NIST SP 800-53 Revision 4 Mapping:
Network Device Protection Profile v1.1 08-Jun-12 (plus Errata2)
NDPP Extended Package
Stateful Traffic Filter Firewall v1.0 19-Dec-11

Introduction

Several of the NIST SP 800-53/CNSS 1253 controls are either fully or partially addressed by compliant TOEs. This section outlines the requirements that are addressed, and can be used by certification personnel to determine what, if any, additional testing is required when the TOE is incorporated into its operational configuration.

General Caveats

- A protection profile describes the security characteristics of a given product; the Risk Management Framework and the NIST SP 800-53 controls are designed for systems. A product, in isolation, can never satisfy a control for an overall system – at minimum, there needs to be assurance that supporting operational policies and practices are in place. At best, a product can support an overall system in satisfying the control.

- Just as Common Criteria SFRs differ based on the completion of assignments and selections, so to do NIST SP 800-53 controls. An underlying assumption in the statement of support is that the assignments (or supporting policies) are completed in congruent fashions. In other words, if the SFR is calling for the use of a particular algorithm for a particular cryptographic function, then the assignment in SC-13 is completed to call for that same algorithm for the same cryptographic function.

- A flaw in the approach taken by many of the newer PPs is to view the SFRs as divisible – that is, some elements (the individual "The TSF shall" statements, xxx_xxx.1.x) can be present or no, with assurance activities for each. The Common Criteria, on the other hand, considers the SFRs to be the indivisible unit (e.g., FAU_GEN.1). This document only maps to the level of the SFR.

