Assurance Activities Report for a Target of Evaluation

Cisco
Integrated Services Router (ISR) 800 Series

Security Target (Version 0.9)

Assurance Activities Report (AAR)
Version 1.0

10/31/2014

Evaluated by:

Booz | Allen | Hamilton

Booz Allen Hamilton Common Criteria Test Laboratory
NIAP Lab # 200423
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090

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

The Developer of the TOE:
Cisco Systems, Inc.,
170 West Tasman Drive,
San Jose, CA 95134-1706 USA

The Author of the Security Target:
Cisco Systems, Inc.,
170 West Tasman Drive,
San Jose, CA 95134-1706 USA

The TOE Evaluation was sponsored by:
Cisco Systems, Inc.,
170 West Tasman Drive,
San Jose, CA 95134-1706 USA

Evaluation Personnel:
Justin Fisher
Christopher Gugel
Josh Jones
Christopher Rakaczky

Applicable Common Criteria Version

Common Criteria for Information Technology Security Evaluation, September 2012 Version 3.1 Revision 4

Common Evaluation Methodology Version

Common Criteria for Information Technology Security Evaluation, Evaluation Methodology, September 2012 Version 3.1 Revision 4

Table of Contents

1 Purpose

The purpose of this document is to serve as a non-proprietary attestation that this evaluation has satisfied all of the TSS, AGD, and ATE Assurance Activities required by the Protection Profiles/Extended Packages to which the TOE claims exact conformance.

2 TOE Summary Specification Assurance Activities

The evaluation team completed the testing of the Security Target (ST) 'Cisco Integrated Services Router 800 Series Security Target, Version 0.9' and confirmed that the TOE Summary Specification (TSS) contains all Assurance Activities as specified by the 'Protection Profile for Network Devices Version 1.1', 'Security Requirements for Network Devices Errata #2', and 'Network Device Protection Profile Extended Package VPN Gateway Version 1.1' (VPN EP). The evaluators were able to individually examine each SFR's TSS statements and determine that they comprised sufficient information to address each SFR claimed by the TOE as well as meet the expectations of the NDPP and VPN EP Assurance Activities. Where Assurance Activities are defined in more than one of the specified sources, the VPN EP's representation takes precedence, followed by the NDPP Errata.

Through the evaluation of ASE_TSS.1-1, described in the ETR, the evaluators were able to determine that each individual SFR was discussed in sufficient detail in the TSS to describe the SFR being met by the TSF in general. However, in some cases the Assurance Activities that are specified in the claimed source material instruct the evaluator to examine the TSS for a description of specific behavior to ensure that each SFR is described to an appropriate level of detail. The following is a list of each SFR, the TSS Assurance Activities specified for the SFR, and how the TSS meets the Assurance Activities. Additionally, each SFR is accompanied by the source material (NDPP, NDPP Errata, VPN EP) that defines where the most up-to-date TSS Assurance Activity was defined.

FAU_GEN.1 (VPN EP) – The Assurance Activity requires the TSS to describe how the packet filter firewall rules can be configured to log network traffic associated with applicable rules. It also requires the TSS to describe how the TOE behaves when one of its interfaces is overwhelmed with network traffic. The TSS states that "Logs are generated when traffic matches acls that are configured with the log operation" and that "logs are generated when traffic that exceeds the settings allowed on an interface is received".

FAU_GEN.2 – This SFR does not contain any TSS Assurance Activities.

FAU_STG_EXT.1 (NDPP) – The Assurance Activity requires the TSS to describe the amount of audit data that is stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The TSS states this information as, "The local logging buffer size can be configured from a range of 4096 (default) to 2147483647 bytes," "The local logging buffer is circular, so newer messages overwrite older messages after the buffer is full," and, "Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents."

FCS_CKM.1(1) (NDPP Errata) – The Assurance Activity requires the TSS to contain a description of how the TSF complies with 800-56A and 800-56B, including the sections in the standards that are implemented by the TSF, such that key establishment is among the claimed sections. The TSS states that "The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP 800-56A. The TOE complies with section 6 and all subsections regarding RSA key pair generation and key establishment in the NIST SP 800-56B."

FCS_CKM.1(2) (VPN EP) – The Assurance Activity requires the TSS to contain a description of how the TSF complies with FIPS 186 to describe how IKE peer authentication key pairs are generated, such that key pair generation is among the claimed sections. The TSS states that "The TOE provides cryptographic

signature services using ECDSA that meets FIPS 186-3, "Digital Signature Standard" with NIST curves P-256 and P-384 and RSA that meets FIPS PUB 186-2 or FIPS 186-3, "Digital Signature Standard."

FCS_CKM_EXT.4 (NDPP) – The Assurance Activity requires the TSS to describe all of the secret key, private keys, and CSPs; when they are zeroed; and the type of procedure that is performed to do this. Section 7.1 of the ST appropriately lists this information.

FCS_COP.1(1) – This SFR does not contain any TSS Assurance Activities.

FCS_COP.1(2) – This SFR does not contain any TSS Assurance Activities.

FCS_COP.1(3) – This SFR does not contain any TSS Assurance Activities.

FCS_COP.1(4) – This SFR does not contain any TSS Assurance Activities.

FCS_IPSEC_EXT.1.1 (VPN EP) – This SFR does not contain any TSS Assurance Activities.

FCS_IPSEC_EXT.1.2 (VPN EP) – The Assurance Activity requires the TSS to state that the TOE can operate in tunnel mode and/or transport mode as selected. The TSS states that both transport and tunnel mode are supported, consistent with the selection. It also states that tunnel mode is the default mode and that the TOE can be configured to explicitly accept only tunnel mode connections if desired.

FCS_IPSEC_EXT.1.3 (VPN EP) – The Assurance Activity requires the TSS to provide a description of how a packet is processed against the SPD and that a final rule exists that causes unprocessed packets to be discarded. The TSS states that traffic that does not match a permit acl and is blocked by non-crypto acls on the interface will be discarded.

FCS_IPSEC_EXT.1.4 (VPN EP) – The Assurance Activity requires the TSS to verify that the selected algorithms are implemented and that the HMAC algorithm is consistent with FCS_COP.1(4). The TSS correctly identifies AES-GCM-128, AES-GCM-256, AES-CBC-128, and AES-CBC-256 as the algorithms used to perform this function. There is only one crypto module used by the TOE so it is assumed that the HMAC implementation is consistent with FCS_COP.1(4).

FCS_IPSEC_EXT.1.5 (VPN EP) – The Assurance Activity requires the TSS to assert that IKEv1 and/or IKEv2 are implemented as selected. The TSS correctly asserts that both IKEv1 and IKEv2 are implemented.

FCS_IPSEC_EXT.1.6 (VPN EP) – The Assurance Activity requires the TSS to identify the algorithms used for encrypting the IKE payload. The TSS correctly identifies AES-CBC-128 and AES-CBC-256 as the algorithms used to perform this function.

FCS_IPSEC_EXT.1.7 (VPN EP) – The Assurance Activity requires the TSS to state that only main mode and not aggressive mode is used for IKEv1 Phase 1 exchanges (this is allowed to be a configurable setting). The TSS describes the ability to disable aggressive mode as configurable and indicates the command used to achieve this.

FCS_IPSEC_EXT.1.8 (VPN EP) – The Assurance Activity requires the TSS to describe how the lifetimes are established and enforced as stated in the applicable RFCs. The TSS states that the 'lifetime' command can be used to set the lifetimes for both Phase 1 and Phase 2 SAs and that the lifetime can be configured either by time or by packets.

FCS_IPSEC_EXT.1.9, FCS_IPSEC_EXT.1.10 (VPN EP) – The Assurance Activity requires the TSS to describe the process for generating "x" for each nonce, that the random number generated for this meets the requirements of the PP, and that the length of "x" and the nonces meet the stipulations in the requirement. The Security Target states that "x" is generated using a NIST-approved AES-CTR DRBG. This is the same

DRBG described in FCS_RBG_EXT.1. Nonces are of a size that ensures that the probability that a specific nonce value will be repeated over the life of the SA is less than 1 in 2^128.

FCS_IPSEC_EXT.1.11 (VPN EP) – The Assurance Activity requires the TSS to list the DH groups that are supported and how a particular group is specified/negotiated with a peer if more than one is supported. The TSS indicates that Groups 14, 19, 24, 20, 15, and 16 are all supported and provides a description of how to prescribe the use of a particular group.

FCS_IPSEC_EXT.1.12 (VPN EP) – The Assurance Activity requires the TSS to identify RSA and/or ECDSA as being used to perform peer authentication in a way that is consistent with FCS_COP.1(2). The TSS indicates that "the IKE protocols implement Peer Authentication using RSA and ECDSA along with X.509v3 certificates, or pre-shared keys," which is consistent with the SFR. Additionally, the TSS clarifies the SFR by stating that OCSP is only supported when RSA encryption is used, while CRLs are supported for either RSA or ECDSA encryption.

FCS_IPSEC_EXT.1.13 (VPN EP) – The Assurance Activity requires the TSS to describe the potential strengths of the algorithms that are allowed for IKE and ESP exchanges and the checks that are done when negotiating Phase 2/CHILD_SA suites to ensure that the strength of this is less than or equal to that of the IKE SA that is protecting the negotiation. The TSS describes these strengths as 128 or 256 bits and instructs the administrator to use a larger key size for ESP than that of the key size used to protect the IKE payload.

FCS_RBG_EXT.1 (NDPP Errata) – The Assurance Activity requires documentation to be produced in accordance with Annex D, Entropy Documentation and Assessment. The TSS provides some overview of these materials, but this requirement is satisfied by the separate entropy documentation provided by Cisco.

FCS_SSH_EXT.1.1 (NDPP Errata) – This SFR does not contain any TSS Assurance Activities.

FCS_SSH_EXT.1.2 (NDPP Errata) – The Assurance Activity requires the TSS to describe the public key algorithms that are acceptable for SSH authentication, that this list conforms to FCS_SSH_EXT.1.5, and that password-based methods are allowed. The TSS lists password-based and public key-based methods for SSH authentication.

FCS_SSH_EXT.1.3 (NDPP Errata) – The Assurance Activity requires the TSS to describe how "large packets" are detected and handled. The TSS states that packets greater than 35,000 bytes are dropped in an SSH transport connection.

FCS_SSH_EXT.1.4 (NDPP Errata) – The Assurance Activity requires the TSS to specify any optional characteristics of the SSH transport implementation and the algorithms that are used for the transport implementation such that they are consistent with the SFR definition. The TSS correctly lists AES-CBC-128 and AES-CBC-256 as the supported transport algorithms. FCS_SSH_EXT.1.5 is also satisfied here because the TSS indicates that RSA signature verification (SSH_RSA) is the public key algorithm used by the SSH implementation.

FCS_SSH_EXT.1.5 (NDPP Errata) – This SFR does not contain any TSS Assurance Activities.

FCS_SSH_EXT.1.6 (NDPP Errata) – he Assurance Activity requires the TSS to list the supported data integrity algorithms consistent with the SFR definition. The TSS and SFR both state that the TOE uses HMAC-SHA1 and HMAC-SHA1-96 for its integrity algorithms.

FCS_SSH_EXT.1.7 (NDPP Errata) – The Assurance Activity requires the TSS to state that the use of DH group 14 is "hard-coded" into the SSH implementation if this is the case.

FDP_RIP.2 (NDPP) – The Assurance Activity requires the TSS to describe packet processing describes how residual data is removed and at what point in the buffer processing this occurs. The TSS states that memory buffer content is zeroed once packet handling has been completed so that no residual data is

inadvertently transmitted. The evaluation team has determined this information to be acceptable because before memory is de-allocated into the memory stack it is zeroed by writing all zeroes and thus, no residual information will be detectable when the memory is then allocated from the memory stack for future system calls.

FIA_AFL.1 (VPN EP) – The Assurance Activity requires the TS to describe how successive unsuccessful authentication attempts are detected and trapped, the method by which the remote administrator is prevented from accessing the TOE, and the actions necessary to restore this ability. The TSS states that consecutive failed logons for a user are tracked and compared to the defined threshold value. Once this value has been met, that user account is locked and an administrator must manually unlock the account via the CLI.

FIA_PMG_EXT.1 (NDPP) – This SFR does not contain any TSS Assurance Activities.

FIA_PSK_EXT.1 (VPN EP) – The Assurance Activity requires the TSS to identify all protocols that allow both text-based and bit-based pre-shared keys and that 22-character pre-shared keys are supported. For each protocol identified in FIA_PSK_EXT.1.1, the TSS must also state the conditioning that transforms the text-based pre-shared key from the key sequence entered by the user to the bit string used by the protocol in a manner that is consistent with the definition in FIA_PSK_EXT.1.3. The TSS indicates that the TOE supports keys from 22 characters to 128 bytes that are conditioned with SHA-1 prior to use.

FIA_UIA_EXT.1 (NDPP) – The Assurance Activity requires the TSS to describe the logon process for each supported logon method including information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a "successful logon". The TSS states that the supported logon method is through the CLI (either through local console or remote SSH connection), the credentials used are username/password, and a "successful logon" is defined by validation of the administrative credentials. The TSS also states that RADIUS, TACACS+, and SSH public key authentication are supported as alternative authentication mechanisms.

FIA_UAU_EXT.2 (NDPP) – This SFR does not contain any TSS Assurance Activities unless other authentication mechanisms have been specified, in which case they are to be discussed in conjunction with FIA_UIA_EXT.1.

FIA_UAU.7.1 (NDPP) – This SFR does not contain any TSS Assurance Activities.

FIA_X509_EXT.1 (VPN EP) – The Assurance Activity requires the TSS to describe all certificate stores implemented that contain certificates used to meet the SFRs. This must include information pertaining to how certificates are loaded and protected from unauthorized access. This will also include a discussion as to how the TOE forms a certification path and how certificates are validated. The TSS specifies configurable locations for where certificates are stored and indicates that they are loaded via USB tokens and protected via physical security assumptions and the TOE's identification and authentication function.

FMT_MOF.1 (VPN EP) – This SFR does not contain any TSS Assurance Activities.

FMT_MTD.1 (NDPP) – This SFR does not contain any TSS Assurance Activities.

FMT_SMF.1 (NDPP with augmentation in VPN EP) – The Assurance Activities for this SFR are expected to be satisfied through completing Assurance Activities for the other SFRs, as indicated in the PP/EP.

FMT_SMR.2 (NDPP) – This SFR does not contain any TSS Assurance Activities.

FPF_RUL_EXT.1.1 (VPN EP) – The Assurance Activity requires the TSS to describe the TOE's startup process which clearly identifies where processing of packets begin to take place such that packets cannot flow during startup. It also requires the TSS to identify the components involved in processing the packets and describes the safeguards that prevent the TSF from failing open. The TSS states the following: "During

the boot cycle, the TOE first powers on hardware, loads the image, and executes the power on self-tests. Until the power on self-tests successfully complete, the interfaces to the TOE are deactivated. Once the tests complete, the interfaces become active and the rules associated with the interface become immediately operational. There is no state during initialization/ startup that the access lists are not enforced on an interface."

FPF_RUL_EXT.1.2 (VPN EP) – The Assurance Activity requires the TSS to indicate that the appropriate protocols are supported and on what basis this conformance is asserted. The TSS lists the correct protocols and states that compliance is verified via regular quality assurance, regression, and interoperability testing.

FPF_RUL_EXT.1.3, FPF_RUL_EXT.1.4, FPF_RUL_EXT.1.5 (VPN EP) – The Assurance Activity requires the TSS to describe the attributes that packet filtering can be based on, the operations that the policy can enforce (permit, deny, log). It also requires the TSS to identify all interface types subject to the packet filtering policy and explain how rules are associated with distinct network interfaces. The TSS lists the appropriate attributes and operations and states that access lists are applied to interfaces using access and crypto map sets.

