Cisco Stealthwatch Enterprise 7.1

Security Target

Version 1.1

July 17, 2020

Americas Headquarters:

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

Table of Contents

List of Tables

List of Figures

List of Acronyms

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

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program (under NIST)
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FC / SFC	Stealthwatch Flow Collector
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FS / SFS	Stealthwatch Flow Sensor
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IT	Information Technology
NDcPP	collaborative Network Device Protection Profile
NIST	National Institute of Standards and Technology
OS	Operating System
PP	Protection Profile
UDP	User Datagram Protocol
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SMC	Stealthwatch Management Console
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDPD	Stealthwatch UDP Director

DOCUMENT INTRODUCTION

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco Stealthwatch Enterprise (Stealthwatch). This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

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

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

1.1 ST and TOE Reference

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

Table 2: ST and TOE Identification

Name	Description
ST Title	Cisco Stealthwatch Enterprise
ST Version	1.1
Publication Date	July 17, 2020
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Stealthwatch Enterprise
TOE Hardware Models	• Stealthwatch Management Console (ST-SMC2200-K9, ST-SMC2210-k9 and L-ST-SMC-VE-K9) • Stealthwatch Flow Collector (ST-FC4200-K9, ST-FC4210-k9, ST-FC5200D with ST-FC5200E, ST-FC5210-D with ST-FC5210-E, and L-ST-FC-VE-K9) • Stealthwatch Flow Sensor (ST-FS1200-K9, ST-FS1210-k9, ST-FS2200-K9, ST-FS3200-K9, ST-FS3210-k9, ST-FS4200-K9, ST-FS4210-k9, and L-ST-FS-VE-K9) • Stealthwatch UDP Director (ST-UDP2200-K9, ST-UDP2210-k9, and L-ST-UDP-VE-K9)
TOE Software Version	7.1
Keywords	Threat Detection, Incident Response, Forensics

1.2 TOE Overview

The Cisco Stealthwatch Enterprise TOE is a centrally managed system of distributed components for collection, storage, analysis, of network telemetry data. The TOE includes the models as defined in Table 2 in section 1.1. The evaluated configurations of the TOE consist of one Stealthwatch Management Console (SMC), one or more Flow Collectors (FC), one or more Flow

Sensors (FS), and one or more UDP Directors (UDPD). Each of the TOE components is available as a stand-alone physical appliance, or as a virtual appliance. The physical and virtual appliances provide equivalent functionality and a mixture of physical and virtual appliances can be deployed together.

1.2.1 TOE Product Type

Cisco Stealthwatch Enterprise provides visibility and security analytics (threat detection, and threat response) using on network traffic telemetry data. Stealthwatch Enterprise can generate telemetry data directly (by directly monitoring traffic flows), or can collect telemetry data generated by devices in an existing network infrastructure.

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 3: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with TLS Client (browser)	Yes	Stealthwatch supports the latest versions of Chrome, Firefox, and Microsoft Edge. The browser is required to remotely manage the TOE via the WebUI on SMC.
Management Workstation with Console Connection	Yes	Required for initial installation of each device, optional thereafter. This includes any workstation that is directly connected to the console port (or keyboard-video-mouse ports) of any TOE component.
Certification Authority	Yes	The external CA is used be used to provide new device identity certificates for each TOE component to replace their initial self-signed certificates. The CA-signed certificates are used for all TLS connections to/from all TOE components.
LDAP Server	No	Any AAA server that supports LDAP over TLS. The TOE maintains local administrative accounts on SMC, and those accounts can be used for remote administration, though most deployments will opt to also use LDAP for authentication of administrative accounts.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Stealthwatch Enterprise Target of Evaluation (TOE). The TOE is a system comprised of four types of servers, each of which is comprised of both software and hardware. The software is a proprietary build of Linux with Cisco Stealthwatch applications; the hardware is Cisco UCS server platforms, which are used for the physical appliances as well as for virtual appliances. The software is comprised of the Stealthwatch software image Release 7.1.

The Cisco Stealthwatch Enterprise components that comprise the TOE have common hardware characteristics. Any hardware differences, e.g. the amount of RAM or drive space, of the number of network interfaces, affect only non-TSF relevant functionality such as throughput and amount of storage, and therefore support security equivalency of the TOE component models.

This TOE is considered a 'distributed' TOE as defined in NDcPP in that this TOE requires multiple distinct TOE components to operate as a logical whole in order to fulfil the requirements of NDcPP, and those TOE components are separated (distributed) across a network. This TOE includes one management component (SMC), and three types of managed network devices (FC, FS, and UDPD). In a distributed TOE not all requirements need to be enforced by each TOE component; a summary table showing which SFRs apply to which TOE component can be found in Annex B: SFR TOE Components Mapping.

The Stealthwatch Management Console (SMC) provides the administrative interface to manage all TOE components. The SMC aggregates, organizes, and presents analysis from up to 25 Flow Collectors, the Cisco Identity Services Engine, and other sources. It provides a graphical representations of network traffic, identity information, customized summary reports, and integrated security and network intelligence for comprehensive analysis.

The Stealthwatch Flow Collector (FC) receives telemetry data from Stealthwatch Flow Sensors and other sources such as routers, switches, firewalls, and endpoint agents. The FC stores collected data in its internal database, analyses the data, sends event notifications to SMC, and supports further forensics and long term data analysis via customized reporting provided by the SMC. Multiple Flow Collectors may be managed by a single SMC, and are available as hardware appliances or as virtual machines.

The Flow Sensor (FS) produces telemetry for segments of the switching and routing infrastructure that can't generate NetFlow natively. The Flow Sensors connect directly to a mirroring port or network tap to monitor network traffic and generate telemetry data. Multiple Flow Sensors can be managed by a single SMC, and are available as hardware appliances or as virtual appliances to monitor virtual machine environments.