Base Security Functional and Assurance Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FAU_GEN.1	**Security Audit Data Generation** Audit Data Generation • Product generates audit records for [*set of events*] that includes startup and shutdown of audit, all administrative actions, and the specified events in a table. • Product records within the audit record at least date, time, type, instigator, outcome, and [*event specific information*]	AC-6(9)	**Least Privilege** | Auditing Use of Privileged Functions • Information system audits the execution of privileged functions.	The auditing aspect of AC-6(9) is satisfied if the assignment in FAU_GEN is completed to include execution of privileged functions (which, in this case, includes all administrative commands).
		AU-2†	**Audit Events ‡** Organization… • Determines system can audit [events] • [⋮] • Determines the following events are to be audited: [events]	FAU_GEN.1.1 gives the definition of what events should be audited (addressing the bulk of this control), but the assignments in AU-2 and AU-12 need to cover at least what is in FAU_GEN.1.1 for the mapping to be valid. Note also that FAU_GEN implies both auditable and audited, which is two distinct controls under 800-53. **NOTE:** The audit table defined in the NDPP may not include all the events called out in the assignment for AU-2 specified in CNSSI No. 1253.
		AU-3	**Content of Audit Records** • Information system generates records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event	FAU_GEN.1.2 details the list of what must be contained in each audit record. AU-3 covers the information identified it FAU_GEN.1.2 a).
		AU-3(1)	**Content of Audit Records** | Additional Audit Information • Information System generates records containing [*additional information*]	The NDPP goes beyond the minimal content called out in AU-3.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
		AU-12†	**Audit Generation** Information system… • Provides audit record generation capability for the auditable events defined in AU-2 a. at [*components*]; • Allows [*personnel or roles*] to select which auditable events are to be audited by specific components of the information system • Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	FAU_GEN.1.1 gives the definition of what events should be audited (addressing the bulk of this control), but the assignments in AU-2 and AU-12 need to cover at least what is in FAU_GEN.1.1 for the mapping to be valid. Note also that FAU_GEN implies both auditable and audited, which is two distinct controls under 800-53.
FAU_GEN.2	**Security Audit Data Generation** User Identity Association • Auditable events are associated with the identity of the user that caused the event	AU-3	**Content of Audit Records** • Information system generates records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event	AU-3 requires that audit records contain "the identity of any individuals or subjects associated with the event "
FCS_CKM.1(1)	**Cryptographic Key Management** Refinement: Cryptographic Key Generation (Key Establishment) Product generates **asymmetric** cryptographic keys **for key establishment** in accordance with [*NIST SP 800-56B, -56A*] and specified cryptographic key sizes [*112 bits*]	SC-12†	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
		SC-12(3)†	**Cryptographic Key Establishment and Management** | Asymmetric Keys • Organization produces, controls, and distributes asymmetric cryptographic keys using [*NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect*	FCS_CKM.1(1) calls for asymmetric key in accordance with the NIST process; as NSA developed the PP, it is by implication an NSA-approved technology and process.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			the user's private key].	
FCS_CKM_EXT.4	[Cryptographic Key Zeroization] Key Zeroization The product zeroizes all plaintext secrety and private cryptographic keys and CSPs when no longer required.	SC-12†	**Cryptographic Key Establishment and Management** - Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
FCS_COP.1(1) [Errata 2]	[Cryptographic Operation] Cryptographic Operation (for data encryption/decryption) - Product performs [***encryption/decryption***] in accordance with [AES operating in [*modes*]] with key sizes of 128, and 256that meets FIPS 197 or NIST SP 800-38*x*.	SC-13 †	**Cryptographic Protection** - Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
		Note: FCS_COP.1(1) may also be viewed as supporting SC-8 and SC-8(1), or SC-28, depending upon the purposes for which the encryption is used.		
FCS_COP.1(2)	[Cryptographic Operation] Cryptographic Operation (for cryptographic signature) - Product performs [***cryptographic signature services***] in accordance with DSA, rDSA, or ECDSA with particular key sizes.	SC-13 †	**Cryptographic Protection** - Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
		Note: FCS_COP.1(2) may also be viewed as supporting AU-10, but that support really depends upon the purpose for which the digital signatures are used. Provision of a digital signature service does not *apriori* give non-repudiation.		
FCS_COP.1(3)	[Cryptographic Operation] Cryptographic Operation (for cryptographic hashing) Product performs [***cryptographic hashing***] in accordance with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512] and [***MD Sizes 160 and others***] that meet FIPS 180-3.	SC-13 †	**Cryptographic Protection** - Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
FCS_COP.1(4)	[Cryptographic Operation] Cryptographic Operation (for keyed-hash message authentication) Product performs [***keyed-hash message authentication***] in accordance with HMAC-[SHA-1, SHA-224, SHA-256, SHA-384, SHA-512] and key sizes of [*HMAC key sizes*] and MD sizes	SC-13 †	**Cryptographic Protection** - Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
	[*sizes*], that meet FIPS 198-1 and 180-3			
FCS_RBG_EXT.1 [Errata 2]	**Random Bit Generation** Random Bit Generation - The product performs all random big generation in accordance with [NIST SP 800-90A algorithms, FIPS 140-2 Annex C algorithms] seeded by an entropy source that … - The deterministic RBG is seeded with a minimum of …	Note: Unclear. This might fit within SC-12 and key generation, but it could also be below the level of any existing NIST control.		
FDP_RIP.2	**Residual Information Protection** Full Residual Information Protection - Product ensures that any previous information content of a resource is made unavailable upon the [*allocation of the resource to, deallocation of the resource from*] **all** objects.	SC-4	**Information in Shared Resources** - Information system prevents unauthorized and unintended information transfer via shared system resources.	The FDP control focuses on objects within the security policy, whereas SC-4 is broader. Additionally, implementation of FDP_RIP only addresses reuse of objects within the given product, not for the overall system.
FIA_PMG_EXT.1	**Password Management** Password Management - Product supports the following password management capabilities for administrative passwords: (1) Complexity requirements; (2) Minimum password length	IA-5(1)	**Authenticator Management** | Password-Based Authentication Information system, for password-based authentication… - Enforces minimum password complexity of [*complexity requirements*]; - Enforces at least the following number of changed characters when new passwords are created: [*number*] - Stores and transmits only encrypted representations of passwords - Enforces password minimum and maximum lifetime restrictions of [*minimum, maximum*]; - Prohibits password reuse for [*number*] generations - Allows the use of a temporary password for system logons with an immediate change to a permanent password.	Note that the SFR supports only a portion of this control. Further, note that what is supported by the SFR is insufficient to meet the assignment specified in CNSSI No. 1253.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FIA_UIA_EXT.1	**User Identification and Authentication** User Identification and Authentication - Product allows the following actions to occur before I&A: (*) Display the Warning Banner,(*) [*other actions*] - Product requires each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.	AC-14	**Permitted Actions without Identification or Authentication** Organization… - Identifies [*user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions - Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.	The identification of the actions in FIA_UAU.1.1 supports identification of the actions for AC-14. AC-14 goes beyond FIA_UAU in that it requires rationale for each permitted action. The assignments must be congruent between FIA_UAU and AC-14. **Note:** FIA_UAU addresses AC-14 only for the particular evaluated product. AC-14 must still be considered in an overall system context.
		IA-2	**Identification and Authentication (Organizational Users)** - Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	IA-2 addresses the authentication of organizational users. **Note:** It is unlikely that non-organizational users will be administrative users; thus IA-8 is not mapped. **Note:** The enhancements to IA-2 discuss a number of requirements for authentication of administrative users that are not met by the NDPP.
		Note: There is an implication in FIA_UIA_EXT.1 that user identifiers exist (IA-4), but the control itself does not explicitly require that the system provide user identifiers – thus it is difficult to say the control supports IA-4.		
FIA_UAU_EXT.2	**User Identification and Authentication** Extended: Password-based Authentication Mechanism - Product provides a local password-based authentication mechanisms [selection: *other* mechanisms, none] to perform administrative user authentication.	**Note:** This SFR really doesn't map to a NIST SP 800-53 control: - IA-5 discusses management of authenticators and authenticator content, but does not require a password-based mechanism. - IA-5(1) discusses the requirements on the password *if* a password based mechanism is used. - IA-2(3) discusses local access to privileged accounts, but explicitly requires multifactor access. **If FIA_UAU_EXT.2 is completed to require multifactor access, it supports IA-2(3)**.		
FIA_UAU.7	**User Authentication** Protected Authentication Feedback - Product provides only [*list of feedback*] to the user while the authentication is in progress.	IA-6	**Authenticator Feedback** - Information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Presuming that FIA_UAU.7 was completed to require obscured feedback, IA-6 is satisfied at the product level.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FMT_MTD.1	**Management of TSF Data** Management of TSF Data • Product restricts the ability to [manage] the [TSF data] to [security administrator].	AC-3	**Access Enforcement** • Information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Depending on the access control policy, the FMT_MTD.1 requirements can be expressed via policy.
		AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Restriction of management functions to particular roles is at least a partial implementation of RBAC.
		AC-6	**Least Privilege** • Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Provision of limited management functionality divided by role supports satisfaction of least privilege. **Note:** Support for the principle of least privilege at a product level does not guarantee it is implemented effectively across the entire system.
		AU-6(7) †	**Audit Review, Analysis, and Reporting** | Permitted Actions • Organization specifies the permitted actions for each [*process; role; user*] associated with the review, analysis, and reporting of audit information.	If the TSF data being managed is audit data, this control may be satisfied.
FMT_SMF.1	**Specification of Management Functions** Specification of Management Functions • Product is of performing the following management functions: (a) administer the TOE locally and remotely; (b) update the TOE; configure the list of TOE-provided services available before I&A; configure crypto functionality, [more]	**Note:** FMT_SMF is an open-ended SFR, and few controls are written as “the administrator shall”. Rather, the controls are that the system provide a particular capability. Additionally, configuration of a capability is often implied and not an explicit requirement.		
		CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved	The explicit requirements regarding updating the TOE support this control.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			by the organization.	
FMT_SMR.2	**Security Management Roles** Restrictions on Security Roles • Product maintains the roles [*authorized administrator*]. • Product can associate users with roles. • Product ensures that the conditions [*administrator can administer the TOE locally and remotely*] are satisfied.	AC-2(7)	**Account Management** | Role-Based Schemes Organization… • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles • Monitors privileged role assignments • Takes [*actions*] when privileged role assignments are no longer appropriate.	The wording of SFR applies it to the information system, whereas the wording of the control applies it to the organization. However, the AC-2(7) control seems to say that all users have a role assignment, which fits with FMT_SMR.
		AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	AC-3(7) supports RBAC by providing the ability to define the roles.
		AC-5	**Separation of Duties** Organization… • Separates [*duties of individuals*] • Documents separation of duties of individuals • Defines information system access authorizations to support separation of duties.	Arguably, if a system provides distinct roles, that supports the provision of separation of duties and supports item c. of AC-5. **Note: This control is only supported if the administrator role is suitably narrow in power (e.g., root is not acceptable).**
		AC-6	**Least Privilege** • Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	If a system provides distinct roles, that supports the provision of separation of duties and the application of the principle of least privilege. **Note: This control is only supported if the administrator role is suitably narrow in power (e.g., root is not acceptable).**
		No Correspondence. There are no controls corresponding to FMT_SMR.2.3.		
FPT_SKP_EXT.1	**Protection of the TSF** Extended: Protection of TSF	AC-3	**Access Enforcement** • Information system	Restriction on reading keys is an access

