Assurance Activity Report (AAR) for a Target of Evaluation

Apple IOS 11 VPN Client on iPhone and iPad

Apple IOS 11 VPN Client Security Target Version 1.3, April 2018
Protection Profile for IPsec Virtual Private Network (VPN) Clients Version 1.4

Evaluated by:

18504 Office Park Dr.
Montgomery Village, MD 20886

Prepared for:
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Apple, Inc.
1 Infinite Loop
Cupertino, California 95014

The Author of the Security Target:
Acumen Security, LLC.
18504 Office Park Drive
Montgomery Village, MD 20886

The TOE Evaluation was Sponsored by:
Apple, Inc.
1 Infinite Loop
Cupertino, California 95014

Evaluation Personnel:
Anthony Busciglio
Kevin Micciche

Common Criteria Version
Common Criteria Version 3.1 Revision 4

Common Evaluation Methodology Version
CEM Version 3.1 Revision 4

Revision History

Version	Date	Changes
Version 1.2	March 2018	Initial Release
Version 1.3	April 2018	Updated based on ECR comments
Version 1.4	May 2018	Updated in prep for posting

Contents

1 TOE Overview

The TOE is the Apple iOS 11 VPN Client which runs on iPad and iPhone devices. The IPsec VPN allows users the ability to have confidentiality, integrity, and protection of data in transit regardless of the transport mechanism (cellular or wifi).

Note: The TOE is the VPN Client software only. The Apple iOS operating system has been separately validated (VID10851). Platform assurance activities, per the PP, may rely upon the evidence provided in VID10851. The evaluation team had access to all required artifacts from the platform evaluation.

1.1 TOE Description

The TOE is a VPN client on a mobile operating system. The TOE is the VPN Client software only. The Apple iOS operating system has been separately validated (VID10851). The mobile operating system and hardware platforms are part of the TOE environment. When deployed, the TOE provides a tunnel to a VPN Gateway. The evaluated version of the TOE is version 11.

1.2 Security Features

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels

1.3 Technical Decisions

The following technical decisions were considered as part of this evaluation:

- TD0140: FCS_IPSEC_EXT.1.12, Test 1 - Importing of Private Key and Certificate
- TD0138: IPsec VPN Client Testing of SPD Rules
- TD0124: Auditable Events in VPN IPSEC Client PP
- TD0107: FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation
- TD0097: VPN Gateway selection for FCS_IPSEC_EXT.1.14
- TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
- TD0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4
- TD0042: Removal of Low-level Crypto Failure Audit from PPs
- TD0037: IPSec Requirement_DN Verification
- TD0014: Satisfying FCS_IPSEC_EXT.1.13 in VPN GW EP

2 Test Identification

Test Case ID	*Assurance Activity*
FMT.SMF.1 TSS 1	*Verification of client credentials and usage.*
FMT.SMF.1 Guidance 1	*Verification that every management function is included in the guidance documentation.*
FCS_CKM.1(1) TSS 1 (platform)	*Verification that the required key establishment is provided by the platform.*
FCS_CKM.1(1) TSS 2 (platform)	*Verification of how platform key management is invoked.*
FCS_CKM.1(2) TSS 1 (platform)	*Verification that the required key generation is provided by the platform.*
FCS_CKM.1(2) TSS 2 (platform)	*Verification of how platform key generation is invoked.*
FCS_CKM.2 TSS 1	*Verification that all persistent keys are specified and described.*
FCS_CKM.2 TSS 2 (platform)	*Verification that the platform ST addresses each of the required persistent keys.*
FCS_CKM_EXT.4 TSS 1	*Verification that all keys and CSPs are specified.*
FCS_CKM_EXT.4 TSS 2 (platform)	*Verification that all keys and CSPs are specified and described.*
FCS_CKM_EXT.4 TSS 3 (platform)	*Verification that all keys and CSPs are specified and described.*
FCS_CKM_EXT.4 TSS 4 (TOE)	*Verification that each key and CSP is zeroized.*
FCS_COP.1(1) TSS 1 (platform)	*Verification that the platform ST covers all required symmetric encryption/decryption.*
FCS_COP.1(1) TSS 2 (platform)	*Verification that the invocation of symmetric encryption/ decryption.*
FCS_COP.1(2) TSS 1 (platform)	*Verification that the platform ST covers all required digital signature operations.*
FCS_COP.1(2) TSS 2 (platform)	*Verification that the invocation of symmetric digital signature operations.*
FCS_COP.1(3) TSS 1	*Verification that each hashing operation is associated with a high order cryptographic function.*
FCS_COP.1(3) TSS 2 (platform)	*Verification that the platform ST covers all required hashing operations.*
FCS_COP.1(3) TSS 3 (platform)	*Verification that the invocation of hashing operations.*
FCS_IPSEC_EXT.1.1 Guidance 1	*Verification that the guidance addresses the creation of an SPD.*
FCS_IPSEC_EXT.1.2 TSS 1	*Verification that the ST addresses which IPsec modes are supported.*
FCS_IPSEC_EXT.1.2 Guidance 1	*Verification that the guidance address configuration of IPsec modes.*
FCS_IPSEC_EXT.1.3 TSS 1	*Verification that the ST addresses the final default rule in an SPD.*
FCS_IPSEC_EXT.1.3 Guidance 1	*Verification that the guidance address how to construct an SPD.*
FCS_IPSEC_EXT.1.4 TSS 1	*Verification that the ST addresses which AES modes are supported for IPsec connections.*
FCS_IPSEC_EXT.1.4 Guidance	*Verification that the guidance addresses configuration of AES for IPsec.*
FCS_IPSEC_EXT.1.5 TSS 1	*Verification that the ST addresses which IKE versions are supported.*
FCS_IPSEC_EXT.1.5 Guidance 1	*Verification that the guidance addresses configuring IKE versions.*
FCS_IPSEC_EXT.1.6 TSS 1	*Verification that the ST addresses which AES modes are supported for IKE connections.*
FCS_IPSEC_EXT.1.6 Guidance 1	*Verification that the guidance addresses configuration of AES for IKE.*
FCS_IPSEC_EXT.1.8 Guidance 1	*Verification that the guidance addresses configuring SA lifetimes.*
FCS_IPSEC_EXT.1.9/10 TSS 1	*Verification that the ST addresses DH "x" value generation.*
FCS_IPSEC_EXT.1.9/10 TSS 2	*Verification that the ST addresses DH nonce value generation.*
FCS_IPSEC_EXT.1.11 TSS 1	*Verification that the ST addresses the supported DH groups*
FCS_IPSEC_EXT.1.12 TSS 1	*Verification that the ST addresses the supported peer authentication.*
FCS_IPSEC_EXT.1.12 Guidance 1	*Verification that the guidance addresses the configuring peer authentication.*
FCS_IPSEC_EXT.1.12 Guidance 2	*Verification that the guidance addresses connections with a trusted CA.*
FCS_IPSEC_EXT.1.14 TSS 1	*Verification that the ST describes the allowed strengths phase 1 and phase 2 SAs.*

Test Case ID	*Assurance Activity*
FCS_RBG_EXT.1 TSS 1 (platform)	*Verification that the platform ST covers all required Random Number Generation.*
FCS_RBG_EXT.1 TSS 2 (platform)	*Verification that the invocation of Random Number Generation.*
FDP_RIP.2 TSS 1	*Verification that the ST describes packet processing.*
FIA_X509_EXT.1 TSS 1	*Verification that the ST describes where certificate verification takes place.*
FIA_X509_EXT.1 TSS 2	*Verification that the ST describes the certificate path validation algorithm.*
FIA_X509_EXT.1 Guidance 1	*Verification that the guidance addresses configuring certificate path validation.*
FIA_X509_EXT.2 TSS 1	*Verification that the ST addresses how certificates are chosen.*
FIA_X509_EXT.2 Guidance 1	*Verification that the guidance addresses configuration of the chosen certificates.*
FPT_TST_EXT.1 TSS 1	*Verification that the TSS describes what self-tests are performed.*
FPT_TST_EXT.1 TSS 2	*Verification that the TSS justifies the sufficiency of the implemented self-tests.*
FPT_TST_EXT.1 TSS 3	*Verification that the integrity test is described.*
FPT_TST_EXT.1 TSS 4 (or Guidance)	*Verification that the ST addresses what happens when the integrity test is failed or passed.*
FPT_TUD_EXT.1 TSS 1	*Verification that the ST describes how software updates are verified.*
FPT_TUD_EXT.1 TSS 2 (or Guidance)	*Verification that the ST describes the update process.*
FTP_ITC.1 TSS 1	*Verification that the ST describe how to connect with other IT devices*
FTP_ITC.1 TSS 2	*Verification that the ST specifies the protocols supported for connecting to other IT devices.*
FTP_ITC.1 Guidance 1	*Verification that the guidance addresses connecting and recovering from a disconnection.*
FCS_CKM_EXT.4 Test 1	*This test is used to verify the clearing of keys is done properly and consistent according to the protection profile.*
FIA_X509_EXT.1 Test #1	*This test demonstrates the proper handling of certificates for validation without a proper certificate path.*
FIA_X509_EXT.1 Test #2	*This test demonstrates that an expired certificate is rejected.*
FIA_X509_EXT.1 Test #3	*This test demonstrates that a revoked certificate is properly handled.*
FIA_X509_EXT.1 Test #4	*This test demonstrates that a CA with a constructed certificate path but without the cA flag basic constraints extension fails.*
FIA_X509_EXT.1 Test #5	*This test demonstrates that a CA with a constructed certificate path but with the cA flag basic constraints extensions not set still fails.*
FIA_X509_EXT.1 Test #6	*This test demonstrates that a CA with a constructed certificate path but without the basic constraints extension set to TRUE.*
FIA_X509_EXT.2 met by TOE, Test #1	*This test demonstrates the ability to validate a certificate from a NON-TOE IT entity properly.*
FPT_TST_EXT.1 Test #1	*This test demonstrates the TOES ability to perform an integrity check on a KNOWN good TSF executable and verify the check is successful*
FPT_TST_EXT.1 Test #2	*This test demonstrates the TOES ability to perform an integrity check on a modified TSF executable and that the check fails.*
FPT_TUD_EXT.1 Test #1	*This demonstrates the TOES ability to update with a legitimate version as well as shows that it is possible to determine the current version on the device.*
FPT_TUD_EXT.1 Test #2	*This test demonstrates the TOES ability to reject an illegitimate copy of the update software.*

Test Case ID	*Assurance Activity*
FTP_ITC.1 Test #1	*This test demonstrates the TOES ability to initiate communication with a VPN gateway using the specified protocols in the requirement.*
FTP_ITC.1 Test #2	*This test verifies that the TOE, for each communication channel with a VPN, does not send channel data as plaintext.*
FTP_ITC.1 Test #3	*This test verifies that the TOE, for each communication channel with the VPN, modification of channel data is detected.*
FTP_ITC.1 Test #4	*This test demonstrates that when the connection is physically interrupted and the connection is physically reestablished, that the TOE does not send any data unencrypted.*
FMT_SMF.1 Test #1	*This test demonstrates the TOE's ability to provide management functions according to the operational guidance.*
FCS_IPSEC_EXT.1.1 Test #2	*This test verifies the TOES ability to process packets in different scenarios that exercise the range of possibilities for SPD entries and modes.*
FCS_IPSEC_EXT.1.2 Test #1	*This test verifies that a successful connection can be made via "Tunnel Mode"*
FCS_IPSEC_EXT.1.3 Test #1	*This test demonstrates the TOES ability to handle SPD rules that cover DISCARD, BYPASS and PROTECT.*
FCS_IPSEC_EXT.1.4 Test #1	*This test demonstrates the TOES ability to establish a connection using each AES-GCM-128, AES-GCM-256, AES-CBC-128 and AES-CBC-256 with ESP.*
FCS_IPSEC_EXT.1.5 Test #1	*This test demonstrates the TOES ability to handle NAT Transversal processing.*
FCS_IPSEC_EXT.1.6 Test #1	*This test demonstrates the TOES ability to use a given ciphersuite to encrypt an IKEv2 payload and establish a connection with a peer device.*
FCS_IPSEC_EXT.1.8 Test #2	*This test demonstrates the TOES ability to maintain and renegotiate a Phase 1 SA.*
FCS_IPSEC_EXT.1.8 Test #3	*This test demonstrates the TOES ability to maintain and renegotiate a Phase 2 SA.*
FCS_IPSEC_EXT.1.11 Test 1	*This test verifies that the TOE can handle all the claimed IKE protocols can be completed using the claimed DH group.*
FCS_IPSEC_EXT.1.12 Test 1	*This test verifies that a TOE can generate a CSR/verify the response.*
FCS_IPSEC_EXT.1.12 Test 2	*This test verifies that for each field of the supported certificate for comparison to the peer, the IKE authentication succeeds. Both SAN and CN are tested here.*
FCS_IPSEC_EXT.1.12 Test 3	*This test demonstrates that the TOE can handle revoked certificates.*
FCS_IPSEC_EXT.1.12 Test 4a	*This test verifies that for each field of the supported certificate for comparison to the peer, the IKE authentication fails due to a mismatch. Here, the CN portion of the DN is tested.*
FCS_IPSEC_EXT.1.12 Test 4b	*This test verifies that when the reference identifier does not match, the IKE authentication fails. Here, the SAN is tested.*
FCS_IPSEC_EXT.1.12 Test 6	*This test verifies whether the TOE will establish an SA or not, if the certificate of the gateway is not able to be validated due to an OCSP responder being unreachable.*
FCS_IPSEC_EXT.1.14 Test 1	*This test verifies that the TOE can properly use the claimed algorithms for each version of IKE in its implementation.*
FCS_IPSEC_EXT.1.14 Test 3	*This test verifies that using an algorithm that is not supported will result in a failed connection.*
FCS_IPSEC_EXT.1.14 Test 4	*This test verifies that you cannot establish an SA for ESP using an encryption algorithm that is not supported*

Table 1 Test Identification

3 Testing Subset

The following table identifies the chosen subset of hardware models on which the TOE (iOS VPN Client) is to be tested.