The UDP Director (UDPD) simplifies the collection and distribution of network and security data across the enterprise. It helps reduce the processing power on network routers and switches by receiving essential network and security information from multiple locations and then forwarding it to a single data stream to one or more destinations. Multiple UDP Directors can be managed by a single SMC, and are available as hardware appliances or as virtual appliances to monitor virtual machine environments.

Table 4 below describes the models that have been claimed within this evaluation:

Table 4 TOE Component Models and Specifications

Appliance	**Part Number**	**Server platform**	**Entropy Source**
Stealthwatch appliances on UCS C-Series M5 servers			
Stealthwatch Management Console	ST-SMC2210-K9 L-ST-SMC-VE-K9	UCSC-C220-M5SX	Intel® Skylake Scalable Processor
Stealthwatch UDP Director	ST-UDP2210-K9		

	L-ST-UDP-VE-K9		
Stealthwatch Flow Sensor	ST-FS1210-K9 ST-FS3210-K9 ST-FS4210-K9 L-ST-FS-VE-K9		
Stealthwatch Flow Collector	ST-FC4210-K9 L-ST-FC-VE-K9		
Stealthwatch Flow Collector Engine	ST-FC5210E		
Stealthwatch Flow Collector Database	ST-FC5210D	UCSC-C240-M5SX	
Stealthwatch appliances on UCS C-Series M4 servers			
Stealthwatch Management Console	ST-SMC2200-K9 L-ST-SMC-VE-K9	UCSC-C220-M4S	Intel® Xeon® E5-26XX
Stealthwatch UDP Director	ST-UDP2200-K9 L-ST-UDP-VE-K9		
Stealthwatch Flow Sensor	ST-FS1200-K9 ST-FS2200-K9 ST-FS3200-K9 ST-FS4200-K9 L-ST-FS-VE-K9		
Stealthwatch Flow Collector	ST-FC4200-K9, or L-ST-FC-VE-K9		
Stealthwatch Flow Collector Engine	ST-FC5200E		
Stealthwatch Flow Collector Database	ST-FC5200D	UCSC-C240-M4S2	

1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.5 below and includes the Cisco Stealthwatch software. The figure below shows each of the four TOE components in the operational environment. The diagram shows one of each appliance (SMC, FC, FS, and UDPD), where each appliance can be either physical or virtual. The diagram shows only a single icon for the FC though the FC physical appliance is available in two forms: as a single appliance (FC4210) with the engine and database installed to the same appliance; or as a pair of appliances with the FC Engine on one appliance (FC5200E) and the FC Database on the other appliance (FC5200D). Regardless of the form-factor, each FC model provides the same TOE security functionality.