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
	Data (for reading all symmetric keys) • Product prevents reading of all pre-shared keys, symmetric keys, and private keys.		enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	control policy, so this might support AC-3.
		IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Protecting authenticator content from unauthorized disclosure and modification • […]	Protecting symmetric keys is a form of protecting authenticator content.
		IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • […] • Enforces authorized access to the corresponding private key; • […]	Preventing reading of private keys addresses this aspect of the control.
		SC-12	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Protecting the key supports key management.
FPT_APW_EXT.1	**Protection of the TSF** Extended: Protection of Administrator Passwords • Product stores passwords in non-plaintext form. • Product prevents reading of plaintext passwords	IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Protecting authenticator content from unauthorized disclosure and modification • […]	Protecting symmetric keys is a form of protecting authenticator content.
		IA-5(1)	**Authenticator Management** | Password-Based Authentication Information system, for password-based authentication…	Supports only storing encrypted representations.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			• […] • Stores and transmits only encrypted representations of passwords • […]	
FPT_STM.1	**Time Stamps** Reliable Time Stamps • Product is able to provide reliable time stamps.	AU-8	**Time Stamps** Information system… • Uses internal system clocks to generate time stamps for audit records • Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*organization-defined granularity of time measurement*].	The SFR talks about providing reliable time stamps, presumably for auditing purposes. Most profiles modify this to integrate with NTP in the environment (giving AU-8(1)), but that is not mandated from the base SFR.
FPT_TUD_EXT.1	**Trusted Update** Extended: Trusted Software Updates and Patches • Product provides the ability to query the current version of the TOE firmware/software • Product provides administrators with the ability to initiates updates … • Product provides a means to verify software updates and patches to … using a [digital signature, published hash] prior to installation	CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	The SFR supports the digital signature aspect of this.
		SI-2	**Flaw Remediation** Organization… • […] • Installs security-relevant software and firmware updates within [*time period*] of the release of the updates; • […]	The SFR supports the installation aspect of this.
		Note: Not all aspects of the SFR correspond to controls – in particular, there is no control to query a version.		