Device	CPU Model	Operating System
iPhone 5S	A7	Apple iOS11
iPhone 6 Plus	A8	Apple iOS11
iPad Air 2	A8X	Apple iOS11
iPhone 6S	A9	Apple iOS11
iPad Pro 9.7	A9X	Apple iOS11
iPhone 7	A10	Apple iOS11
iPad Pro	A10X	Apple iOS11
iPhone 8	A11	Apple iOS11

Table 2 Models Tested

4 TSS and Guidance Activities

4.1 FMT.SMF.1 TSS 1

The evaluator shall check to ensure the TSS describes the client credentials and how they are used by the TOE.

4.1.1 Evaluator Findings

The evaluator checked to ensure the TSS describes the client credentials and how they are used by the TOE. Table 6 of the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the following security management functions are provided directly by the TOE,

- Selection of the VPN gateway,
- Presentation of credentials (X.509v3 certificate) used to connect to the gateway.

The client itself uses ANSI X.509 digital certificates for authenticating to a VPN gateway when establishing an IPsec connection. This certificate may be imported by a user (if allowed by the policy) or installed using configuration profiles. The list of supported certificate and formats, include,

- X.509 certificates,
- File extensions cer, .crt, .der, .p12, and .pfx

Based on these findings, this activity is considered satisfied.

4.1.1.1 Verdict

PASS

4.2 FMT.SMF.1 Guidance 1

The evaluator shall check to make sure that every management function mandated in the ST for this requirement are described in the operational guidance and that the description contains the information required to perform the management duties associated with each management function.

4.2.1 Evaluator Findings

The evaluator examined the TOE guidance documentation and found that it describes all the management functions as mandated by the ST for this requirement. The AGD was used to determine the verdict of this Assurance Activity.

The information can be found in sections listed below

- Configuration of IKE protocol: Connection Type, section 3.2.3.1, Connection Type
- Configuration of IKE authentication: Machine Authentication, section 3.2.3.3
- Crypto period: SA Lifetime, section 3.2.3.4.4
- Algorithm Suites: Encryption Algorithm, section 3.2.3.4.1
- Algorithm Suites: Integrity Algorithm, section 3.2.3.4.2
- Load X.509v3 certificates: Configuration of TOE, section 3
- Ability to update the TOE: Updating the TOE, section 3.3.2

Based on these findings the assurance activity is considered satisfied.

4.2.1.1 Verdict

PASS

4.3 FCS_CKM.1(1) TSS 1 (platform)

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the key establishment claimed in that platform's ST contains the key establishment requirement in the VPN Client's ST

4.3.1 Evaluator Findings

The evaluator examined the ST of the platforms to ensure that the key establishment claimed in the platforms ST contains the key establishment requirement in the VPN clients ST. The platform ST, section 6.2 (FCS_CKM.2(1) Cryptographic Key Establishment), and the TOE ST, Table 6 of section 6, were used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the key establishment references in both STs include SP 800-56A and SP 800-56B. These are consistent. In addition to the algorithm validation certificates (CAVP) listed in the platform Security Target, the following CAVP certificates were obtained for SP 800-56A, 1628, 1627, 1626, 1625, 1624, 1623, 1622, 1621.

Based on these findings, this assurance activity is considered satisfied.

4.3.1.1 Verdict

PASS

4.4 FCS_CKM.1(1) TSS 2 (platform)

The evaluator shall also examine the TSS of the VPN Client's ST to verify that it describes (for each supported platform) how the key establishment functionality is invoked.

4.4.1 Evaluator Findings

The evaluator examined the TSS of the VPN client's ST to verify that it describes how the key establishment functionality is invoked. Section 6, table 6, of the client ST was used to determine the verdict of this Assurance Activity.

Upon investigation the evaluator found that the client makes use of the platform by linking against the platform cryptographic library. This makes it possible for the client to invoke the key establishment operations provided by the platform.

Based on these findings, this assurance activity is considered satisfied.

4.2.1.1 Verdict

PASS

4.5 FCS_CKM.1(2) TSS 1 (platform)

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the key generation function claimed in that platform's ST contains the key generation requirement in the VPN Client's ST.

4.5.1 Evaluator Findings

The evaluator examined the ST of both the platform and the client to ensure that the key generation function claimed in the platform ST contains the key generation requirement in the VPN clients. The platform ST, section 6.2 (FCS_CKM.2(1) Cryptographic Key Generation), and the TOE ST, Table 6 of section 6, were used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the key generation references in both STs include FIPS 186-4 RSA and FIPS 186-4 ECDSA. Additionally, for ECDSA both ST reference the P-256 and P-384 curves. These are consistent.

Based on these findings, this assurance activity is considered satisfied.

4.5.1.1 Verdict

PASS

4.6 FCS_CKM.1(2) TSS 2 (platform)

The evaluator shall also examine the TSS of the VPN Client's ST to verify that it describes (for each supported platform) how the key generation functionality is invoked.

4.6.1 Evaluator Findings

The evaluator examined the TSS of the VPN clients ST to verify that it describes how the key generation function functionality is invoked. Table 6 of section 6 of the ST was used to determine the verdict of the Assurance Activity.

Upon investigation, the TSS describes that the TOE leverages the platform signature services for asymmetric cryptography, including, both FIPS 186-4 RSA and FIPS 186-4 ECDSA.

Based on these findings this assurance is considered satisfied.

4.4.1.1 Verdict

PASS

4.7 FCS_CKM.2 TSS 1

The evaluator will check the TSS to ensure that it lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator will confirm that the TSS lists for what purpose it is used, and how it is stored.

4.7.1 Evaluator Findings

The evaluator checked the TSS to ensure that it lists each persistent secret and private key needed to meet the requirements in the ST. Tables 6 and 7 of section 6 of the ST was used to determine the verdict of the Assurance Activity.

Upon investigation the evaluator found that Table 7 in the ST lists each of the keys used by the module and how/where they are stored. Additionally, Table 7 identifies the usage of each of the keys.

Based on these findings, this assurance activity is considered satisfied.

4.5.1.1 Verdict

PASS

4.8 FCS_CKM.2 TSS 2 (platform)

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the persistent secrets and private keys listed as being stored by the platform in the VPN client ST are identified as being protected in that platform's ST.

4.8.1 Evaluator Findings

The evaluator examined the ST of the platform and ensured that the persistent secrets and private keys listed as being stored by the platform in the VPN client ST are identified as being protected in the platforms ST. The platform ST and Tables 6 and 7 of section 6 of the TOE ST were used to determine the verdict of this Assurance Activity.

Upon investigation the evaluator found that the TOE ST identifies that the only keys/secrets stored persistently on the platform are the keys associated with the X.509 certificates used to authenticate the IKE/IPsec session. Upon investigation, the evaluator found that the platform ST identifies that the platforms stores the certificates used for "setting up trusted channels" including IPsec channels (section 8.4.2).

Based on these findings, this assurance activity is considered satisfied.

4.1.6.1 Verdict

PASS

4.9 FCS_CKM_EXT.4 TSS 1

The evaluator shall ensure that all plaintext secret and private cryptographic keys and CSPs (whether manipulated by the TOE or exclusively by the platform) are identified in the VPN Client ST's TSS, and that they are accounted for by the assurance activities in this section.

4.9.1 Evaluator Findings

The evaluator ensured that all plaintext, secret and private cryptographic keys as well as CSP's (whether manipulated by the TOE or exclusively by the platform) are identified in the VPN clients ST TSS and are accounted for in the assurance activities. Tables 6 and 7 of section 6 of the TOE ST were used to determine the verdict of this work unit.

Upon investigation, the evaluator found that Table 7 identifies each of the keys used by the TOE. Additionally, the ST identifies that there are no persistently stored Plaintext keys. Each key that is used by the TOE is overwritten with zeros.

Based on these findings the activity is considered satisfied.

4.7.1.1 Verdict

PASS

4.10 FCS_CKM_EXT.4 TSS 2 (platform)

The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and CSPs used to generate keys that are not otherwise covered by the FCS_CKM_EXT.4 requirement levied on the TOE.

4.10.1 Evaluator Findings

The evaluator checked to ensure the TSS describes each of the secret keys, private keys, and CSPs used to generate key that are not otherwise covered by the FCS_CKM_EXT.4 requirement levied on the TOE. Tables 6 and 7 of section 6 of the TOE ST were used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that Table 7 identifies each of the keys used by the TOE. Additionally, the ST identifies that there are no persistently stored Plaintext keys. Each key that is used by the TOE is overwritten with zeros.

Based on these findings the activity is considered satisfied.

4.10.1.1 Verdict

PASS

4.11 FCS_CKM_EXT.4 TSS 3 (platform)

For each platform listed in the ST, the evaluator shall examine the TSS of the ST of the platform to ensure that each of the secret keys, private keys, and CSPs used to generate key listed above are covered.

4.11.1 Evaluator Findings

The evaluator examined the TSS of the platform ST to ensure that each of the secret keys, private keys and CSPs used to generate key listed above are covered. The platform ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the platform ST states that keys stored in flash memory are zeroized by a block erase. Additionally, the platform ST identifies that the platform stores the X.509 certificates used for IPsec authentication. Therefore, the platform ST covers the zeroization of each of the persistently stored keys used by the TOE.

Based on these findings, the assurance activity is considered satisfied.

4.11.1.1 Verdict

PASS

4.12 FCS_CKM_EXT.4 TSS 4 (TOE)

The evaluator shall check to ensure the TSS describes when each of the plaintext keys are cleared (e.g., system power off, disconnection of an IPsec connection, when no longer needed by the VPN channel per the protocol); and the type of clearing procedure that is performed (cryptographic erase, overwrite with zeros, overwrite three or more times by a different alternating pattern, overwrite with random pattern, or block erase). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the clearing procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are cleared by overwriting once with zeros, while secret keys stored on the internal persistent storage device are cleared by overwriting three times with a random pattern that is changed before each write").

4.12.1 Evaluator Findings

The evaluator checked to ensure the TSS describes when each of the plaintext keys are cleared and the type of clearing procedure that is performed. Tables 6 and 7 of the TOE ST were used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that there are no persistently stored plaintext keys by the TOE. The evaluator found that several keys are stored in RAM (IPsec session related keys). Each of these keys are zeroized by overwriting the value with zeros.

Based on these findings, the assurance activity is considered satisfied.

4.12.1.1 Verdict

PASS

4.13 FCS_COP.1(1) TSS 1 (platform)

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the encryption/decryption function(s) claimed in that platform's ST contains the encryption/decryption function(s) in the VPN Client's ST.

4.13.1 Evaluator Findings

The evaluator examined the platform ST to ensure that the encryption/decryption functions claimed by the platform are also contained in encryption/decryption functions of the VPN clients ST. The platform ST and Table 6 of section 6 of the TOE ST were used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the TOE ST claims that 128-bit and 256-bit AES-CBC and AES-GCM are used to encrypt IPsec traffic. The evaluator also found that the platform ST references support for 128-bit and 256-bit AES-CBC and AES-GCM. These are consistent.

Based on these findings, the assurance activity is considered satisfied.

4.13.1.1 Verdict

PASS

4.14 FCS_COP.1(1) TSS 2 (platform)

The evaluator shall also examine the TSS of the VPN Client's ST to verify that it describes (for each supported platform) how the encryption/decryption functionality is invoked for the indicated modes and key sizes in the VPN Client's ST

4.14.1 Evaluator Findings

The evaluator examined the TSS of the VPN client’s ST to verify that is describes how the encryption/decryption functionality is invoked for the indicated modes and key sizes in the VPN clients ST. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found the cryptographic functionality used for IPsec connections is invoked by the TOE by linking to the platform cryptographic modules. These modules, include, Apple iOS CoreCrypto Kernel Module and Apple iOS CoreCrypto Module. When the TOE needs cryptographic services in support of an IKE/IPsec connection, the TOE calls the platform module API.

Based on these findings, the assurance activity is satisfied.

4.14.1.1 Verdict

PASS

4.15 FCS_COP.1(2) TSS 1 (platform)

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the digital signature functions claimed in that platform's ST contains the digital signature functions in the VPN Client's ST

4.15.1 Evaluator Findings

The evaluator examined the platform ST to ensure that the digital signature functions claimed in the platforms ST contain the digital signature functions in the VPN clients ST. The platform ST and Table 6 of section 6 of the TOE ST were used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the TOE ST claims that 2048-bit FIPS 186-4 RSA and FIPS 186-4 ECDSA using P-256 and P-384 curves are used by the TOE to provide signature services for IKE/IPsec connections. The evaluator also found that the platform ST references support for 2048 bit FIPS 186-4 RSA and FIPS 186-4 ECDSA using P-256 and P-384 curves. These are consistent.

Based on these findings, the assurance activity is considered satisfied.

4.15.1.1 Verdict

PASS

4.16 FCS_COP.1(2) TSS 2 (platform)

The evaluator shall also examine the TSS of the VPN Client's ST to verify that it describes (for each supported platform) how the digital signature functionality is invoked for each operation they are used for in the VPN client

4.16.1 Evaluator Findings

The evaluator examined the TSS of the VPN client's ST to verify that is describes how the digital signature functionality is invoked for the each operation they are used for in the VPN client. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found the cryptographic functionality used for IPsec connections is invoked by the TOE by linking to the platform cryptographic modules. These modules, include, Apple iOS CoreCrypto Kernel Module and Apple iOS CoreCrypto Module. When the TOE needs cryptographic services in support of an IKE/IPsec connection, the TOE calls the platform module API.

Based on these findings, the assurance activity is satisfied.

4.16.1.1 Verdict

PASS

4.17 FCS_COP.1(3) TSS 1

The evaluator shall check that the association of the hash function with other cryptographic functions (for example, the digital signature verification function) specified in the VPN Client ST (whether these are performed by the platform or by the TOE) is documented in the TSS.

4.17.1 Evaluator Findings

The evaluator checked that the association of the hash function with other cryptographic functions specified in the VPN client ST is documented. Table 6 of section 6 was used to determine the verdict of this work unit.

Upon investigation, the evaluator found that the TOE uses the supported hashes in two ways, as follows,

- In support of digital signatures for IKE/IPsec authentication
- In support of HMACs used to verify the integrity of IKE/IPsec traffic

Based on these findings the assurance activity is considered satisfied.