Figure 1: TOE and Environment

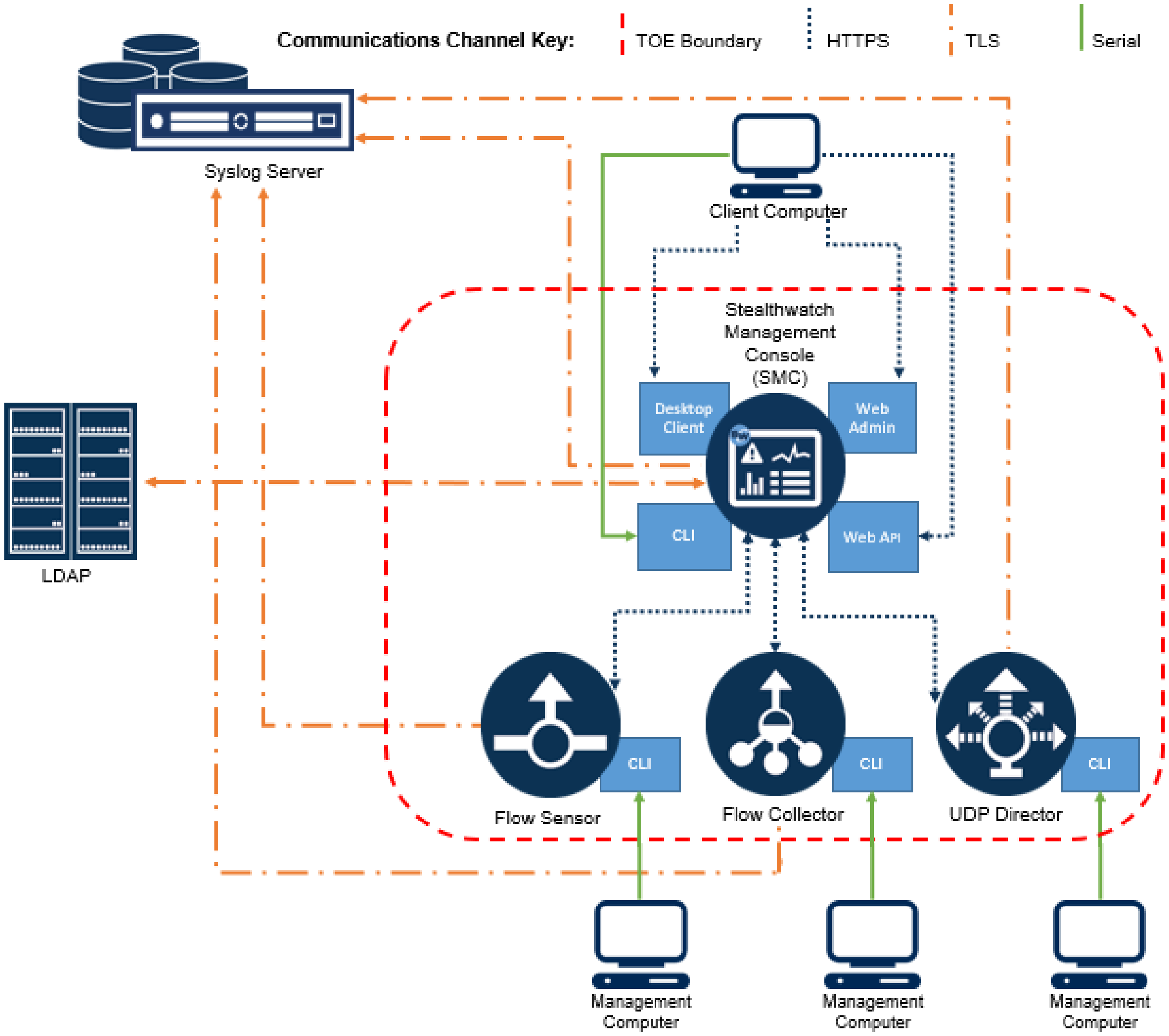

Figure 1 shows the protocols and connections (TLS, HTTPS, and the serial connections) that are relevant to requirements within NDcPP. The TOE components also use other protocols (e.g. DNS, NetFlow and sFlow) that are not relevant to NDcPP requirements as that traffic does not contain TSF data. Each appliance contains a DNS client for FQDN resolution (e.g. for LDAP servers, CAs, URL distribution points, and OCSP responders). The FC receives NetFlow or sFlow traffic (depending on whether the FC was installed in sFlow or NetFlow mode) from UDPD and FS. The FS monitors network traffic (via its promiscuous (passive) interface) and generates sFlow or NetFlow data to transmit to an FC. The UDPD receives sFlow or NetFlow traffic from monitored devices and forwards that traffic to an FC.

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution composed of four major components: SMC, FC, FS, and UDPD. The network, on which they reside, is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE and includes the Cisco

Stealthwatch Compliance Guide and additional guidance documents referenced therein, all of which are downloadable from the http://cisco.com web site. The TOE is comprised of the physical specifications as described in Table 4 in section 1.3 above.

1.6 Logical Scope of the TOE

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

1. Security Audit
2. Communication
3. Cryptographic Support
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels

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

1.6.1 Security Audit

The Cisco Stealthwatch Enterprise provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Stealthwatch Enterprise generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, configures secure transmission of audit records to a remote audit server, and manages audit data storage. The TOE provides the administrator with a local circular audit trail. Audit messages are stored locally and transmitted over an encrypted channel to an external audit server.

1.6.2 Communication

The TOE allows authorized administrators to control which Stealthwatch appliance (FC, FS, and UDPD) is managed by the SMC. This is performed through a registration process over TLS. The administrator can also de-register an appliance if he or she wishes to no longer manage it through the SMC. For this TOE the process of registration/joining a new managed appliance (FC, FS, UDPD) to the SMC is manually initiated by the administrator installing each appliance. The initial TLS connection is authenticated to the SMC using the SMC administrator’s username/password, at which point the appliances exchange their X.509 certificates, and from that point forward all TLS communications among appliances are authenticated using X.509 certificates.

1.6.3 Cryptographic Support

The TOE provides cryptography in support of other Cisco Stealthwatch security functionality. This cryptography has been validated by the NIST CAVP (see section 7.2 for certificate references).

The TOE provides cryptography in support for TLS, which is used for remote administrative management, and secure communication among TOE components, and connects from the TOE to LDAP and syslog servers. The cryptographic services provided by the TOE are described in Table 5 below.

Table 5: TOE Provided Cryptography

Cryptographic Method	Use within the TOE
AES	Used to encrypt TLS session traffic.
ECDH	Used to provide key exchange in TLS.
RSA Signature Services	X.509 certificate signing and verification. Data signing and verification in TLS.
HMAC	Used for keyed hash, integrity services in TLS session establishment.
DRBG	Used for random number generation Used in TLS session establishment.
SHA	Used to provide TLS traffic integrity verification
Transport Layer Security (TLS)	Used in TLS session establishment.

During initial installation each TOE component generates its own unique self-signed X.509v3 certificate, and during initial configuration all those certificates are replaced with new CA-signed identity certificates which are then used for all TLS connections including mutual authentication of TLS connections among TOE components. Each TOE component generates its own unique keypair and its own certificate signing requests (CSR), and imports TLS certificates that have been signed by an external CA server.

1.6.4 Identification and authentication

TOE components perform two types of authentication: password-based authentication of administrators for remote administration TOE; and certificate-based authentication of devices. Device-level authentication allows TOE components to establish secure channels with other TOE components, and with external servers (LDAP and syslog).

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console, and the GUI (accessible via HTTPS/TLS). For authentication to the GUI, the TOE optionally supports use of a AAA server (using LDAP over TLS), which would be outside the TOE boundary.

The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters.

After a configurable number of incorrect login attempts at administrative interfaces where authentication is processed locally (i.e. where LDAP is not used), the TOE will lock the offending account until an Administrator defined time period has elapsed.

1.6.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure HTTPS/TLS session or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users; all identification and authentication; all audit functionality of the TOE; all TOE cryptographic functionality; the timestamps maintained by the TOE; and updates to the TOE.

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. This is used to provide any information deemed necessary by the administrator. After a set amount of time of inactivity, the administrator will be locked out of the administrator interface.

1.6.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of plaintext cryptographic keys and passwords.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE’s clock manually.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software. The TOE performs self-testing to verify correct operation of its cryptographic module. The TOE components are not general-purpose operating systems; root access is not permitted, external software applications cannot be installed, and access to memory space is restricted to TOE functions.

The TOE is distributed, including multiple appliances that communicate with each other over a network. These internal TOE communications between TOE components are protected within TLS, and authenticated using X.509 certificates.

1.6.7 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the CLI management interface and the WebUI prior to allowing any administrative access to the TOE.

1.6.8 Trusted Path/Channels

The TOE establishes a trusted path with syslog servers using TLS, and with LDAP servers using TLS. Remote administration of the TOE uses TLS/HTTPS. All communications between TOE components are protected within TLS; the initial joining of TOE components is authenticated using a username and password that’s manually entered during the joining process, and subsequent communications between TOE components are automatically authenticated using X.509 certificates.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation. The exclusion of this functionality does not affect compliance to the collaborative Protection Profile for Network Devices (NDcPP).