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FPT_TST_EXT.1	**TSF Self-Test** Extended: TSF Self-Test Product runs a suite of self-tests during initial start up (on power on) to demonstrate the correct operation of the TSF.	SI-6	**Security Function Verification** Information system… • Verifies the correct operation of [*security functions*]; • Performs this verification [*(one or more): [system transitional states]; upon command by user with appropriate privilege; [frequency]*]; • […]	The SFR supports the testing and when it is performed.
FTA_SSL_EXT.1	**Session Locking** TSF -Initiated Session Locking • For local users sessions, the TSF [locks the session requiring reauthentication, terminates the session] after an administrator-specified period of inactivity.	AC-11	**Session Lock** Information system… • Prevents further access to the system by initiating a session lock after [*time period*] of inactivity or upon receiving a request from a user • Retains the session lock until the user reestablishes access using established identification and authentication procedures.	SFR supports satisfaction of AC-11 if locking is implemented.
		AC-12	**Session Termination** • Information system automatically terminates a user session after [*conditions or trigger events requiring session disconnect*].	SFR supports satisfaction of AC-12 if termination is implemented.
		Note: As this is specific to local sessions, SC-10 is not supported.		
FTA_SSL.3	**Session Locking and Termination** TSF-Initiated Termination • Product terminates an **remote** interactive session after a [*time interval of user inactivity*].	AC-12	**Session Termination** • Information system automatically terminates a user session after [*conditions or trigger events requiring session disconnect*].	Complete the assignment in AC-12 to correspond to the time period of user inactivity.
		SC-10	**Network Disconnect** • Information system terminates the network connection associated with a communications session at the end of the session or after [*time period*] of inactivity.	SC-10 addresses FTA_SSL.3 for other types of sessions – particularly network sessions (such as web sessions).
FTA_SSL.4	**Session Locking and Termination** User-Initiated Termination • Product allows user-initiated termination of the user's own	AC-12(1)	**Session Termination** | User-Initiated Logouts / Message Displays Information system… • Provides a logout capability	Although AC-12(1) is broader than FTA_SSL.4, it suffices to cover the requirements of FTA_SSL.4.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
	interactive session.		for user-initiated communications sessions whenever authentication is used to gain access to [*information resources*] • Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.	
FTA_TAB.1	**TOE Access Banners** Default TOE Access Banners • Before establishing a user session, product displays an advisory warning message regarding unauthorized use of the product.	AC-8	**System Use Notification** Information system… • Displays to users [*system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws … and states that: (1) users are accessing a U.S. Government information system; (2) usage may be monitored, recorded, and subject to audit; (3) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and (4) use of the information system indicates consent to monitoring and recording; • Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system • For publicly accessible systems: (1) displays system use information [*conditions*], before granting further access; (2) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (3) includes a description of the authorized uses of the system.	The AC-8 control is much more specific than the FTA_TAB.1 SFR regarding the content of the message and the fact that acknowledgement is required.
FTP_ITC.1	**Inter-TSF Trusted Channel**	IA-3*	**Device Identification and Authentication**	FTP_ITC.1 discusses provision of a

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	Inter-TSF Trusted Channel • Product **shall use [IPsec, SSH, TLS, TLS/HTTPS] to** provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [selection: authentication server, assignment [other]]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**. • Product permits [*the TSF **or authorized IT entities***] to initiate communication via the trusted channel. • Product initiates communication via the trusted channel for [*list of services for which the TSF is able to initiate communications*].		• Information system uniquely identifies and authenticates [*specific and/or types of devices*] before establishing a [*(one or more): local; remote; network*] connection.	communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. This control provides the identification of the end-points.
		IA-3(1)	**Device Identification and Authentication** | Cryptographic Bidirectional Authentication • Information system authenticates [*specific devices and/or types of devices*] before establishing [*local; remote; network*] connection using bidirectional authentication that is cryptographically based.	FTP_ITC.1 discusses provision of a communication channel between itself and another trusted IT product. If that trusted channel is provided using cryptographic mechanisms, this control is also addressed **at the product level**.
		IA-5(1) †*	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… • [⋮] • Stores and transmits only encrypted representations of passwords • [⋮]	FTP_ITC.1 requires protection of channel data from disclosure. If it is refined to use encryption, it would serve to ensure that passwords are transmitted encrypted, addressing IA-5(1) item c. Note that this does not mandate the password itself is encrypted; that requires an explicitly-specified component.
		SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	FTP_ITC.1 calls for protection of channel data “from modification or disclosure”. SC-8 should be completed to provide such protection (note: the SFR is ambiguous as to whether the “or” is inclusive or exclusive, but inclusive is a reasonable assumption).
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical	Whether this control is satisfied depends on the implementation method for meeting the SFR.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	
		SC-23 *	**Session Authenticity** • Information system protects the authenticity of communications sessions.	The normal use of trusted channels provides identification of the endpoints, supporting session authenticity.
FTP_TRP.1	**Trusted Path** Trusted Path • Product **shall use [IPsec, SSH, TLS, TLS/HTTPS] to** provide a **trusted** communication path between itself and [*remote*] **administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification, disclosure, [other types of integrity or confidentiality violation]*]. • Product permits [*remote **administrators***] to initiate communication via the trusted path. • Product requires the use of the trusted path for [*initial user authentication, [other services]*].	IA-5(1) †*	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… • [⋮] • Stores and transmits only encrypted representations of passwords • [⋮]	FTP_TRP.1 requires protection of communicated data. If it is completed to protect from disclosure and refined to use encryption, it would serve to ensure that passwords are transmitted encrypted, addressing IA-5(1) item c. Note that this does not mandate the password itself is encrypted; that requires an explicitly-specified component.
		SC-11†	**Trusted Path** • Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	Satisfaction of the SC-11 control depends on the completion of the assignments in the SFR.
		SC-11(1) †*	**Trusted Path** | Logical Isolation • Information system provides a trusted communications path that is logically isolated and distinguishable from other paths.	SC-11(1) addresses the "logically distinct" aspect.
		SC-23 *	**Session Authenticity** • Information system protects the authenticity of communications sessions.	The normal use of trusted path provides identification of the endpoints, supporting

