certificate during the IKEv2 authentication phase of IPsec.</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>The TOE also relies upon the TOE platform to provide cryptographic signature verification services for the TOE software during the trusted update process.

This operation is invoked by the TOE via a programmatic call to a cryptographic function (Cryptography API: Next Generation (CNG) provided by the TOE platform.

The relevant FIPS certificate numbers are listed below:

<table>
<tr><th>TOE Platform</th><th>Cryptographic Operation</th><th>NIST CAVP #</th></tr>
<tr><td>Windows 8</td><td>Digital Signature – ECDSA</td><td>341</td></tr>
<tr><td>Windows 8</td><td>Digital Signature - RSA</td><td>1134, 1133</td></tr>
<tr><td>Windows 8.1</td><td>Digital Signature – ECDSA</td><td>505</td></tr>
<tr><td>Windows 8.1</td><td>Digital Signature - RSA</td><td>1519, 1494, 1493, 1487</td></tr>
</table></td></tr>
<tr><td>FCS_COP.1(3)</td><td>When performing AES cryptographic operations in CBC mode, the TOE provides cryptographic hashing to ensure data integrity for the ESP protocol using SHA-256 and SHA-384 as specified in FIPS Pub 180-4 “Secure Hash Standard.”

The relevant FIPS certificate numbers are listed below:

<table>
<tr><th>Cryptographic Operation</th><th>Mode</th><th>NIST CAVP Cert #</th></tr>
<tr><td>SHS</td><td>SHA-256, SHA-384</td><td>2256, 2247</td></tr>
</table>
The TOE platform provides cryptographic hashing services using SHA-256, and SHA-384 as specified in FIPS Pub 180-4 “Secure Hash Standard.” The TOE relies upon the TOE platform for cryptographic hash functions required to verify the integrity of a certificate during the IKEv2 authentication phase of IPsec. This operation is invoked by the TOE via a programmatic call to a cryptographic function (Cryptography API: Next Generation (CNG) provided by the TOE platform.

The relevant FIPS certificate numbers are listed below:

<table>
<tr><th>TOE Platform</th><th>Cryptographic Operation</th><th>NIST CAVP #</th></tr>
<tr><td>Windows 8</td><td>Hashing (SHA-256, SHA-384, SHA-512)</td><td>1903</td></tr>
<tr><td>Windows 8.1</td><td>Hashing (SHA-256, SHA-384, SHA-512)</td><td>2396</td></tr>
</table></td></tr>
<tr><td>FCS_COP.1(4)</td><td>To verify the data integrity and authentication of IPsec bulk traffic the TOE provides keyed-hashing message authentication services within the encryption of IKEv2 payloads. Additionally, the TOE provides keyed-hashing message authentication services for Pseudo-Random Functions (PRFs) in IKEv2. Both use HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 as specified in FIPS Pub 198-1," The Keyed-Hash Message Authentication Code,” and FIPS 180-4, “Secure Hash Standard.”
The TOE does not implement any truncation of the hash for data integrity and authentication. Truncation does not apply to Pseudo-Random Functions (PRFs) in IKEv2.

The relevant FIPS certificate numbers are listed below:
<table>
<tr><th>Algorithm</th><th>Mode</th><th>NIST CAVP Cert #</th></tr>
<tr><td>HMAC</td><td>SHA-1, SHA-256, SHA-384, SHA-512</td><td>1672, 1664</td></tr>
</table></td></tr>
</table>