Table 6: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
SNMP	This feature is disabled by default and cannot be configured for use in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target.
RADIUS and TACACS+	LDAP over TLS can be used instead of RADIUS and TACACS+, which cannot be secured in TLS.
NTP	The NTP client feature is enabled by default on all Stealthwatch appliances. Use of NTP was not tested during the CC evaluation, so the NTP clients must be disabled on all appliances to conform to the CC-evaluated configuration.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated April 2017. For a listing of Assurance Requirements claimed see section 5.5.

The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 7 below:

Table 7: Protection Profiles

Protection Profile	Version	Date
collaborative Protection Profile for Network Devices (NDcPP)	2.1	24-September-2018

The TOE and ST are conformant with the Protection Profiles as listed in Table 7 above. NIAP Technical Decisions (TDs) have been applied as indicated in Table 8 below:

Table 8: NIAP Technical Decisions

TD #	TD Name	Protection Profiles	Applied to this TOE
TD0484	NIT Technical Decision for Interactive sessions in FTA_SSL_EXT.1 & FTA_SSL.3	CPP_ND_V2.1	FTA_SSL_EXT.1 & FTA_SSL.3
TD0483	NIT Technical Decision for Applicability of FPT_APW_EXT.1	CPP_ND_V2.1	FPT_APW_EXT.1
TD0482	NIT Technical Decision for Identification of usage of cryptographic schemes	CPP_ND_V2.1	TSS for FCS_CKM.1.1, and FCS_CKM.2.1
TD0481	NIT Technical Decision for FCS_(D)TLSC_EXT.X.2 IP addresses in reference identifiers	CPP_ND_V2.1	FCS_TLSC_EXT.1.2, FCS_TLSC_EXT.2.2
TD0480	NIT Technical Decision for Granularity of audit events	CPP_ND_V2.1	FAU_GEN.1
TD0478	NIT Technical Decision for Application Notes for FIA_X509_EXT.1 iterations	CPP_ND_V2.1	FIA_X509_EXT.1/Rev, FIA_X509_EXT.1/ITT
TD0477	NIT Technical Decision for Clarifying FPT_TUD_EXT.1 Trusted Update	CPP_ND_V2.1	FPT_TUD_EXT.1, ND SD V2.1
TD0475	*NIT Technical Decision for Separate traffic consideration for SSH rekey*	*CPP_ND_V2.1*	*Not applied because this ST does not include FCS_SSHC_EXT.1.1, or FCS_SSHS_EXT.1.1.*
TD0453	*NIT Technical Decision for Clarify authentication methods SSH clients can use to authenticate SSH se*	*CPP_ND_V2.1*	*Not applied because this ST does not include FCS_SSHC_EXT.1.9*
TD0451	NIT Technical Decision for ITT Comm UUID Reference Identifier	CPP_ND_V2.1	FCS_TLSS_EXT.1.2, FCS_TLSS_EXT.2.2
TD0450	NIT Technical Decision for RSA-based ciphers and the Server Key Exchange message	CPP_ND_V2.1	FCS_TLSS_EXT.*.3, ND SD v2.1

TD0447	*NIT Technical Decision for Using 'diffie-hellman-group-exchange-sha256' in FCS_SSHC/S_EXT.1.7*	*CPP_ND_V2.1*	*Not applied because this ST does not include FCS_SSHC_EXT.1.7, or FCS_SSHS_EXT.1.7.*
TD0425	NIT Technical Decision for Cut-and-paste Error for Guidance AA	CPP_ND_V2.1	FTA_SSL.3, ND SD V2.1
TD0424	*NIT Technical Decision for NDcPP v2.1 Clarification - FCS_SSHC/S_EXT1.5*	*CPP_ND_V2.1*	*Not applied because this ST does not include FCS_SSHC_EXT.1.5, or FCS_SSHS_EXT.1.5.*
TD0423	NIT Technical Decision for Clarification about application of RfI#201726rev2	CPP_ND_V2.1	ND SD V2.1
TD0412	*NIT Technical Decision for FCS_SSHS_EXT.1.5 SFR and AA discrepancy*	*CPP_ND_V2.1*	*Not applied because this ST does not include FCS_SSHS_EXT.1.5.*
TD0411	*NIT Technical Decision for FCS_SSHC_EXT.1.5, Test 1 - Server and client side seem to be confused*	*CPP_ND_V2.1*	*Not applied because this ST does not include FCS_SSHC_EXT.1.5.*
TD0410	NIT technical decision for Redundant assurance activities associated with FAU_GEN.1	CPP_ND_V2.1	FAU_GEN.1, ND SD V2.1
TD0409	NIT decision for Applicability of FIA_AFL.1 to key-based SSH authentication	CPP_ND_V2.1	FIA_AFL.1, ND SD v2.1
TD0408	NIT Technical Decision for local vs. remote administrator accounts	CPP_ND_V2.1	FIA_AFL.1, FIA_UAU_EXT.2, FMT_SMF.1
TD0407	*NIT Technical Decision for handling Certification of Cloud Deployments*	*CPP_ND_V2.1*	*Not applied because this ST does not include Cloud Deployments*
TD0402	NIT Technical Decision for RSA-based FCS_CKM.2 Selection	CPP_ND_V2.1	FCS_CKM.2, ND SD V2.1
TD0401	NIT Technical Decision for Reliance on external servers to meet SFRs	CPP_ND_V2.1	FTP_ITC.1
TD0400	NIT Technical Decision for FCS_CKM.2 and elliptic curve-based key establishment	CPP_ND_V2.1	FCS_CKM.1, FCS_CKM.2
TD0399	NIT Technical Decision for Manual installation of CRL (FIA_X509_EXT.2)	CPP_ND_V2.1	FIA_X509_EXT.2, ND SD V2.1
TD0398	*NIT Technical Decision for FCS_SSH*EXT.1.1 RFCs for AES-CTR*	*CPP_ND_V2.1*	*Not applied because this ST does not include FCS_SSHC_EXT.1.1, or FCS_SSHS_EXT.1.1.*
TD0397	NIT Technical Decision for Fixing AES-CTR Mode Tests	CPP_ND_V2.1	FCS_COP.1/DataEncryption, ND SD V2.1
TD0396	NIT Technical Decision for FCS_TLSC_EXT.1.1, Test 2	CPP_ND_V2.1	FCS_TLSC_EXT.1.1, ND SD V2.1
TD0395	*NIT Technical Decision for Different Handling of TLS1.1 and TLS1.2*	*CPP_ND_V2.1*	*Not applied because this ST does not include FCS_TLSS_EXT.2.4, or FCS_TLSS_EXT.2.5.*