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
				session authenticity.
ADV_FSP.1	**Functional Specification** Security-Enforcing Functional Specification • Developer provides a functional specification and a tracing from the functional specification to the SFRs. • Functional specification: 1. Describe the purpose and method of use for each SFR-enforcing and SFR-supporting interface. 2. Identifies all parameters associated with each SFR-enforcing and SFR-supporting interface. 3. Provides rationale for the implicit categorisation of interfaces as SFR-non-interfering. • Tracing demonstrates that the SFRs trace to interfaces in the functional specification. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator determines that the functional specification is an accurate and complete instantiation of the SFRs.	SA-4(1)	**Acquisition Process** | Functional Properties of Security Controls • Organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	The ADV_FSP family provides information about functional interfaces. The SA-4(1) control requires describing the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.
		SA-4(2)	**Acquisition Process** | Design / Implementation Information for Security Controls • Organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*(one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [design/implementation information]*] at [*level of detail*].	The ADV_FSP family provides information about functional interfaces. The SA-4(2) control requires design and implementation information; it should be completed to require them at the level of the security-relevant external system interfaces. **Note**: There is no requirement that requires separation of interfaces into security-enforcing, security non-enforcing, security non-interfering, etc.
AGD_OPE.1	**Operational User Guidance** Operational User Guidance • Developer provides operational user guidance. • Operational user guidance: 1. Describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. 2. Describes, for each user role, how to use the available interfaces provided by the	SA-5	**Information System Documentation‡** Organization… • Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms;	AGD_OPE is the combined requirement for administrator and user documentation.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	product in a secure manner. 3. Describes, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate. 4. For each user role, clearly presents each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the product. 5. Identifies all possible modes of operation of the product (including operation following failure or operational error), their consequences and implications for maintaining secure operation. 6. For each user role, describes the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST. 7. Is written to be clear and reasonable. - Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.		3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; - Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions / mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; 3. User responsibilities in maintaining the security of the system, component, or service; - [⋮]	
		Note: NIST SP 800-53 parallels the CC v2 approach, which distinguished administrator and user documentation (AGD_USR, AGD_ADM). CC v3 combined these into a single SAR, reflecting the situation that some products do not have non-administrative users.		
AGD_PRE.1	**Preparative Procedures** Preparative Procedures - Developer provides the product including its preparative procedures. - Preparative procedures: 1. Describe all the steps necessary for secure acceptance of the delivered product in accordance with the developer's delivery procedures. 2. Describe all the steps necessary for secure installation of the product and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST. - Evaluator confirms that the	SA-5	**Information System Documentation ‡** Organization… - Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. [⋮] - [⋮]	AGD_PRE.1 calls for describing all the steps necessary for secure acceptance and secure delivery. The control calls for documentation or secure configuration and installation.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	information provided meets all requirements for content and presentation of evidence. • Evaluator applies the preparative procedures to confirm that the product can be prepared securely for operation.			
ALC_CMC.1	**CM Capabilities** Labeling of the TOE • Developer provides the product and a reference for the product. • The product is labelled with its unique reference. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.	CM-9	**Configuration Management Plan ‡** Organization develops, documents, and implements a configuration management plan for the information system that… • [⋮] • Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; • [⋮]	At the product level, identification of the configuration items would include identification of the product with a unique reference.
ALC_CMS.1	**CM Scope** TOE CM Coverage • Developer provides a configuration list for the TOE. • Configuration list includes the following: the TOE itself; and the evaluation evidence required by the SARs. • Configuration list uniquely identifies the configuration items. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.	CM-3(6)*	**Configuration Change Control** | Cryptography Management • Organization ensures that cryptographic mechanisms used to provide [*security safeguards*] are under configuration management.	At the product level, if the cryptographic mechanisms providing the safeguards are part of the TOE, they would be covered by CM.
		CM-9	**Configuration Management Plan ‡** Organization develops, documents, and implements a configuration management plan for the information system that… • [⋮] • Defines the configuration items for the information system and places the configuration items under configuration management;. • [⋮]	This addresses defining the configuration items and the CM system. Note that ALC_CMC focuses on the *product*, whereas CM-9 focuses on the *system.*
		SA-10	**Developer Configuration Management ‡** Organization requires the developer of the information system, system component, or information system service to: • […] • Document, manage, and control the integrity of changes to [*configuration*	ALC_CMS captures the "[*configuration items under configuration management*]"