TOE SFRs	How the SFR is Met
FCS_IPSEC_EXT.1	The TOE's implementation of the IPsec standard (in accordance with RFC 4301) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services. By default ESP operates in tunnel mode. No configuration is required by the user or administrator for the TOE to operate in tunnel mode. Remote access policies on the ASA VPN Gateway provide an interface for the administrator to create ACL(s), defining network segment(s) requiring IPsec protection. An XML format of the policy on client defines the remote access policy the TOE will use. After successful client authentication to the ASA VPN Gateway, a "Cisco AnyConnect Secure Mobility Client" virtual interface is created and assigned an IP address from the Gateway's VPN address pool. The TOE's virtual interface includes a kernel mode driver digitally signed by Cisco Systems, Inc. The Security Policy Database (SPD) is implemented by the underlying TOE Platform and the TOE interacts with the SPD through insertions of entries to the routing table on the host OS platform. This enforces what traffic is protected with IPsec by the TOE and what traffic isn't. Traffic that is protected is processed by ESP and tunneled through the TOE's virtual interface. The default behavior of the remote access policy on the VPN Gateway is for the TOE to protect all traffic with IPsec. When all traffic is tunneled, a new default route is added to the host OS platform with a lower metric directing all host network traffic through the "Cisco AnyConnect Secure Mobility Client" virtual interface. The TOE uses active SA settings or creates new SAs for initial connections with the ASA VPN Gateway peer. All ESP processing to authenticate, encrypt, and tunnel the traffic is performed by the TOE. If an organization explicitly permits use of split-tunneling, a remote access policy on the ASA VPN Gateway allows the administrator to define IPsec protection for the organization's network(s) but bypass protection for other traffic. When a portion of traffic is tunneled, a route is added to the host OS platform corresponding to the network segment requiring IPsec protection, directing that portion of host network traffic for ESP processing and tunneling through the "Cisco AnyConnect Secure Mobility Client" virtual interface. Network(s) and subnet(s) not subjected to the remote access policy, but reachable from the host platform, such as Internet traffic, travels outbound from the host without being protected with IPsec by the TOE. TOE Platform provides an interface where an administrator configures firewall rules to block bypass traffic not permitted to traverse the network. Traffic that does not match network segments that bypass IPsec protection can be configured by the platform administrator to be dropped. A drop rule results in discarded network traffic. This applies only when split-tunneling is enabled; when split tunneling is not configured all traffic is tunneled. The TOE implements IKEv2 and does not support IKEv1. IPsec Internet Key Exchange is the negotiation protocol that lets the TOE and a VPN Gateway agree on how to build an IPsec Security Association (SA). IKE separates negotiation into two phases: phase 1 and phase 2. During IKE Phase 1, the TOE authenticates the remote VPN Gateway using device-level authentication with ECDSA or RSA X.509v3 certificates provided by the TOE platform.

TOE SFRs	How the SFR is Met
	Phase 1 creates the first tunnel, which protects later IKE negotiation messages. The key negotiated in phase 1 enables IKE to communicate securely in phase 2. The TOE supports only IKEv2 session establishment. As part of this support, the TOE by default does not support aggressive mode used in IKEv1 exchanges. The TOE supports Diffie-Hellman Group 14 (2048-bit keys), 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), and 20 (384-bit Random ECP) in support of IKE Key Establishment negotiated in phase 1. These keys are generated using the DRBG specified in FCS_RBG_EXT.1 having 256 bits of entropy. The administrator is instructed in the AGD to select a supported DH group using one of the following corresponding key sizes (in bits): 320 (for DH Group 14), 256 (for DH Group 19), 256 (for DH Group 24), and 384 (for DH Group 20) bits. For each DH Group, the TOE generates the secret value 'x' used in the IKEv2 Diffie-Hellman key exchange ('x' in g^x mod p) using its DH private key, the IPsec peer's public key and a nonce. When a random number is needed for a nonce, the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^{256}. The nonce is likewise generated using the DRBG specified in FCS_RBG_EXT.1. During Phase 2, IKE negotiates the IPsec SA and includes: • The negotiation of mutually acceptable IPsec SA parameters; • The Pseudo-Random Function (PRF) is used for the construction of keying material for cryptographic algorithms used in the SA. • The establishment of IPsec Security Associations to protect packet flows using Encapsulating Security Payload (ESP). The resulting potential strength of the symmetric key will be 128, 192, or 256 bits of security depending on the algorithms negotiated between the two IPsec peers. The TOE ensures by default 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. After IKE phase 2 completes, the IPsec SA is established, providing a secure tunnel to a remote VPN Gateway. The VPN Gateway allows the administrator to configure AES-GCM-128, AES_GCM-256, AES-CBC-128, and AES-CBC-256 for the TOE to perform bulk IPsec encryption. The TOE supports administratively configured lifetimes for both Phase 1 SAs and Phase 2 SAs. The default time value for Phase 1 SAs is 24 hours. The value for Phase 2 SAs is configurable to 8 hours. Both values are configurable using management functions provided by the VPN Gateway.
FCS_RBG_EXT.1	The TOE invokes RBG functionality provided by the TOE platform through the CryptGenRandom function. The CryptGenRandom function provides the TOE with cryptographically random bytes.
FDP_RIP.2	The processing of network packets for residual information is handled by the TOE platform. The TOE platform ensures that packets transmitted from the TOE platform do not contain residual information from previous network packets. Buffers allocated for a network packet are not reused for subsequent network packets. The TOE platform ensures the memory allocated to the buffer once it's no longer needed is released back to the Windows Operating System.
FIA_X509_EXT.1 FIA_X509_EXT.2	The TOE uses X.509v3 certificates as defined by RFC 5280 for device level authentication of the VPN Gateway. Portions of the certificate validation are performed on both the TOE and TOE platform. The user is provided with an X.509v3 certificate which is loaded into the Windows OS certificate store. Upon initiation of an IPsec connection, the TOE will validate the VPN