FPF_RUL_EXT.1.6 (VPN EP) – The Assurance Activity requires the TSS to describe the algorithm applied to incoming packets to include the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset. The TSS states that rule matching is performed on a top-down basis, which is understood to be administratively defined. There are no default rules other than the fact that the TSF rejects traffic for which there is no explicitly-defined rule (see FPF_RUL_EXT.1.7).

FPF_RUL_EXT.1.7 (VPN EP) – The Assurance Activity requires the TSS to describe the process for applying rules and that the behavior is to deny packets when there is no match unless another condition allows it. The TSS states that network interfaces pass traffic only when the source address matches the network interface originating the traffic through another network interface corresponding to the traffic's destination address.

FPT_FLS.1 (VPN EP) – The Assurance Activity requires the TSS to describe how the TOE ensures a shutdown upon a self-test, integrity check, or noise source health test failure. The TSS states that interfaces are disabled when any of these failures occur and indicates that there are no non-security-relevant exceptions to this.

FPT_SKP_EXT.1 (NDPP) – The Assurance Activity requires the TSS to detail how pre-shared keys, symmetric keys, and private keys are stored such that they're unable to be viewed. The TSS states that in the evaluated configuration, the 'password encryption aes' command is used to encrypt key data and that the 'hidekeys' command is used to hide key data that is stored in configuration files when these files are being viewed.

FPT_APW_EXT.1 (NDPP) – The Assurance Activity requires the TSS to detail all of the authentication data that is subject to this requirement and the method used to obscure the password plaintext data. The TSS is also required to assert that passwords are stored in such a way that there is no interface designed for the purpose of viewing this data. The TSS states that there is a master passphrase that can be used to encrypt all locally-defined passwords such that administrators do not have access to plaintext password data. There is no other authentication data that requires protection.

FPT_STM.1.1 (NDPP Errata) – The Assurance Activity requires the TSS to list each security function that makes use of time and a description of how time is maintained and considered to be reliable. The TSS indicates that the TOE can use the hardware clock or optionally can synchronize with an NTP server. It also states that time data is used for timestamps on audit records and for determining administrator inactivity periods and IPsec values such as key/SA lifetimes.

FPT_TUD_EXT.1 (NDPP) – The Assurance Activity requires the TSS to define the authorized source of digital signatures and a description of how the certificates are stored on the device. The TSS indicates that

digital signatures are published by Cisco and information about their storage and use is detailed in the operational guidance.

FPT_TST_EXT.1 (NDPP with augmentation in VPN EP) – The Assurance Activity requires the TSS to detail the self-tests that are run at startup, including an outline of what the tests are actually doing. The TSS is also required to have an argument outlining why this is sufficient to assert the TSF is operating correctly and any errors that may result from self-tests. The TSS lists the self-tests and references the FIPS Security Policy for more information about the self-tests for error information. These self-tests are sufficient to ensure proper operation of the TSF because it tests all cryptographic functions, software integrity, and RNG capabilities.

FTA_SSL_EXT.1 (NDPP) – This SFR does not contain any TSS Assurance Activities.

FTA_SSL.3 (NDPP) – This SFR does not contain any TSS Assurance Activities.

FTA_SSL.4 (NDPP) – This SFR does not contain any TSS Assurance Activities.

FTA_TAB.1 – The Assurance Activity requires the TSS to detail each method of access (local and remote) available to the administrator. The TSS details local console and remote SSH access.

FTP_ITC.1 (NDPP Errata) – The Assurance Activity requires the TSS to describe that, for all communications with authorized IT entities, each mechanism is identified in terms of the allowed protocols, and that these protocols are consistent with the SFR. The TSS states that all trusted channels (VPN clients/peers, CA server, AAA server, and audit server) can be secured using IPsec.

FTP_TRP.1 (NDPP Errata) – The Assurance Activity requires the TSS to describe the methods of remote TOE administration and how these communications are protected, such that they are consistent with the protocols defined elsewhere in the ST. The TSS states that remote administration is only done via a CLI that is protected by SSH, which is consistent with the protocol claims made by the ST.

Additionally, the assurance activity for ALC_CMC.1 requires the ST to identify the product version that meets the requirements of the ST such that the identifier is sufficiently detailed to be usable for acquisitions. The ST clearly identifies the product model numbers that comprise the ISR 800 series as well as the specific version of the Cisco IOS software that is running on each of these appliances.

3 Operational Guidance Assurance Activities

The evaluation team completed the testing of the Operational Guidance, which includes the following documents,

- Cisco Integrated Services Router (ASR) 800 Series Common Criteria Operational User Guidance And Preparative Procedures version 0.5 [OPE]
- Cisco IOS Command Reference Guide [COMMANDREF]
- Securing User Services Configuration Guide Library, Cisco IOS Release 15M&T [USER SERVICES]
- Software Configuration Guide [SOFTWARE CONFIG]

and confirmed that the Operational Guidance contains all Assurance Activities as specified by the 'Protection Profile for Network Devices Version 1.1' (NDPP), 'Security Requirements for Network Devices Errata #2' (Errata), and 'NDPP Extended Package VPN Gateway Version 1.1' (VPN EP). The evaluators reviewed the NDPP, Errata, and VPN EP to identify the security functionality that must be discussed for the operational guidance. This is prescribed by the Assurance Activities for each SFR and the AGD SARs. The evaluators have listed below each of the SFRs defined in the NDPP and VPN EP that have been claimed by the TOE (some SFRs are conditional or optional) as well as the AGD SAR, along with a discussion of where in the operational guidance the associated Assurance Activities material can be found.

If an SFR is not listed, one of the following conditions applies:

- There is no Assurance Activity for the SFR.
- The Assurance Activity for the SFR specifically indicates that it is simultaneously satisfied by completing a different Assurance Activity (a testing Assurance Activity for the same SFR, a testing Assurance Activity for a different SFR, or a guidance Assurance Activity for another SFR).
- The Assurance Activity for the SFR does not specify any actions to review the operational guidance.

Note that some SFRs list multiple different Assurance Activities in multiple references. The evaluators determined the proper Assurance Activity to use through the following process:

- If an Assurance Activity for the SFR was defined in the VPN EP, that Assurance Activity was used.
- If an Assurance Activity for the SFR was not defined in the VPN EP but was defined in the NDPP Errata, the NDPP Errata Assurance Activity was used.
- If an Assurance Activity for the SFR was only defined in the NDPP, that Assurance Activity was used.

The exception to this is where an Assurance Activity in the VPN EP clearly specifies testing for the portion of an SFR that applies just to the VPN EP (e.g. FAU_GEN.1 talking about only the auditing for packet filtering). In these cases, the Assurance Activities from the VPN EP and NDPP (or NDPP Errata, as needed) are combined.

FAU_GEN.1 –
"The evaluator shall check the administrative guide and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN.1.2, and the additional information specified in Table 1."

Section 5 of the OPE provides a table of auditable events that is consistent with the auditable events table in the NDPP for the claimed SFRs. This table includes examples of audit records for different situations that are associated with the requirement. For example, FCS_IPSEC_EXT.1 provides logs for establishment of an IPsec session, termination of an IPsec session, and failure of IPsec session establishment. Section 5 provides an example of an audit record before this table and breaks it down into the individual fields that are prescribed by FAU_GEN.1.2. From this example, the relationship between the audit logs shown in the table and the required fields can be determined clearly.

"The evaluator shall also make a determination of the administrative actions that are relevant in the context of this PP. The evaluator shall examine the administrative guide and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are security relevant with respect to this PP. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements."

The "Cisco Integrated Services Router 800 Series Common Criteria Operational User Guidance And Preparative Procedures" [AGD] was developed by Cisco with the purpose to provide the specific guidance for managing TOE functionality or a pointer to the necessary documentation as defined by the Purpose statement in Section 1.2: "This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining ISR-800 operations. All security relevant commands to manage the TSF data are provided in this document within each functional section."

Based upon this information, the evaluation team has determined that only the commands located within the AGD and the specific pointers to other documents are considered to be security relevant for this evaluation, except where the AGD states that the information provided is outside the scope of the Common Criteria evaluation.

Through the completion of the independent functional testing, the evaluation team created manual test cases or reviewed vendor automated test cases to ensure that they contained only commands that were defined within the AGD and then tested each SFR by executing the commands in each SFR's relevant test case(s). As part of the testing, the evaluation team reviewed the audit records that were produced when running each test case which included audit records for all management commands. The evaluation team then produced a document that contained an example of each management command audit record and compared it against Tables 8 and 9 in the AGD for consistency.

FAU_STG_EXT.1 –
"The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server (for TOEs that are not acting as an audit log server)."

Section 5 of the OPE states that the TOE can be configured to store audit records internally as well as simultaneously offload them to an external syslog server.

"The evaluator shall also examine the operational guidance to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server."

Section 3.3.3 of the OPE specifies the set of commands that are required to ensure that all TSF-relevant events are audited and that these audited events are sent to a remote syslog server. Section 3.3.4 provides a similar example for the configuration of logging using an Embedded Event Manager (EEM) script.

Section 3.3.5 of the OPE discusses how to configure the trusted channel between the TOE and the remote syslog server using IPsec for cases where the server is an IPsec peer of the TOE and for cases where the server is adjacent to an IPsec peer within a trusted facility such that audit records are tunneled over the public network.

FCS_IPSEC_EXT.1.1 –
"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."

Section 4.6.4 of the OPE states the following:

"The VPNGW Extended Package requires that the TOE be able to support options for information flow policies that include discarding, bypassing, and protecting. On the TOE, an authorized administrator can define the traffic rules on the box by configuring access lists (with permit, deny, and/or log actions) and applying these access lists to interfaces using access and crypto map sets:

- The 'discard' option is accomplished using access lists with deny entries, which are applied to interfaces within access-groups. Guidance for configuration of IOS Information Flow Policies is located in the [4] Under "Zone-based Policy Firewall" or "Zone-Based Policy Firewall IPv6 Support" *for IPv6.*
- The 'bypassing' option is accomplished using access lists with deny entries, which are applied to interfaces within crypto maps for IPsec. Guidance for configuration of entries for IPsec is in [18].
- The 'protecting' option is accomplished using access lists with permit entries, which are applied to interfaces within crypto maps for IPsec VPN."

As per the references in the OPE, [4] refers to http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-zone-pol-fw.html and [18] refers to http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/15-1mt/Configuring_Internet_Key_Exchange_Version_2.html. The evaluators reviewed [4] and observed that it references the creation of ACLs and the ability to apply permit deny rules to them. The evaluators reviewed [18] and observed that it references the creation of crypto maps and the ability to apply permit and deny rules to them.

FCS_IPSEC_EXT.1.2 –
"The evaluator shall confirm that the operational guidance instructs the Administrator how the TOE is configured in each mode selected."

The operational guidance provides the following instructions for configuring the two IPsec modes:

"TOE-common-criteria(config-crypto)#**mode tunnel**
This configures tunnel mode for IPsec. Tunnel is the default, but by explicitly specifying tunnel mode, the router will request tunnel mode and will accept only tunnel mode.
TOE-common-criteria(config-crypto)#**mode transport**
This configures transport mode for IPsec."

FCS_IPSEC_EXT.1.3 –
"The evaluator checks that the operational guidance provides instructions on how to construct the SPD and uses the guidance to configure the TOE for the following tests."

Refer to FCS_IPSEC_EXT.1.1. The operational guidance references instructions on how to construct the SPD through permit and deny rules on both access lists and crypto maps.

FCS_IPSEC_EXT.1.4 –
"The evaluator checks the operational guidance to ensure it provides instructions on how to configure the TOE 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."

Section 4.6.2 of the OPE provides a sample command for setting an ESP algorithm as follows:
"TOE-common-criteria(config)# crypto ipsec transform-set example esp-aes 128 esp-sha-hmac"
It also provides instructions for how to set the other three ESP algorithms that are defined in the Security Target as being supported.

FCS_IPSEC_EXT.1.5 –
"The evaluator checks the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and uses the guidance to configure the TOE to perform NAT traversal for the following test."

Sections 4.6.1.1 and 4.6.1.2 of the OPE provide instructions for how to configure the TOE to use IKEv1 and IKEv2, respectively.

FCS_IPSEC_EXT.1.6 –
"The evaluator ensures that the operational guidance describes how the TOE can be configured to use the mandated algorithms, as well as any additional algorithms selected in the requirement. The guidance is then used to configure the TOE to perform the following test."

Sections 4.6.1.1 and 4.6.1.2 of the OPE provide instructions on how to configure the TOE to use the supported IKE payload encryption algorithms through use of the 'encryption' command.

FCS_IPSEC_EXT.1.7 –
"If the mode requires configuration of the TOE prior to its operation, the evaluator shall check the operational guidance to ensure that instructions for this configuration are contained within that guidance."

Section 4.6.1.1 of the OPE correctly states the configuration instructions for main mode as follows: "Main mode is the default mode and the crypto isakmp aggressive-mode disable ensures all IKEv1 Phase 1 exchanges will be handled in the default main mode."

FCS_IPSEC_EXT.1.8 –
"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. The evaluator ensures that the Administrator is able to configurable Phase 1 SAs values for 24 hours and 8 hours for Phase 2 SAs. Currently there are no values mandated for the number of packers[sic], the evaluator just ensures that this can be configured. The TOE may limit the lifetime on the number of bytes that have been transmitted and this would be acceptable."

Sections 4.6.1.1 and 4.6.1.2 of the OPE provide instructions and guidance for setting the lifetimes for Phase 1 SAs, both in terms of length of time and of number of packets (total traffic). Section 4.6.2 provides instructions and guidance for setting the lifetime for Phase 2 SAs in the same manner.

FCS_IPSEC_EXT.1.12 –
"The evaluator ensures the operational guidance describes how to set up the TOE to use the cryptographic algorithms RSA and/or ECDSA.

Sections 4.6.3 and 4.6.3.1 of the OPE indicate that the TSF supports both RSA and ECDSA for peer authentication and provide instructions and external references for configuring and loading certificates that use these algorithms. The external reference, labeled as [19] and found at http://www.cisco.com/c/en/us/td/docs/ios/sec_secure_connectivity/configuration/guide/15_0/sec_secure_connectivity_15_0_book/sec_cert_enroll_pki.pdf, correctly shows the configuration and use of certificates that use these algorithms.

In order to construct the environment and configure the TOE for the following tests, the evaluator will ensure that the operation guidance also describes how to configure the TOE to connect to a trusted CA, and ensure a valid certificate for that CA is loaded into the TOE and marked "trusted".

Sections 4.6.3.5, 4.6.3.6, and 4.6.3.7 of the OPE provide instructions for how to configure certificate status checking using CRL, OCSP, and/or certificate chain validation. Additionally, the guidance referenced at [19] lists instructions for configuring and loading certificates such that a CA certificate can be loaded into the TSF and marked as a trusted root.

FCS_IPSEC_EXT.1.13 –
"The evaluator simply follows the guidance to configure the TOE to perform the following tests."

Since no specific AGD review activities were prescribed by this Assurance Activity, it is deferred to testing.

FCS_SSH_EXT.1.4 –
"The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements)."

Section 3.3.1 of the OPE describes the method for configuring the TSF to use AES-CBC-128/256 as the transport algorithms in step 7. Because enabling SSHv2 also enables the FIPS-approved 3DES-CBC mode, a further recommendation is provided to ensure that the administrator's SSH client is correctly configured in the Operational Environment.

FCS_SSH_EXT.1.6 –
"The evaluator shall also check the operational guidance to ensure that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed)."

Section 3.3.1 of the OPE describes the method of configuring the allowed data integrity algorithms in step 8. Both the allowed algorithms and the instructions for configuring the TSF to only accept these algorithms are provided.

FCS_SSH_EXT.1.7 –
"The evaluator shall ensure that operational guidance contains configuration information that will allow the security administrator to configure the TOE so that all key exchanges for SSH are performed using DH group 14 and any groups specified from the selection in the ST."