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			items under configuration management]; - [⁝]	
		Note: This is a *developer* process – a missing area in SA. Installation of remediated flaws is SI-2.		
ATE_IND.1	**Independent Testing** Independent Testing – Conformance - Developer provides the product for testing. - The product shall be suitable for testing. - Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. - Evaluator tests a subset of the TSF to confirm that the TSF operates as specified.	CA-2	**Security Assessments** Organization… - Develops a security assessment plan that describes the scope of the assessment including: (1) Security controls and control enhancements under assessment; (2) Assessment procedures to be used to determine security control effectiveness; and (3) Assessment environment, assessment team, and assessment roles and responsibilities; - Assesses the security controls in the information system and its environment of operation [*frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; - Produces a security assessment report that documents the results of the assessment - Provides the results of the security control assessment to [*individuals or roles*].	Independent testing *at the product level* supports testing of the overall system. As such, the *product-level* test plan can support the system-level test plans in terms of eliminating test redundancy, and the results of testing can feed into the system results.
		CA-2(1)	**Security Assessments** | Independent Assessors - Organization employs assessors or assessment teams with [*level of independence*] to conduct security control assessments.	Assessment teams for ATE_IND are drawn from NIAP-approved CCTLs that are independent from the developer. However, the CCTLs may not meet the *level of independence* dictated by the SCA.
AVA_VAN.1	**Vulnerability Analysis** Vulnerability Survey - Developer provides the product for testing. - The product is suitable for testing.	CA-2(2)	**Security Assessments** | Specialized Assessments - Organization includes as part of security control assessments, [*frequency*], [*announced; unannounced*], [(*one or*	If the assignment in CA-2(2) is completed to include a public domain search and subsequent testing of any potential vulnerabilities identified, then AVA_VAN.1

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	- Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. - Evaluator performs a search of public domain sources to identify potential vulnerabilities in the product. - Evaluator conducts penetration testing, based on the identified potential vulnerabilities, to determine that the product is resistant to attacks performed by an attacker possessing Basic attack potential.		*more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [other forms of security assessment]*].	addresses CA-2(2) *at the product level*. **Note:** Vulnerability testing at the product level does not ensure the product integrated into the complete system is configured correctly, nor does it ensure there are no other integration flaws.
		CA-8	**Penetration Testing** - Organization conducts penetration testing [*frequency*] on [*information systems or system components*].	AVA_VAN.1.3E supports CA-8 with respect to testing on the product.
		SA-11(2)	**Developer Security Testing and Evaluation** | Threat and Vulnerability Analyses - Organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.	AVA_VAN requires that there be a vulnerability analysis performed.
		Note:* RA-3 and SA-11(5) were included in the mapping published in NIST SP 800-53 Revision 4. Upon further reflection, the mappings to RA-3 and SA-11(5) are erroneous. RA-3 is risk assessment, including the likelihood and magnitude of harm, from attacks. It is not the determination of vulnerabilities. Risk assessment can only be done in the context of a particular mission and installation. As for SA-11(5), under the Common Criteria, it is the *evaluator*, not the *developer*, that performs vulnerability assessment.		

Annex C: Additional Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FCS_IPSEC_EXT.1 [Errata 2]	**IPSEC Communications** IPSEC Communications - The product implements IPSEC	SC-8	**Transmission Confidentiality and Integrity** - Information system protects	The assignment in SC-8 should be completed to correspond with the requirement for

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	architecture as specified in RFC 4301. • The product implements [tunnel mode, transport mode] • The product has a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it. • The product implements the IPsec protocol ESP as defined by RFC 4303 using [*AES algorithms and SHA-based HMACs*] • The product implements the protocol [IKEv1 as defined in RFCs…], IKEv2 as defined in … • The product ensures that IKEv1 Phase 1 exchanges only use main mode. • The product ensures that [IKEv2 SA lifetimes …, IKEv1 lifetimes…] • The product ensures all IKE protocols implement DH Groups 14… • The product perform Peer Authentication using [RSA, ECDSA] algorithm and pre-shared keys….		the [*(one or more): confidentiality; integrity*] of transmitted information.	protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Use of IPSEC supports SC-8(1)
		SC-12	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Some of the specific crypto requirements support this control.
		SC-12(2)	**Cryptographic Key Establishment and Management** | Symmetric Keys • Organization produces, controls, and distributes symmetric cryptographic keys using [*NIST FIPS-compliant; NSA-approved*] key management technology and processes.	The SFR supports this control through the approaches used for symmetric key distribution.
		SC-13 †	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches.
		SC-23 †	**Session Authenticity** Information system protects the authenticity of communications sessions.	IPSEC is used for communication sessions.
FCS_TLS_EXT.1	**TLS Protocol** TLS Protocol	SC-8	**Transmission Confidentiality and Integrity**	The assignment in SC-8 should be completed to correspond with the

