# Supporting Document Mandatory Technical Document



PP-Module for Core Protections Version: 0.6

2021-01-08

#### National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

#### Technical Editor:

National Information Assurance Partnership (NIAP)

#### Document history:

|  |  |  |
| --- | --- | --- |
| Version | Date | Note |
| 0.1 | 03-19-2020 | Initial Draft |
| 0.2 | 05-20-2020 | Revision for release to WG |
| 0.3 | 08-06-2020 | Revision based upon comments |
| 0.4 | 10-08-2020 | Revision to incorporate cryptographic requirements |
| 0.5 | 10-15-2020 | Revisions prior to release for comments |
| 0.6 | 1-8-2021 | Release for comments |

#### General Purpose:

The purpose of this SD is to define evaluation methods for the functional behavior of products.

#### Acknowledgements:

This SD was developed with support from NIAP Technical Community members, with representatives from industry, Government agencies, Common Criteria Test Laboratories, and members of academia.

# Table of Contents

[1 Supporting Document Mandatory Technical Document 1](#_Toc62054380)

[Table of Contents 3](#_Toc62054381)

[2 Introduction 5](#_Toc62054382)

[2.1 Technology Area and Scope of Supporting Document 5](#_Toc62054383)

[2.2 Structure of the Document 5](#_Toc62054384)

[2.3 Terms 5](#_Toc62054385)

[2.3.1 Technical Terms 5](#_Toc62054386)

[2.3.2 Acronyms 6](#_Toc62054387)

[3 Evaluation Activities for SFRs 7](#_Toc62054388)

[3.1 Evaluation Activities for Mandatory SFRs 7](#_Toc62054389)

[3.1.1 NDcPP Evaluation Activities 7](#_Toc62054390)

[3.1.2 TOE SFR Evaluation Activities 7](#_Toc62054391)

[4 Evaluation Activities for Optional SFRs 11](#_Toc62054392)

[4.1 Security Audit (FAU) 11](#_Toc62054393)

[4.1.1 FAU\_DRM\_EXT.1 Debug and Recovery Audit Mechanisms 11](#_Toc62054394)

[4.2 Protection of the TSF (FPT) 11](#_Toc62054395)

[4.2.1 FPT\_VCT\_EXT.1 Vendor Configuration Tool 11](#_Toc62054396)

[5 Evaluation Activities for Selection-Based SFRs 12](#_Toc62054397)

[5.1 Cryptographic Support (FCS) 12](#_Toc62054398)

[5.1.1 SSH Server Default Configuration FCS\_SSHS\_EXT.2 12](#_Toc62054399)

[5.1.2 SSH Client Default Configuration FCS\_SSHC\_EXT.2 13](#_Toc62054400)

[5.1.3 TLS Server Default Configuration FCS\_ TLSS\_EXT.3 13](#_Toc62054401)

[5.1.4 TLS Client Default Configuration FCS\_ TLSC\_EXT.3 14](#_Toc62054402)

[5.1.5 IPsec Default Configuration FCS\_IPSEC\_EXT.2 14](#_Toc62054403)

[6 Evaluation Activities for Objective SFRs 15](#_Toc62054404)

[7 Vulnerability Analysis 16](#_Toc62054405)

[7.1 Sources of Vulnerability Information 16](#_Toc62054406)

[7.1.1 Type 1 Hypotheses – Public-Vulnerability-Based 16](#_Toc62054407)

[7.1.2 Type 2 Hypotheses – iTC-Sourced 16](#_Toc62054408)

[7.1.3 Type 3 Hypotheses – Evaluation-Team-Generated 16](#_Toc62054409)

[7.1.4 Type 4 Hypotheses – Tool-Generated 16](#_Toc62054410)

[7.2 Process for Evaluator Vulnerability Analysis 17](#_Toc62054411)

[7.3 Reporting 17](#_Toc62054412)

[7.4 Additional Public Vulnerability Sources 17](#_Toc62054413)

[7.5 Additional Flaw Hypotheses 17](#_Toc62054414)

[8 Required Supplementary Information 18](#_Toc62054415)

# Introduction

## Technology Area and Scope of Supporting Document

This PP-Module defines requirements for the evaluation of the Core Protections in addition to the requirements of the Base-PP which specifies requirements on network devices in general. These Core Protections includes Address Space Layout Randomization (ASLR), Stack Protection, Password Defaults, Default Administrator Privileges, Separate Trusted Path, and Automatic Updates by Default. These protections ensure that the TOE provides a ‘Secure by Default’ approach to Security.