Section 3.3.1 of the OPE provides instructions to the administrator to configure the TSF to use DH group 14 through use of the 'ip ssh dh min size 2048' command.

FIA_AFL.1 –
The evaluator shall also examine the operational guidance to ensure that instructions for configuring the number of successive unsuccessful authentication attempts (1.1) and time period (1.2, if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.

Section 3.2.6 of the OPE instructs the administrator to configure user lockout and provides the command syntax for performing this operation, which includes setting the maximum number of failures before lockout occurs. No time period is supported, either for resetting the lockout counter or for unlocking the user after they have been locked out for a certain period of time. This section also provides relevant commands for managing this function, including resetting the lockout counter for a user, unlocking a user, and listing all of the users who have been locked out. It also mentions that privileged administrators (privilege level 15) cannot be locked out. The evaluators consider this to be acceptable because otherwise it would be possible for an attacker to perform a denial of service attack against the privileged administrator account and prevent the TOE from being managed. Finally, this section also indicates that the number of failures is tracked internally to the TSF and independent of the mechanism used to request access to the TOE.

FIA_PMG_EXT.1 –
"The evaluator shall examine the operational guidance to determine that it provides guidance to security administrators on the composition of strong passwords, and that it provides instructions on setting the minimum password length."

Section 4.2 of the OPE provides instruction on how to configure the TOE to prevent insecure passwords. It references the COMMANDREF for more information about using the commands described in the OPE as well as any prerequisite commands for their use. Secure values for the password parameter are defined when specifying its mandatory minimum strength and providing optional instructions for additional security.

FIA_PSK_EXT.1 –
"The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the merits of shorter or longer pre-shared keys. The guidance must specify the allowable characters for pre-shared keys, and that list must be a super-set of the list contained in FIA_PSK_EXT.1.2.

Section 4.6.1.1 of the OPE provides information about the allowed character set and length of pre-shared keys. The character set is appropriate with respect to its definition in the FIA_PSK_EXT.1 SFR. The OPE also provides a note about the maximum length of pre-shared keys and indicates that while longer keys are more secure, system performance is diminished if they are used.

The evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both)."

Section 4.6.1.2 of the OPE provides information about the ability of the TSF to accept bit-based pre-shared keys in hexadecimal formatting through use of the 'pre-shared-key hex' command.

FIA_UIA_EXT.1 –
"The evaluator shall examine the operational guidance to determine that any necessary preparatory steps (e.g., establishing credential material such as pre-shared keys, tunnels, certificates, etc.) to logging in are described."

Section 3.2.1 of the OPE describes initial configuration of the TOE including logging in locally for the first time. Sections 3.2.4 and 3.3.2 of the OPE references USER SERVICES for instructions on how to configure the TOE to use RADIUS and TACACS+, including the configuration of keys. The OPE also instructs the reader to use best practices for selection and protection of the key. Section 4.6 of the OPE describes the process of setting up an IPsec trusted channel, which is the mechanism by which AAA communications are expected to be secured in the evaluated configuration.

Sections 3.3.4 and 4.7.2 of the OPE discuss the configuration of the IPsec trusted channel for the use of protecting AAA server communications. Section 3.3.4 also describes how to point the TOE at the AAA server for the purposes of establishing a connection.

"For each supported the login method, the evaluator shall ensure the operational guidance provides clear instructions for successfully logging on."

The AAA configuration guide, located at http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/15-mt/secuser-15-mt-library.html, describes the preparation of the authentication servers.

The AAA, located at http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/xe-3s/sec-usr-aaa-xe-3s-book.html describes the preparation of the authentication servers. In SOFTWARE CONFIG, under section "Basic Router Configuration" it discusses how to log into the TOE.

"If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the operational guidance provides sufficient instruction on limiting the allowed services."

Section 3.2.1 of the OPE provides instructions on the initial setup steps that are used to enable a password so that the services allowed prior to authentication are limited. Section 4.5 of the OPE describes the configuration of login banners which is the only allowed services prior to authentication.

FMT_MTD.1 –
"The evaluator shall review the operational guidance to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of this PP is identified, and that configuration information is provided to ensure that only administrators have access to the functions."

The OPE describes the commands that are used to manipulate TSF data. The administrative commands used to configure the TSF are included in the sections that apply to the corresponding TSF behavior. For example, section 3.3.1 of the AGD is entitled "Remote Administration Protocols" and provides instructions to configure RADIUS and TACACS+, which includes the management commands used to do so. Section 4.1 of the OPE describes how the TOE can be configured to limit privileges of different users within the constraints of the Authorized Administrator role. The COMMANDREF document provides detailed instructions on the usage of all administrative commands. The evaluator can determine the TSF relevance of commands in the COMMANDREF document by checking to see if they are mentioned in the AGD. As shown in the other AGD_OPE.1 work units, configuration and secure usage of the TSF's cryptographic, I&A, management, and update functions are discussed in various places throughout the OPE document (or

in other administrative documents that are referenced by it). The privilege levels and guidance surrounding their use in enforcing strict separation of duties is considered to be secure administration of the user privilege level parameter.

FMT_SMF.1 –
"The security management functions for FMT_SMF.1 are distributed throughout the PP and are included as part of the requirements in FMT_MTD, FPT_TST_EXT, and any cryptographic management functions specified in the reference standards. Compliance to these requirements satisfies compliance with FMT_SMF.1."

The NDPP does not prescribe specific assurance activities for this SFR.

"The evaluator shall verify that the operational guidance describes how to configure the Packet filter firewall rules, including how to set any configurable defaults and how to configure each of the applicable rule attributes, actions, and associated interfaces. The evaluator must ensure that the operational guidance also provides instruction that would allow an administrator to ensure that configured rules are properly ordered. Note that this activity should have been addressed with the Guidance assurance activities for FPF_RUL_EXT.1."

The VPN EP indicates that the assurance activity for this SFR is synonymous with that of FPF_RUL_EXT.1 so this analysis has been deferred to that SFR.

FMT_SMR.2 –
"The evaluator shall review the operational guidance to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration."

Section 3.2 of the OPE describes how to perform initial configuration of the TOE locally. Once configured, it can continue to be administered in this manner. Section 3.3.1 of the OPE describes how to subsequently configure the TOE to allow for remote administration. Administration of the TOE in terms of how to use the CLI and what commands are available is described fully in the COMMANDREF.

FPF_RUL_EXT.1.2 –
"The evaluator shall verify that the operational guidance indicates that the following protocols are supported:

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

The guidance will describe the other protocols contained within the ST (e.g., IPsec, IKE, potentially HTTPS, SSH, and TLS) that are processed by the TOE. The evaluator ensures it is made clear what protocols were not considered as part of the TOE evaluation."

Section 3.3.6 of the OPE identifies the protocols that are supported for the TOE's packet filtering capability. The list provided in the OPE is not exhaustive, but it includes the following protocols that are required by the SFR: IPv4, IPv6, TCP, UDP, IKEv1, IKEv2, IPsec, SSH. Section 7 notes that OSI Layer 2 protocols and routing protocols are excluded from the TSF because they are not applicable to the requirements that have been claimed.

FPF_RUL_EXT.1.3/FPF_RUL_EXT.1.4/FPF_RUL_EXT.1.5
"The evaluators shall verify that the operational guidance identifies the following attributes as being configurable within Packet filtering rules for the associated protocols:

- *IPv4*
  - *Source address*
  - *Destination Address*

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

Section 3.3.6 of the OPE identifies the appropriate set of traffic attributes for each protocol as specified in FPF_RUL_EXT.1.3.

"The evaluator shall verify that the operational guidance indicates that each rule can identify the following actions: permit, deny, and log."

Section 3.3.6 of the OPE provides examples for the configuration of access lists, which are indicated in the OPE as being required to meet the requirements of the VPN EP. The OPE references COMMANDREF for the list of commands that are used to manipulate access lists. The evaluators reviewed COMMANDREF and observed that for commands that are used to create rules (such as access-list) both "permit" and "deny" are operations that can be associated with the rule. Additionally, a "log" option is provided such that the triggering of any permit or deny rule can also be logged.

"The evaluator shall verify that the operational guidance explains how rules are associated with distinct network interfaces."

Section 3.3.6 of the OPE provides examples for how rules are associated with network interfaces. The actual rules themselves (defined by the "access-list") command are assigned source and destination IP addresses. If the IP address of a TOE interface is known, matching a host in the rule with that IP address is an implicit association with the interface. In addition, each access-list entry can be associated with a numeric group number. Within the "interface" command options, the "access-group" command is used to explicitly assign the access-list entries with a given number to a certain interface such that that interface in particular enforces all of the rules with that number. This is further discussed in the COMMANDREF.

"The evaluator shall verify that the operational guidance explains how to determine the interface type of a distinct network interface (e.g., how to determine the device driver for a distinct network interface)."

Section 3.3.6 of the AGD shows how to apply an ACL to a specific network interface by going into the config-if menu for the desired interface.

FPF_RUL_EXT.1.6
"The evaluator shall verify that the operational guidance describes how the order of Packet filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing."

Section 3.3.6 of the OPE indicates that traffic matching is done from the top down. It also indicates how a "drop all" rule should be applied to the end of an access list.

FPT_STM.1 –
"The evaluator examines the operational guidance to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the operational guidance instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication."

Section 4.3 of the OPE references documentation that provides instructions for how to configure the TOE's local clock and how to establish a connection to an NTP server.

FPT_TST_EXT.1 –
"The evaluator shall also ensure that the operational guidance describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS."

Section 3.2.3 of the OPE describes how to manually execute the power-on self-tests. Section 6 describes what happens when the self-tests fail and what steps should be taken to attempt to restore the TOE to an operational state following this failure.

FPT_TUD_EXT.1 –
"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."

Section 2 of the OPE lists the steps for secure acceptance of the TOE, which includes verification of both the hardware and software. The OPE provides expected hashes for the evaluated software as well as instructions to validate these hashes. The OPE also provides instructions for downloading and installing the software image, which is applicable to subsequent TOE updates. Verification steps cover validation of the certificate (Step 9) and the hash (Step 11).

FTA_SSL_EXT.1, **FTA_SSL.3**, **FTA_SSL.4 –** There is no specific assurance activity. However, the assurance activity for testing requires the tester to follow the operational guidance to configure the system inactivity period. The OPE discusses the ability to configure this using the "exec-timeout" command defined in Section 3.2.5.

FTA_TAB.1 – There is no specific assurance activity. However, the assurance activity for testing requires the tester to follow the operational guidance to configure the banner. The OPE discusses the ability to configure this using the "banner" command described in Section 4.5.

FTP_ITC.1 –
"The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken."

The OPE discusses how to send log data to a remote syslog server in section 3.3.3 and how to configure the IPsec connection in section 3.3.5. The OPE discusses how to configure a AAA server in section 3.3.2 and specifies that the method of configuring the IPsec connection is the same as for syslog. Section 4.6 discusses the process for establishing IPsec VPN connections.

FTP_TRP.1 –
"The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method".

The OPE discusses instructions for configuring SSH for administrative access in Section 3.3.1. This SSH connection can be encapsulated in an IPsec connection by following peer configuration instructions described in section 4.6.

AGD_OPE.1 –
"The operational guidance shall at a minimum list the processes running (or that could run) on the TOE in its evaluated configuration during its operation that are capable of processing data received on the network interfaces (there are likely more than one of these, and this is not limited to the process that "listens" on the network interface). It is acceptable to list all processes running (or that could run) on the

TOE in its evaluated configuration instead of attempting to determine just those that process the network data. For each process listed, the administrative guidance will contain a short (e.g., one- or two-line) description of the process' function, and the privilege with which the service runs. "Privilege" includes the hardware privilege level (e.g., ring 0, ring 1), any software privileges specifically associated with the process, and the privileges associated with the user role the process runs as or under."

The OPE discusses all network services/protocols that are available to run on the TOE in Section 7, all of which run as system-level processes.

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

Section 3.2.3 of the OPE states that "The TOE must be run in the FIPS mode of operation. The use of the cryptographic engine in any other mode was not evaluated nor tested during the CC evaluation of the TOE."

"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.
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."

Section 2 of the OPE provides the hashes for the validated version of the TOE software for each model as well as information on where to find hash information for updated versions in the future. Section 2 of the OPE also provides a URL from where software packages can be downloaded. Finally, Section 2 of the OPE provides a set of instructions for loading the downloaded software onto the TOE and validating both its signature and published hash.

"The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities."

With regards to the relevant examples of administrative actions, the evaluators have found that the COMMANDREF document provides detailed instructions on the usage of all administrative commands. The evaluator can determine the TSF relevance of commands in the COMMANDREF document by checking to see if they are mentioned in the AGD.

AGD_PRE.1 –
As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.

The installation and configuration of the TOE is discussed in the AGD_PRE.1 SARs in the ETR. Within the OPE, Table 5 specifies the 819, 881, and 891 models described in the ST. Software hashes are provided for the 819, 881, and 891 models. The vendor's web site lists a large number of ISR 800 series models. Included in this list of models are the same 819, 881, and 891 models listed in both the ST and OPE. It is understood by the evaluator that models that are not present in this list are considered to be outside the scope of the evaluation.

4 Test Assurance Activities (Test Report)

The following sections demonstrate that all ATE Assurance Activities for the TOE have been met. This evidence has been presented in a manner that is consistent with the "Reporting for Evaluations Against NIAP-Approved Protection Profiles" guidance that has been provided by NIAP. Specific test steps and associated detailed results are not included in this report in order for it to remain non-proprietary. The test report is a summarized version of the test activities that were performed as part of creating the Evaluation Technical Report (ETR).

4.1 Platforms Tested and Composition

The evaluation team set up a test environment for the testing that allowed them to perform all test assurance activities across several of the claimed models and over the relevant interfaces. The testing performed has a sufficient level of overlap between the tested models and interfaces to validate that the TOE performs the same regardless of the specific model and interface configurations.

The selection of models for testing was based upon the three model types within the product line (819, 881, and 891) that are provided for the performance, interoperability, and/or scalability needs of the network infrastructure that model is intended to support. The models that were tested in the laboratory were C819-4G-V-K9, CISCO881-K9, and CISCO891-K9. Additionally, the vendor conducted testing at their own facility while the evaluation team directly observed the tests in order to confirm that they were consistent with the defined test procedures and expected results.

This sample was chosen so that each of the three sub-models of the ISR 800 series (819, 881, and 891) is represented. Within the individual sub-models, there are no differences to the software or methods of administration. The only functional differences are the specific LAN/WAN interfaces that are used to route traffic between networks. The method of administering these interfaces is the same, regardless of the physical method of data transmission.

ISR 819 Image Tested: C819-4G-V-K9 with Cisco IOS, Version 15.2(4)M7 (laboratory), C819G-S-K9 with Cisco IOS, Version 15.2(4)M7 (vendor)
ISR 881 Image Tested: C881-K9 with Cisco IOS, Version 15.2(4)M7 (laboratory)
ISR 891 Image Tested: C891-K9 with Cisco IOS, Version 15.2(4)M7 (laboratory), CISCO891W-AGN-A-K9 with Cisco IOS, Version 15.2(4)M7 (vendor)

The TOE does not contain any pluggable or modular components that require special configuration. In order to bring the TOE into the evaluated configuration, the evaluation team and vendor followed the appropriate configuration steps that are defined in the OPE materials.