4.17.1.1 Verdict

PASS

4.18 FCS_COP.1(3) TSS 2 (platform)

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the hash function(s) claimed in that platform's ST contains the hash function(s) in the VPN Client's ST.

4.18.1 Evaluator Findings

The evaluator examined the ST of the platform to ensure that the hash function(s) claimed in the platform ST are also contained in the VPN Client ST hash functions. The platform ST and Table 6 of section 6 of the TOE ST were used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the TOE ST claims that SHA-1, SHA-256, SHA-384, and SHA-512 are supported to provide hashing services for IKE/IPsec connections. The evaluator also found that the platform ST references support for SHA-1, SHA-256, SHA-384, and SHA-512. These are consistent.

Based on these findings the assurance activity is considered satisfied.

4.18.1.1 Verdict

PASS

4.19 FCS_COP.1(3) TSS 3 (platform)

The evaluator shall also examine the TSS of the VPN Client's ST to verify that it describes (for each supported platform) how the hash functionality is invoked for each digest size selected in the VPN Client's ST.

4.19.1 Evaluator Findings

The evaluator examined the TSS of the VPN clients ST to verify that it describes how the hash functionality is invoked for each digest size that is selected in the VPN clients ST. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found the cryptographic functionality used for IPsec connections is invoked by the TOE by linking to the platform cryptographic modules. These modules, include, Apple iOS CoreCrypto Kernel Module and Apple iOS CoreCrypto Module. When the TOE needs cryptographic services in support of an IKE/IPsec connection, the TOE calls the platform module API.

Based on these findings, the assurance activity is considered satisfied.

4.19.1.1 Verdict

PASS

4.20 FCS_IPSEC_EXT.1.1 Guidance 1

The evaluator shall examine the operational guidance to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for DISCARD, BYPASS and PROTECT.

4.20.1 Evaluator Findings

The evaluator examined the operational guidance to verify that it instructs the administrator how to construct entries into the SPD in order to specify a rule for DISCARD, BYPASS and PROTECT. The AGD was used to determine the verdict of this Assurance Activity.

Upon investigation the evaluator found the operational guidance contained instructions on how to construct entries in the SPD in order to specify rules. This information can be found in section 3.2.3.6.

Based on these findings the assurance activity is considered satisfied.

4.20.1.1 Verdict

PASS

4.21 FCS_IPSEC_EXT.1.2 TSS 1

The evaluator checks the TSS to ensure it states that the VPN can be established to operate in tunnel mode and/or transport mode (as selected).

4.21.1 Evaluator Findings

The evaluator checked the TSS to ensure it states that the VPN can be established to operate in tunnel mode and/or transport mode. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that in the evaluated configuration TOE supports tunnel mode exclusively. This is consistent with the FCS_IPSEC_EXT.1.* SFRs.

Based on these findings the assurance activity is considered satisfied.

4.21.1.1 Verdict

PASS

4.22 FCS_IPSEC_EXT.1.2 Guidance 1

The evaluator shall confirm that the operational guidance contains instructions on how to configure the connection in each mode selected.

4.22.1 Evaluator Findings

The evaluator shall confirm that the operational guidance contains instructions on how to configure the connection mode. The AGD was used to determine the verdict of this Assurance Activity.

Upon investigation the evaluator found that the TOE only supports IPSEC tunnel mode. The instructions are present on how to configure the connection. The information can be found in 3.2.3 of the guidance document.

Based on these findings the assurance activity is considered satisfied.

4.22.1.1 Verdict

PASS

4.23 FCS_IPSEC_EXT.1.3 TSS 1

The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is processed against the SPD and that if no “rules” are found to match, that a final rule exists, either implicitly or explicitly, that causes the network packet to be discarded.

4.23.1 Evaluator Findings

The evaluator examined the TOE Security Target to verify that the TSS provides a description of how a packet is processed against the SPD and that if no “rules” are found, that a final rule exists either implicitly or explicitly that causes the network packet to be discarded. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that all data is sent through an encrypted tunnel unless an explicit exception is configured. Any other plaintext data that is received is ignored.

Based on these findings the assurance activity is considered satisfied.

4.23.1.1 Verdict

PASS

4.24 FCS_IPSEC_EXT.1.3 Guidance 1

The evaluator checks that the operational guidance provides instructions on how to construct the SPD.

4.24.1 Evaluator Findings

The evaluator checked that the operational guidance provides instructions on how to construct the SPD. The AGD was used to determine the verdict of this Assurance Activity.

Upon investigation the evaluator found that section 3.2.3.6 of the AGD describes service exceptions (configuring the SPD).

Based on these findings the assurance activity is considered satisfied.

4.24.1.1 Verdict

PASS

4.25 FCS_IPSEC_EXT.1.4 TSS 1

The evaluator shall examine the TSS to verify that the algorithms AES-GCM-128 and AES-GCM-256 are implemented. If the ST author has selected either AES-CBC-128 or AES-CBC-256 in the requirement, then the evaluator verifies the TSS describes these as well. In addition, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(4) Cryptographic Operations (for keyed-hash message authentication).

4.25.1 Evaluator Findings

The evaluator examined the TSS to verify that AES-GCM-128, AES-GCM-256, AES-CBC-128 and AES-CBC-256 are implemented and described in the TOE ST. This is consistent with FCS_COP.1(1). Table 6 of section 6 was used to determine the verdict of this work unit.

Additionally, the evaluator verified that Table 6 of section 6 identifies the SHA-based HMAC used in the IKE/IPsec connections. These SHA-based HMAC algorithms are consistent with the algorithms specified in FCS_COP.1(4).

Based on these findings the assurance activity is considered satisfied.

4.25.1.1 Verdict

PASS

4.26 FCS_IPSEC_EXT.1.4 Guidance

The evaluator checks the operational guidance to ensure it provides instructions on how to configure the TOE/platform to use the AES-GCM-128, and AES-GCM-256 algorithms, and if either AES-CBC-128 or AES-CBC-256 have been selected the guidance instructs how to use these as well.

4.26.1 Evaluator Findings

The evaluator inspected the operational guidance to ensure it provides instruction on how to configure the TOE/platform to use AES-CBC-256, AES-CBC-128, AES-GCM-256 and AES-GCM-128.

Upon investigation, the evaluator found that section 3.2.3.4.1 of the AGD provides instructions for configuration of the algorithms. These algorithms include,

- AES-CBC-128
- AES-CBC-256
- AES-GCM-128
- AES-GCM-256

Based on these findings the assurance activity is considered satisfied.

4.26.1.1 Verdict

PASS

4.27 FCS_IPSEC_EXT.1.5 TSS 1

The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.

4.27.1 Evaluator Findings

The evaluator examined the TSS to verify that IKEv1 and/or IKEv2 are implemented. Table 6 of section 6 was used to determine the verdict of this work unit.

Upon investigation the evaluator found that TSS implements IKEv2 (as defined in RFCs 5996 and 4307) is implemented.

Based on these findings the assurance activity is considered satisfied.

4.27.1.1 Verdict

PASS

4.28 FCS_IPSEC_EXT.1.5 Guidance 1

The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE/platform to use IKEv1 and/or IKEv2 (as selected).

4.28.1 Evaluator Findings

The evaluator checked the operational guidance to ensure that it instructs the administrator how to configure the TOE/platform to use IKEv2. The AGD was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that guidance document instructs on how to configure the TOE to use IKEv2. The information can be found in section 3.2.3.1.

Based on these findings the assurance activity is considered satisfied.

4.28.1.1 Verdict

PASS

4.29 FCS_IPSEC_EXT.1.6 TSS 1

The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.

4.29.1 Evaluator Findings

The evaluator ensured that the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified and if others are chosen in the selection of the requirement, those are included in the TSS. Table 6 of section 6 was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AES-GCM-128, AES-GCM-256, AES-CBC-128, and AES-CBC-256 are all specified. This is consistent with the algorithms specified in the SFR.

Based on these findings the assurance activity is considered satisfied.

4.29.1.1 Verdict

PASS

4.30 FCS_IPSEC_EXT.1.6 Guidance 1

The evaluator ensures that the operational guidance describes the configuration of the mandated algorithms, as well as any additional algorithms selected in the requirement.

4.30.1 Evaluator Findings

The evaluator ensured that the operational guidance describes the configuration of the mandated and additional algorithms. The AGD was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that in section 3.2.3.4.1 all algorithms and the necessary configuration instructions are present.

Based on these findings the assurance activity is considered satisfied.

4.30.1.1 Verdict

PASS

4.31 FCS_IPSEC_EXT.1.8 Guidance 1

The evaluator verifies that the values for SA lifetimes can be configured and that the instructions for doing so are located in the operational guidance. If time-based limits are supported, the evaluator ensures that either the Administrator or VPN Gateway are able to configurable Phase 1 SAs values for 24 hours and 8 hours for Phase 2 SAs.

4.31.1 Evaluator Findings

The evaluator verified that the values for the SA lifetimes can be configured and that the instructions are located in the operational guidance. The AGD was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found the necessary configuration instructions in guidance documentation in section 3.2.3.4.4 and 3.2.3.5.

Based on these findings the assurance activity is considered satisfied.

4.31.1.1 Verdict

PASS

4.32 FCS_IPSEC_EXT.1.9/10 TSS 1

The evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating "x" (as defined in FCS_IPSEC_EXT.1.9) and each nonce.

4.32.1 Evaluator Findings

The evaluator checked to ensure that for each DH group supported, the TSS describes the process for generating “x” and each nonce. Table 7 of section 6 was used to determine the verdict of this work unit.

Upon investigation, the evaluator found that the TOE generates the secret value ‘x’ and nonces used in the IKEv2 Diffie-Hellman key exchanges using the TOE platform FIPS validated DRBG specified (as specified in FCS_RBG_EXT.1).

Based on these findings the assurance activity is considered satisfied.

4.32.1.1 Verdict

PASS

4.33 FCS_IPSEC_EXT.1.9/10 TSS 2

The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of "x" and the nonces meet the stipulations in the requirement.

4.33.1 Evaluator Findings

The evaluator verified that the TSS indicates the random number generated meets the requirements in this PP is used and the length of “x” and the nonces meet the stipulations in the requirements. Table 6 of section 6 was used to determine the verdict of this work unit.

Upon investigation, the evaluator found that the TOE generates the secret value ‘x’ and nonces used in the IKEv2 Diffie-Hellman key exchanges using the TOE platform DRBG specified (as specified in FCS_RBG_EXT.1). Additionally, the possible lengths of ‘x’ and the nonces are 224, 256, or 384 bits.

Based on these findings the assurance activity is considered satisfied.

4.33.1.1 Verdict

PASS

4.34 FCS_IPSEC_EXT.1.11 TSS 1

The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.

4.34.1 Evaluator Findings

The evaluator checked to ensure that the DH groups specified in the requirement are listed as being supports in the TSS. Table 7 of section 6 was used to determine the verdict of this work unit.

Upon investigation the evaluator found that the following DH groups are supported.

- 1(768-bit MODP)
- 2(1024-bit MODP)
- 5(1536-bit MODP)
- 14(2048-bit MODP)
- 15(3072-bit MODP)
- 16(4096-bit MODP)
- 17(6144-bit MODP)
- 18(8192-bit MODP)
- 19(256-bit Random ECP)
- 20 (384-bit Random ECP)

Additionally, the TOE will only negotiate Diffie-Hellman groups based on the configuration applied by the administrator. Groups not included in the configuration profile are not be used.

Based on these findings the assurance activity is considered satisfied.

4.34.1.1 Verdict

PASS

4.35 FCS_IPSEC_EXT.1.12 TSS 1

The evaluator ensures that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication. The description must be consistent with the algorithms as specified in FCS_COP.1(2) Cryptographic Operations (for cryptographic signature).

4.35.1 Evaluator Findings

The evaluator ensured that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication. The evaluator also ensured that the description is consistent with FCS_COP.1(2). Table 6 of section 6 was used to determine the verdict of this work unit.

Upon investigation, the evaluator found that the TSS identifies the authentication mechanisms used by the TOE, RSA and ECDSA. Additionally, the evaluator compared this to FCS_COP.1(2) and found that the algorithms described in the TSS were consistent with those in the specified in the SFR.

Based on these findings the assurance activity is considered satisfied.

4.35.1.1 Verdict

PASS

4.36 FCS_IPSEC_EXT.1.12 Guidance 1

The evaluator ensures the operational guidance describes how to set up the TOE/platform to use the cryptographic algorithms RSA and/or ECDSA.

4.36.1 Evaluator Findings

The evaluator ensured that the operational guidance describes how to set up the TOE/platform to use the cryptographic algorithms RSA and/or ECDSA. The AGD was used to determine the verdict of this work unit.

Upon investigation the evaluator found that configuration of the signature algorithms/ certificates used are described in sections 3.2.3.3 and 3.1.1.

Based on these findings the assurance activity is considered satisfied.

4.36.1.1 Verdict

PASS

4.37 FCS_IPSEC_EXT.1.12 Guidance 2

The evaluator will ensure that the operational guidance describes how to configure the TOE/platform to connect to a trusted CA, and ensure a valid certificate for that CA is loaded into the TOE/platform and marked “trusted”.

4.37.1 Evaluator Findings

The evaluator ensured the operational guidance describes how to configure the TOE/platform to connect to a trusted CA. The AGD was used to determine the verdict of this work unit.

Upon investigation, the evaluator found that the AGD provides, in Section 3.2.2 “Add Certificate Payloads,” the following instructions for configuring the TOE to connect to a trusted CA, “If the TOE will be authenticating to the VPN with the use of X.509v3 client certificates, then the device certificate, as well as the enterprise CA certificate used to sign both the device certificate as well as the VPN gateway certificate will need to be added and trusted”

Based on these findings the assurance activity is considered satisfied.

4.37.1.1 Verdict

PASS

4.38 FCS_IPSEC_EXT.1.14 TSS 1

The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the

checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA this is protecting the negotiation.

4.38.1 Evaluator Findings

The evaluator checked that the TSS describes the potential strengths of the algorithms that are allowed for the IKE and ESP exchanges. Also, the evaluator verified the TSS describes the checks that are done when negotiating. Table 6 of section 6 was used to determine the verdict of this work unit.