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

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

- collaborative Protection Profile for Network Devices, Version 2.1, 24-September-2018

2.3.2 TOE Security Problem Definition Consistency

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

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

2.3.3 Statement of Security Requirements Consistency

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

3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

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

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with "osp" specifying a unique name.

3.1 Threats

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

Table 9 Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

Threat	Threat Definition
T.WEAK_AUTHENTICATION_ ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALIT Y_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALIT Y_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.2 Assumptions

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

Table 10 TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

Assumption	Assumption Definition
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.3 Organizational Security Policies

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

Table 11 Organizational Security Policies

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4 SECURITY OBJECTIVES

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

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

4.1 Security Objectives for the TOE

The collaborative Protection Profile for Network Devices v2.0 does not define any security objectives for the TOE.

4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.2 are considered to be security objectives for the environment. The following are the Protection Profile non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 12 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

Environment Security Objective	IT Environment Security Objective Definition
OE.COMPONENTS_RUNNING	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated April 2017* and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Assignment completed within a selection in the PP: the completed assignment text is indicated with *<u>italicized and underlined text</u>*;
- Refinement made by PP author: Indicated with **bold** text;
- Refinement made by ST author: Indicated with **<u>bold and underlined</u>** text;
- Selection: Indicated with <u>underlined</u> text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the NDcPP itself, the formatting used in the NDcPP has been retained.

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs. Formatting conventions outside of operations and iterations matches the formatting specified within the NDcPP.

5.2 TOE Security Functional Requirements

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

Table 13 Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_GEN_EXT.1	Security Audit Generation
	FAU_STG_EXT.1	Protected Audit Event Storage
	FAU_STG_EXT.3	Protected Local Audit Event Storage for Distributed TOEs
FCO: Communication	FCO_CPC_EXT.1	Component Registration Channel Definition
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (Refined)
	FCS_CKM.2	Cryptographic Key Establishment (Refined)
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)

Class Name	Component Identification	Component Name
	FCS_HTTPS_EXT.1	HTTPS Protocol
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_TLSC_EXT.1	TLS Client Protocol
	FCS_TLSC_EXT.2	TLS Client Protocol with Authentication
	FCS_TLSS_EXT.1	TLS Server Protocol
	FCS_TLSS_EXT.2	TLS Server Protocol with Mutual Authentication
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management (Refinement)
	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1/ITT	X.509 Certificate Validation
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
FMT: Security management	FMT_MOF.1/ManualUpdate	Management of security functions behaviour
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing (Extended)
	FPT_TUD_EXT.1	Trusted update
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1/Admin	Trusted Path
	FTP_TRP.1/Join	Trusted Path (Refinement)

5.3 SFRs Drawn from NDcPP

5.3.1 Security audit (FAU)

5.3.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) All administrator actions comprising:

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*
- *[no other actions];*

d) *Specifically defined auditable events listed in Table 14.*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, [*information specified in column three of Table 14*].

Table 14 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_GEN_EXT.1	None.	None.
FAU_STG_EXT.1	None.	None.
FAU_STG_EXT.3	None.	None.
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Identities of the endpoints pairs enabled or disabled.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	Reason for failure.
FCS_RBG_EXT.1	None.	None.
FCS_TLSC_EXT.1	Failure to establish an TLS session	Reason for failure.
FCS_TLSC_EXT.2	Failure to establish an TLS session	Reason for failure.
FCS_TLSS_EXT.1	Failure to establish an TLS session	Reason for failure.
FCS_TLSS_EXT.2	Failure to establish an TLS session	Reason for failure.

SFR	Auditable Event	Additional Audit Record Contents
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/ITT	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation. Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation. Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.

SFR	Auditable Event	Additional Audit Record Contents
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.
FTP_TRP.1/Join	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.

Application Note

NIAP TD0410 has been applied to FAU_GEN.1, though it does not change the text of this SFR.

NIAP TD0480 has been applied to FAU_GEN.1, though it doesn't impact the SFR text.

5.3.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.3.1.1 FAU_GEN_EXT.1 Security Audit Generation

FAU_GEN_EXT.1.1 The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

5.3.1.2 FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself [The TOE shall be a distributed TOE that stores audit data on the following TOE components: *[SMC, FC, FS, and UDPD]*.

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule: [*oldest records will be overwritten*], [*no other action*]] when the local storage space for audit data is full.

5.3.1.1 FAU_STG_EXT.3 Protected Local Audit Event Storage for Distributed TOEs

FAU_STG_EXT.3.1 The TSF of each TOE component which stores security audit data locally shall perform the following actions when the local storage space for audit data is full: [

Component:	*Action:[*
SMC	Overwrite previous audit records according to the following rule: *[oldest records will be overwritten when the local storage space for audit data is full]*
FC	Overwrite previous audit records according to the following rule: *[oldest records will be overwritten when the local storage space for audit data is full]*
FS	Overwrite previous audit records according to the following rule: *[oldest records will be overwritten when the local storage space for audit data is full]*
UDPD	Overwrite previous audit records according to the following rule: *[oldest records will be overwritten when the local storage space for audit data is full]*

]].