The functional test sample was chosen to ensure a proper balance between demonstrating coverage and making reasonable arguments that equivalent functionality has been demonstrated. Detailed information about the tests conducted on each platform in each environment has been provided in the ISR Test Matrix that accompanies the Evaluation Technical Report. As a summary, the following general points apply to the test sample:

- The vendor test environment contained only 819 and 891 devices. The evaluation team executed a large subset of the vendor testing to demonstrate that the behavior of the 881 device was identical to what was observed for the other two devices. This subset includes every major security function of the TSF with additional emphasis placed on the IPsec capabilities of the TOE since that is its primary functionality.
- Some testing was conducted entirely within the laboratory environment. This includes the following:
    - Auditing of startup and shutdown of audit functions
    - Establishment of transport mode communications
    - NAT traversal processing
    - All X.509 certificate/CA server handling
    - SSH password-based authentication and use of HMAC-SHA1-91 integrity algorithm
    - Authentication failure handling

- Password management
- Use of pre-shared keys
- TACACS+ authentication
- Handling of packet filtering during TOE initialization
- Establishment of IPsec trusted channel with CA server and remote syslog server

The vast majority of these tests were performed on all three ISR models.

4.2 Omission Justification

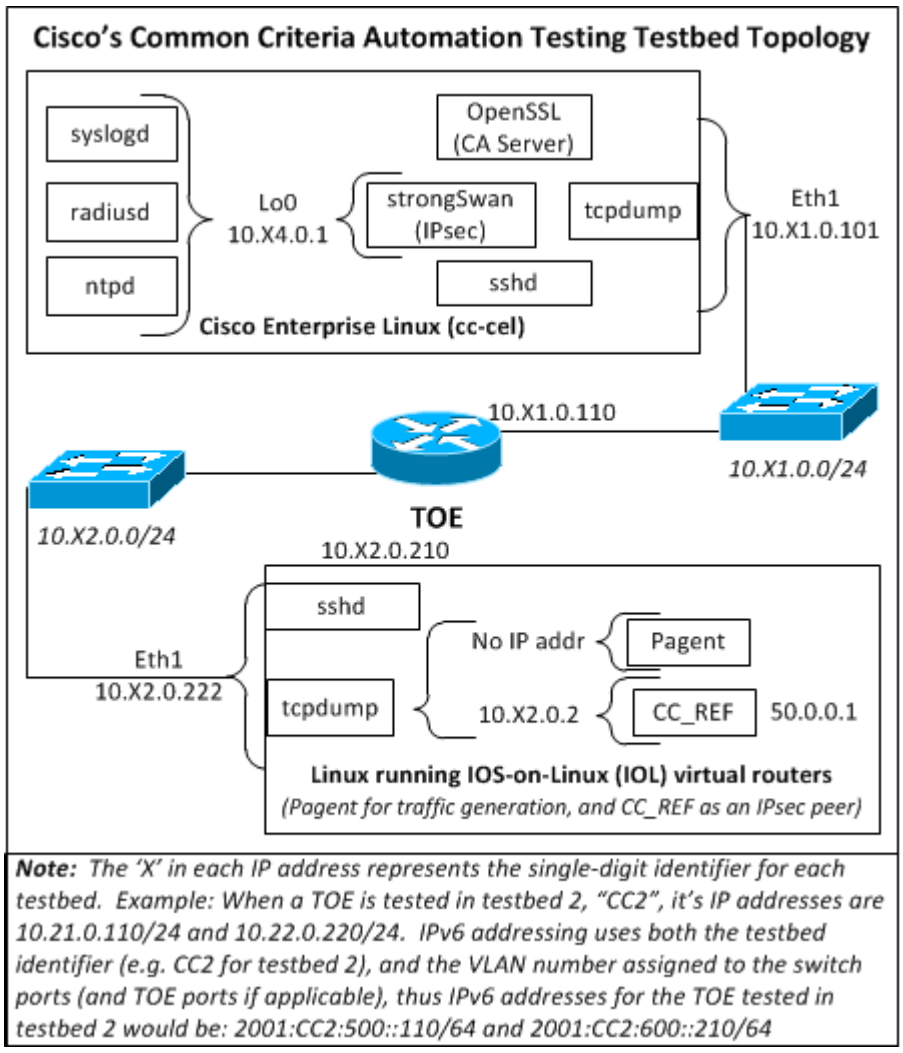
Not all platforms defined in the ST were tested as part of the testing effort. The following rationale has been provided for the chosen set of platforms:

- Each platform defined in the ST has fundamentally the same type of external interfaces (power/status, management, data loading, LAN, WAN). Of these, only the following differences are relevant to the TSF:
  - Management port: includes both a serial console port and an RJ-45 port. Both types of management ports were tested as part of the evaluation process.
  - WAN port: includes a variety of different physical/data link layer interfaces for customer traffic. At layer 3 and 4, these interfaces all use TCP/IP which is the focus of the customer packet filtering tests (FPF_RUL_EXT.1).
- At least one of each of the three main series of platforms (819, 881, 891) was included in the sample.
- There are no differences in how the TSF is implemented between the different platforms. All PP-relevant security functionality is implemented equivalently in each platform.
- Each platform defined in the ST is using identical Cisco IOS software.

4.3 Test Environment

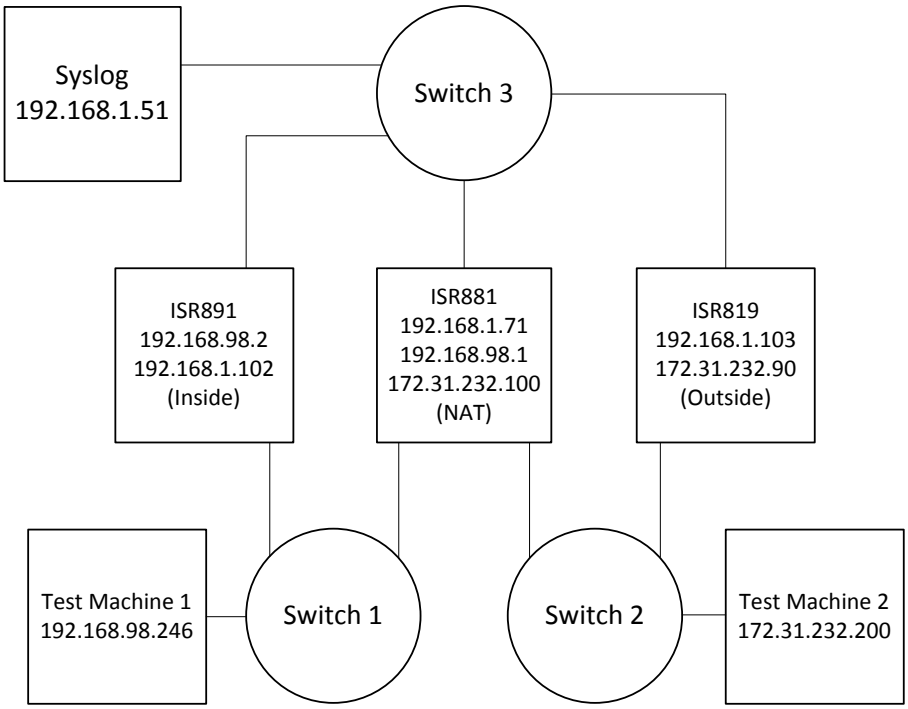
Testing was conducted as a combination of vendor test cases and evaluation team independent test cases. Separate test environments were used for the vendor test environment and the evaluation team test environment. However, each test environment was consistent with the evaluated configuration of the TOE in that they included remote VPN peers, additional Cisco ISR instances, CA server, syslog server, AAA server(s), and remote SSH terminal as needed to conduct the testing. Not all tests were performed in each environment so not all environmental components were required to be present. For example, the evaluation team conducted CA testing in the laboratory environment so there is no CA server in the vendor environment.

The following diagram depicts the vendor test environment:



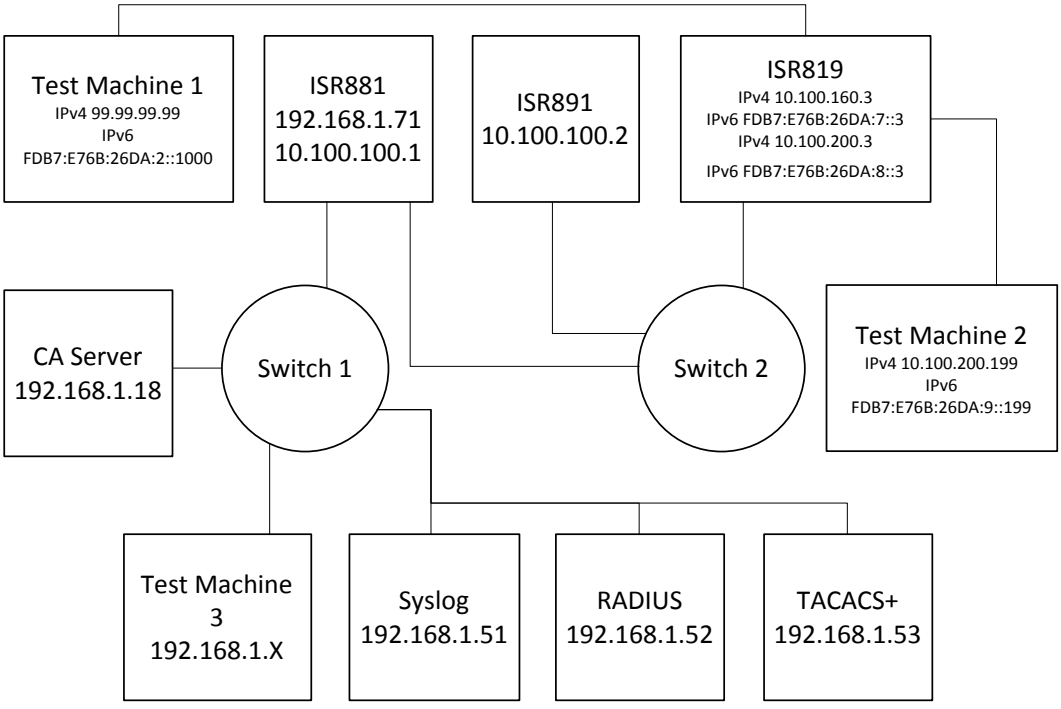
The following diagrams depict the laboratory environment. Note that network assets needed to be rearranged at points to accommodate different testing activities. The topology and IP addresses of some of the test systems will differ between configurations, but the same hardware is used throughout.

The following diagram depicts the network configuration used during the FCS_IPSEC_EXT.1 NAT traversal testing:

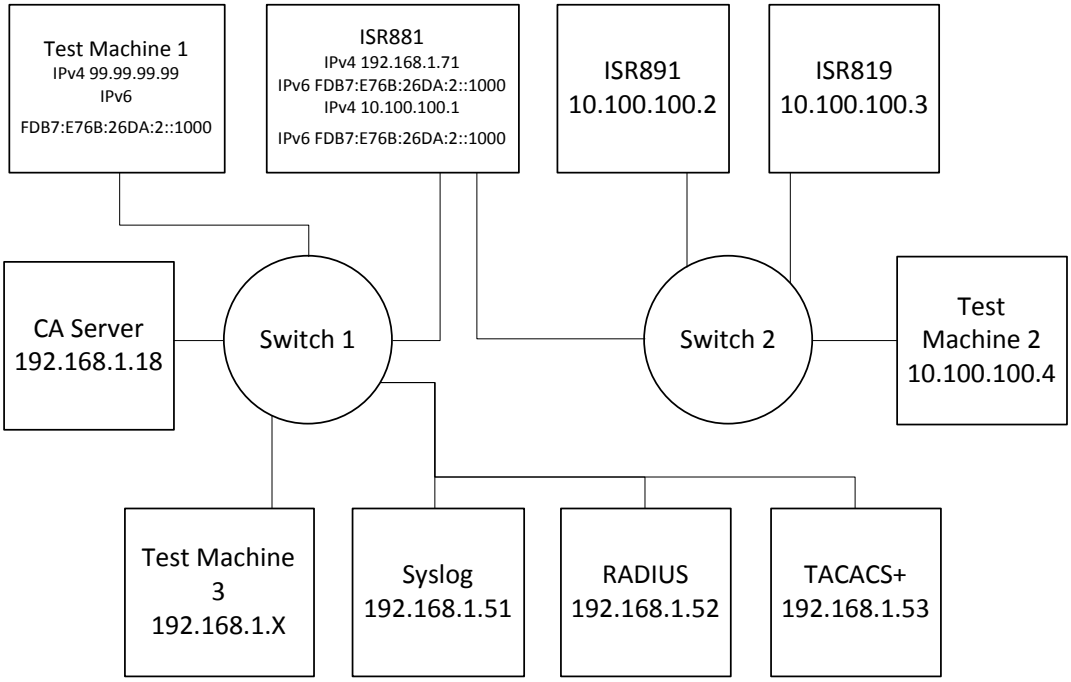


The following three diagrams depict the network configuration during the VPNGW extended package's AVA_VAN.1 assurance activity against each model of the TOE tested:

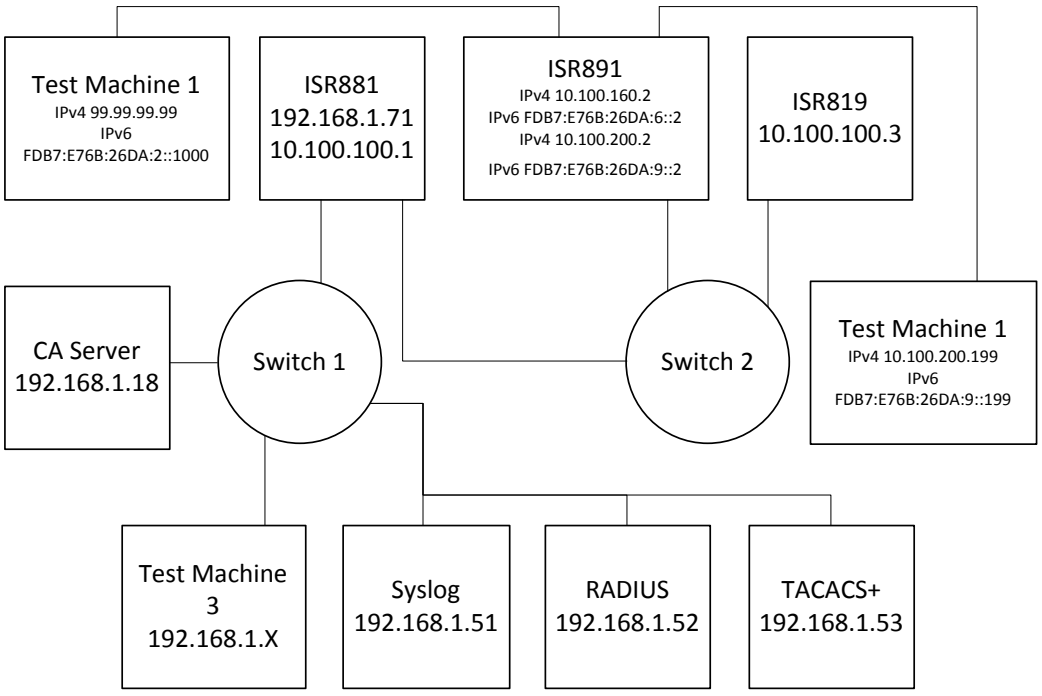
819 Diagram:



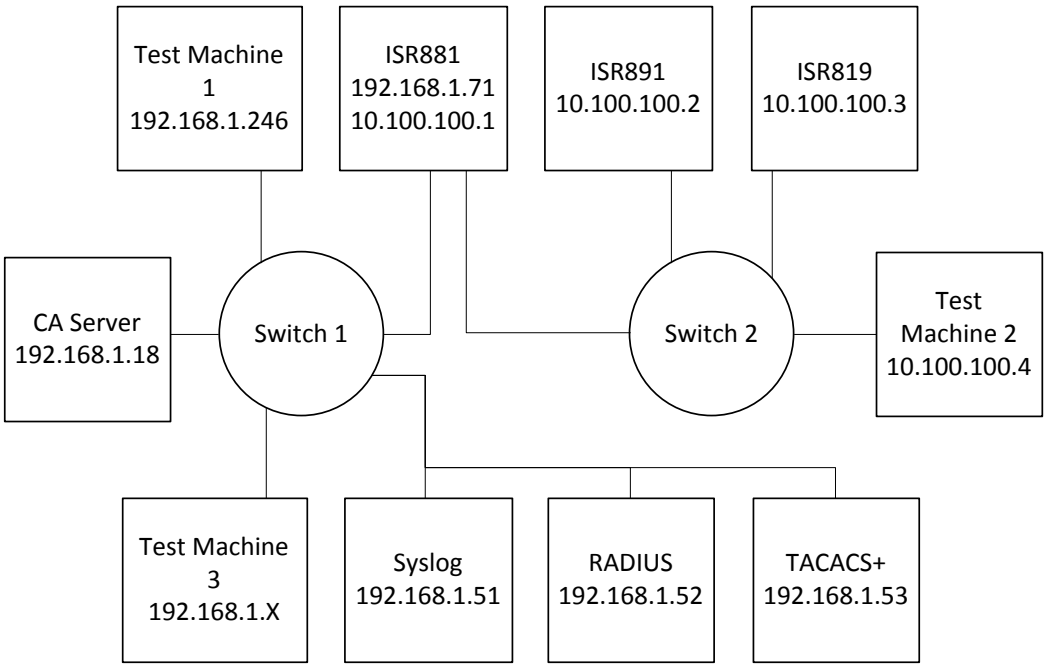
881 Diagram:



891 Diagram:



The following diagram depicts the network configuration used during the remainder of the laboratory manual testing:



4.4 Test Cases

The evaluation team completed the functional testing activities through a combination of functional testing within the laboratory environment and review of vendor test evidence gathered from the vendor environment. The evaluation team conducted and/or reviewed a set of testing that includes all ATE Assurance Activities as specified by the 'Protection Profile for Network Devices Version 1.1' (NDPP), 'Security Requirements for Network Devices Errata #2' (Errata), and 'NDPP Extended Package VPN Gateway Version 1.1' (VPN EP). The evaluators reviewed the NDPP, Errata, and VPN EP to identify the security functionality that must be verified through functional testing. This is prescribed by the Assurance Activities for each SFR.