Upon investigation, the evaluator found the description of the strengths, the exchanges and the description of the checks performed when negotiating and as configured. Additionally, the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the IKEv2/IKE_SA connection and the strength of the symmetric algorithm negotiated to protect the IKEv2 CHILD_SA connection is configured using .xml configuration files. The administrator must explicitly choose the cryptographic algorithms (including key strength) used for each SA.

Based on these findings the assurance activity is considered satisfied.

4.38.1.1 Verdict

PASS

4.39 FCS_RBG_EXT.1 TSS 1 (platform)

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the RBG functions claimed in that platform's ST contains the RBG functions in the VPN Client's ST.

4.39.1 Evaluator Findings

The evaluator examined the platform ST to ensure that the RBG functions claimed by the platform are also contained in encryption/decryption functions of the VPN clients ST. The platform ST and Table 6 of section 6 of the TOE ST were used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the TOE ST claims that a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90 are used to encrypt IPsec traffic. The evaluator also found that the platform ST references support for a 128-bit and 256-bit NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90. These are consistent.

Based on these findings, the assurance activity is considered satisfied.

4.39.1.1 Verdict

PASS

4.40 FCS_RBG_EXT.1 TSS 2 (platform)

The evaluator shall also examine the TSS of the VPN Client's ST to verify that it describes (for each supported platform) how the RBG functionality is invoked for each operation they are used for in the VPN client's ST.

4.40.1 Evaluator Findings

The evaluator examined the TSS of the VPN client’s ST to verify that is describes how the RBG functionality is invoked for each operation in the VPN clients ST. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found the random number generation functionality used for IPsec connections is invoked by the TOE by linking to the platform cryptographic modules. These modules, include, Apple iOS

CoreCrypto Kernel Module and Apple iOS CoreCrypto Module. When the TOE needs random numbers in support of an IKE/IPsec connection, the TOE calls the platform module API.

Based on these findings, the assurance activity is satisfied.

4.40.1.1 Verdict

PASS

4.41 FDP_RIP.2 TSS 1

The evaluator shall check to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. The evaluator shall ensure that this description at a minimum describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs.

4.41.1 Evaluator Findings

The evaluator checked to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. The evaluator also ensured that this description, at a minimum, describes how the previous data are zeroized/overwritten and what point in the buffer processing this occurs. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation the evaluator found that the TSS contains a description of packet processing, how the data is overwritten/zeroized and when it occurs. When the TOE allocates a new packet buffer, the new packet data is used to overwrite any previous data in the buffer. If the totality of the new packet data is less than the allocated buffer, the additional allocated space will be filled with zeros prior to sending the packet to its destination.

Based on these findings the assurance activity is considered satisfied.

4.41.1.1 Verdict

PASS

4.42 FIA_X509_EXT.1 TSS 1

The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place – the TOE or the TOE platform

4.42.1 Evaluator Findings

The evaluator ensured that the TSS describes where the check of validity of certificates takes place. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the check of validity of certificates takes place on the platform.

Based on these findings the assurance activity is considered satisfied.

4.42.1.1 Verdict

PASS

4.43 FIA_X509_EXT.1 TSS 2

The evaluator ensures the TSS also provides a description of the certificate path validation algorithm, ensuring that it describes how the validation chain will terminate in a trusted root certificate.

4.43.1 Evaluator Findings

The evaluator ensured that the TSS provides a description of the certificate path validation algorithm and how the validation chain will terminate in a trusted root certificate. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that X.509 certificates are validated using the certificate path validation algorithm defined in RFC 5280, as well as a summary of the stops involved:

- the public key algorithm and parameters are checked
- the current date/time is checked against the validity period
- revocation status is checked
- issuer name of X matches the subject name of X+1
- name constraints are checked
- policy OIDs are checked
- policy constraints are checked; issuers are ensured to have CA signing bits
- path length is checked
- critical extensions are processed

Based on these findings the assurance activity is considered satisfied.

4.43.1.1 Verdict

PASS

4.44 FIA_X509_EXT.1 Guidance 1

The evaluator ensures the guidance documentation provides the user with the necessary information to setup the validation check whether it is done by the TOE or TOE platform. The guidance documentation provides instructions how to select the method used for checking, as well as how to setup a protected communication path with the entity providing the information pertaining to certificate validity.

4.44.1 Evaluator Findings

The evaluator checked to ensure that the guidance documentation provides the user with the necessary information to setup the validation check, instructions on how to select the method used for checking and how to setup a protected communication path. The AGD document was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that section 3 of the AGD, “Configuration of the TOE,” contains a description of how to configure a profile. These profiles include all of the configuration options available for the TOE. There are no configuration activities required to setup the validation checks.

Based on these findings the assurance activity is considered satisfied.

4.44.1.1 Verdict

PASS

4.45 FIA_X509_EXT.2 TSS 1

The evaluator shall check the TSS to ensure that it describes how the TOE/platform chooses which certificates to use.

4.45.1 Evaluator Findings

The evaluator checked that the TOE ST describes how the TOE/platform chooses which certificates to use. Table 7 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the TOE supports X.509 certificates for the following services, IPsec VPN connections, code signing for software updates, and software integrity checks. The method used for the selection of each of these certificates is described in the ST.

Based on these findings the assurance activity is considered satisfied.

4.45.1.1 Verdict

PASS

4.46 FIA_X509_EXT.2 Guidance 1

The evaluator shall ensure that instructions in the administrative guidance for configuring the operating environment so that the TOE/platform can use the certificates. If this functionality is implemented entirely by the platform, the operational guidance for the TOE shall reference the applicable guidance for each platform.

4.46.1 Evaluator Findings

The evaluator ensured that the instructions in the administrative guidance document provides configuration information for the operating environment so that the TOE/platform can use the certificates. The AGD document was used to determine the verdict of this work unit.

Upon investigation, the evaluator found that section 3.2.3.3 of the AGD document describes the process of configuration authentication using digital certificates. Additionally, section 3.3.2 of the AGD describes that TOE updates are handled automatically and use digital certificates.

Based on these findings the assurance activity is considered satisfied.

4.46.1.1 Verdict

PASS

4.47 FPT_TST_EXT.1 TSS 1

The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used).

4.47.1 Evaluator Findings

The evaluator examined the TSS to ensure that it details the self-tests that are run by the TSF on startup. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the following tests are run:

- An integrity test.
- Known Answer Tests (KATs) on each implemented cryptographic algorithm.

Each of the tests listed in the TSS are described in terms of what the test is actually doing. Each of the tests listed in the TSS are described in terms of what the test is actually doing. For example, the AES KAT description includes the following text explaining the actual operations being performed, “These test take a known plaintext value and encrypts it using a known key. The test is also performed in reverse using a known encrypted value and a known key." A similar description is provided for each test.

Based on these findings the assurance activity is considered satisfied.

4.47.1.1 Verdict

PASS

4.48 FPT_TST_EXT.1 TSS 2

The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. If some of the tests are performed by the TOE platform, the evaluator shall check the TSS to ensure that those tests are identified, and that the ST for each platform contains a description of those tests.

4.48.1 Evaluator Findings

The evaluator ensured that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the TOE ST states "The implemented self-tests verify both that the software itself hasn't been tampered with and corrupted (ensuring that the functions operate as expected) and that the cryptography (which is vital to the operation of a VPN client) is operating correctly. Both of these tests ensure the product is operating correctly."

This argument describes why the implemented test sufficiently ensure the TSF is operating correctly.

Based on these findings the assurance activity is considered satisfied.

4.48.1.1 Verdict

PASS

4.49 FPT_TST_EXT.1 TSS 3

The evaluator shall examine the TSS to ensure that it describes how the integrity of stored TSF executable code is cryptographically verified when it is loaded for execution. The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the integrity of stored TSF executable code has not been compromised. The evaluator shall check to ensure that the cryptographic requirements listed are consistent with the description of the integrity verification process.

4.49.1 Evaluator Findings

The evaluator examined the TSS to ensure it describes how the integrity of the stored TSF executable code is cryptographically verified when loaded for execution. The evaluator also ensured that the TSS makes an argument that the tests are sufficient to demonstrate the integrity of the stored TSF executable code has not been compromised. Finally, the evaluator ensured the cryptographic requirements listed are consistent with the description of the integrity verification process. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the ST states that the software integrity test verifies the integrity of the stored software via a 2048-bit RSA digital signature. The ST argues that if the test verifies that the software hasn't been tampered with or corrupted ensuring correct operations. Finally, the test uses 2048-bit RSA digital signatures. These ciphers are consistent with the ciphers included in the FCS_*** requirements.

Based on these findings, the assurance activity is considered satisfied.

4.49.1.1 Verdict

PASS

4.50 FPT_TST_EXT.1 TSS 4 (or Guidance)

The evaluator also ensures that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases. For checks implemented entirely by the platform, the evaluator ensures that the operational guidance for the TOE references or includes the platform-specific guidance for each platform listed in the ST.

4.50.1 Evaluator Findings

The evaluator ensured that the TSS (or operational guidance) described the actions that take place for successful and unsuccessful cases. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that the TOE ST describes what happens for successful completion of the integrity test and for unsuccessful completion of the integrity tests, as follows.

- Successful: The TOE moves to an operational state.
- Unsuccessful: the TOE platform kernel will panic, rendering the device inoperable.

Based on these findings the assurance activity is considered satisfied.

4.50.1.1 Verdict

PASS

4.51 FPT_TUD_EXT.1 TSS 1

Updates to the TOE are signed by an authorized source and may also have a hash associated with them, or are signed by an authorized source. If digital signatures are used, the definition of an authorized source is contained in the TSS, along with a description of how the certificates used by the update verification mechanism are contained on the device. The evaluator ensures this information is contained in the TSS.

4.51.1 Evaluator Findings

The evaluator ensured that a description of how updates are verified and a description of the mechanisms used for verification. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation the evaluator found that TOE ST contains a description. It states;
"The TOE platform cryptographically verifies the integrity of all software updates it receives prior to execution. The TOE platform verifies the software update using a PKCS#1 (using SHA-256) signature of the software executable code to ensure that it has not been modified or corrupted. If the integrity test on the software update fails, the TOE will not load the software update."

Additionally, the evaluator found that only updates signed by Apple, Inc. may be installed. The certificates used to verify any downloaded software is stored encrypted in the platform protected key chain.

Based on these findings the assurance activity is considered satisfied.

4.51.1.1 Verdict

PASS

4.52 FPT_TUD_EXT.1 TSS 2 (or Guidance)

The evaluator also ensures that the TSS (or the operational guidance) describes how the candidate updates are obtained; the processing associated with verifying the digital signature or calculating the hash of the updates; and the actions that take place for successful (hash or signature was verified) and unsuccessful (hash or signature could not be verified) cases. If these activities are performed entirely by the underlying platform, a reference to the ST of

each platform indicating that the required functionality is included for each platform shall be verified by the evaluator.

4.52.1 Evaluator Findings

The evaluator ensured that the TSS (or operational guidance) described how updates are obtained, the processing associated with verifying the digital signature or calculating the hash of the updates: and the actions that place for unsuccessful and successful cases. Table 6 of section 6 of the ST and the AGD were used to determine the verdict of this Assurance Activity.

Upon investigation the evaluator found that the section 3.3.2 of AGD states; “Updating the TOE is done by updating the iOS software on the TOE Platform itself, as the TOE is the native client built into the Apple iOS software. Verification of update packages are conducted by the TOE platform, using digital signatures to verify authenticity and integrity.”

Based on these findings the assurance activity is considered satisfied.

4.52.1.1 Verdict

PASS

4.53 FTP_ITC.1 TSS 1

The evaluator shall examine the TSS to determine that it describes the details of the TOE connecting to a VPN Gateway in terms of the cryptographic protocols specified in the requirement, along with TOE-specific options or procedures that might not be reflected in the specification.

4.53.1 Evaluator Findings

The evaluator examined the TSS to determine that it describes the details to connecting to a VPN gateway in terms of the cryptographic protocols specified in the requirement, along with TOE-specific options or procedures that might not be reflected in the specification. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation the evaluator found that the ST described the details of the TOE connecting to a VPN Gateway. This connection is protected via an IKE/IPsec connection (as described in the FCS_IPSEC_EXT.1.* requirements).

Based on these findings the assurance activity is considered satisfied.

4.53.1.1 Verdict

PASS

4.54 FTP_ITC.1 TSS 2

The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

4.54.1 Evaluator Findings

The evaluator shall confirmed that all protocols listed in the TSS are specified and included in the requirements in the ST. Table 6 of section 6 of the ST was used to determine the verdict of this Assurance Activity.

Upon investigation, the evaluator found that connections with the CA are protected via IPsec (as described in the FCS_IPSEC_EXT.1.* requirements). This is consistent with the requirements specified in the ST.

Based on these findings the assurance activity is considered satisfied.

4.54.1.1 Verdict

PASS

4.55 FTP_ITC.1 Guidance 1

The evaluator shall confirm that the operational guidance contains instructions for establishing the connection to the access point, and that it contains recovery instructions should a connection be unintentionally broken

4.55.1 Evaluator Findings

The evaluator confirmed that the operational guidance contains instructions for establishing the connection to the access point and it contains recovery instructions should a connection be unintentionally broken. The AGD was used to determine the verdict of this work unit.

Upon investigation, the evaluator found that Section 3.2 of the AGD describes all of the configuration options for configuring a VPN tunnel. Section 3.3 of the AGD describes the usage of these features including that the "configurations can be used to connect to any gateway IKE/IPsec device [including] any CA used to verify certificate validity."

Based on these findings, the assurance activity is considered satisfied.

4.55.1.1 Verdict

PASS

5 Test Infrastructure

For this evaluation, the iOS VPN Client was tested at the Apple, Inc. facilities in Cupertino, CA. Testing was conducted in concert with Apple engineering staff due to the special requirements necessary for accessing the back-end of the TOE platform.

5.1 Test Tools

The following tools are used in support of TOE testing.