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	• Product implements one or more of TLS 1.2, TLS 1.0, TLS 1.1 with the following cyphersuites [list]		• Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Whether this control is satisfied depends on the implementation method for meeting the SFR. At the SFR level, this can be addressed either through refinement of the SFR, or through appropriate specifications in the TSS that would indicated FDP_ITT is implemented through FCS operations.
		SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches fo r TLS.
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	TLS is used for communication sessions.
		Note: The second part of the SFR does not correspond to an 800-53 control.		
FCS_SSH_EXT.1	**SSH Implementation** SSH Implementation • The product implements SSH protocol in accordance with RFCs 4251… • The product ensures the SSH protocol supports the following authentication methods: public key based, password based • The product ensures that packets greater than [*bytes*] bytes are dropped • The product ensures that the SSH transport implementation uses the following encryption algorithms… • The product ensures that SSH transport implementation uses	IA-2	**Identification and Authentication (Organizational Users)** • Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	The requirement to support password or PKI authentication supports IA-2 and IA-8
		IA-8	**Identification and Authentication (Non-Organizational Users)** • Information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	The requirement to support password or PKI authentication supports IA-2 and IA-8

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	SSH_RSA and … as its public key algorithms • The product ensures that data integrity algorithms used in the SSH transport connection is … • The product ensures that DH group 14 is the only allowed key exchange method.	SC-5	**Denial of Service Protection** • Information system protects against or limits the effects of the following types of denial of service attacks: [*types of denial of service attacks*] by employing [*security safeguards*].	The requirement to drop packets larger than a certain size protects against denial of service.
		SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Use of SSH supports SC-8(1)
		SC-13 †	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches for SSH.
		SC-23 †	**Session Authenticity** Information system protects the authenticity of communications sessions.	SSH is used for communication sessions.
FCS_HTTPS_EXT.1	**HTTPS Implementation** HTTPS Implementation • The product implements HTTPS protocol in accordance with RFC 2818 • The product implements HTTPS using TLS	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system	Whether this control is satisfied depends on the implementation method for meeting the SFR. At the SFR level, this can be addressed either through refinement of

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	the SFR, or through appropriate specifications in the TSS that would indicated FDP_ITT is implemented through FCS operations.
		SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches fo r HTTPS.
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	HTTPS is used for communication sessions.
FPT_ITT.1	**Internal TOE TSF Data Transfer** Basic Internal TSF Data Transfer Protection • Product protects TSF data from ***disclosure, and detect its modification*** when it is transmitted between separate parts of the product **through the use of [IPsec, SSH, TLS, TLS/HTTS]**.	IA-5(1) †*	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… • [⋮] • Stores and transmits only encrypted representations of passwords • [⋮]	FPT_ITT.1 would serve to ensure that passwords are transmitted encrypted to a distributed component of the product, addressing IA-5(1) item c. FPT_ITT.1 should be completed to specify protection from disclosure, and refined to use encryption. Note that this does not mandate the password itself is encrypted; that requires an explicitly-specified component.
		SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The completion of the assignment in the FPT_ITT SFR must correspond with the assignment in SC-8. Note that SC-8 is not specific to internal transfers.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*(one or more): prevent unauthorized disclosure of information; detect changes to information*] during	Whether this control is satisfied depends on the implementation method for meeting the SFR. Complete the assignment in SC-8(1) to correspond with the SFR. Note that SC-8(1) is not specific to internal transfers.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			transmission unless otherwise protected by [*alternative physical safeguards*].	
Additional Audit Events for: FCS_ICS_EXT.1 FCS_TLS_EXT.1 FCS_SSH_EXT.1 FCS_HTTPS_EXT.1		AU-2†	**Audit Events ‡** Organization… • Determines system can audit [events] • [⁝] • Determines the following events are to be audited: [events]	These would need to be an additional assignment for AU-2
		AU-3(1)	**Content of Audit Records** | Additional Audit Information • Information System generates records containing [*additional information*]	These would need to be an additional assignment for AU-3(1)
		AU-12†	**Audit Generation** Information system… • Provides audit record generation capability for the auditable events defined in AU-2 a. at [*components*]; • Allows [*personnel or roles*] to select which auditable events are to be audited by specific components of the information system • Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	These would need to be an additional assignment for AU-12
FIA_PSK_EXT.1	**Identification and Authentication** Extended: Pre-Shared Key Composition • Product is able to use pre-shared keys for IPsec • Product is able to accept text-based pre-shared keys that meet [complexity requirements] • Product conditions the text-based pre-shared kesy using [SHA… method] and must be able to [restrictions]	**No Correspondence.** There are no NIST SP 800-53 controls that address the quality of the pre-shared keys.		