If an SFR is not listed, one of the following conditions applies:

- The Assurance Activity for the SFR specifically indicates that it is simultaneously satisfied by completing a test Assurance Activity for a different SFR (e.g. FIA_X509_EXT.1).
- The Assurance Activity for the SFR does not specify any actions related to ATE activities (e.g. FPT_APW_EXT.1).

Note that some SFRs do not have Assurance Activities associated with them at the element level (e.g. FCS_SSH_EXT.1.1). In such cases, testing for the SFR is considered to be satisfied by completion of all Assurance Activities at the component level.

Also note that some SFRs list multiple different Assurance Activities in multiple references. The evaluators determined the proper Assurance Activity to use through the following process:

- If an Assurance Activity for the SFR was defined in the VPN EP, that Assurance Activity was used.
- If an Assurance Activity for the SFR was not defined in the VPN EP but was defined in the NDPP Errata, the NDPP Errata Assurance Activity was used.
- If an Assurance Activity for the SFR was only defined in the NDPP, that Assurance Activity was used.

The exception to this is where an Assurance Activity in the VPN EP clearly specifies testing for the portion of an SFR that applies just to the VPN EP (e.g. FAU_GEN.1 talking about only the auditing for packet

filtering). In these cases, the Assurance Activities from the VPN EP and NDPP (or NDPP Errata, as needed) are combined.

The following lists for each ATE Assurance Activity, the test objective, test instructions, test steps, and test results. This also indicates whether the test was executed by the vendor as part of their automated test harness and witnessed by the evaluation team or whether the test was executed manually by the evaluation team within the test laboratory.

Note that unless otherwise specified, the test configuration is to be in the evaluated configuration as defined by the OPE. Each copy of each Operational Environment item is expected to be present in at least one instance when a relevant SFR is tested so that every selection can be tested appropriately. For example, both a RADIUS and a TACACS+ server are expected to be present in the Operational Environment so that testing can validate that either of them can be used as a remote authentication server.

The administrator is expected to be logged in to the TOE as a precondition for executing each test unless the test is specifically related to the TOE's authentication function. Also note that by definition, some tests require the TOE to be brought out of the evaluated configuration (for example, temporarily disabling cryptography to prove that the context of transmitted data is accurate). Additionally, it is expected that verbose debugging is enabled prior to testing by following the steps in "Enable Verbose Debugging" below. Tests that involve the use of certificates for IPsec communication assume that a public key infrastructure to include a Certification Authority and Online Certificate Status Protocol Responder has been setup and configured. As part of the cleanup for each test, the TOE is returned to the evaluated configuration.

Each automated test script includes an echo of all commands used by the script to configure the TOE and execute the test. For any testing that was conducted by the laboratory against the 881 device, the evaluation team manually executed the test case by setting up a functionally equivalent environment and manually executing the commands that are relevant to executing the test (i.e. commands that sufficiently generate all evidence that is required by the assurance activity).

Enable Verbose Debugging	1. Login to the TOE via the CLI. 2. At the prompt type the following: debug crypto ikev2 debug crypto isakmp debug crypto ipsec debug crypto pki API debug crypto pki callbacks debug crypto pki messages debug crypto pki scep debug crypto pki server debug crypto pki transactions debug crypto pki validation configure terminal logging trap 7

4.4.1 Security Audit

Test Case Number	1
SFR	FAU_GEN.1 and FAU_GEN.2
Test Objective	The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in table 1 and administrative actions. This should include all instances of an event--for instance, if

	there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. For administrative actions, the evaluator shall test that each action determined by the evaluator above to be security relevant in the context of this PP is auditable. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.
Test Instructions	Execute this test after all other tests have been executed through review of log data
Test Steps	1. Type 'no logging on' 2. Type 'logging on' 3. Start up and shut down the TOE. 4. Review results of testing for each of the other SFRs that are associated with auditable events. 5. Review the log information to confirm that the events and associated management commands were audited.
Test Results	Pass
Execution Method	Manual/Automated

Test Case Number	2
SFR	FAU_GEN.1 and FAU_GEN.2
Test Objective	The following test is expected to execute outside the context of the other requirements. While testing the TOE's compliance against the SFRs, either specific tests are developed and run in the context of this SFR, or as is typically done, the audit capability is turned on while testing the TOE's behavior in complying to the other SFRs in this EP. Test 1: The evaluator shall attempt to flood the TOE with network packets such that the TOE will be unable to process all the packets. This may require the evaluator to configure the TOE to limit the bandwidth the TOE is capable to handling (e.g., use of a 10 MB interface).
Test Instructions	N/A
Test Steps	As stated in the TSS, the TOE's audit function occurs at a higher level of the processing stack than the network traffic handling. Therefore, when the TOE is flooded with an excessive amount of packets, it will not cause a denial of service of the TOE's processing because only packets that are successfully processed by the TSF will be logged.
Test Results	N/A
Execution Method	N/A

Test Case Number	3
SFR	FAU_STG_EXT.1
Test Objective	[TOE is not an audit server] The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.
Test Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Send logs over trusted channel and capture the output as being encrypted. 2. Disable encryption.

	3. Send logs over trusted channel and observe the correct log data is being transmitted in cleartext. 4. Re-enable encryption. 5. Send logs over trusted channel and capture the output as being encrypted.
Test Results	Pass
Execution Method	Automated

4.4.2 Cryptographic Security

In addition to the test cases listed below, the following SFRs have assurance activities that are expected to be performed against NIST-prescribed validation system documentation:

- FCS_CKM.1(1)
- FCS_CKM.1(2)
- FCS_COP.1(1)
- FCS_COP.1(2)
- FCS_COP.1(3)
- FCS_COP.1(4)
- FCS_RBG_EXT.1

For each of these SFRs, the testing requirements were satisfied by the vendor producing Cryptographic Algorithm Validation System (CAVP) certificates for the AES, 3DES, SHS, HMAC, RSA, ECDSA, and DRBG algorithm implementations used by the TOE's cryptographic module. Refer to the Security Target for the specific algorithm certificates. Refer to the CAVP validation lists for each of the above algorithms for the key sizes, modes, and other permutations that were tested for each algorithm. In each case, the set of validated algorithms include those used by the TOE in the evaluated configuration.

Test Case Number	4
SFR	FCS_IPSEC_EXT.1
Test Objective	The evaluator shall configure the TOE's SPD such that there is a rule for DISCARD, BYPASS, PROTECT. The selectors used in the construction of the rule shall be different such that the evaluator can send in three network packets with the appropriate fields in the packet header that each packet will match one of the three rules. The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packet was dropped, allowed through without modification, was encrypted by the IPsec implementation.
Test Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Configure the access-list to deny some traffic (DISCARD). 2. Configure the crypto map to deny some traffic that isn't denied by the access-list (BYPASS). 3. Configure the crypto map to allow some traffic that isn't denied by the access-list (PROTECT). 4. Transmit traffic matching each of these three characteristics through the TOE. 5. Observe via packet captures and audit logs that traffic matching the DISCARD element is dropped, traffic matching the BYPASS element is transmitted in the clear, and traffic matching the PROTECT element is transmitted using ESP.
Test Results	Pass
Execution Method	Automated

Test Case Number	5
SFR	FCS_IPSEC_EXT.1
Test 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 Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Create an SPD entry that has a PROTECT rule for a set of traffic before a BYPASS rule for the same set of traffic. 2. Transmit traffic matching these characteristics through the appropriate interface. 3. Observe via packet captures and audit logs that the traffic is encrypted using ESP. 4. Observe via TSF status that the tunnel has been established with the remote peer via the existence of the QM_IDLE state for the tunnel. 5. Terminate the tunnel and reverse the SPD entry defined in step 1. 6. Transmit the traffic from step 2. 7. Observe that the traffic is transmitted in the clear and that no tunnel with the remote peer has been established.
Test Results	Pass
Execution Method	Automated

Test Case Number	6
SFR	FCS_IPSEC_EXT.1
Test Objective	The evaluator shall repeat the procedure above, except that the two entries should be devised where one is a subset of the other (e.g., a specific address vs. a network segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.
Test Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Repeat test 5 with the following changes: a. In step 1, associate the PROTECT rule with a network segment that includes the traffic to be transmitted and the BYPASS rule with the exact source/destination address of the traffic. b. In step 5, associate the BYPASS rule with a network segment that includes the traffic to be transmitted and the PROTECT rule with the exact source/destination address of the traffic.
Test Results	Pass
Execution Method	Automated

Test Case Number	7
SFR	FCS_IPSEC_EXT.1
Test Objective	(conditional): If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE in tunnel mode, and a TOE peer in tunnel mode. The evaluator configures the two peer TOEs 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 session between the peers. The evaluator observes in the audit trail and the captured packets that a successful connection was established using the tunnel mode.
Test Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Configure tunnel mode connection on TOE to use pre-shared key, AES-256, ESP-AES AES-ESP-SHA transform, and DH group 14. 2. Configure crypto map that defines peer as tunnel endpoint 3. Configure tunnel mode connection on peer with same properties. 4. Send a ping from TOE to peer, observe successful result, logging of tunnel establishment, and packet capture of ESP traffic.
Test Results	Pass
Execution Method	Automated

Test Case Number	8
SFR	FCS_IPSEC_EXT.1
Test Objective	(conditional): If transport mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in transport mode when it receives packets from the VPN client. The evaluator configures the TOE and VPN client to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection with the TOE using the VPN client. The evaluator observes in the audit trail and the captured packets that a successful connection was established using the transport mode.
Test Instructions	Execute the Test Steps and observe the packet capture and syslog outputs.
Test Steps	1. Configure transport mode connection on the TOE for the transform set that is applied to the cryptomap being used for IPsec communication. 2. Configure a crypto map that defines the peer as the tunnel endpoint. 3. Configure the tunnel mode connection on the peer with the same properties.
Test Results	Pass
Execution Method	Manual

Test Case Number	9
SFR	FCS_IPSEC_EXT.1
Test Objective	The evaluator shall configure the TOE's SPD, such that it has entries that contain operations that DISCARD, BYPASS, and PROTECT network packets. The evaluator also configures the TOE so that all auditable events with respect to FCS_IPSEC_EXT.1 are enabled. 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 to the TOE. The evaluator should observe that the network packet is passed by the TOE to the proper destined 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 to the TOE, and observes that the packet was not permitted to flow to any of the TOE's interfaces. The evaluator shall verify that an audit record is generated that specifies that the packet was discarded as expected.
Test Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Create the same SPD that was used for test 5 but ensure the 'log' parameter has been applied to each entry. 2. Send traffic through the TOE that matches the BYPASS characteristics. 3. Observe that the traffic is transmitted in the clear and logged. 4. Send traffic through the TOE that doesn't match any of the entries in the SPD. 5. Observe that the traffic is dropped and logged.
Test Results	Pass
Execution Method	Automated

Test Case Number	10
SFR	FCS_IPSEC_EXT.1
Test Objective	The evaluator shall configure the TOE as indicated in the operational guidance configuring the TOE to using each of the AES-GCM-128, and AES-GCM-256 algorithms, and attempt to establish a connection using ESP in confidentiality and integrity mode. If the ST Author has selected either AES-CBC-128 or AES-CBC-256, the TOE is configured to use those algorithms and the evaluator attempts to establish a connection using ESP in confidentiality and integrity mode for those algorithms selected.

Test Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Configure ESP to use AES-GCM-128. 2. Configure IKE to use AES-CBC-128. 3. Clear the SAs to verify that there is no active SA with the peer. 4. Capture traffic from a point between the TOE and the peer. 5. Send a ping from the TOE to the peer. 6. Observe that the ping was successful. 7. Stop the packet capture. 8. Review the audit log to determine that a connection was established using the desired algorithm. 9. Review the packet capture to confirm that ESP traffic was sent between the TOE and peer. 10. Repeat steps 1-9 for each other supported ESP algorithm. For AES-CBC algorithms, additionally ensure that an appropriate integrity algorithm (as defined by the ST) is chosen.
Test Results	Pass
Execution Method	Automated

Test Case Number	11
SFR	FCS_IPSEC_EXT.1
Test Objective	The evaluator shall configure the TOE 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 Instructions	Execute the steps described below and review the captured network packets for adherence to RFC 5996, section 2.23 (NAT Traversal).
Test Steps	1. Configure the TOE so that it will perform NAT traversal processing by entering the following commands: config terminal interface <inside-facing-interface> ip nat inside interface <outside-facing-interface> ip nat outside exit ip nat inside source list <ACL-number> interface <outside-facing-interface> overload ip nat service list <ACL-number> ESP spi-match access-list <ACL-number> permit <protocol> <local-range-address(es)> <remote-range-address(es)> end 2. Configure the IPsec peer endpoints to perform SPI matching: config terminal crypto ipsec nat-transparency spi-matching end 3. Configure an IPsec IKEv2 policy, proposal, and crypto map as appropriate on both peer endpoints. 4. On both the inside and outside facing peers, enter the following commands to clear any existing connections: clear crypto isakmp clear crypto ikev2 sa clear crypto sa 5. Begin capturing network packets between the inside peer and the TOE's inside facing interface and between the outside peer and the TOE's outside facing interface. 6. On the inside facing peer, initiate an IPsec connection to the outside facing peer by entering the following commands:

	ping <outside-facing-peer IP address> 7. Stop capturing network packets. 8. Examine the captured network packets for adherence to RFC 5996, section 2.23 (NAT Traversal).
Test Results	Pass
Execution Method	Manual