- Wireshark version 2.4.6
- StrongSwan version 5.3.3
- Windows Server 2008R2
- Variable Attenuator JFW PA2015
- R&S CMW500 LTE CallBox
- Apple Configurator version 2.6

5.2 Physical Component Overview – TESTBED #1

The TOE was placed in a JRE 2025 STA Box with ST fiber and SMA bulkheads and a USB 2.0 filter in order to shield the test environment from outside RF interference, as well as to facilitate the use of the LTE callbox within FCC regulations.

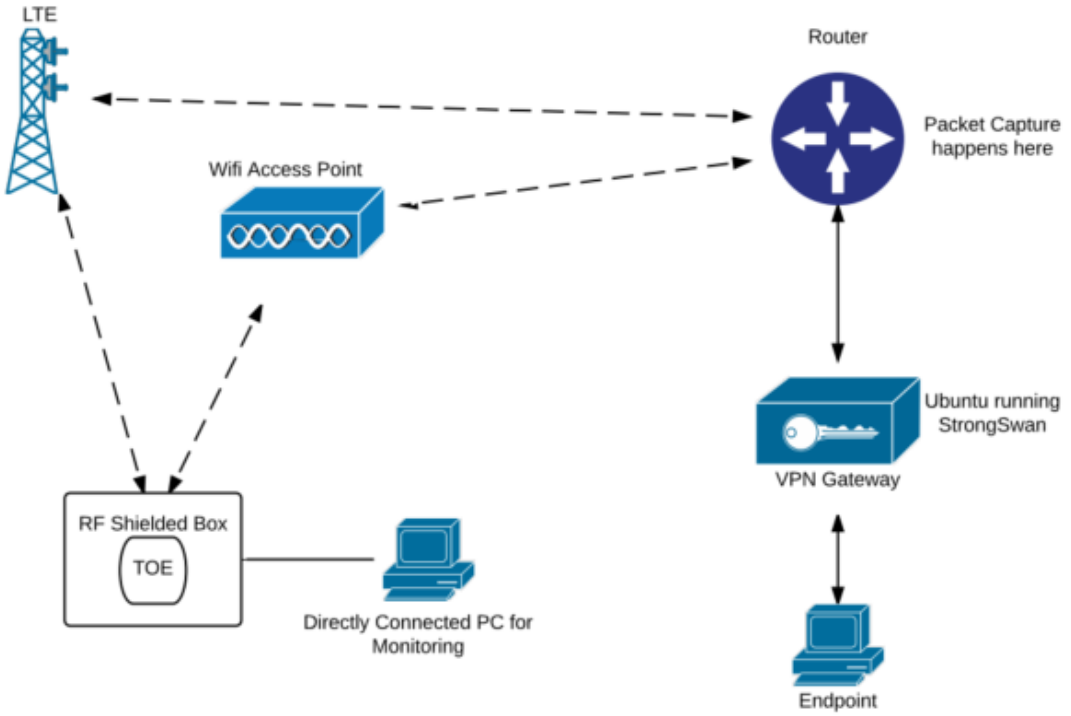
Wireless antennas for both the WiFi and LTE networks were placed inside the JRE 2025 as well. The TOE platforms was connected via the USB filter to an iMac serving as the controller for automated testing.

The TOE Platform was configured to use either WiFi or LTE depending on the test run. When WiFi was running, the LTE antennas in the test bed were disabled and the device had its cellular antennas turned off as well. When LTE tests were running, device Wifi was turned off and the signal on the WAP was put out of range.

Both the LTE call box and the Wifi AP/WLC were connected to a Cisco Nexus switch stack, which was then connected via a 10Gigabit Ethernet connection containing an 802.1Q port channel carrying the VLANs to a Penguin Computing server running VMWware ESXi where the rest of the test bed lived as virtual machines connected via VNIC to a VSwitch.

5.3 Testbed Diagram – TESTBED #1

The following diagram provides a high-level logical description of the test bed used for testing.



5.4 Testbed Component Overview – TESTBED #1

The following identifies the network addresses and other relevant information for the testbed components, including software versions and any special supporting software installed to facilitate testing:

- **WiFi**
  - TOE
    - CPU model: A7, A8, A8X, A9, A9X, A10, A10X, A11
    - iOS version: 11
  - Antenna
    - Model: JFW PA2015
  - AP
    - JRE AP with Cisco 2602 AP
    - 5Ghz –Ch149 HT –Power1
  - Wireless Lan Controller
    - Model: Cisco WLC 5508
    - Software Version: 8.0.120.0
- **LTE**
  - TOE
    - CPU model: A7, A8, A8X, A9, A9X, A10, A10X, A11
    - iOS Version: 11
  - Callbox
    - Model: R&S CMW500 LTE
    - Band: 17
- **Common Elements:**
  - Switch
    - Model: Cisco Nexus 3k stack
    - Software version: 6.0(2)U6(4)
    - Performs L2 switching only

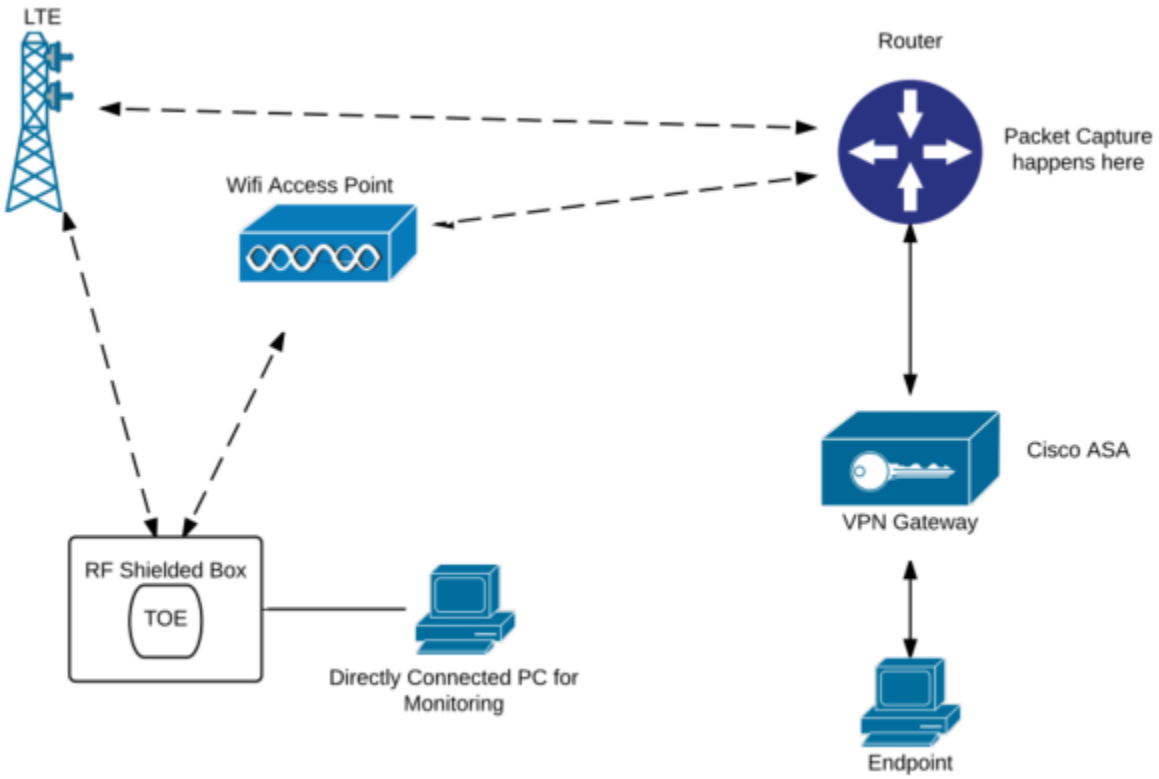
- VM Server
  - Model: Penguin Computing Relion 1800i
  - Software: ESXi
    - VMkernel petfish-eric 6.0.0 #1 SMP Release build-3073146 x86_64 ESXi
- Linux "Router"
  - Software version: Ubuntu 14.04 Server (kernel 3.13.0-55)
  - Special software installed: Hexinject 1.5
  - Roles: DNS, DHCP, packet sniffer
- StrongSwan VPN gateway
  - Software version: Ubuntu 14.04 Server (kernel 3.13.0-55)
  - Special software installed: StrongSwan 5.3.3
  - Role: VPN gateway
- Web server (host on the right side of the VPN)
  - Software version: Ubuntu 14.04 Server (kernel 3.13.0-55)
  - Special installed software: Apache from packages
  - Role: servers a binary file requested by the TOE through the VPN in order to generate sufficient packets to gather evidence

5.5 Physical Component Overview – TESTBED #2

This test bed is essentially the same as Testbed #1 in so far as how it is set up, with the exception of the introduction of the Cisco 2951 router, which serves as the NAT point for FCS_IPSEC_EXT1.5 Test #1.

5.6 Testbed Diagram – TESTBED #2

The following diagram provides a high-level logical description of the test bed used for testing.



5.7 Testbed Component Overview – TESTBED #2

- **WiFI**
  - TOE
    - CPU model: A7, A8, A8X, A9, A9X, A10, A10X, A11
    - iOS version: 11
- **LTE**
  - TOE
    - CPU model: A7, A8, A8X, A9, A9X, A10, A10X, A11
    - iOS version: 11

5.8 Testbed Component Overview – Testbed #2

The only new component in this test bed is the NAT router:

- NAT Router:
  - Model: Cisco 2951
  - Software version: 15.4.(3)M2

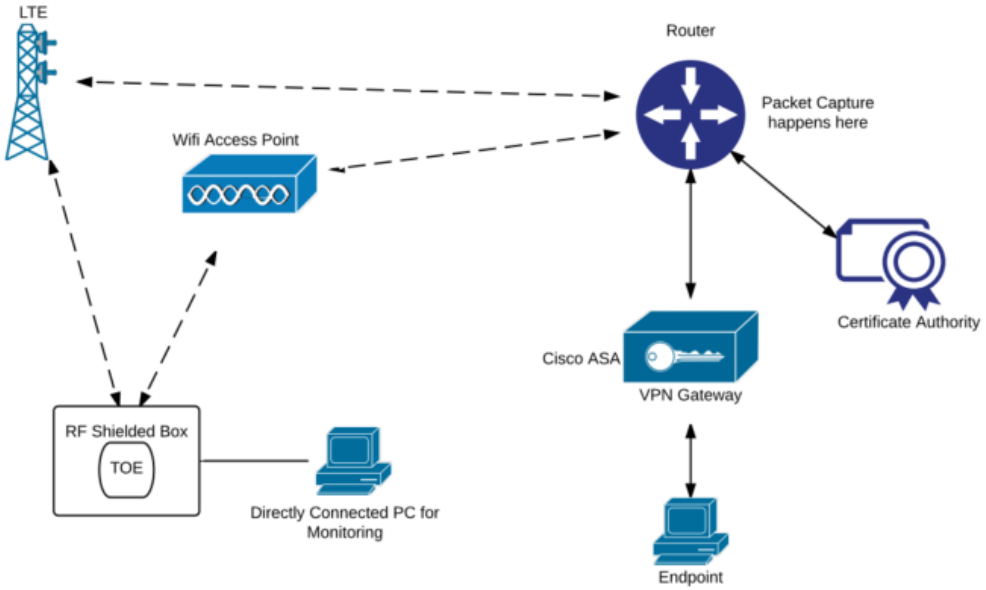
5.9 Physical Component Overview – TESTBED #3

This testbed is, again, largely similar to Testbed #1. However, the Strongswan server has been swapped out for a Cisco ASAv. Additionally, a number of Windows VMs have been added in order to facilitate the roles of Certificate Authority (CA) and OCSP responder, with a single Windows VM serving both roles for each of the four supported certificate types and key/curve lengths.

The Windows servers live on a separate server and subnet which is reachable by the TOE and is also connected to the Cisco Nexus switch stack.

5.10 Testbed Diagram – TESTBED #3

The following diagram provides a high-level logical description of the test bed used for testing.



5.11 Testbed Component Overview – TESTBED #3

All components of the testbed are the same as TESTBED #1, with the exception of the following, which are common to both the WiFi and LTE test environments:

VPN Gateway

- Model: Cisco ASAv

- Software version: 9-4-1-2000

RSA 2048-bit CA/OCSP responder

- Software version: Windows 2008R2

ECDSA-256 CA/OCSP responder

- Software version: Windows 2008R2

ECDSA-384 CA/OCSP responder

- Software version: Windows 2008R2

5.12 Testbed Component Overview – TESTBED #4

The IKEv2 and ESP re-key tests were conducted over the open internet, leveraging the Apple corporate Wi-Fi and the infrastructure set up for their VPN test pilot program. Due to the sensitivity, this test bed is not described in detail, but a high-level overview is provided

VPN Gateway

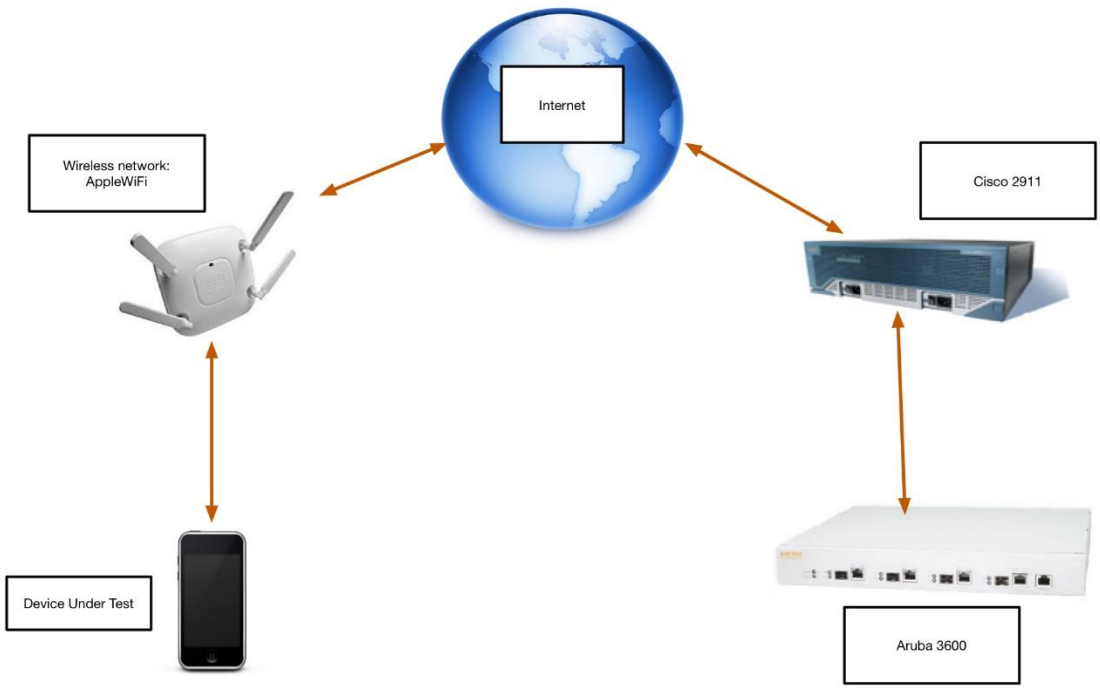
Hardware: Aruba Networks 3600

TOE Platform:

CPU Model: A7, A8, A8X, A9, A9X, A10, A10X, A11

Software Version: 11

5.13 Testbed Diagram – TESTBED #4



5.14 Testbed Component Overview – TESTBED #5.1

Captive portal websheet application exceptions (used to test BYPASS rules) were tested leveraging a test setup with British Telecom's BT Openzone captive portal. Testbed equipment necessary to facilitate the connection to the BT servers is described below:

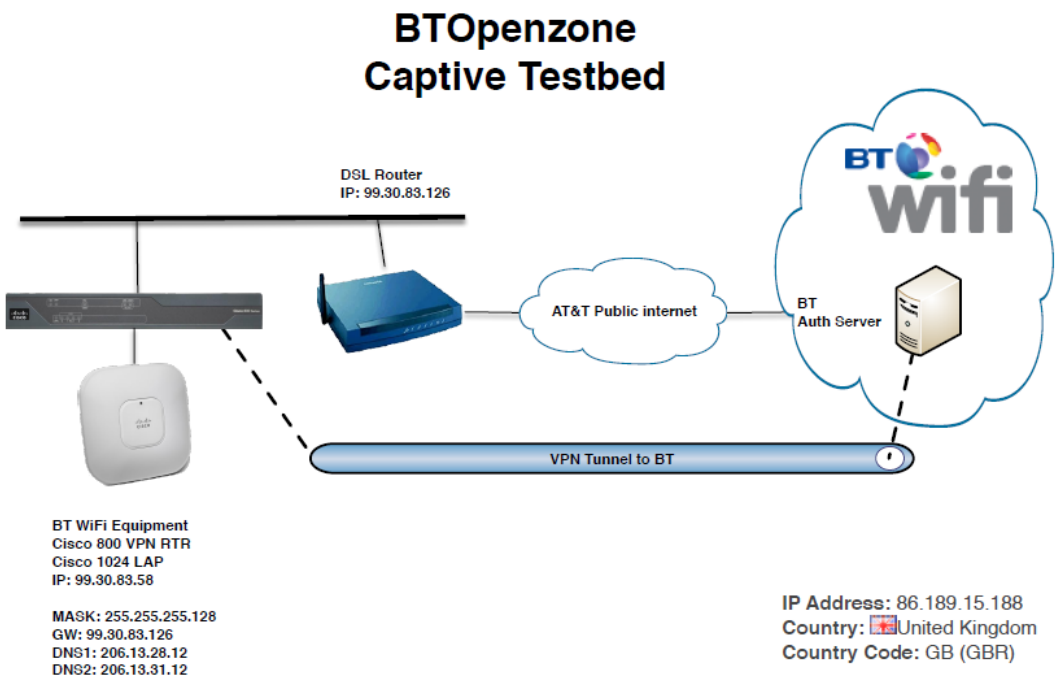
Access Point equipment:

- Cisco ISR 800 VPN router

- Cisco 1024 LAP

DSL router
BT Auth Server

5.15 Testbed Diagram – TESTBED #5.1

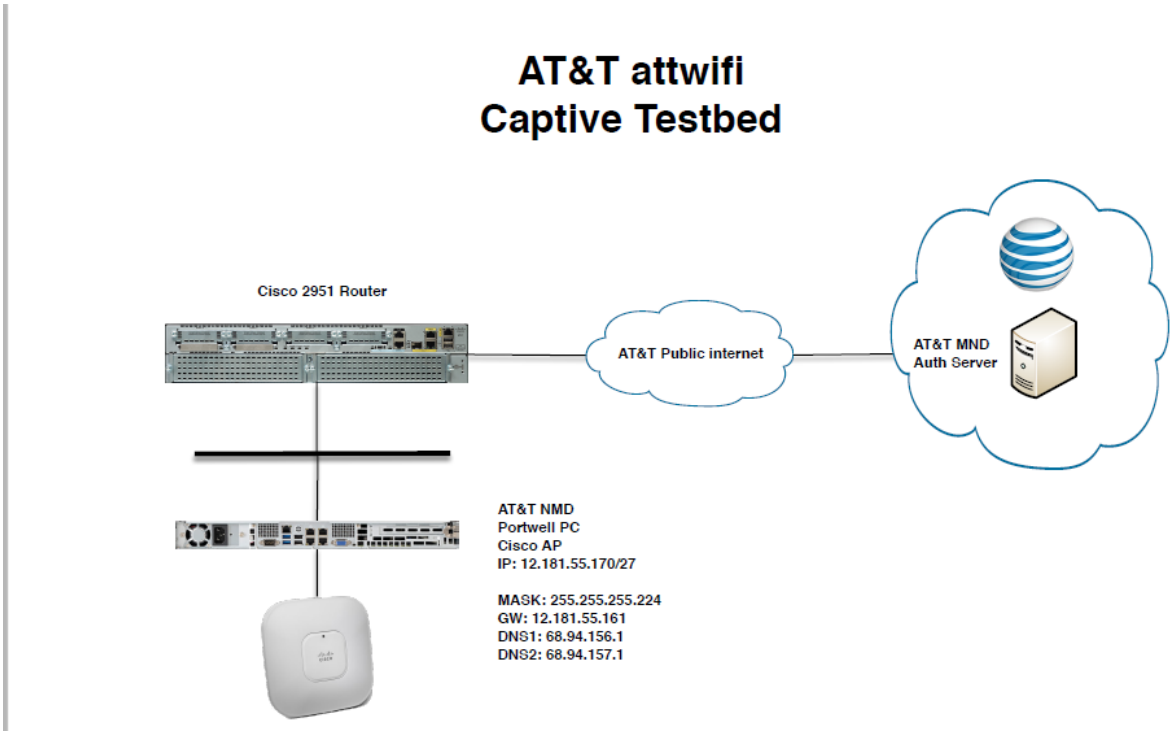


5.16 Testbed Component Overview – TESTBED #5.2

Lack of captive portal websheet application exceptions (used to test outbound DROP rules) was conducted using the AT&T attwifi captive testbed described below:

Access Point
Portwell PC
Cisco wireless AP
Router
Cisco 2951 connected to the internet
Frontend
AT&T Authorization server controlled by AT&T

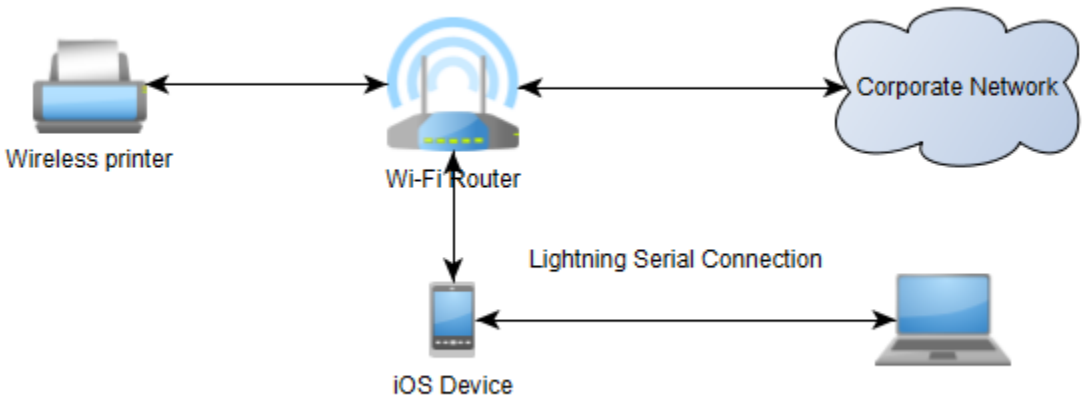
5.17 Testbed Diagram – TESTBED #5.2



5.18 Testbed Component Overview – TESTBED #6

In cases where the TOE/TOE Platform needed to be manipulated in some way, but traffic capture and control of the gateway was not necessary, the test bed essentially consists of the TOE Platform connected to a MacBook Pro via a proprietary serial device which leverages the Lightning connection, and the available wireless connection in the test location.

5.19 Testbed Diagram – TESTBED #6



6 Assurance Activity Testing Summary

6.1 FCS_CKM_EXT.4 Test 1

Item	*Data/Description*
Test ID	*FCS_CKM_EXT.4 Test 1*
Test Type	*Testing*
Objective	*The evaluator shall utilize appropriate combinations of specialized operational environment and development tools (debuggers, simulators, etc.) for the TOE and instrumented TOE builds to test that keys are cleared correctly, including all intermediate copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key.* *Cryptographic TOE implementations in software shall be loaded and exercised under a debugger to perform such tests. The evaluator shall perform the following test for each key subject to clearing, including intermediate copies of keys that are persisted encrypted by the TOE:* *1. Load the instrumented TOE build in a debugger.* *2. Record the value of the key in the TOE subject to clearing.* *3. Cause the TOE to perform a normal cryptographic processing with the key from #1.* *4. Cause the TOE to clear the key.* *5. Cause the TOE to stop the execution but not exit.* *6. Cause the TOE to dump the entire memory footprint of the TOE into a binary file.* *7. Search the content of the binary file created in #4 for instances of the known key value from #1.* *The test succeeds if no copies of the key from #1 are found in step #7 above and fails otherwise.* *The evaluator shall perform this test on all keys, including those persisted in encrypted form, to ensure intermediate copies are cleared.*
Prerequisites	*Access to a development build of iOS, development tools (debugger) and tools capable of parsing memory dumps to match key data*
Test Bed	*Testbed #4*
Test Flow (generic test steps)	*1. Load the instrumented TOE build in a debugger.* *2. Record the value of the key in the TOE subject to clearing.* *3. Cause the TOE to perform a normal cryptographic processing with the key from #1.* *4. Cause the TOE to clear the key.* *5. Cause the TOE to stop the execution but not exit.* *6. Cause the TOE to dump the entire memory footprint of the TOE into a binary file.* *7. Search the content of the binary file created in #4 for instances of the known key value from #1.*
Pass/Fail Criteria	*Certificate key data (for RSA and ECDSA) and generated session encryption/authentication (AES) keys are unobservable in heap/stack data in second memory dumps and full inspection shows complete zeroization of memory regions known to have held key data*
Results	*PASS*

6.2 FIA_X509_EXT.1 Test 1

Item	*Data/Description*

Test ID	*FIA_X509_EXT.1.1 Test #1*
Test Type	*Testing*
Objective	*The evaluator shall demonstrate that validating a certificate without a valid certification path results in the function (trusted channel setup, trusted software update, integrity check) failing. The evaluator shall then load a certificate or certificates needed to validate the certificate to be used in the function, and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that the function fails.*
Test Bed	*Testbed #3*
Test Flow (generic test steps)	1. *Load a digital certificate that does not have a complete validation path available* 2. *Attempt to use the certificate (it should fail/not be able to be used)* 3. *Make available the certificate needed to validate the original certificate* 4. *Attempt to use the original certificate (this time it should pass)* 5. *Remove the validation path* 6. *Attempt to use the original certificate (this time it should fail again)*
Pass/Fail Criteria	*Inability to establish an SA due to being unable to validate the certificate path*
Results	*PASS*

6.3 FIA_X509_EXT.1 Test 2

Item	***Data/Description***
Test ID	*FIA_X509_EXT.1.1 Test #2*
Objective	*The evaluator shall demonstrate that validating an expired certificate results in the function failing.*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	1. *Modify the clock setting on the TOE platform to set the system time into the future beyond the expiry date of the gateway's certificate* 2. *Configure the TOE to connect to the VPN gateway* 3. *See that the VPN does not establish a connection* 4. *Check system logs to verify that the certificate failed to verify due to having expired*
Pass/Fail Criteria	*Expired certificate is rejected and an SA is not established*
Results	*PASS*

6.4 FIA_X509_EXT.1 Test 3

Item	***Data/Description***
Test ID	*FIA_X509_EXT.1.1 Test #3*
Test Type	*Testing*
Objective	*The evaluator shall test that revoked certificates are properly handled – conditional on whether CRL or OCSP is selected; if both are selected, and then a test is performed for each method. For this draft of the PP, the evaluator has to only test one up in the trust chain (future drafts may require to ensure the validation is done up the entire chain). The evaluator shall ensure that a valid certificate is used, and that the SA is established. The evaluator then attempts the test with a certificate that will be revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that an SA will not be established.*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	*This test is identical to FCS_IPSEC_EXT.1.12 Test #3 and is considered tested by that test.*

Pass/Fail Criteria	*FCS_IPSEC_EXT.1.12 Test #3 passes*
Results	*PASS*

6.5 FIA_X509_EXT.1 Test 4

Item	***Data/Description***
Test ID	*FIA_X509_EXT.1.1 Test #4*
Test Type	*Testing*
Objective	*The evaluator shall construct a certificate path, such that the certificate of the CA issuing the certificate does not contain the basicConstraints extension. The validation of the certificate path fails.*
Prerequisites	*None*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	1. *Create a root CA* 2. *Create an intermediary CA lacking a basicConstraints in the X509v3 extensions* 3. *Sign the intermediary with the root* 4. *CSR for the gateway and generate a certificate signed by the intermediary* 5. *Configure the TOE platform with the appropriate payloads for the TOE connect to the gateway* 6. *Verify that the TOE is unable to connect to the gateway*
Pass/Fail Criteria	*A server certificate signed by an invalid CA certificate should be rejected and no connection should be established.*
Results	*PASS*