TOE SFRs	How the SFR is Met
	Gateway certificate and CA issued certificate as follows: • The TOE checks Basic Constraint by met by ensuring the CA for the certificate of VPN Gateway is an issuer for certificates (cA flag is TRUE). It also checks VPN Gateway certificate is an end-certificate. • The TOE check the issuer field of the VPN Gateway certificate matches that of the CA certificate, as well as any intermediate CAs that are identified in the chain below the root. The root certificates are provided in the Windows OS certificate store. • The TOE relies upon the TOE platform to check the revocation status of the VPN Gateway certificate. The TOE invokes the Crypto API function provided by the Windows OS, which in turn uses OCSP or CRL to check if the certificate has been revoked. By performing the checks described above, the TOE ensures certificate validation results in a trusted root certificate. At any point if a certificate cannot be successfully validated, the AGD guidance instructs the administrator to configure the TOE to not allow the user an option for continuing the connection. In all cases, if a certificate or certificate path cannot be validated, the TOE will not establish an IPsec connection to an untrusted VPN Gateway.
FMT_SMF.1(1)	Security management functions are provided by the TOE as specified below: • The **TOE** is capable of specifying VPN gateways to use for connections, • The **TOE** is capable of prompting the user to select the authentication certificate to use as well as specifying the location to search. Certificates are used for device-level authentication of the VPN Gateway. • The **TOE** is capable of specifying Username/password credentials used to authenticate remote VPN users to an authentication server.
FMT_SMF.1(2)	Security management functions are provided by the TOE, the TOE platform, or the VPN Gateway as specified below: • The **VPN Gateway** is capable of configuring IKEv2 IPsec proposals • The **VPN Gateway** is capable of configuring IKEv2 authentication • The **VPN Gateway** is capable of configuring the cryptoperiod for the established session keys. The unit of measure for configuring the cryptoperiod shall be no greater than an hour, • The **TOE** is capable of configuring certificate revocation check, • The **VPN Gateway** is capable of specifying the algorithm suites that may be proposed and accepted during the IPsec exchanges, • The **TOE platform** is capable of loading an X.509v3 certificate used by the TOE to authenticate the VPN gateway during IPsec authentication. • The **TOE platform** is capable of updating the TOE, and capable of verifying the updates, • The **TOE** is capable of configuring all security management functions identified in FMT_SMF.1(1), • The **TOE** is capable of allowing the administrator to choose whether to accept the certificate when a connection to determine the validity of a certificate cannot be established.
FPT_TST_EXT.1	As a software product incorporating a FIPS 140-2 validated module, the TOE runs a suite of self-tests during start-up to verify its correct operation.

TOE SFRs	How the SFR is Met
	These tests include: • AES Known Answer Test • RSA Signature Known Answer Test (both signature/verification) • FIPS 186-3 ECDSA Sign/Verify Test • KAS ECC Primitive "Z" KAT • HMAC Known Answer Test • SHA-1/256/512 Known Answer Test • Software Integrity Test If any self-test fails subsequent invocation of any cryptographic function calls is prevented. If all components of the power-up self-test are successful then the product is in FIPS mode. Upon launch, the TOE platform performs an executable code integrity verification check, invoking the TOE platform to perform digital signature verification operations on executable files. These tests are sufficient to verify that the TOE software is operating correctly as well as the cryptographic operations are all performing as expected.
FPT_TUD_EXT.1	The TOE has specific versions that can be queried by a user. Updates are a new version of the TOE. When updates are made available by Cisco, an administrator can obtain and install those updates. The updates can be downloaded from the Cisco.com web site. Administrators can download the software update from Cisco.com onto the TOE platform. Software updates are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html The authorized source for the digitally signed updates is "Cisco Systems, Inc." Upon installation of a TOE update, a digital signature verification check will automatically be performed. The authorized source for the digitally signed updates is "Cisco Systems, Inc.". Verification includes a check that the certificate is valid and has a Code Signing Value of 1.3.6.1.5.5.7.3.3 in the EKU field. Updates are a new version of the TOE. The TOE performs digital signature verification prior to update installation, invoking cryptographic services provided by the TOE platform.
FTP_ITC.1	The TOE implements IPsec to protect all communication transmitted from the host destined for a VPN gateway.

7 ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 14: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-20012-09-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-20012-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-004
[VPNv1.4]	Protection Profile for IPsec Virtual Private Network (VPN) Clients, 1.4, 12 October 2013