Test Case Number	12
SFR	FCS_IPSEC_EXT.1
Test Objective	The evaluator shall configure the TOE to use AES-CBC-128 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 AES-CBC-128. The evaluator will consult the audit trail to confirm the algorithm was that used in the negotiation.
Test Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Configure the TOE and peer to use IKEv1. 2. Configure IKEv1 to use AES-CBC-128. 3. Clear the SAs to verify that there is no active SA with the peer. 4. Capture traffic from a point between the TOE and the peer. 5. Send a ping from the TOE to the peer. 6. Observe that the ping was successful. 7. Stop the packet capture. 8. Review the audit log to determine that a connection was established using the desired algorithm. 9. Review the packet capture to confirm that the first ISAKMP packet sent out by the TOE includes the desired algorithm in the proposal. 10. Repeat steps 1-9 for IKEv2.
Test Results	Pass
Execution Method	Automated

Test Case Number	13
SFR	FCS_IPSEC_EXT.1
Test Objective	(conditional): The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported. This test is not applicable if IKEv1 is not selected above in the FCS_IPSEC_EXT.1.5 protocol selection.
Test Instructions	Executed automated test and observe output on TOE and peer router.
Test Steps	1. Configure the TOE using the 'crypto isakmp aggressive-mode disable' command shown in the AGD to disable aggressive mode. 2. Configure peer router to use aggressive mode. 3. Attempt to ping the TOE using the peer router and observe failure. 4. Reconfigure peer router to use main mode. 5. Attempt to ping the TOE using the peer router and observe success.
Test Results	Pass
Execution Method	Automated

Test Case Number	14
SFR	FCS_IPSEC_EXT.1
Test Objective	When testing this, the evaluator needs to ensure that both sides are configured appropriately. From the RFC "A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends

	have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered." Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection: The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is closed.
Test Instructions	Executed automated test and observe output on TOE and peer router.
Test Steps	1. Configure an IKEv1 Phase 1 lifetime to be 24 hours. 2. Establish connection with peer. 3. Over the next 24 hours, periodically transmit pings over the peer connection to verify that connection remains active. 4. At some point more than 24 hours after step 2 was completed, review the TOE's audit logs and determine that the SA was re-keyed exactly 24 hours after the logs show the initial establishment of the SA. 5. Configure a Phase 2 lifetime to be 8 hours. 6. Over the next 8 hours, periodically transmit pings over the peer connection to verify that connection remains active. 7. At some point more than 8 hours after step 5 was completed, review the TOE's audit logs and determine that the SA was re-keyed exactly 8 hours after the logs show the initial establishment of the SA. 8. Repeat steps 1 through 7 with the following substitutions: a. Use arbitrary traffic amounts (kB) instead of time values as the threshold for re-keying. b. Instead of sending periodic pings over the channel to verify that it is active, use a traffic generator to send a known volume of traffic greater than the re-keying threshold. c. When reviewing the logs, verify the re-keying occurs during the transmission of the known volume of traffic. It is not necessary to verify the timestamp of the re-keying event in this case. 9. Repeat steps 1 through 8 for IKEv2 SAs (the Phase 2 SA is expected to be implemented independently of the version of IKE to be used but the test should be repeated regardless).
Test Results	Pass
Execution Method	Automated

Test Case Number	15
SFR	FCS_IPSEC_EXT.1
Test Objective	When testing this, the evaluator needs to ensure that both sides are configured appropriately. From the RFC "A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered." Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection: 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 Instructions	Execute automated test and observe output on TOE and peer router.
Test Steps	1. Refer to test 14. The TOE does not implicitly define a maximum timeout period for Phase 1 SAs. As specified in the AGD, it is necessary to explicitly configure the timeout value to be 24 hours or less if this functionality is intended. Therefore, test 14 demonstrates the ability of the TOE both to perform re-keying after an arbitrarily-defined time period and that the SA can be re-keyed in at most 24 hours.
Test Results	Pass
Execution Method	Automated

Test Case Number	16
SFR	FCS_IPSEC_EXT.1
Test Objective	When testing this, the evaluator needs to ensure that both sides are configured appropriately. From the RFC "A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered." Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection: 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 Instructions	Execute automated test and observe output on TOE and peer router.
Test Steps	1. Refer to test 14. The TOE does not implicitly define a maximum timeout period for Phase 1 SAs. As specified in the AGD, it is necessary to explicitly configure the timeout value to be 8 hours or less if this functionality is intended. Therefore, test 14 demonstrates the ability of the TOE both to perform re-keying after an arbitrarily-defined time period and that the SA can be re-keyed in at most 8 hours.
Test Results	Pass
Execution Method	Automated

Test Case Number	17
SFR	FCS_IPSEC_EXT.1
Test Objective	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 Instructions	Execute automated test script and review console output and packet capture.
Test Steps	1. Configure the TOE to negotiate a DH group 14 connection for IKEv1 and IKEv2. 2. Observe via packet capture that the connection was successful. 3. Repeat steps 1 and 2 for group 15. 4. Repeat steps 1 and 2 for group 16. 5. Repeat steps 1 and 2 for group 19. 6. Repeat steps 1 and 2 for group 20. 7. Repeat steps 1 and 2 for group 24.
Test Results	Pass
Execution Method	Automated

Test Case Number	18
SFR	FCS_IPSEC_EXT.1
Test Objective	The following test shall be repeated for each peer authentication protocol selected in the FCS_IPSEC_EXT.1.12 selection: The evaluator shall have the TOE generate a public-private key pair, and submit a CSR (Certificate Signing Request) to a CA (trusted by both the TOE 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.
Test Instructions	Follow the manual procedures defined in vendor test plan. TOE/peer/CA configuration is based on duplicating the initial settings for each device shown in the test plan and is performed by following the configuration instructions defined in the AGD. This test is to be done with an RSA algorithm and an ECDSA algorithm for the cryptographic signature of the certificates used in this test.
Test Steps	1. Use the TOE to generate a key pair using RSA. 2. Generate a CSR on the TOE using this key pair and submit to CA. 3. On the CA, verify that the CSR was received and that DN information was included with it. 4. Repeat steps 1-3 using ECDSA for the method of key pair generation.
Test Results	Pass
Execution Method	Manual

Test Case Number	19
SFR	FCS_IPSEC_EXT.1
Test Objective	The following test shall be repeated for each peer authentication protocol selected in the FCS_IPSEC_EXT.1.12 selection: The evaluator shall use a certificate signed using the RSA or ECDSA algorithm to authenticate the remote peer during the IKE exchange. This test ensures the remote peer has the certificate for the trusted CA that signed the TOE's certificate and it will do a bit-wise comparison on the DN. This bit-wise comparison of the DN ensures that not only does the peer have a certificate signed by the trusted CA, but the certificate is from the DN that is expected. The evaluator will configure the TOE to associate a certificate (e.g., a certificate map in some implementations) with a VPN connection. This is what the DN is checked against.
Test Instructions	Follow the manual procedures defined in vendor test plan. TOE/peer/CA configuration is based on duplicating the initial settings for each device shown in the test plan and is performed by following the configuration instructions defined in the AGD. This test is to be done with an RSA algorithm and an ECDSA algorithm for the cryptographic signature of the certificates used in this test.
Test Steps	1. Use the CA to issue a certificate for the TOE that is signed using RSA. 2. Use the TOE to establish a tunnel with the remote peer. 3. On the remote peer, use the logs to verify that the TOE's certificate was used to allow the tunnel to be established. 4. Repeat steps 1-3 using ECDSA as the certificate signing method.
Test Results	Pass
Execution Method	Manual

Test Case Number	20
SFR	FCS_IPSEC_EXT.1
Test Objective	The following test shall be repeated for each peer authentication protocol selected in the FCS_IPSEC_EXT.1.12 selection: The evaluator shall test that the TOE 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 EP, 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 will not establish an SA.
Test Instructions	Follow the manual procedures defined in vendor test plan. TOE/peer/CA configuration is based on duplicating the initial settings for each device shown in the test plan and is performed by following the configuration instructions defined in the AGD.
Test Steps	1. Log in to the TOE. 2. Configure the TOE to perform CRL checking. 3. Clear any SAs that exist on the TOE and peer. 4. Use the TOE to ping the peer. 5. Observe and capture audit logs on both the TOE and peer to confirm that a security association was established (IPsec VPN). 6. On the Certification Authority, revoke the peer's certificate. 7. On the TOE, repeat steps 3 and 4. 8. Observe and capture audit logs on both the TOE and peer to confirm that a security association was NOT established (IPsec VPN). 9. Repeat steps 2-8 with OCSP being used instead of a CRL.
Test Results	Pass
Execution Method	Manual

Test Case Number	21
SFR	FCS_IPSEC_EXT.1
Test Objective	The following test shall be repeated for each peer authentication protocol selected in the FCS_IPSEC_EXT.1.12 selection: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.
Test Instructions	Follow the manual procedures defined in vendor test plan. TOE/peer/CA configuration is based on duplicating the initial settings for each device shown in the test plan and is performed by following the configuration instructions defined in the AGD.
Test Steps	1. Alter the CA certificate such that the basicConstraints extension is missing from it. 2. Use the TOE to attempt to validate the certificate path and observe that this fails because the CA certificate is not valid. 3. Revert the CA certificate to its original condition.
Test Results	Pass
Execution Method	Manual

Test Case Number	22
SFR	FCS_IPSEC_EXT.1
Test Objective	The following test shall be repeated for each peer authentication protocol selected in the FCS_IPSEC_EXT.1.12 selection:

	The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension not set. The validation of the certificate path fails.
Test Instructions	Follow the manual procedures defined in vendor test plan. TOE/peer/CA configuration is based on duplicating the initial settings for each device shown in the test plan and is performed by following the configuration instructions defined in the AGD.
Test Steps	1. Alter the CA certificate such that the cA flag in the basicConstraints extension is not set. 2. Use the TOE to attempt to validate the certificate path and observe that this fails because the CA certificate is not valid. 3. Revert the CA certificate to its original condition.
Test Results	Pass
Execution Method	Manual

Test Case Number	23
SFR	FCS_IPSEC_EXT.1
Test Objective	The following test shall be repeated for each peer authentication protocol selected in the FCS_IPSEC_EXT.1.12 selection: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.
Test Instructions	Follow the manual procedures defined in vendor test plan. TOE/peer/CA configuration is based on duplicating the initial settings for each device shown in the test plan and is performed by following the configuration instructions defined in the AGD.
Test Steps	1. Ensure the CA certificate is defined such that the cA flag in the basicConstraints extension is present and set to TRUE. 2. Use the TOE to attempt to validate the certificate path and observe that this succeeds.
Test Results	Pass
Execution Method	Manual

Test Case Number	24
SFR	FCS_IPSEC_EXT.1
Test Objective	The following test shall be repeated for each peer authentication protocol selected in the FCS_IPSEC_EXT.1.12 selection: The evaluator shall test that given a signed certificate from a trusted CA, that when the DN does not match – any of the four fields can be modified such that they do not match the expected value, that an SA does not get established.
Test Instructions	Follow the manual procedures defined in vendor test plan. TOE/peer/CA configuration is based on duplicating the initial settings for each device shown in the test plan and is performed by following the configuration instructions defined in the AGD.
Test Steps	1. Alter the certificate issued to the TOE such that some aspect of the DN is mismatched with what is expected on the peer's expected DN list. 2. Use the TOE to attempt to establish a tunnel with the peer and observe that it fails because the DN in the TOE certificate does not match any of the entries in peer's expected DN list. 3. Revert the certificate issued to the TOE to its original condition.
Test Results	Pass
Execution Method	Manual

Test Case Number	25
SFR	FCS_IPSEC_EXT.1
Test Objective	The following test shall be repeated for each peer authentication protocol selected in the FCS_IPSEC_EXT.1.12 selection: 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 Instructions	Follow the manual procedures defined in vendor test plan. TOE/peer/CA configuration is based on duplicating the initial settings for each device shown in the test plan and is performed by following the configuration instructions defined in the AGD.
Test Steps	1. Ensure both the TOE and peer each have valid certificates for each other signed by the CA. 2. Bring the CA offline. 3. Set the TOE and peer to use the no certificate revocation check setting. 4. Clear any SAs on the TOE and peer. 5. Attempt to establish a tunnel and observe it succeeds. 6. Repeat steps 3 and 4 with the 'revocation-check crl' setting applied and observe the tunnel is not established. 7. Repeat steps 3 and 4 with the 'revocation-check ocsp' setting applied and observe the tunnel is not established.
Test Results	Pass
Execution Method	Manual

Test Case Number	26
SFR	FCS_IPSEC_EXT.1
Test Objective	This test shall be performed for each version of IKE supported by the TOE. The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.
Test Instructions	Execute test script and review log data
Test Steps	1. Configure and establish an IPsec connection using IKEv1. 2. Alter the configuration of this connection to use each algorithm and hash function defined in the ST and ensure that each connection can be successfully established. 3. Repeat each connection type for IKEv2 where applicable.
Test Results	Pass
Execution Method	Automated

Test Case Number	27
SFR	FCS_IPSEC_EXT.1
Test Objective	This test shall be performed for each version of IKE supported by the TOE. The evaluator shall attempt to establish an SA for ESP that selects an encryption algorithm with more strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.
Test Instructions	Execute test script and review console output/log data.
Test Steps	1. Perform a modified version of test 10 that specifies AES-CBC-256 for the ESP algorithm and AES-CBC-128 for the IKE algorithm. 2. Observe that when a ping is sent to the peer, it is not successfully

	transmitted. 3. Review the audit logs to determine that the SA failed to be established.
Test Results	Pass
Execution Method	Automated

Test Case Number	28
SFR	FCS_IPSEC_EXT.1
Test Objective	This test shall be performed for each version of IKE supported by the TOE. 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 Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Perform the steps of test 12 with a prohibited algorithm (such as DES) instead of AES-CBC-128. 2. Observe via failed pings, packet captures, and log data that the SA was not successfully established.
Test Results	Pass
Execution Method	Automated

Test Case Number	29
SFR	FCS_IPSEC_EXT.1
Test Objective	This test shall be performed for each version of IKE supported by the TOE. 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 Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Perform the steps of test 12 with a prohibited algorithm (such as AES-CBC-192). 2. Observe via failed pings, packet captures, and log data that the SA was not successfully established.
Test Results	Pass
Execution Method	Automated

Test Case Number	30
SFR	FCS_SSH_EXT.1
Test Objective	The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection. Any configuration activities required to support this test shall be performed according to instructions in the operational guidance.
Test Instructions	Execute test script and review packet captures/log data.
Test Steps	As a pre-requisite to this test, ensure that a public key is generated for the SSH user that is used to conduct this test. 1. Copy the remote user's public key to the TOE. 2. Add this key to the TOE for key-based authentication of that remote user. 3. Ensure the known_hosts file is deleted so that there is no pre-existing connection data to disrupt the accuracy of the results. 4. Attempt to perform key-based authentication with a user other than the one mapped in step 2 and observe that login fails. 5. Verify on the TOE that failed authentication is logged. 6. Establish an SSH connection using the user account mapped in step 2 with their corresponding local key. 7. Observe that login is successful. 8. Verify on the TOE that successful authentication is logged.
Test Results	Pass
Execution Method	Automated

Test Case Number	31
SFR	FCS_SSH_EXT.1
Test Objective	Using the operational guidance, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that a user can be successfully authenticated to the TOE over SSH using a password as an authenticator.
Test Instructions	Execute test script and review packet captures/log data.
Test Steps	1. On the TOE, define a local password for a user. 2. On the SSH client system, attempt to log in with that user's username and an incorrect password. 3. Observe that authentication fails and that the failure is logged. 4. Repeat step 2 with the correct password. 5. Observe that authentication succeeds and that the success is logged.
Test Results	Pass
Execution Method	Automated