The PP-Module is intended for use with the following Base-PPs:

* collaborative Protection Profile for Network Devices, v2.2E

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for Core Protections, Version 2.2E. Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help Developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

## Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not appropriate for that TOE.

Similarly, at the more granular level of Assurance Components, if the Evaluation Activities for an Assurance Component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the Assurance Component is a ‘pass’. To reach a ‘fail’ verdict for the Assurance Component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not appropriate for that TOE.

## Terms

### Technical Terms

The following definitions define Technical terms used in this document:

|  |  |
| --- | --- |
| Term | Meaning |
| Administrator | See Security Administrator. |
| Assurance | Grounds for confidence that a TOE meets the SFRs [CC1]. |
| Security Administrator | The terms “Administrator” and “Security Administrator” are used interchangeably in this document at present. |
| Target of Evaluation | A set of software, firmware and/or hardware possibly accompanied by guidance. [CC1] |
| TOE Security Functionality (TSF) | A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs. [CC1] |
| User | See Security Administrator |

### Acronyms

|  |  |
| --- | --- |
| Acronym | Meaning |
| CC | Common Criteria |
| IP | Internet Protocol |
| PP | Protection Profile |
| RFC | Request for Comments |
| SFR | Security Functional Requirement |
| SPD | Security Problem Definition |
| ST | Security Target |
| TCP | Transmission Control Protocol |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| UDP | User Datagram Protocol |

# Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE\_TSS.1, ADV\_FSP.1, AGD\_OPE.1, and ATE\_IND.1) – this is in addition to the CEM work units that are performed in 6 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labelled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator’s verdicts will be associated with the CEM work unit ASE\_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE\_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the cPP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator’s verdicts will be associated with CEM work units ADV\_FSP.1-7, AGD\_OPE.1-4, and AGD\_OPE.1-5.

Finally, the subsection labelled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer’s tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM work units that are associated with the EAs specified in this section are: ATE\_IND.1-3, ATE\_IND.1-4, ATE\_IND.1-5, ATE\_IND.1-6, and ATE\_IND.1-7.

## Evaluation Activities for Mandatory SFRs

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the NDcPP.

### NDcPP Evaluation Activities

#### Trusted Path/Channels (FTP)

##### FTP\_ITC\_EXT.1 Inter-TSF Trusted Channel

###### TSS

*The evaluator shall examine the TSS to confirm that a description of the connection between the TOE and the remote update server is provided. This description must include information relating to the trusted communication channel used in ensuring the connection provides disclosure and detection of modification of the channel data.*

###### Guidance

*The evaluator shall examine the guidance documentation to confirm that it describes the configuration of the connection to the update server, including configuration of the communication channel, update server credentials (if applicable), and polling period from the TOE to the update server to query for new versions (if applicable).*

###### Tests

*(If update server is selected within FTP\_ITC\_EXT.1.1) The evaluation activities specified for FTP\_ITC.1 in the Supporting Document for the Base-PP shall be applied for update server communications.*

### TOE SFR Evaluation Activities

#### Identification and Authentication (FIA)

##### FIA\_PMG\_EXT.2 Password Management

###### TSS

*None.*

###### Guidance

*The evaluator shall examine the guidance documentation to confirm that it:*

* *identifies the accounts that will need to be changed during installation, on first login, or initial enablement of the interface*
* *identifies the default credential used with the account*
* *describes the process for changing the passwords on these accounts during initial configuration, on first login, or initial enablement of the interface*

*Note: It is acceptable for the account identification and password changes to be achieved by using a script or wizard supplied with the product.*

###### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *The evaluator shall follow the operational guidance for configuration of the TOE and shall confirm that the default account credentials identified to the Security Administrator as described in the operational guidance, are required to be changed during initial configuration or first enablement of the account..*
2. *The evaluator shall perform an analysis of the TOE in its evaluated configuration and identify any default accounts through examination of the TOE interfaces and configuration which are not documented within the Security Target or Guidance documentation. If a default account is found that is not documented in the vendor documentation, this test fails.*
3. *If passwords are changed during the initial configuration of the TOE, the evaluator shall follow the preparatory guidance and verify that all documented administrative accounts are prompted to change the default credentials prior to completion of the evaluated configuration. The evaluator shall verify that the passwords are compliant to FIA\_PMG\_EXT.1.*
4. *If passwords are changed during the first authentication on a default administrative account, the evaluator shall exercise each default administrative account and verify that a prompt is provided after authentication that requires the credentials to be updated. The evaluator shall verify that the passwords are compliant to FIA\_PMG\_EXT.1.*
5. *If passwords are changed during first initialization of an account or service, the evaluator shall invoke each service/account and verify that a prompt is provided after authentication that requires the credentials to be updated. The evaluator shall verify that the passwords are compliant to FIA\_PMG\_EXT.1.*

#### Protection of the TSF (FPT)

##### FPT\_AEX\_EXT.1 Anti-Exploitation Capabilities

###### TSS

*The evaluator shall ensure that the TSS describes the compiler flags used to enable ASLR when the TOE is compiled.*

###### Guidance

*None.*

###### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *The evaluator shall perform a static or dynamic analysis to determine that no memory mappings are placed at an explicit and consistent address. The method of doing so varies per platform.*
2. *The evaluator shall verify that no memory mapping requests are made with write and execute permissions. The method of doing so varies per platform.*

##### FPT\_SBT\_EXT.1 Secure Boot

###### TSS

*The evaluator shall verify that the TSS describes the digital signature hash-based message authentication verification or performed by the TOE at boot.*

*Application Note: Due to the proprietary nature of this information, the vendor may provide the information pertaining to the root of trust in a separate document. This document must be provided for review to the evaluation lab and the scheme for review but will not be posted on the approved products list page.*

###### Guidance

*The evaluator shall examine the guidance documentation and verify that procedures are provided on the remediation of a secure boot failure.*

***Application Note:*** *Acceptable actions for remediation of the device include reverting to a previous TOE image, reinstalling the TOE, performing a factory reset of the TOE, or contacting vendor support for assistance.*

###### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *During initial boot of the TOE, the evaluator shall review the initialization output or audited events and verify that the TOE successfully performs a digital signature or hash-based verification of the firmware/software.*
2. *The evaluator shall attempt to boot the TOE using firmware/software with an invalid digital signature or hash-based verification and verify that the verification check fails and the TOE halts initialization.*
3. *The evaluator shall attempt to boot the TOE using an invalid firmware image and verify that upon failure, the TOE performs the action selected within FPT\_SBT\_EXT.1.2.*
4. *If ‘revert to previous TOE image’ is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation and perform the actions and confirm that the TOE returns to an operational state following the remediation action.*
5. *If ‘boot into single user mode’ is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation and perform the actions and confirm that the TOE returns to an operational state following the remediation action.*
6. *If ‘reinstall TOE’ is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation and perform the actions and confirm that the TOE returns to an operational state following the remediation action.*
7. *If ‘factory reset’ is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation and perform the actions and confirm that the TOE returns to an operational state following the remediation action. The vendor must also ensure that following a factory reset, the default configurations present within this PP module are still enforced.*

***Application Note****: If ‘contact vendor support’ is selected, the evaluator may work directly with the vendor point of contact for the evaluation to exercise the guidance actions. An actual ticket is not required to be generated and submitted on the vendor support page.*

##### FPT\_TUD\_EXT.3 Automatic Update Management

###### TSS

*None.*

###### Guidance

*The evaluator shall examine the guidance documentation to confirm that it describes the configuration of update options and explains that at the end of installation the product is configured to perform queries to an update server periodically.*

###### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *(Optional) If configuration of a polling interval is provided by the TOE, the evaluator shall verify that at the configured time interval, the TOE will establish a connection with the update server to query for updates.*
2. *The evaluator shall wait the identified polling time interval and ensure that the TOE requests information from the update server pertaining to new firmware/software releases. If the polling interval is configurable, the evaluator shall set the upper and lower limits …*
3. *(Optional) If manual querying of the update server by the TOE is provided, the evaluator shall follow the operational guidance for the TOE to perform a manual query of the update server.*
4. *The evaluator shall place a valid update image on the update server. The evaluator shall verify, for each selection made in FPT\_TUD\_EXT.3.2, that the image can either be manually downloaded by a Security Administrator or automatically downloaded by the TOE. The evaluator verifies that the TOE update firmware/software can either be installed manually by the Security Administrator or is installed automatically by the TOE following the download (if selected).*

#### Trusted Path/Channels (FTP)

##### FTP\_TRP\_EXT.2 Trusted Management Path

###### TSS

*None.*

###### Guidance

*The evaluator shall examine the guidance documentation to confirm that it identifies and describes configuration through the use of access control lists, VLAN, and/or physical ethernet to provide a logically or physically separate interface for remote administration*.

###### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *The evaluator shall follow the operational guidance for configuration of the administration interfaces and shall confirm that, by default after installation, unprotected connections for management activities cannot be made.*
2. *The evaluator shall exercise the TOE management interface(s) and verify that the TOE can be accessed when using the interface configured with an access control list or VLAN that permits the traffic. The evaluator shall then attempt to connect to the TOE management interface(s) and verify that the TOE cannot be accessed when using the interface if an ACL or VLAN is not configured to permit the connection.*
3. *If physical ethernet is selected in FPT\_TRP\_EXT.2, the evaluator shall exercise the TOE management interface(s) and confirm that the traffic is permitted when connecting through an approved administrative interface. The evaluator shall then attempt to send traffic through the interface using a port or service not permitted for administration and verify that the traffic is denied (e.g. ICMPv4 or ICMPv6).*

# Evaluation Activities for Optional SFRs

## Security Audit (FAU)

### FAU\_DRM\_EXT.1 Debug and Recovery Audit Mechanisms

#### TSS

*None.*

#### Guidance

*The evaluator will examine the operational guidance to ensure that the TOE by default or through configuration will generate an auditable event on the occurrence of invocation of the debug interface.*

#### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *The evaluator shall attempt to establish a connection to the debug interface for the TOE with an authorized user account. The evaluator shall verify that the attempt is successful, and an auditable event is generated that includes the user within the record.*
2. *The evaluator shall attempt to establish a connection to the debug interface for the TOE with an unauthorized user account. The evaluator shall verify that the attempt is unsuccessful, and an auditable event is generated that includes the user within the record.*

## Protection of the TSF (FPT)

### FPT\_VCT\_EXT.1 Vendor Configuration Tool

#### TSS

*The evaluator shall verify that the TSS describes the vendor configuration tool and the method and interface through which it is invoked*.

*The evaluator shall verify that the TSS describes the scope of the vendor configuration tool and explicitly lists which SFRs are configured through this tool*.

*Application Note: It is not a requirement for the entirety of the TOE configuration to be performed through the configuration tool. However, it must be clearly documented within the TSS or operational guidance regarding which SFRs are included or excluded from the tool.*

#### Guidance

*The evaluator shall verify that operational guidance documents whether the vendor configuration tool is performed through a script or wizard.*

*If the configuration tool is provided as a wizard, the evaluator shall verify that the operational guidance provides instructions to the Security Administrator documenting which interface can be used for use of the wizard as well as each step taken to complete the initial configuration of the TOE.*

*If the configuration tool is provides as a script, the evaluator shall verify that the operational guidance provides instructions to the Security Administrator documenting which interface can be used for execution of the script as well as the prefix (if applicable) that must be used through command line to trigger the script execution.*

*The evaluator shall verify that the operational guidance documents each parameter that can be specified during use of the configuration tool to place the TOE in the evaluated configuration.*

#### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *If the vendor configuration tool is provided as a script, the evaluator shall follow the operational guidance and execute the script through the documented interface. The evaluator shall demonstrate each parameter available and verify that upon completion of the script the TOE is in the evaluated configuration.*
2. *If the vendor configuration tool is provided as a wizard, the evaluator shall follow the operational guidance and complete the wizard process. The evaluator shall demonstrate each parameter available and verify that upon completion of the script the TOE is in the evaluated configuration.*
3. *The evaluator, following execution of the vendor configuration tool, shall perform a subset of the requirements documented within the Base-PP and verify that the TOE is compliant to the SFRs.*

*Application Note: The subset of requirements to be tested shall be based upon the list of SFRs within the AGD or TSS that are configured through use of the tool. It is not a requirement to test every SFR listed but sufficient sampling should be performed to ensure that the TOE is compliant. It is recommended that the evaluator run the configuration tool prior to execution of the other TOE SFRs to simplify this process.*

# Evaluation Activities for Selection-Based SFRs

## Cryptographic Support (FCS)

### SSH Server Default Configuration FCS\_SSHS\_EXT.2

#### TSS

*The evaluator shall examine the TSS and verify that it describes the state at which the replacement of default host keys occurs.*

#### Guidance

**FCS\_SSHS\_EXT.2.1**

*The evaluator shall examine the guidance documentation and ensure that no procedures are required to be compliant with FCS\_SSHS\_EXT.1. If any configuration steps are required to restrict the encryption algorithms, MAC algorithms, public-key algorithms, key exchange methods, or rekeying intervals in order to gain compliance, this requirement fails.*

**FCS\_SSHS\_EXT.2.2**

*The evaluator shall examine the guidance documentation and ensure information is provided on when the regeneration of host keys is performed.*

#### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *The evaluator shall follow the preparatory guidance and prior to any configuration of the SSH server interface attempt to establish a connection using an unsupported cryptographic algorithm. The evaluator shall verify that the connection fails.*
2. *The evaluator shall follow the preparatory guidance and prior to any configuration of the SSH server interface attempt to establish a connection using an unsupported hash. The evaluator shall verify that the connection fails.*
3. *The evaluator shall follow the preparatory guidance and prior to any configuration of the SSH server interface attempt to establish a connection using an unsupported Diffie Hellman group. The evaluator shall verify that the connection fails.*
4. *The evaluator shall follow the preparatory guidance and prior to any configuration of the SSH server interface attempt to establish a connection using an unsupported public key. The evaluator shall verify that the connection fails.*
5. *The evaluator shall follow the preparatory guidance and verify that the TOE prompts the security administrator to regenerate a new host key.*

### SSH Client Default Configuration FCS\_SSHC\_EXT.2

#### TSS

*No assurance activity.*

#### Guidance

*The evaluator shall examine the guidance documentation and ensure that no procedures are required to be compliant with FCS\_SSHC\_EXT.1. If any configuration steps are required to restrict the encryption algorithms, MAC algorithms, public-key algorithms, key exchange methods, or rekeying intervals in order to gain compliance, this requirement fails.*

#### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *The evaluator shall follow the preparatory guidance and prior to any configuration of the SSH client interface attempt to establish a connection to an SSH server that is using an unsupported cryptographic algorithm. The evaluator shall verify that the connection fails.*
2. *The evaluator shall follow the preparatory guidance and prior to any configuration of the SSH client interface attempt to establish a connection to an SSH server that is using an unsupported hash. The evaluator shall verify that the connection fails.*
3. *The evaluator shall follow the preparatory guidance and prior to any configuration of the SSH client interface attempt to establish a connection to an SSH server that is using an unsupported Diffie Hellman group. The evaluator shall verify that the connection fails.*
4. *The evaluator shall follow the preparatory guidance and prior to any configuration of the SSH client interface attempt to establish a connection to an SSH server that is using an unsupported public key. The evaluator shall verify that the connection fails.*

### TLS Server Default Configuration FCS\_ TLSS\_EXT.3

#### TSS

*The evaluator shall examine the TSS and verify that it describes the state at which the replacement of factory default certificates occurs.*

#### Guidance

*The evaluator shall examine the guidance documentation and verify that specific procedures are identified for replacing the factory default certificates for the TLS interface(s) that occur at the time identified in FCS\_TLSS\_EXT.3.2.*