6.6 FIA_X509_EXT.1 Test 5

Item	***Data/Description***
Test ID	*FIA_X509_EXT.1.1 Test #5*
Test Type	*Testing*
Objective	*The evaluator shall construct a certificate path, such that the certificate of the CA issuing the certificate has the cA flag in the basicConstraints extension not set. The validation of the certificate path fails.*
Test Bed	*Testbed #3*
Test Flow (generic test steps)	1. *Create a root CA* 2. *Create an intermediary CA where the basicConstriants has ca:FALSE set* 3. *Sign the intermediary with the root* 4. *CSR for the gateway and generate a certificate signed by the intermediary* 5. *Configure the TOE platform with the appropriate payloads for the TOE connect to the gateway* 6. *Verify that the TOE is unable to connect to the gateway*
Pass/Fail Criteria	*A server certificate signed by an invalid CA certificate should be rejected and no connection should be established.*
Results	*PASS*

6.7 FIA_X509_EXT.1 Test 6

Item	***Data/Description***
Test ID	*FIA_X509_EXT.1.1 Test #6*

Test Type	*Testing*
Objective	*The evaluator shall construct a certificate path, such that the certificate of the CA issuing the certificate has the cA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.*
Test Flow (generic test steps)	*This test case constitutes the general "good" case for use of X.509 certificates and is demonstrated by FCS_IPSEC_EXT.1.12 Test #2, among others*
Pass/Fail Criteria	*A good certificates should be accepted and, barring any other issue, a VPN connection should be established.*
Results	*PASS*

6.8 FIA_X509_EXT.2 Test 1

Item	***Data/Description***
Test ID	*FIA_X509_EXT.2.2 met by TOE, Test #1*
Test Type	*Testing*
Objective	The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational guidance to determine that all supported administrator-configurable options behave in their documented manner.
Test Bed	*Testbed #1*
Test Flow (generic test steps)	*This test is identical to FCS_IPSEC_EXT.1.12 Test #6 and should be considered tested by that test.*
Pass/Fail Criteria	*FCS_IPSEC_EXT.1.12 Test #6 passes*
Results	*PASS*

6.9 FPT_TST_EXT.1 Test 1

Item	***Data/Description***
Test ID	*FPT_TST_EXT.1 Test 1*
Test Type	*Testing*
Objective	The evaluator performs the integrity check on a known good TSF executable and verifies that the check is successful.
Test Bed	*Testbed #1*
Test Flow (generic test steps)	1. *Load the special build of the VPN client* 2. *Verify that the TOE can never load* 3. *Check log files to show failed integrity test*
Pass/Fail Criteria	*Deviation between recorded HMAC and calculated HMAC should trigger a kernel panic and prevent the system from loading*
Results	*PASS*

6.10 FPT_TST_EXT.1 Test 2

Item	***Data/Description***
Test ID	*FPT_TST_EXT.1 Test 2*
Test Type	*Testing*

Objective	*Test 2: The evaluator modifies the TSF executable, performs the integrity check on the modified TSF executable and verifies that the check fails.*
Test Bed	*Testbed #6*
Test Flow (generic test steps)	1. *Load the special build of the VPN client* 2. *Verify that the TOE can never load* 3. *Check log files to show failed integrity test*
Pass/Fail Criteria	*Deviation between recorded HMAC and calculated HMAC should trigger a kernel panic and prevent the system from loading*
Results	*PASS*

6.11 FPT_TUD_EXT.1 Test 1

Item	***Data/Description***
Test ID	*FPT_TUD_EXT.1 Test #1*
Test Type	*Testing*
Objective	*Test 1: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains a legitimate update using procedures described in the operational guidance and verifies that it is successfully installed on the TOE. Then, the evaluator performs a subset of other assurance activity tests to demonstrate that the update functions as expected. After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update.*
Test Bed	*TestBed #6*
Test Flow (generic test steps)	*As the TOE is a built-in component of the TOE Platform (Apple iOS 10.2), this testing is covered by testing conducted in VID10782 on the same TOE Platforms used in this evaluation, against SFR FPT_TUD_EXT.2 in the Protection Profile for Mobile Device Fundamentals version 3.0*
Pass/Fail Criteria	*Evaluator was able to view the version of the TOE*
Results	*PASS*

6.12 FPT_TUD_EXT.1 Test 2

Item	***Data/Description***
Test ID	*FPT_TUD_EXT.1 Test #2*
Test Type	*Testing*
Objective	*The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains or produces an illegitimate update, and attempts to install it on the TOE. The evaluator verifies that the TOE rejects the update.*
Test Bed	*Testbed #6*
Test Flow (generic test steps)	*As the TOE is a built-in component of the TOE Platform (Apple iOS 10.2), this testing is covered by testing conducted in VID10782 on the same TOE Platforms used in this evaluation, against SFR FPT_TUD_EXT.2 in the Protection Profile for Mobile Device Fundamentals version 3.0*
Pass/Fail Criteria	*The TOE rejects the update.*
Results	*PASS*

6.13 FTP_ITC.1 Test 1

Item	***Data/Description***
Test ID	*FTP_ITC.1 Test #1*

Test Type	*Testing*
Objective	*Test 1: The evaluators shall ensure that the TOE is able to initiate communications with a VPN Gateway using the protocols specified in the requirement, setting up the connections as described in the operational guidance and ensuring that communication is successful.*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	*1. Set up the client to talk to the VPN gateway via an encrypted channel* *2. Initiate an encrypted channel with the VPN gateway* *3. Verify via packet capture that the channel is encrypted and uses IKEv2 as the key establishment method*
Pass/Fail Criteria	*VPN connection is established between the TOE and gateway*
Results	*PASS*

6.14 FTP_ITC.1 Test 2

Item	***Data/Description***
Test ID	*FTP_ITC Test #2*
Test Type	*Testing*
Objective	*The evaluator shall ensure, for each communication channel with a VPN Gateway, modification of the channel data is detected by the TOE.*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	*1. Set up the client to talk to the VPN gateway via an encrypted channel* *2. Initiate an encrypted channel with the VPN gateway* *3. Verify via packet capture that the channel is encrypted and uses IKEv2 as the key establishment method*
Pass/Fail Criteria	*VPN connection is established between the TOE and gateway*
Results	*PASS*

6.15 FTP_ITC.1 Test 3

Item	***Data/Description***
Test ID	*FTP_ITC.1 Test #3*
Test Type	*Testing*
Objective	*VPN Gateway, modification of the channel data is detected by the TOE.*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	*1. Set up the client to talk to the VPN gateway via an encrypted channel* *2. Initiate an encrypted channel with the VPN gateway* *3. Capture the traffic from the gateway to the client* *4. Modify the traffic and pass it to the client* *5. Verify that the client detected and dropped the modified traffic*
Pass/Fail Criteria	*TOE detects modified packets and discards them accordingly*
Results	*PASS*

6.16 FTP_ITC.1 Test 4

Item	***Data/Description***
Test ID	*FTP_ITC.1 Test 4*
Test Type	*Testing*

Objective	*Test 4: The evaluators shall physically interrupt the connection from the TOE to a VPN Gateway. The evaluators shall ensure that subsequent communications are appropriately protected, at a minimum in the case of any attempts to automatically resume the connection or connect to a new access point.*
Test Bed	*TESTBED #1*
Test Flow (generic test steps)	1. *Set up the client to talk to the VPN gateway via an encrypted channel* 2. *Initiate an encrypted channel with the VPN gateway* 3. *Disrupt the connection between gateway and client (disconnecting the gateway from the network is one possibility)* 4. *Attempt to send traffic from the client to the gateway* 5. *Ensure that the traffic is not sent unencrypted* 6. *Reconnect the gateway to the network* 7. *Attempt to send additional traffic from the client to the gateway* 8. *Ensure that the connection was automatically encryption (via Wireshark capture and logs showing reestablishment of connection)*
Pass/Fail Criteria	*No unencrypted data observed between the TOE and gateway other than ICMP control packets*
Results	*pass*

6.17 FMT_SMF.1 Test 1

Item	***Data/Description***
Test ID	*FMT_SMF.1 Test 1*
Test Type	*Testing*
Objective	*The evaluator shall test the TOE's ability to provide the management functions by configuring the TOE according to the operational guidance and testing each management activity listed in the Security Target.*
Test Bed	*Testbed #6*
Test Flow (generic test steps)	1. *Create VPN configuration via Apple Configurator.* 2. *Perform all possible configuration option.* 3. *Apply configuration to the TOE.*
Pass/Fail Criteria	*TOE is able to be configured through Apple Configurator*
Results	*PASS*

6.18 FCS_IPSEC_EXT.1.1 Test 2

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.1 Test #2*
Test Type	*Testing*
Objective	*The evaluator shall devise two equal SPD entries with alternate operations – BYPASS and PROTECT. The entries should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first entry is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation.*
Test Bed	*Testbed #2*

Test Flow (generic test steps)	1. *Configure an SPD with rules covering a DISCARD, BYPASS, and PROTECT operation, rules should include (note this may require the reconfiguration of the SPD for each scenario listed below),*
	    1. *Voicemail: Allow traffic via tunnel*
	    2. *Voicemail: Allow traffic outside of tunnel*
	    3. *Voicemail: Drop traffic*

	4. *AirPrint: Allow traffic outside of tunnel* 5. *AirPrint: Drop traffic* 2. *Send traffic flows that each meet one of the rules.* 3. *Verify that each rule was appropriately enforced.*
Pass/Fail Criteria	*Proper behavior should be observed for AirPrint and Visual Voicemail traffic vis-à-vis PROTECT/BYPASS/DISCARD functionality*
Results	*PASS*

6.19 FCS_IPSEC_EXT.1.2 Test 1

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.2 Test #1*
Test Type	*Testing*
Objective	*If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in tunnel mode and also configures a IPsec Peer to operate in tunnel mode. The evaluator configures the TOE and the IPsec Peer to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the client to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.*
Test Bed	*Testbed #2*
Test Flow (generic test steps)	1. *Configure an IPsec session in tunnel mode with logging.* 2. *Establish the session between the TOE and its peer.* 3. *Verify that the session was established in tunnel mode.*
Pass/Fail Criteria	*A VPN connection was established with ESP "tunnel" mode.*
Results	*PASS*

6.20 FCS_IPSEC_EXT.1.3 Test 1

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.3 Test #1*
Test Type	*Testing*
Objective	*The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD, BYPASS, and PROTECT network packets. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a "TOE created" final entry that discards packets that do not match any previous entries). The evaluator sends the packet, and observes that the packet was not permitted to flow to any of the TOE's interfaces.*
Test Bed	*Testbed #2*
Test Flow (generic test steps)	1. *TOE does not support manual SPD manipulation* 2. *Establish a VPN connection to the gateway* 3. *Modify traffic coming back from the gateway to the TOE in a similar manner to FCS_IPSEC_EXT.1.1 Test #2.* 4. *Verify via packet capture that the packets no longer matching the SA rules are discarded*

	5. *Configure the TOE to allow an exception for a captive portal application* 6. *Verify the ability to access the captive portal* 7. *Change the configuration to disallow access to the portal* 8. *Verify the inability to access the captive portal*
Pass/Fail Criteria	*Packets not matching the PASS rule on an established VPN connection should be discarded. This includes packets modified outright, as well as packets sent/received from processes which are not given permission to communicate inside or outside of the tunnel*
Results	*PASS*

6.21 FCS_IPSEC_EXT.1.4 Test 1

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.4 Test #1*
Test Type	*Testing*
Objective	*Test 1: The evaluator shall configure the TOE/platform as indicated in the operational guidance configuring the TOE/platform to using each of the AES-GCM-128, and AES-GCM-256 algorithms, and attempt to establish a connection using ESP. If the ST Author has selected either AES-CBC-128 or AESCBC-256, the TOE/platform is configured to use those algorithms and the evaluator attempts to establish a connection using ESP for those algorithms selected.*
Test Bed	*Testbed #2*
Test Flow (generic test steps)	1. *Configure an IPsec SA to support the identified encryption algorithm.* 2. *Establish an encrypted session.* 3. *Verify that the configured algorithm was used.* 4. *Repeat for each supported algorithm.*
Pass/Fail Criteria	*TOE is able to establish an SA with all four selected AES cipher suites*
Results	*PASS*

6.22 FCS_IPSEC_EXT.1.5 Test 1

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.5 Test #1*
Test Type	*Testing*
Objective	*Test 1: The evaluator shall configure the TOE/platform so that it will perform NAT traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed*
Test Bed	*TESTBED #2*
Test Flow (generic test steps)	1. *Ensure that the test set up supports NAT Transversal.* 2. *Test: Configure an IPsec connection, including, logging the session.* 3. *Test: Establish an IPsec session.* 4. *Test: Verify that NAT transversal was possible.*
Pass/Fail Criteria	*TOE is able to establish a VPN tunnel with a VPN gateway while behind a router or firewall performing network address translation (NAT)*
Results	*PASS*

6.23 FCS_IPSEC_EXT.1.6 Test 1

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.6 Test #1*

Test Type	*Testing*
Objective	*The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation.*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	1. *Configure an IKE SA to support the identified encryption algorithm.* 2. *Establish an encrypted session* 3. *Verify that the configured algorithm was used.* 4. *Repeat for each supported algorithm and IKE version*
Pass/Fail Criteria	*The TOE should successfully establish a tunnel with the gateway when using the encryption settings mandated by the gateway's configuration*
Results	*PASS*

6.24 FCS_IPSEC_EXT.1.8 Test 2

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.8 Test #2*
Test Type	*Testing*
Objective	*Test 2 (Conditional): The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.*
Test Bed	*Testbed #4*
Test Flow (generic test steps)	1. *Configure the IKE Phase 1 SA lifetime for 24 hours.* 2. *Establish an IPsec session.* 3. *Transmit packets across the connections repeatedly (to keep the session active).* 4. *Verify that when the time threshold is crossed a rekey is initiated.*
Pass/Fail Criteria	*Parent and Child SAs are re-keyed at the appropriate interval*
Results	*PASS*