Test Case Number	32
SFR	FCS_SSH_EXT.1
Test Objective	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
Test Instructions	Execute the steps described below and review the packet capture data to ensure that excessively large SSH packets are dropped.
Test Steps	1. Open Wireshark on the test system and begin packet capture. 2. Initiate a connection to the TOE by running scapy and executing the following commands: from scapy.all import * s=socket.socket() s.connect((“TOE_IP_Address”,22)) ss=StreamSocket(s,Raw) ss.sr1(Raw(“SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1\r\n”)) ss.sr1(Raw(RandString(size=35001))) 3. Stop Wireshark packet capture. 4. Analyze Wireshark packet capture for TCP [RST] responses to the test system from the TOE.
Test Results	Pass
Execution Method	Manual

Test Case Number	33
SFR	FCS_SSH_EXT.1
Test Objective	The evaluator shall establish a SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.
Test Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Enable packet capturing on the SSH client system. 2. Execute an SSH login using a valid username/password combination while specifying to the SSH client that AES-CBC-128 be used. 3. Observe that authentication was successful. 4. Stop packet capturing on the SSH client system. 5. Review the packet capturing and observe that AES-CBC-128 was agreed upon in the SSH handshake. 6. Repeat steps 1-5 using AES-CBC-256.
Test Results	Pass
Execution Method	Automated

Test Case Number	34

SFR	FCS_SSH_EXT.1
Test Objective	The evaluator shall establish a SSH connection using each of the integrity algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.
Test Instructions	Execute test script/manually initiate an SSH connection and review packet captures
Test Steps	1. Enable packet capturing on the SSH client system. 2. Execute an SSH login using any username/password combination while specifying to the SSH client that HMAC-SHA1 be used. 3. Observe that the SSH connection was opened by the client either accepting (if valid credentials) or rejecting (if invalid credentials) the login attempt. Note that depending on the TOE's configuration for other tests, a warning banner might alternatively be displayed first; this is also acceptable. 4. Stop packet capturing on the SSH client system. 5. Review the packet capturing and observe that HMAC-SHA1 was agreed upon in the SSH handshake. 6. Repeat steps 1-5 using HMAC-SHA1-96.
Test Results	Pass
Execution Method	Automated, Manual

Test Case Number	35
SFR	FCS_SSH_EXT.1
Test Objective	The evaluator shall attempt to perform a diffie-hellman-group1-sha1 key exchange, and observe that the attempt fails. For each allowed key exchange method, T the evaluator shall then attempt to perform a key exchange using that method, and observe that the attempt succeeds.
Test Instructions	Execute test script and review packet captures/log data.
Test Steps	1. Configure the TOE such that the minimum accepted modulus size is 2048 bits (this will disallow DH group 1) 2. Execute an SSH login using a valid username/password combination while specifying to the SSH client that diffie-hellmnan-group1-sha1 be used. 3. Observe that a password prompt is not echoed because the SSH trusted path cannot be established. 4. Review the audit log data and observe a "no matching kex algorithm found" message is present in the logs. 5. Execute an SSH login using a valid username/password combination while specifying to the SSH client that diffie-hellmnan-group14-sha1 be used. 6. Observe that authentication is successful and that the TOE logs the authentication event.
Test Results	Pass
Execution Method	Automated

4.4.3 User Data Protection

There are no ATE Assurance Activities for any SFRs in this class.

4.4.4 Identification and Authentication

Test Case Number	36
SFR	FIA_AFL.1
Test Objective	The evaluator shall perform the following tests for IPsec, and for each other method by which remote administrators access the TOE (e.g., TLS, SSH): The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE. The evaluator shall test that once the limit is reached, attempts with valid credentials are not successful. For each action specified by the requirement, the evaluator shall show

	that following the operational guidance and performing each action to allow the remote administrator access are successful.
Test Instructions	Execute the test steps with the TOE configured to use local username/password authentication – when a remote authentication server is used to validate administrator credentials instead of the TSF, administrator lockout is the responsibility of the authentication server. Verify the test results using console output and system logs.
Test Steps	1. Configure a maximum number of authentication failures using the 'aaa local authentication attempts max-fail' command. 2. Have an administrator enter invalid passwords a number of times equal to the value of the max-fail setting. 3. Enter the administrator's password correctly and observe authentication is rejected because the failure threshold was exceeded. 4. Unlock the administrator's account. 5. Repeat step 3 but observe that authentication is now successful.
Test Results	Pass
Execution Method	Manual

Test Case Number	37
SFR	FIA_AFL.1
Test Objective	The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE and a time period after which valid logins will be allowed for a remote administrator. After exceeding the specified number of invalid login attempts and showing that valid login is not possible, the evaluator shall show that waiting for the interval defined by the time period before another access attempt will result in the ability for the remote administrator to successfully log on using valid credentials.
Test Instructions	N/A – the selection for time-based lockout was not chosen in the Security Target.
Test Steps	N/A – the selection for time-based lockout was not chosen in the Security Target.
Test Results	Pass
Execution Method	N/A

Test Case Number	38
SFR	FIA_PMG_EXT.1
Test Objective	The evaluator shall compose passwords that either meet the requirements, or fail to meet the requirements, in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, rule characteristics, and a minimum length listed in the requirement are supported, and justify the subset of those characters chosen for testing.
Test Instructions	Verify the test results using console output and system logs.
Test Steps	1. Set the minimum password length to be 15 characters. 2. Define a series of username/password combinations such that at least one of each supported character is included in at least one password. 3. Observe that each of these passwords can be set and used to log in to the TOE. 4. Repeat step 2 but use a 15-character password that contains a disallowed character (such as '?') and observe that the password cannot be set to the desired value. 5. Repeat step 2 but use an arbitrary 14-character password composed entirely of allowed characters and observe that the password cannot be set to the desired value.
Test Results	Pass
Execution Method	Manual

Test Case Number	39
SFR	FIA_PSK_EXT.1
Test Objective	The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case. The evaluator shall compose a pre-shared key of 22 characters that contains a combination of the allowed characters in accordance with the operational guidance, and demonstrates that a successful protocol negotiation can be performed with the key.
Test Instructions	Repeat the steps defined in the vendor's automated test script with modifications to the actual pre-shared key value.
Test Steps	1. Configure the IPsec protocol to use a 22-character pre-shared key that contains at least one of each supported character type, such as 12345!@#$%ABCDEFabcdef. 2. Observe that a connection to the peer can be successfully established.
Test Results	Pass
Execution Method	Manual

Test Case Number	40
SFR	FIA_PSK_EXT.1
Test Objective	[conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and an invalid length. The minimum and maximum length tests should be successful, and the invalid length must be rejected by the TOE.
Test Instructions	Repeat the steps defined in the vendor's automated test script with modifications to the actual pre-shared key value.
Test Steps	1. The minimum key length is 22 characters and was therefore addressed by Test 39. 2. Repeat Test 39 with a 127-character key that includes at least one of each supported character and observe the connection is successful. 3. Repeat Test 39 with an arbitrary 128-character key and observe that the connection is not successful.
Test Results	Pass
Execution Method	Manual

Test Case Number	41
SFR	FIA_PSK_EXT.1
Test Objective	[conditional]: If the TOE does not generate bit-based pre-shared keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.
Test Instructions	Repeat the steps defined in the vendor's automated test script with modifications to the actual pre-shared key value.
Test Steps	1. Generate a bit-based pre-shared key and import it into both the TOE and the IPsec peer. 2. Observe that a connection can be successfully established.
Test Results	Pass
Execution Method	Manual

Test Case Number	42
SFR	FIA_PSK_EXT.1
Test Objective	[conditional]: If the TOE does generate bit-based pre-shared keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it

	according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.
Test Instructions	N/A – The TOE only consumes bit-based pre-shared keys and does not generate them. Therefore this conditional test does not apply and was not executed.
Test Steps	N/A – The TOE only consumes bit-based pre-shared keys and does not generate them. Therefore this conditional test does not apply and was not executed.
Test Results	Pass
Execution Method	N/A

Test Case Number	43
SFR	FIA_UIA_EXT.1 and FIA_UAU_EXT.2
Test Objective	The evaluator shall use the operational guidance to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.
Test Instructions	Execute test script and review console and log data
Test Steps	1. Execute tests 30 and 31 to validate the ability of the TSF to process SSH public key and local password authentication. 2. Configure the TOE to use RADIUS authentication. 3. Provide valid and invalid RADIUS credentials to the TOE and observe expected results occur. 4. Repeat steps 2 and 3 for TACACS+ authentication.
Test Results	Pass
Execution Method	Automated

Test Case Number	44
SFR	FIA_UIA_EXT.1 and FIA_UAU_EXT.2
Test Objective	The evaluator shall configure the services allowed (if any) according to the operational guidance, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.
Test Instructions	Execute test script and perform manual test while observing console output
Test Steps	1. Manually attempt to establish a connection to the TOE's admin interface via remote SSH. Observe that a warning banner is displayed prior to the password being entered and that the only data that can be entered are user credentials (i.e. other TSF-mediated functions are not accepted). 2. Execute the automated test script and observe that in addition to requiring authentication to the TOE itself, the TSF must be brought into enable mode in order for other TSF-mediated actions to be performed.
Test Results	Pass
Execution Method	Automated/Manual

Test Case Number	45
SFR	FIA_UIA_EXT.1 and FIA_UAU_EXT.2
Test Objective	For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.
Test Instructions	Execute test script and perform manual test while observing console output
Test Steps	1. Repeat test 44 with local console instead of remote SSH.
Test Results	Pass
Execution Method	Automated/Manual

Test Case Number	46
SFR	FIA_UAU.7

Test Objective	The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.
Test Instructions	Execute test script and observe console output
Test Steps	1. Establish a local connection to the TOE and provide administrative credentials. 2. Observe that when the script populates the password field, no characters are echoed to the console.
Test Results	Pass
Execution Method	Automated

4.4.5 Security Management

The ATE assurance activities for this class are described in the NDPP and VPNGWEP as being implicitly satisfied through the execution of other testing. Therefore, there are no independent assurance activities for this class.

4.4.6 Packet Filtering

Test Case Number	47
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be directed at the TOE's interfaces, with packet sniffers listening to see if any network traffic is allowed through.
Test Instructions	Execute test steps based on AGD setup instructions. Review test system output and TOE audit logs.
Test Steps	1. Define and apply packet filtering rule such that ICMP traffic originating from the test system's IP address will be rejected. 2. Restart the TOE. 3. While the TOE is booting, send steady traffic to a destination through the TOE using the 'ping –t' command. 4. Observe that the pings are all timing out. 5. Stop sending the traffic before the TOE has finished booting. 6. When the TOE has finished booting, review the audit logs and verify that the rejected traffic from step 4 is not present (i.e. the traffic was dropped because the TOE was not processing network packets and not because an access-list entry was actively rejecting it).
Test Results	Pass
Execution Method	Manual

Test Case Number	48
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall use the instructions in the operational guidance to test that packet filter rules can be created that permit, deny, and log packets for each of the following attributes: • IPv4 o Source address o Destination Address o Protocol • IPv6 o Source address o Destination Address o Next Header (Protocol) • TCP

	o Source Port o Destination Port • UDP o Source Port o Destination Port
Test Instructions	Execute test script and observe output
Test Steps	1. Verify through execution of the test script that for IPv4 and IPv6, permit, deny, and log rules are available to be configured for tcp, ip, icmp, and udp for source/destination addresses, and that for TCP and UDP traffic, port ranges to which the rule applies can be configured.
Test Results	Pass
Execution Method	Automated

Test Case Number	49
SFR	FPF_RUL_EXT.1
Test Objective	Repeat the test assurance activity above to ensure that Packet filtering rules can be defined for each distinct network interface type supported by the TOE. Note that these test activities should be performed in conjunction with those of FPF_RUL_EXT.1.7 where the effectiveness of the rules is tested; here the evaluator is just ensuring the guidance is sufficient and the TOE supports the administrator creating a ruleset based on the above attributes. The test activities for FPF_RUL_EXT.1.7 define the protocol/attribute combinations required to be tested. If those combinations are configured manually, that will fulfill the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.
Test Instructions	Execute test script and observe output
Test Steps	1. Verify through execution of the test script that packet filtering rules can be applied to different physical interfaces (FastEthernet, GigabitEthernet) and logical interfaces (VLAN).
Test Results	Pass
Execution Method	Automated

Test Case Number	50
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall devise two equal Packet filtering rules with alternate operations – permit and deny. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation.
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Create a permit rule and a deny rule for traffic between test system and a remote destination through the TOE such that the permit rule is ordered first. 2. Send traffic from the test system to the remote destination specified in the packet filtering rules and observe that the traffic reaches the destination. 3. Reverse the order of the permit and deny rules. 4. Repeat step 2 and observe that the traffic is being denied by the rule.
Test Results	Pass
Execution Method	Automated

Test Case Number	51
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall repeat the procedure above, except that the two rules should be devised where one is a subset of the other (e.g., a specific address vs. a network

	segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Create a permit rule and a deny rule for traffic between test system and a remote destination through the TOE such that the permit rule is ordered first, the permit rule identifies source/destination by subnet, and the deny rule identifies source/destination by specific IP addresses. 2. Send traffic from the test system to the remote destination specified in the packet filtering rules and observe that the traffic reaches the destination. 3. Change the permit rule to be associated with specific hosts and the deny rule to be associated with network segment. 4. Repeat step 2 and observe that the traffic is still being allowed by the rule. 5. Change the rules such that 'subnet deny' is listed before 'host permit'. 6. Repeat step 2 and observe that traffic is being denied by the rule. 7. Change the rules such that 'host deny' is listed before 'host permit'. 8. Repeat step 2 and observe that traffic is being denied by the rule.
Test Results	Pass
Execution Method	Automated

Test Case Number	52
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall configure the TOE to permit and log each defined IPv4 Transport Layer Protocol (see table 9-1 Defined Protocol-specific Values) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged.
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Define an object group that contains each of the 100 IPv4 protocols defined in the VPNGWEP. 2. Map four different sets of permit rules to this group: a. Specific source and specific destination b. Specific source and 'wildcard' (subnet) destination c. Wildcard source and specific destination d. Wildcard source and wildcard destination 3. Using a test system that matches the source address, generate traffic matching each of the defined IPv4 protocols and transmit it to a destination that matches the destination address. 4. Observe via review of traffic and log data that each of the packets were permitted and logged.
Test Results	Pass
Execution Method	Automated

Test Case Number	53
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall configure the TOE to permit all traffic except to deny and log each defined IPv4 Transport Layer Protocol (see table 9-1 Defined Protocol-specific Values) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv4 Transport Layer Protocol and within the configured

	source and destination addresses in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged.
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Define an object group that contains each of the 100 IPv4 protocols defined in the VPNGWEP. 2. Map four different sets of deny rules to this group: a. Specific source and specific destination b. Specific source and 'wildcard' (subnet) destination c. Wildcard source and specific destination d. Wildcard source and wildcard destination 3. Using a test system that matches the source address, generate traffic matching each of the defined IPv4 protocols and transmit it to a destination that matches the destination address. 4. Observe via review of traffic and log data that each of the packets were denied and logged.
Test Results	Pass
Execution Method	Automated

Test Case Number	54
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall configure the TOE to permit and log each defined IPv4 Transport Layer Protocol (see table 9-1 Defined Protocol-specific Values) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to deny and log each defined IPv4 Transport Layer Protocol (see table 9-1 Defined Protocol-specific Values) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv4 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE).
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Repeat tests 51 and 52 except transmit traffic that does not match the source/destination information of any of the defined rules. 2. Observe that the traffic is denied.
Test Results	Pass
Execution Method	Automated

Test Case Number	55
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall configure the TOE to permit and log each defined IPv6 Transport Layer Protocol (see table 9-1 Defined Protocol-specific Values) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged.
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Define an object group that contains each of the 142 IPv6 protocols

	defined in the VPNGWEP. 2. Map four different sets of permit rules to this group: a. Specific source and specific destination b. Specific source and 'wildcard' (subnet) destination c. Wildcard source and specific destination d. Wildcard source and wildcard destination 3. Using a test system that matches the source address, generate traffic matching each of the defined IPv4 protocols and transmit it to a destination that matches the destination address. 4. Observe via review of traffic and log data that each of the packets were permitted and logged.
Test Results	Pass
Execution Method	Automated