*The evaluator shall also verify that no procedures are required to be compliant with FCS\_TLSS\_EXT.1 (or FCS\_TLSS\_EXT.2 if claimed). If any configuration steps are required to gain compliance, this requirement fails*

#### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *The evaluator shall follow the preparatory guidance and prior to any configuration of the TLS server interface attempt to establish a connection using an unsupported cipher suite. The evaluator shall verify that the connection fails.*
2. *The evaluator shall follow the preparatory guidance and prior to any configuration of the TLS server interface attempt to establish a connection using an unsupported SSL or TLS version. The evaluator shall verify that the connection fails.*
3. *The evaluator shall follow the preparatory guidance and verify that the TOE prompts the security administrator to generate and install a new server certificate.*

### TLS Client Default Configuration FCS\_ TLSC\_EXT.3

#### TSS

*The evaluator shall examine the TSS and verify that it describes the state at which the replacement of factory default certificates occurs.*

#### Guidance

*The evaluator shall examine the guidance documentation and verify that specific procedures are identified for replacing the factory default certificates for the TLS interface(s) that occur at the time identified in FCS\_TLSC\_EXT.3.2.*

*The evaluator shall also verify that no procedures are required to be compliant with FCS\_TLSC\_EXT.1 (or FCS\_TLSC\_EXT.2 if claimed). If any configuration steps are required to gain compliance, this requirement fails.*

#### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *The evaluator shall follow the preparatory guidance and prior to any configuration of the TLS server interface attempt to establish a connection to a TLS server that is using an unsupported cipher suite. The evaluator shall verify that the connection fails.*
2. *The evaluator shall follow the preparatory guidance and prior to any configuration of the TLS server interface attempt to establish a connection to a TLS server that is using an unsupported SSL or TLS version. The evaluator shall verify that the connection fails.*

### IPsec Default Configuration FCS\_IPSEC\_EXT.2

#### TSS

*No assurance activity.*

#### Guidance

*The evaluator shall review the guidance documentation and verify that steps are provided for removal or modification of the default pre-shared key(s) and/or certificates.*

*If configuration of the default policies is required to gain compliance to FCS\_IPSEC\_EXT.1, the evaluator shall verify that steps are provided to remove or modify the policies This requirement fails if the policies cannot be updated or disabled.*

#### Tests

*The evaluator shall carry out the following tests. For a distributed TOE the tests shall be repeated for each component.*

1. *The evaluator shall review the default TOE configuration and ensure that all provided default IPsec policies do not contain unsupported of disallowed algorithms, hashes, of Diffie Hellman groups. The preparatory guidance must provide guidance on how to change these policies if present. This test fails if the policies cannot be updated or disabled to be compliant to the base protection profile requirements.*
2. *If pre-shared keys are implemented by the TOE, the evaluator shall review the TOE default configuration and ensure that all pre-shared keys present in default policies are compliant to FIA\_PSK\_EXT.1 in the base protection profile.*
3. *If certificate-based authentication is present on the TOE, the evaluator shall review the TOE default configuration and ensure that the certificates are compliant to FIA\_X509\_EXT.1/Rev in the base protection profile. The evaluator must also generate a new certificate and verify the policy can be updated to use the new certificate.*

# Evaluation Activities for Objective SFRs

There are no objective requirements within the PP-Module.

# Vulnerability Analysis

[SD-ND] contains the details of the vulnerability analysis process to be followed; that information is not repeated here. The additional information that is needed for vulnerability analysis for TOEs conforming to [MOD-CP] is contained in the following sections.

## Sources of Vulnerability Information

[SD-ND] identifies the 4 types of flaws to be considered by the evaluation team. For each type, the following additional information is provided for TOEs conforming to [MOD-CP].

### Type 1 Hypotheses – Public-Vulnerability-Based

The list of public sources of vulnerability information selected by the iTC is given in Section A.4 of [SD-ND]. Any additional sources specifically for firewalls will be specified in chapter A.4 of this document.