6.25 FCS_IPSEC_EXT.1.8 Test 3

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.8 Test #3*
Test Type	*Testing*
Objective	*Test 3 (Conditional): The evaluator shall perform a test similar to Test 1 for Phase 2 SAs, except that the lifetime will be 8 hours instead of 24*
Test Bed	*Testbed #4*
Test Flow (generic test steps)	1. *Configure the IKE Phase 2 SA lifetime for 8 hours.* 2. *Establish an IPsec session.* 3. *Transmit packets across the connections repeatedly (to keep the session active).* 4. *Verify that when the time threshold is crossed a rekey is initiated.*
Pass/Fail Criteria	*Parent and Child SAs are re-keyed at the appropriate interval*
Results	*PASS*

6.26 FCS_IPSEC_EXT.1.11 Test 1

Item	*Data/Description*
Test ID	*FCS_IPSEC_EXT.1.11 Test #1*
Test Type	*Testing*
Objective	*Test 1: For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully completed using that particular DH group.*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	*1. Configure an IPsec session with the supported DH group and logging.* *2. Establish an IPsec session.* *3. Ensure the configured DH group is used in session establishment.* *4. Repeat for each supported DH group.* *5. Repeat for each IKE version supported.*
Pass/Fail Criteria	*The TOE is able to establish a tunnel using each supported DH group*
Results	*PASS*

6.27 FCS_IPSEC_EXT.1.12 Test 1

Item	*Data/Description*
Test ID	*FCS_IPSEC_EXT.1.12 Test #1*
Test Type	*Testing*
Objective	*Test 1: The evaluator shall have the TOE/platform generate a public-private key pair, and submit a CSR (Certificate Signing Request) to a CA (trusted by both the TOE/platform and the peer VPN used to establish a connection) for its signature. The values for the DN (Common Name, Organization, Organizational Unit, and Country) will also be passed in the request. Alternatively, the evaluator may import to the TOE/platform a previously generated private key and corresponding certificate.*
Pass/Fail Criteria	*This test was performed in conjunction with the FIA_X509_EXT.* and FCA_IPSEC_EXT.* tests which all require the ability to import a certificate as a perquisite for testing.*
Results	*PASS*

6.28 FCS_IPSEC_EXT.1.12 Test 2

Item	*Data/Description*
Test ID	*FCS_IPSEC_EXT.1.12 Test #2*
Test Type	*Testing*
Objective	*Test 2: For each field of the certificate supported for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the field in the peer's presented certificate and shall verify that the IKE authentication succeeds.*
Test Bed	*Testbed #3*
Test Flow (generic test steps)	*1. Configure the VPN gateway's reference identifier on the VPN Client* *2. A previously generated certificate of the appropriate type was provided to use for authentication* *3. Verify that an encrypted session could be established (via wireshark and audit logs)* *4. Repeat for each type of certificate supported and each type of reference identifier (CN and SAN)* *5. This should be done for each support key type and length/curve, including,* *a. RSA:*

	i. 2048-bits b. ECDSDA: i. P-256 ii. P-384
Pass/Fail Criteria	*The TOE should be able to properly use both the CN and SAN as reference identifiers and establish a connection if they are correct.*
Results	*PASS*

6.29 FCS_IPSEC_EXT.1.12 Test 3

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.12 Test #3*
Test Type	*Testing*
Objective	*Test 3: The evaluator shall test that the TOE/platform can properly handle revoked certificates –conditional on whether CRL or OCSP is selected; if both are selected, and then a test is performed for each method. For this draft of the PP, the evaluator has to only test one up in the trust chain (future drafts may require to ensure the validation is done up the entire chain). The evaluator shall ensure that a valid certificate is used, and that the SA is established. The evaluator then attempts the test with a certificate that will be revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the TOE/platform will not establish an SA.*
Test Bed	*Testbed #3*
Test Flow (generic test steps)	1. *Using the trusted certificate from the previous test case, establish a VPN connection with a VPN gateway* 2. *Verify that an encrypted session could be established (via wireshark and audit logs)* 3. *Disconnect the encrypted session* 4. *Revoke the certificate of the VPN gateway* 5. *Attempt to establish an encrypted session between the client and gateway* 6. *Verify that the session could not be established* 7. *Repeat for each supported revocation method (CRL and/or OCSP)* 8. *This should be done for each support certificate key type and length/curve, including,* a. *RSA:* i. *2048-bits* b. *ECDSDA:* i. *P-256* ii. *P-384*
Pass/Fail Criteria	*The TOE should fail to establish an SA when the certificate passed back to it from the gateway in the IKE_SA_INIT phase shows up as revoked when the OCSP responder for the certificate is queried. An SA should be established when a non-revoked certificate is used and the OCSP responder tells the TOE the certificate is valid.*
Results	*PASS*

6.30 FCS_IPSEC_EXT.1.12 Test 4a

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.12 Test #4a*
Test Type	*Testing*

Objective	*Test 4: For each field of the certificate support for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to not match the field in the peer's presented certificate and shall verify that the IKE authentication fails.*
Test Bed	*Testbed #3*
Test Flow (generic test steps)	1. *Modify the VPN gateway's reference identifier configured on the VPN Client to not match the equivalent field in the VPN gateway's presented certificate* 2. *Attempted to establish an encrypted* 3. *Verify that the session is not established (via generated logs and wireshark capture)* 4. *This should be done for each supported reference identifier, certificate key type and length/curve, including,* a. *RSA:* i. *2048-bits* b. *ECDSA:* i. *P-256* ii. *P-384*
Pass/Fail Criteria	*Certificates whose CN do not match the expected reference identifier should be rejected and no VPN connection should be established*
Results	*PASS*

6.31 FCS_IPSEC_EXT.1.12 Test 4b

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.12 Test #4b*
Test Type	*Testing*
Objective	*Test 5: The evaluator shall configure the peer's reference identifier on the TOE to not match the SAN in the peer's presented certificate but to match the Common Name in the peer's presented certificate, and verify that the IKE authentication fails.*
Test Bed	*Testbed #3*
Test Flow (generic test steps)	1. *Modify the VPN Gateway's reference identifier on the TOE such that the SAN matches the VPN Gateway's certificate but Common Name does not match the certificate* 2. *Attempted to establish an encrypted* 3. *Verify that the session is not established (via generated logs and wireshark capture)* 4. *This should be done for each certificate key type and length/curve, including,* a. *RSA:* i. *2048-bits* b. *ECDSA:* i. *P-256* ii. *P-384*
Pass/Fail Criteria	*The TOE should reject certificates with an invalid SAN and no VPN connection should be established*
Results	*PASS*

6.32 FCS_IPSEC_EXT.1.12 Test 6

Item	***Data/Description***

Test ID	*FCS_IPSEC_EXT.1.12 Test #6*
Test Type	*Testing*
Objective	*Test 5: The evaluator shall ensure that the TOE is configurable to either establish an SA, or not establish an SA if a connection to the certificate validation entity cannot be reached. For each method selected for certificate validation, the evaluator attempts to validate the certificate – for the purposes of this test, it does not matter if the certificate is revoked or not. For the "mode" where an SA is allowed to be established, the connection is made. Where the SA is not to be established, the connection is refused.*
Test Bed	*TESTBED #3*
Test Flow (generic test steps)	1. *Configure the VPN client to establish a VPN session if a Cert validation authority cannot be reached* 2. *Disconnect the CA from the network* 3. *Attempt to establish a connection with the VPN gateway* 4. *Verify that a connection could be established* 5. *This should be done for each support certificate key type and length/curve, including,* a. *RSA:* i. *2048-bits* b. *ECDSDA:* i. *P-256* ii. *P-384*
Pass/Fail Criteria	*The TOE should proceed with establishing an SA with the gateway even if the OCSP responder is unable to be contacted*
Results	*PASS*

6.33 FCS_IPSEC_EXT.1.14 Test 1

Item	***Data/Description***
Test ID	*FCS_IPSEC_EXT.1.14 Test #1*
Test Type	*Testing*
Objective	*Test 1: This test shall be performed for each version of IKE supported. The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	1. *Configure the VPN client to establish an encrypted session with the VPN gateway.* 2. *Verify that an encrypted session is established* 3. *Repeat for each supported encryption algorithm, including,* a. *AES-CBC-128* b. *AES-CBC-256* c. *AES-GCM-128* d. *AES-GCM-256* 4. *Repeat for each supported hash algorithm, including,* a. *HMAC-SHA1* b. *HMAC-SHA-256* c. *HMAC-SHA2-384* d. *HMAC-SHA2-512*
Pass/Fail Criteria	*Each hash algorithm may be used for IPsec connections.*
Results	*PASS*

6.34 FCS_IPSEC_EXT.1.14 Test 3

Item	*Data/Description*
Test ID	*FCS_IPSEC_EXT.1.14 Test #3*
Test Type	*Testing*
Objective	*Test 3: This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an IKE SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	1. *Configure the VPN client for an IKE SA using AES-CBC 128* 2. *Configure the VPN gateway for an IKE SA using Triple-DES* 3. *Attempt to establish an encrypted session with the VPN gateway.* 4. *Verify that the connection fails via Wireshark capture and audit logs* 1. *Configure the VPN client for an IKE SA using HMAC-SHA1* 2. *Configure the VPN gateway for an IKE SA using HMAC-MD5* 3. *Attempt to establish an encrypted session with the VPN gateway.* 4. *Verify that the connection fails via Wireshark capture and audit logs*
Pass/Fail Criteria	*TOE fails to establish a VPN tunnel with the gateway*
Results	*PASS*

6.35 FCS_IPSEC_EXT.1.14 Test 4

Item	*Data/Description*
Test ID	*FCS_IPSEC_EXT.1.14 Test #4*
Test Type	*Testing*
Objective	*Test 4: This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an SA for ESP (assumes the proper parameters where used to establish the IKE SA) that selects an encryption algorithm that is not identified in FCS_IPSEC_EXT.1.4. Such an attempt should fail.*
Test Bed	*Testbed #1*
Test Flow (generic test steps)	1. *Configure the VPN client for an IPsec SA using AES-CBC 128* 2. *Configure the VPN gateway for an IPsec SA using Triple-DES* 3. *Attempt to establish an encrypted session with the VPN gateway.* 4. *Verify that the connection fails via wireshark capture and audit logs* 5. *Configure the VPN client for an IPsec SA using HMAC-SHA1* 6. *Configure the VPN gateway for an IPsec SA using HMAC-MD5* 7. *Attempt to establish an encrypted session with the VPN gateway.* 8. *Verify that the connection fails via wireshark capture and audit logs*
Pass/Fail Criteria	*TOE fails to establish a VPN tunnel with the gateway*
Results	*PASS*

7 Security Assurance Requirements

7.1 AGD_OPE.1 Guidance 1

For TOE that implement a cryptographic engine, the operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

7.1.1 Evaluator Findings

The evaluator examined the TOE operational guidance to ensure it included instructions for configuration of the cryptographic engine associated with the evaluated configuration. The evaluator found that the TOE implements cryptographic modules, which are mentioned in section 1.2 of the TOE operational guidance. Configuration settings for implementation of security functions that make use of the cryptographic engine are found in section 3 of the AGD.

Upon investigation the evaluator found that the cryptographic engine is not explicitly configured but that the TOE takes advantage of the cryptographic engine when security functions are configured for an always on VPN.

Based on these findings, the assurance activity is considered satisfied.

7.1.1.1 Verdict

PASS

7.2 AGD_OPE.1 Guidance 2

The documentation must describe the process for verifying updates to the TOE, either by checking the hash or by verifying a digital signature. The evaluator shall verify that this process includes the following steps:

1. For hashes, a description of where the hash for a given update can be obtained. For digital signatures, instructions for obtaining the certificate that will be used by the FCS_COP.1(2) mechanism to ensure that a signed update has been received from the certificate owner. This may be supplied with the product initially, or may be obtained by some other means.
2. Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).
3. Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature.

7.2.1 Evaluator Findings

The evaluator examined the documentation to ensure it describes the process for verifying updates to the TOE. The evaluator also verified the steps that are included in the process. According to the TOE documentation, section 3.3.2, the TOE platform verifies the updates using a digital signatures. This information can be found with greater detail in the TOE platform operational guidance, section 2.

Upon investigation the evaluator found that the operational guidance of the TOE platform contains the information that describes the process for verifying that updates to the TOE are secure.

Based on these findings, the assurance activity is considered satisfied.

7.2.1.1 Verdict

PASS

7.3 AGD_PRE.1 Guidance 1

The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.

7.3.1 Evaluator Findings

The evaluator checked that the guidance provided by the TOE addresses all platforms adequately that are claimed in the TOE ST. The inspection of section 1.1 of the operational guidance was used to make this assertion.

Upon investigation of the operational guidance the evaluator found that all platforms were adequately represented.

Based on these findings, the activity is considered satisfied.

7.3.1.1 Verdict

PASS

7.4 ATE_IND.1

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators must document in the test plan that each applicable testing requirement in the ST is covered.

7.4.1 Evaluator Findings

This security assurance requirement is satisfied by the test plan created for this evaluation.

7.4.1.1 Verdict

PASS

7.5 AVA_VAN.1

As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document.

7.5.1 Evaluator Findings

The evaluator conducted a vulnerability analysis against the TOE in accordance with the requirements contained in the Protection Profile. The following sources of public vulnerability information were searched:

- http://nv.nist.gov
- http://www.us-cert.gov
- http://www.securityfocus.com
- http://cve.mitre.org

The terms searched include:

- Apple iOS 11
- iPhone
- iPad
- CoreCrypto v8

Several CVEs reporting vulnerabilities were found related to the TOE platform (not the TOE). The vendor supplied patches and fixes to the platform for these issues. Independent testing was then completed on the TOE and patched platform.

7.5.1.1 Verdict

PASS

8 Conclusions

For each of the test cases required for VPN Client Protection Profile version 1.4, the TOE was able to demonstrate each of the desired functionalities. Each test case passed without any additional qualifications.

The TOE meets all of the requirements for VPN Client Protection Profile version 1.4.

End of Document