5.3.2 Communication Partner Control (FCO)

5.3.2.1 FCO_CPC_EXT.1 Component Registration Channel Definition

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [

- A channel that meets the secure registration channel requirements in FTP_TRP.1/Join]

for at least TSF data.

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

5.3.3 Cryptographic Support (FCS)

5.3.3.1 FCS_CKM.1 Cryptographic Key Generation (Refinement)

FCS_CKM.1.1 Refinement: The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]~~.

Application Note

NIAP TD0400 has been applied to FCS_CKM.1, though it doesn't impact the SFR text.

5.3.3.2 FCS_CKM.2 Cryptographic Key Establishment (Refinement)

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- RSA-based key establishment schemes that meets the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1;
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

~~] that meets the following: [assignment: list of standards].~~

Application Note

NIAP TD0400 has been applied to FCS_CKM.2, though it doesn't impact the SFR text.

NIAP TD0402 has been applied to FCS_CKM.2.

5.3.3.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- *For plaintext keys in volatile storage, the destruction shall be executed by a [*destruction of reference to the key directly followed by a request for garbage collection*];*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [*
    - o instructs a part of the TSF to destroy the abstraction that represents the key*]]*

that meets the following: *No Standard*.

5.3.3.4 FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption Refinement: The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm *AES used in* [CBC, GCM] *mode* and cryptographic key sizes [128 bits, 256-bits] that met the following: *AES as specified in ISO 18033-3*, [CBC as specified in ISO 10116, GCM as specified in ISO 19772].

Application Note

NIAP TD0397 has been applied to FCS_COP.1/DataEncryption, though it impacts only the tests, not the text of SFR.

5.3.3.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen Refinement: The TSF shall perform *cryptographic signature services* **(***generation and verification*) in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes **(modulus)** *[4096 bits]*,
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes *[256, 384, and 521 bits]*

]

that meet the following: [

- For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS2v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,
- For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4

]

5.3.3.6 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ and **message digest sizes [*160, 256, 384, 512*] bits** that meet the following: *ISO/IEC 10118-3:2004*.

5.3.3.7 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384] and cryptographic key sizes [*160-bit, 256-bit, 384-bit*] **and message digest sizes** [**160, 256, 384**] **bits** that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.

5.3.3.8 FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [not require client authentication] if the peer certificate is deemed invalid.

5.3.3.9 FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*1*] hardware based noise source] with minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011, of the keys and CSPs that it will generate.

5.3.3.10 FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

  ].

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifiers of the following types: [identifiers defined in RFC 6125, IPv4 addresses in CN or SAN] are matched to the reference identifiers.

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSC_EXT.1.4 The TSF shall [present the Supported Elliptic Curves Extension with the following NIST curves: [secp256r1, secp384r1, secp521r1] and no other curves] in the Client Hello.

Application Note

NIAP TD0396 has been applied to FCS_TLSC_EXT.1.1, though it impacts only the tests, not the text of SFR.

NIAP TD0481 has been applied to FCS_TLSC_EXT.1.2. This SFR is applicable to LDAP-over-TLS initiated from the SMC TOE component for which the reference identifier can be the FQDN of the LDAP server, or the IPv4 address of the LDAP server.

5.3.3.11 FCS_TLSC_EXT.2 TLS Client Protocol with Authentication

FCS_TLSC_EXT.2.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

].

FCS_TLSC_EXT.2.2 The TSF shall verify that the presented identifiers of the following types: [identifiers defined in RFC 6125 **(for distributed TOE communications)**, IPv4 addresses in CN or SAN **(for syslog-over-TLS)**] are matched to reference identifiers.

FCS_TLSC_EXT.2.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- *Not implement any administrator override mechanism*

].

FCS_TLSC_EXT.2.4 The TSF shall [present the Supported Elliptic Curves Extension with the following NIST curves: [secp256r1, secp384r1, secp521r1] and no other curves] in the Client Hello.

FCS_TLSC_EXT.2.5 The TSF shall support mutual authentication using X.509v3 certificates.

Application Note

NIAP TD0396 has been applied to FCS_TLSC_EXT.2.1, though it impacts only the tests, not the text of SFR.

NIAP TD0481 has been applied to FCS_TLSC_EXT.2.2. This SFR is applicable to distributed TOE communications (per FPT_ITT.1) for which the reference identifier is the FQDN of each interconnected TOE component. This SFR is also applicable to syslog-over-TLS used by each TOE component for which the reference identifier is the IPv4 address of the syslog server.

5.3.3.12 FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

].

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [*none*].

FCS_TLSS_EXT.1.3 The TSF shall [perform RSA key establishment with key size [4096 bits]; generate EC Diffie-Hellman parameters over NIST curves [secp256r1, secp384r1, secp521r1] and no other curves; generate Diffie-Hellman parameters of size [2048 bits]].

Application Note

NIAP TD0450 has been applied to this SFR, though it does not impact the text of this SFR.

5.3.3.13 FCS_TLSS_EXT.2 TLS Server Protocol with Mutual Authentication

FCS_TLSS_EXT.2.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
  ].

FCS_TLSS_EXT.2.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [*none*].

FCS_TLSS_EXT.2.3 The TSF shall [perform RSA key establishment with key size [4096 bits]; generate EC Diffie-Hellman parameters over NIST curves [secp256r1, secp384r1, secp521r1] and no other curves; generate Diffie-Hellman parameters of size [2048 bits]].

FCS_TLSS_EXT.2.4 The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.5 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

  ].

FCS_TLSS_EXT.2.6 The TSF shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

Application Note

NIAP TD0450 has been applied to this SFR, though it does not impact the text of this SFR.

5.3.4 Identification and authentication (FIA)

5.3.4.1 Authentication Failure Management (FIA_AFL)FIA_AFL.1 Authentication Failure Management (Refinement)

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*1-99*] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

Application Note

NIAP TD0408 has been applied to this SFR.

NIAP TD0409 has been applied to this SFR, though it does not impact the text of this SFR.