Test Case Number	56
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall configure the TOE to permit all traffic except to deny and log each defined IPv6 Transport Layer Protocol (see table 9-1 Defined Protocol-specific Values) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged.
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Define an object group that contains each of the 142 IPv6 protocols defined in the VPNGWEP. 2. Map four different sets of deny rules to this group: a. Specific source and specific destination b. Specific source and 'wildcard' (subnet) destination c. Wildcard source and specific destination d. Wildcard source and wildcard destination 3. Using a test system that matches the source address, generate traffic matching each of the defined IPv4 protocols and transmit it to a destination that matches the destination address. 4. Observe via review of traffic and log data that each of the packets were denied and logged.
Test Results	Pass
Execution Method	Automated

Test Case Number	57
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall configure the TOE to permit and log each defined IPv6 Transport Layer Protocol (see table 9-1 Defined Protocol-specific Values) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to deny and log each defined IPv6 Transport Layer Protocol (see table 9-1 Defined Protocol-specific Values) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer

	Protocol and outside the scope of all source and destination addresses configured above in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE).
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Repeat tests 54 and 55 except transmit traffic that does not match the source/destination information of any of the defined rules.
Test Results	Pass
Execution Method	Automated

Test Case Number	58
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall configure the TOE to permit and log protocol 6 (TCP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged.
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Configure a rule to permit and log TCP traffic that matches certain port and address information. Use a range of ports. 2. Generate traffic through the TOE that matches the characteristics of the permit rule. 3. Observe that the traffic is logged by the TOE and allowed through it.
Test Results	Pass
Execution Method	Automated

Test Case Number	59
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall configure the TOE to deny and log protocol 6 (TCP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged.
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Configure a rule to deny and log TCP traffic that matches certain port and address information. Use a range of ports. 2. Generate traffic through the TOE that matches the characteristics of the deny rule. 3. Observe that the traffic is logged by the TOE and not allowed through it.
Test Results	Pass
Execution Method	Automated

Test Case Number	60
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall configure the TOE to permit and log protocol 17 (UDP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Here the evaluator ensures that the UDP port 500 (IKE) is included in the set of tests.
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Configure a rule to permit and log TCP traffic that matches certain port and address information. Use a range of ports that includes port 500. 2. Generate traffic through the TOE that matches the characteristics of the permit rule.

	3. Observe that the traffic is logged by the TOE and allowed through it.
Test Results	Pass
Execution Method	Automated

Test Case Number	61
SFR	FPF_RUL_EXT.1
Test Objective	The evaluator shall configure the TOE to deny and log protocol 17 (UDP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Again, the evaluator ensures that UDP port 500 is included in the set of tests.
Test Instructions	Execute test script and observe packet captures and audit logs.
Test Steps	1. Configure a rule to deny and log TCP traffic that matches certain port and address information. Use a range of ports that includes port 500. 2. Generate traffic through the TOE that matches the characteristics of the deny rule. 3. Observe that the traffic is logged by the TOE and not allowed through it.
Test Results	Pass
Execution Method	Automated

4.4.7 Protection of the TSF

Test Case Number	62
SFR	FPT_STM.1
Test Objective	The evaluator uses the operational guide to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.
Test Instructions	Execute the test script and observe console output and audit logs. For this script, NTP will be disabled.
Test Steps	1. Perform some trivial (non-TSF) configuration activities on the TOE. 2. Review the audit log and note the timestamp of the activities. 3. Manually set the system time back by an hour 4. Repeat steps 1 and 2 and note that the logged data correctly reflects the earlier time. 5. Reset the clock to the current time to clean up.
Test Results	Pass
Execution Method	Automated

Test Case Number	63
SFR	FPT_STM.1
Test Objective	[conditional] If the TOE supports the use of an NTP server; the evaluator shall use the operational guidance to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe that the NTP server has set the time to what is expected. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the operational guidance.
Test Instructions	Execute the test script and observe console output and audit logs.
Test Steps	1. Configure and enable an NTP server connection. 2. Perform some trivial (non-TSF) configuration activities on the TOE. 3. Review the audit log and note the timestamp of the activities. 4. Disable NTP. 5. Manually set the system time to an arbitrary incorrect value. 6. Repeat steps 1 and 2 and note that the logged data correctly reflects the earlier time.

	7. Enable NTP. 8. After a short period of time, repeat steps 1 and 2 and note that the logged data correctly reflects the correct time.
Test Results	Pass
Execution Method	Automated

Test Case Number	64
SFR	FPT_TUD_EXT.1
Test Objective	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 Instructions	Execute the test script and observe console output and audit logs.
Test Steps	1. Use the 'show version' command to verify that the TOE is running the evaluated configuration version of the software. 2. View the contents of the flash memory storage and verify that no image files are present. 3. Take an update (alternate product software image) with different version identification and upload it to storage on the TOE. 4. Verify that the image is now present in flash storage. 5. Edit the system's boot loader configuration to point to the image that was uploaded to the TOE. Leave the original image in the list, below the new image in the boot order. 6. Reboot the TOE and observe that the desired image was launched. 7. Clean up by reverting to the original image and removing the entry from the boot loader configuration.
Test Results	Pass
Execution Method	Automated

Test Case Number	65
SFR	FPT_TUD_EXT.1
Test 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 Instructions	Execute the test script and observe console output and audit logs.
Test Steps	1. Repeat test 63 with a software image that is valid but is designed for the use of a product other than the TOE. 2. Observe that the image does not successfully boot and the TOE reverts to the second entry on the boot loader list, which is the original image. 3. Repeat steps 1 and 2 with a corrupted version of an image that is actually intended for use with the TOE. 4. Clean up by reverting to the original image and removing the entry from the boot loader configuration.
Test Results	Pass
Execution Method	Automated

4.4.8 TOE Access

Test Case Number	66
SFR	FTA_SSL_EXT.1

Test Objective	The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that re-authentication is needed when trying to unlock the session.
Test Instructions	Execute the test script and observe console output and audit logs.
Test Steps	1. Log into the local console. 2. Configure the system idle timeout to 30 seconds. 3. Wait 20 seconds and issue a command to confirm the session is still active. 4. Wait more than 30 seconds and try and fail to issue a command to confirm the session was terminated. 5. Log back in and confirm via log data that the session was terminated 30 seconds after the most recent activity was performed. 6. Repeat steps 2 through 5 for a timeout value of 60 seconds.
Test Results	Pass
Execution Method	Automated

Test Case Number	67
SFR	FTA_SSL.3
Test Objective	The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Test Instructions	Execute the test script and observe console output and audit logs.
Test Steps	1. Repeat test 65 using remote console instead of local.
Test Results	Pass
Execution Method	Automated

Test Case Number	68
SFR	FTA_SSL.4
Test Objective	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes that the session has been terminated.
Test Instructions	Execute the test script and observe console output and audit logs.
Test Steps	1. Log in to the TOE locally. 2. Log out and observe the session has been terminated. 3. Review the audit log to confirm that the session was terminated.
Test Results	Pass
Execution Method	Automated

Test Case Number	69
SFR	FTA_SSL.4
Test Objective	The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes that the session has been terminated.
Test Instructions	Execute the test script and observe console output and audit logs.
Test Steps	1. Log in to the TOE remotely. 2. Log out and observe the session has been terminated. 3. Review the audit log to confirm that the session was terminated.
Test Results	Pass
Execution Method	Automated

Test Case Number	70
SFR	FTA_TAB.1
Test Objective	The evaluator follows the operational guidance to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.
Test Instructions	Execute the test script and observe console output and audit logs.
Test Steps	1. Log in to the TOE and set a login banner message. 2. Log out of the TOE 3. Log in to the TOE remotely and observe that the login banner that was configured in step 1 is displayed in the SSH terminal. 4. Log in to the TOE locally and observe that the login banner that was configured in step 1 is displayed in the SSH terminal.
Test Results	Pass
Execution Method	Automated

4.4.9 Trusted Path/Channels

Test Case Number	71
SFR	FTP_ITC.1
Test Objective	The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.
Test Instructions	Review the results of other testing.
Test Steps	1. TOE-initiated communications over each trusted channel defined in the ST were established in the following tests: a. External audit server using IPsec – Test 3 b. Remote AAA server using IPsec – Test 43 c. Remote VPN gateways/peers using IPsec – this is a generic version of the other items because they are all examples of remote VPN gateways/peers themselves, so no additional testing is performed here. d. Another instance of the TOE using IPsec – Test 19 e. CA server using IPsec – Test 20 2. Communications were observed to be successful by virtue of packet captures of the encrypted traffic in transit and functionally appropriate behavior occurring as a result of it (e.g. audit server channel is observed to be functioning properly by virtue of syslog data appearing on it, AAA server is observed to be functioning properly by virtue of validating user credentials that are not defined locally to the TOE, etc.).
Test Results	Pass
Execution Method	Automated/Manual

Test Case Number	72
SFR	FTP_ITC.1
Test Objective	For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE.
Test Instructions	Review the results of other testing.
Test Steps	1. Refer to test 71. All establishment of trusted channels were initiated by the TOE in the tests that are referenced there.
Test Results	Pass
Execution Method	Automated/Manual

Test Case Number	73
SFR	FTP_ITC.1
Test Objective	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Test Instructions	Review the results of other testing.
Test Steps	1. Refer to test 71. All trusted channels are shown to be encrypted through use of packet captures.
Test Results	Pass
Execution Method	Automated/Manual

Test Case Number	74
SFR	FTP_ITC.1
Test Objective	The evaluators shall, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.
Test Instructions	Review the results of other testing.
Test Steps	1. Refer to test 71. Re-execute the tests referenced there with the following exceptions: a. Set up a packet capture so that the trusted channel connection can be observed. b. Sever the connection between the TOE and the other endpoint of the trusted channel during the test's execution. c. Restore the connection and observe that the test completes successfully and the trusted channel traffic remains encrypted.
Test Results	Pass
Execution Method	Automated/Manual

Test Case Number	75
SFR	FTP_TRP.1
Test Objective	The evaluators shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.
Test Instructions	Review the results of other testing.
Test Steps	1. The only method of establishing a trusted path to the TOE is through SSH. Tests 30 through 35 show proper establishment of SSH including packet captures that show the traffic is being encrypted.
Test Results	Pass
Execution Method	Automated/Manual

Test Case Number	76
SFR	FTP_TRP.1
Test Objective	For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path.
Test Instructions	Review the results of other testing.
Test Steps	1. Execute a port scan of the TOE from an external (non-management) network interface. 2. Observe that there are no services made available that could allow for unencrypted management of the TOE (such as Telnet).
Test Results	Pass

Execution Method	Automated/Manual

Test Case Number	77
SFR	FTP_TRP.1
Test Objective	The evaluator shall ensure, for each method of remote administration, the channel data is not sent in plaintext.
Test Instructions	Review the results of other testing.
Test Steps	1. Refer to test 74. The only method of remote administration is via SSH, which was shown to be sent in encrypted format through conducting the FCS_SSH_EXT.1 testing.
Test Results	Pass
Execution Method	Automated/Manual

4.5 Vulnerability Testing

The evaluation team completed vulnerability testing as prescribed by the NDPP and VPNGWEP. Listed below are the assurance activities from each. Note that the wording of the VPNGWEP has been updated to reflect the change indicated in NIAP Technical Decision "TD0013: AVA_VAN.1 in VPN GW EP".

(NDPP) *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. The evaluator performs a search of public information to determine the vulnerabilities that have been found in network infrastructure devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.*

The evaluation team created the Cisco Integrated Services 800 Series Vulnerability Analysis (VAN) document to satisfy the AVA_VAN.1 SARs that are required by the NDPP. This assurance activity is interpreted as being a summary of these SARs so the assurance activity is considered to be satisfied by the satisfactory completion of the SARs. The VAN document contains an overview of the TOE's SPD and search for potentially applicable vulnerabilities based on public research. If the vulnerability is considered to be unsuitable, rationale is provided for why this is believed to be the case. If the vulnerability is considered to be suitable, an appropriate test is devised and described. Additionally, basic vulnerability tests based on the TOE's general functionality (as opposed to being based on its name or components) have been devised. The results of these tests are described and any applicable evidence is referenced and included with the test package.

(VPNGWEP) *The evaluator shall generate network packets that cycle through all of the values for the Transport Layer Protocol attribute that are undefined by the RFCs for IPv4 and IPv6. For example, IPv4 has an eight-bit field for Transport Layer Protocol. Only 100 Transport Layer Protocol values are defined in the RFC for IPv4 (see Table 9-1 in Appendix E), but there are 256 possible values. The evaluator is required to construct packets that exercise each possible value not defined in the RFC (the defined values are already tested in FPF_RUL_EXT.1.7) of Transport Layer Protocol (including all possible combinations) and target each distinct interface type to determine that the TOE handles these packets appropriately. Since none of these packets will match a rule, or belong to an allowed session the packets should be dropped. Since there are no requirements that the VPN Gateway audit a packet being dropped under these circumstances, the evaluator shall ensure the VPN Gateway does not allow these packets to flow through the TOE. Note that for IPv6, protocol numbers 0 (Hop-by-Hop options), 60 (Destination*

options), 44 (Fragment), 51 (AH), and 50 (ESP) are extension header numbers rather than transport layer protocol numbers and should be excluded from testing.

The evaluation team conducted testing where each instance of the TOE appliance deployed in the laboratory was targeted with a series of IPv4 and IPv6 packets. For each of these packet streams, the evaluator cycled through incrementing header values using a packet generator such that the range of unknown protocol headers was traversed. The evaluation team also configured the TOE as instructed in the Operational Guidance to ensure that the SPD would be expected to deny the unknown protocol traffic. In all cases, the traffic was observed on the wire and by the TOE's logs to be dropped by the TOE. Additionally, packet captures on the packet generator system showed the traffic being sent to the TOE with the appropriate header data.

5 Conclusions

The TOE was evaluated against the ST and has been found by this evaluation team to be conformant with the ST. The overall verdict for this evaluation is: Pass.

6 Glossary of Terms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CA	Certificate Authority
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	*Internet Control Message Protocol*
ISDN	*Integrated Services Digital Network*
ISR	Integrated Services Router
IT	Information Technology
NDPP	Network Device Protection Profile
OS	Operating System
PBKDF2	Password-Based Key Derivation Function version 2
PoE	Power over Ethernet
POP3	Post Office Protocol
PP	Protection Profile
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SIP	Session Initiation Protocol

Acronyms / Abbreviations	Definition
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
WAN	Wide Area Network
WIC	WAN Interface Card

Table 7-1: Acronyms

Terminology	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Peer	Another router on the network that the TOE interfaces with.
Privilege level	Assigns a user specific management access to the TOE to run specific commands. The privilege levels are from 1-15 with 15 having full administrator access to the TOE similar to root access in UNIX or Administrator access on Windows. Privilege level 1 has the most limited access to the CLI. By default when a user logs in to the Cisco IOS, they will be in user EXEC mode (level 1). From this mode, the administrator has access to some information about the TOE, such as the status of interfaces, and the administrator can view routes in the routing table. However, the administrator can't make any changes or view the running configuration file. The privilege levels are customizable so that an Authorized Administrator can also assign certain commands to certain privilege levels.
Remote VPN Gateway/Peer	A remote VPN Gateway/Peer is a another network device that the TOE sets up a VPN connection with. This could be a VPN client or another router.
Role	An assigned role gives a user varying access to the management of the TOE. For the purposes of this evaluation the privilege level of user is synonymous with the assigned privilege level.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vty	vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term). For configuration purposes vty defines the line for remote access policies to the router.

Table 7-2: Terminology