The evaluators shall perform a search on the sources listed in Section A.4 of [SD-ND] to determine a list of potential flaw hypotheses that are more recent that the publication date of the PP-Module, and those that are specific to the TOE and its components as specified by the additional documentation mentioned above. Any duplicates – either in a specific entry, or in the flaw hypothesis that is generated from an entry from the same or a different source – can be noted and removed from consideration by the evaluation team.

The search criteria to be used when searching the sources published after the publication date of the cPP shall include:

* The term “firewall”
* The following protocols: TCP, UDP, IPv4, IPv6
* Any protocols not listed above supported (through an SFR) by the TOE.
* The TOE name (including appropriate model information as appropriate)

As part of type 1 flaw hypothesis generation for the specific components of the TOE, the evaluator shall also search the component manufacturer’s websites to determine if flaw hypotheses can be generated on this basis (for instance, if security patches have been released for the version of the component being evaluated, the subject of those patches may form the basis for a flaw hypothesis).

### Type 2 Hypotheses – iTC-Sourced

Section A.5 of [SD-ND] contains the list of flaw hypothesis generated by the iTC for this technology that must be considered by the evaluation team as flaw hypotheses in performing the vulnerability assessment. Section A.5 of this document contains additional flaw hypothesis generated by the iTC specifically for firewalls.

If the evaluators discover a Type 3 or Type 4 flaw that they believe should be considered as a Type 2 flaw in future versions of this PP-Module, they should work with their Certification Body to determine the appropriate means of submitting the flaw for consideration by the iTC.

### Type 3 Hypotheses – Evaluation-Team-Generated

Type 3 flaws are formulated by the evaluator based on information presented by the product (through on-line help, product documentation and user guides, etc.) and product behaviour during the (functional) testing activities. The evaluator is also free to formulate flaws that are based on material that is not part of the baseline evidence (e.g., information gleaned from an Internet mailing list, or reading interface documentation on interfaces not included in the set provided by the developer), although such activities have the potential to vary significantly based upon the product and evaluation facility performing the analysis.

If the evaluators discover a Type 3 flaw that they believe should be considered as a Type 2 flaw in future versions of this PP-Module, they should work with their Certification Body to determine the appropriate means of submitting the flaw for consideration by the iTC.

### Type 4 Hypotheses – Tool-Generated

There are no Type 4 hypotheses that apply to the TOE beyond those defined by [SD-ND].

If the evaluators discover a Type 4 flaw that they believe should be considered as a Type 2 flaw in future versions of this PP-Module, they should work with their Certification Body to determine the appropriate means of submitting the flaw for consideration by the iTC.

## Process for Evaluator Vulnerability Analysis

The process to be followed is described in [SD-ND].

## Reporting

Reporting activities are described in [SD-ND].

## Additional Public Vulnerability Sources

[SD-ND] identifies the relevant public vulnerability sources to be consulted. There are no additional public vulnerability sources identified specifically for firewalls

## Additional Flaw Hypotheses

The following additional tests shall be performed:

1. The evaluator shall perform a review of the vendor-provided guidance documentation as well as a public search for all identified built-in administrative accounts. These accounts include service accounts, disaster recovery accounts, developer interfaces, debug accounts, and APIs which are able to configure the TOE or read security-sensitive information from the TOE. The evaluator shall attempt to invoke each interface or access each identified account and determine that all methods to access the TOE are restricted with the appropriate user authentication credentials defined under FIA\_PMG\_EXT.1 in the base PP.
2. The evaluator shall authenticate to the TOE with an authorized administrative account and using the guidance documentation verify that all accounts defined within the documentation are present on the TOE. The evaluator shall then verify that all account credentials are compliant to the password complexity requirements. For those credentials that are non-compliant, the evaluator shall verify that the credentials can either be configured to meet the requirement or be disabled.
3. The evaluator shall attempt one of the privileged actions that is identified in operational guidance as not being available by default, without performing the relevant additional action to perform the command and shall confirm that the action is not carried out. (If the TOE does not provide an environment in which such an attempt can be made then the evaluator shall report this and explain why it is not possible. An example of such a situation might be where actions can only be carried out by selection from an offered menu rather than by entering commands over a command line interface.)

# Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.