5.3.4.2 FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: *[*“!”, “@”, “#”, “$”, “%”,“(“, “)”, *[“<”, “>”, “.”, “?”, “/”, “’”, “””, “\”, “|”, “:”, “;”, “`”, “~”, “-“, “_”, “+”, “=”, “{”, “}”, “[“, and “]”]*];

b) Minimum password length shall be configurable to between [*8*] and [*30*] characters.

5.3.4.3 FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [no other actions]

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated action on behalf of that administrative user.

5.3.4.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local [password-based, [*LDAP*]] authentication mechanism, to perform local administrative user authentication.

Application Note

NIAP TD0408 has been applied to this SFR.

5.3.4.5 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress **at the local console**.

5.3.4.1 FIA_X509_EXT.1/ITT X.509 Certificate Validation

FIA_X509_EXT.1.1/ITT The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of two certificates**.
- The certification path must terminate with a trusted CA certificate.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [no revocation method]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - o *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
    - o *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
    - o *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field*.

FIA_X509_EXT.1.2/ITT The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

Application Note

NIAP TD0478 has been applied to FIA_EXT_EXT.1/ITT, though it doesn't impact the SFR text.

5.3.4.2 FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates**.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the

certification path contain the basicConstraints extension with the CA flag is set to TRUE.

- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
    - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
    - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
    - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

Application Note

NIAP TD0478 has been applied to FIA_EXT_EXT.1/Rev, though it doesn't impact the SFR text.

5.3.4.3 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS], and [no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

Application Note

NIAP TD0399 has been applied to FIA_X509_EXT.2, though it doesn't impact the SFR text.

5.3.4.4 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.3.5 Security management (FMT)

5.3.5.1 FMT_MOF.1/ManualUpdate Management of security functions behaviour

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to* *perform manual update to Security Administrators.*

5.3.5.2 FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1.1/CoreData The TSF shall restrict the ability to *manage* the *TSF data to the Security Administrators.*

5.3.5.3 FMT_MTD.1/CryptoKeys Management of TSF data

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.3.5.4 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using* [*hash comparison*] *capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- [
    - Ability to configure audit behavior;
    - Ability to manage the cryptographic keys;
    - Ability to configure the cryptographic functionality;
    - Ability to configure the interaction between TOE components;
    - Ability to set the time which is used for time-stamps;
    - Ability to configure the reference identifier for the peer;
    - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
    - Ability to import X.509v3 certificates to the TOE's trust store;
    - No other capabilities.]

5.3.5.5 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator*.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely*

are satisfied.

5.3.6 Protection of the TSF (FPT)

5.3.6.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and **detect its** modification when it is transmitted between separate parts of the TOE **through the use of [TLS]**.

5.3.6.2 FPT_SKP_EXT.1 Extended: Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.3.6.3 FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

Application Note

NIAP TD0483 has been applied to FPT_APW_EXT.1.

5.3.6.4 FPT_STM_EXT.1 Reliable time stamps

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [allow the Security Administrator to set the time*]*.

5.3.6.5 FPT_TST_EXT.1: TSF Testing (Extended)

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [during initial start-up (on power on), periodically during normal operation] to demonstrate the correct operation of the TSF: [*power-on self-tests (during initial start-up), file integrity tests (periodically during normal operation), and file permission tests (periodically during normal operation)*].

5.3.6.6 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [no other TOE firmware/software version].

FPT_TUD_EXT.1.2 The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [no other update mechanism].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [published hash] prior to installing those updates.

Application Note

NIAP TD0477 has been applied to FPT_TUD_EXT.1, though it doesn't impact the SFR text.

5.3.7 TOE Access (FTA)

5.3.7.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [

- terminate the session]

after a Security Administrator-specified time period of inactivity.

Application Note

NIAP TD0484 has been applied to FTA_SSL_EXT.1, though it doesn't impact the SFR text.

5.3.7.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 Refinement: The TSF shall terminate **a remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

Application Note

NIAP TD0484 has been applied to FTA_SSL.3, though it doesn't impact the SFR text.

5.3.7.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow **Administrator**-initiated termination of the **Administrator**'s own interactive session.

5.3.7.4 FTA_TAB.1 Default TOE Access Banners (Refinement)

FTA_TAB.1.1 Before establishing **an administrative user** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

5.3.8 Trusted Path/Channels (FTP)

5.3.8.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall be capable of using [TLS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [authentication server, no other capabilities] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2 The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*syslog over TLS, LDAP over TLS*].

Application Note

NIAP TD0401 has been applied to FTP_ITC.1, though it doesn't impact the SFR text.

5.3.8.1 FTP_TRP.1/Admin Trusted Path (Refinement)

FTP_TRP.1.1/Admin The TSF shall be capable of using [TLS, HTTPS] to provide a communication path between itself and authorized 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 disclosure and provides detection of modification of the channel data.

FTP_TRP.1.2/Admin The TSF shall permit remote Administrators to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

5.3.8.1 FTP_TRP.1/Join Trusted Path (Refinement)

FTP_TRP.1.1/Join The TSF shall provide a communication path between itself and **a joining component** ~~[selection: remote, local] users~~ that is logically distinct from other communication paths and provides assured identification of **[**both joining component and TSF endpoint**]** ~~its end points~~ and protection of the communicated data from modification [and disclosure**]**.

FTP_TRP.1.2/Join The TSF shall permit [the joining component] to initiate communication via the trusted path.