Network Device Protection Profile (NDPP) Extended Package – Stateful Traffic Filter Firewall

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
Overall NDPP STFFW PP		SC-7†	**Boundary Protection** Information system… • Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system • Implements subnetworks for publicly accessible system components that are [*physically; logically*] separated from internal organizational networks • Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	In general, products that provide a Traffic-Filter Firewall will support the ability for the overall system to satisfy SC-7.
FFW_RUL_EXT.1	**Firewall Requirements** Stateful Traffic Filtering • Product performs statefull traffic filtering on network packets • Product processes the following protocols: ICMPv4, ICMPv6, IPv4, IPv6, TCP, UDC, and is capable of inspecting network packet header fields defined by the following RFCs (RFC list). • Product allows the definition of stateful traffic filtering rules using the following network protocol fields… • Product allows the following operations to be associated with STF: permit, deny, and log • Product allows STF rules to be assigned to each distinct network interface • Product (a) accepts a network packet without further processing if … (b) remotes existing flows from the set of established flowed based on the following [session inactivity timeout, completion..] • Product can process the following network protocols (1) FTP, (2) … to dynamically define rules or	CM-7	**Least Functionality** Organization… • Configures the information system to provide only essential capabilities • Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*prohibited or restricted functions, ports, protocols, and/or services*].	The ability of the firewall to restrict the protocols supported supports the ability for the system to meet the ports, protocols, and services requirements of CM-7.
		SC-7†	**Boundary Protection** Information system… • Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system • Implements subnetworks for publicly accessible system components that are [*physically; logically*] separated from internal organizational networks • Connects to external networks or information systems only through managed interfaces	The basic firewall rule set supports the ability to control communications at the points where the STFFW is installed, and provides the boundary protection device called out in SC-7.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	establish sessions… • Product enforces the following default STF rules on all network traffic… (long list of rules) • When RUL_EXT.1.6 or RUL_EXT.1.7 do not apply, the product processes the applicable STF rules in the following order: administrator defined • When RUL_EXT.1.6 or RUL_EXT.1.7 do not apply, the product denies packet flow if a matching rule is not identified		consisting of boundary protection devices arranged in accordance with an organizational security architecture.	
		SC-7(5)	**Boundary Protection** | Deny by Default / Allow by Exception • Information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).	The SFR element that denies traffic unless there is a matching rule supports satisfaction of SC-7(5).
		SC-7(17)	**Boundary Protection** | Automated Enforcement of Protocol Formats • Information system enforces adherence to protocol formats.	The restriction to particular protocol fields may support enforcement to specific protocol formats.
		SC-10	**Network Disconnect** • Information system terminates the network connection associated with a communications session at the end of the session or after [*time period*] of inactivity.	The ability to terminate connections after a period of inactivity supports SC-10.
Additional audit events for FFW_RUL_EXT.1		AU-2†	**Audit Events ‡** Organization… • Determines system can audit [events] • [⋮] • Determines the following events are to be audited: [events]	These would need to be an additional assignment for AU-2
		AU-3(1)	**Content of Audit Records** | Additional Audit Information • Information System generates records containing [*additional information*]	These would need to be an additional assignment for AU-3(1)
		AU-12†	**Audit Generation** Information system… • Provides audit record generation capability for the auditable events defined in AU-2 a. at [*components*]; • Allows [*personnel or roles*] to select which auditable events are to be audited by specific components of the	These would need to be an additional assignment for AU-12

Common Criteria Version 3.x SFR/SAR	**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
		information system • Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	
Additional management functions for FFW_RUL_EXT.6	**Note:** There are no enhancements within SC-7 that specifically address *administrator configuration* of the firewall rules. AC-6 (Least Privilege) might be a possibility, but given that the PPs allow a single monolithic roll, it is difficult to call that least privilege. If the specific configuration and restrictions are intended to meet a specific STIG requirement, then the additional management function might support CM-6, which discusses configuration in accordance with organizational standards.		
Additional assurance activities for AVA_VAN.1	CA-2(2)	**Security Assessments** | Specialized Assessments • Organization includes as part of security control assessments, [*frequency*], [*announced; unannounced*], [*(one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [other forms of security assessment]*].	These would be additional assessments.
	CA-8	**Penetration Testing** • Organization conducts penetration testing [*frequency*] on [*information systems or system components*].	AVA_VAN.1.3E supports CA-8 with respect to testing on the product.
	SA-11(2)	**Developer Security Testing and Evaluation** | Threat and Vulnerability Analyses • Organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.	AVA_VAN requires that there be a vulnerability analysis performed.
	Note:* RA-3 and SA-11(5) were included in the mapping published in NIST SP 800-53 Revision 4. Upon further reflection, the mappings to RA-3 and SA-11(5) are erroneous. RA-3 is risk assessment, including the likelihood and magnitude of harm, from attacks. It is not the determination of vulnerabilities. Risk assessment can only be done in the context of a particular mission and installation. As for SA-11(5), under the Common Criteria, it is the *evaluator*, not the *developer*, that performs vulnerability assessment.		

Additional Recommendations

- CCEVS should standardize the extended requirements and iterations across all of its profiles, so that (for example) FCS_COP.1(1) is reliably asymmetric encryption, COP.1(2) is reliably hashing, and COP.1(3) is digital signatures, etc. This will drastically make it easier to compare different profiles.