FTP_TRP.1.3/Join The TSF shall require the use of the trusted path for *joining components to the TSF under environmental constraints identified in [none (no environmental constraints)].*

5.4 TOE SFR Dependency Rationale

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

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPP and derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Table 15: Assurance Measures

Assurance Class	Components	Components Description
Security Target (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
Development (ADV)	ADV_FSP.1	Basic Functional Specification
Guidance documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support (ALC)	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests (ATE)	ATE_IND.1	Independent testing - sample
Vulnerability assessment (AVA)	AVA_VAN.1	Vulnerability survey

5.5.2 Security Assurance Requirements Rationale

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

5.6 Assurance Measures

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

Table 16: Assurance Measures

Component	How requirement will be met
ADV_FSP.1	There are no specific assurance activities associated with ADV_FSP.1. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other assurance activities being performed. The functional specification is comprised of the information contained in the AGD_OPE and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The AGD and ST implicitly meet this assurance requirement. The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST.
ALC_CMS.1	
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 17: TOE SFR Measures

TOE SFRs	How the SFR is Met
FAU_GEN.1 FAU_GEN_EXT.1	The TOE generates an audit record that is stored internally within the TOE whenever an audited event occurs. Each TOE component generates its own audit messages, and stores its own audit messages locally. None of the TOE components transmit their audit messages to other TOE components. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in Table 14). Audit messages contain enough detail to identify the origin of the event, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited. For audit messages related to management of cryptographic keys, the audit message details include the name of the certificate associated with the key (keys cannot be managed independently from the certificates with which they're associated). Example audit message (clock update): Apr 16 09:30:10 SMC-01 AuditLogger[179327]: AuditLogger: osaxsd/179327,1100,2019-04-16T09:30:10TZD+0000,root (0),localhost,1,System time updated from [2019-04- 16T07:37:42] to [2019-04-16T09:30:10]
FAU_GEN.2	The TOE ensures each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. For example a human user, user identity, or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. Example audit messages: Account 'sysadmin' logged out from console: 2018-06-20 01:12:58 I&A User Logout The user has logged out of Console sysadmin(75) 127.0.0.1 osaxsd(229997) Yes Account 'admin' logged out from remote GUI: 2018-06-20 01:36:32 I&A User Logout The user has logged out admin 10.150.34.20 svc-token-authority(1) Yes

TOE SFRs	How the SFR is Met
FAU_STG_EXT.1 FAU_STG_EXT.3	Each TOE component is configured to export syslog records to a specified, external syslog server. The TOE uses TLS to protect communications with external syslog server. The TOE transmits its audit events in real time to all configured syslog servers at the same time logs are written to the local log buffer. When the local audit data storage on each TOE component is full, the TOE component will overwrite the oldest stored audit records when writing new audit records. Each TOE component stores its own audit records and each TOE component has the same audit retention rules: each TOE component maintains a log buffer that stores up to 5MB of log messages (the average message size on the TOE is ~180 bytes, so each 5MB file contains an average of ~27,000 messages.), and when the 5MB limit is reached the entire log is overwritten with a new log. No administrative interface allows Administrators to clear the local audit logs or to modify the contents of local audit logs.
FCO_CPC_EXT.1	In order for a new TOE component to become part of the distributed TOE it must successfully complete a registration process. The SMC is the management server within this distributed TOE and each other appliance type (FC, FS, and UDPD) must individually register with the SMC in order to become part of the TOE. Registration of a new appliance cannot be initiated by the SMC, registration is initiated by the administrator performing the initial configuration of the FC, FS, or UDPD. During the initial configuration process the administrator is asked whether the new appliance will be managed by an SMC, and after answering affirmatively that administrator is prompted to provide the IP address or hostname of the SMC and a valid SMC administrator username and password to authenticate to the SMC. During that initial TLS session the SMC and the new appliance exchange their unique X.509 certificates. Once the certificates have been exchanged, the new appliance has been joined with the SMC and all subsequent (automated) communications between the SMC and managed appliances use X.509 certificates for authentication in accordance with FPT_ITT.1 and FIA_X509_EXT.1/ITT. The SMC administrator can de-register an appliance by selecting "Remove This Appliance" from the Central Management page of the WebUI on SMC. A local administrator of the managed appliance can remove the registration by selecting “RemoveAppliance” from the System Configuration menu. Either of these actions, whether initiated from SMC or from the managed appliance, will result in each TOE component deleting the device association from its local configuration, and no further TSF data will be exchanged between the appliances without completing a new registration process.
FCS_CKM.1 FCS_CKM.2	The TOE generates asymmetric keys in accordance with the RSA schemes using key sizes of 4096-bit that are conformant to the FIPS Pub 186-4, Appendix B.3. In addition, ECC schemes are used with P-256, P-384, and P-521. The TOE can create a RSA public-private key

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>pair that can be used to generate a Certificate Signing Request (CSR). Via offline CSR transfer the TOE can provide its CSR for a Certificate Authority (CA) generate a certificate, and the TOE’s signed certificate can be imported.
The key pair generation portions of "The RSA Validation System" for FIPS 186-4 were used as a guide in testing the FCS_CKM.1 during the FIPS validation.
The TOE implements FFC key establishment schemes in TLS. The FFC key generation meets FPS PUB 186-4 Appendix B1, and FFC establishment meets NIST SP 800-56A Revision 2. ECC for ECDH key exchange for TLS.
<table>
<tr><th>Scheme</th><th>SFR</th><th>Services</th></tr>
<tr><td>RSA</td><td>FCS_TLSC_EXT.1</td><td>LDAP over TLS</td></tr>
<tr><td>RSA</td><td>FCS_TLSC_EXT.2</td><td>Syslog over TLS
Distributed TOE communication</td></tr>
<tr><td>RSA</td><td>FCS_TLSS_EXT.1</td><td>HTTPS Remote Administration</td></tr>
<tr><td>RSA</td><td>FCS_TLSS_EXT.2</td><td>Distributed TOE communication</td></tr>
<tr><td>ECC (P-256, P-348, P-521)</td><td>FCS_TLSC_EXT.1</td><td>LDAP over TLS</td></tr>
<tr><td>ECC (P-256, P-348, P-521)</td><td>FCS_TLSC_EXT.2</td><td>Syslog over TLS
Distributed TOE communication</td></tr>
<tr><td>ECC (P-256, P-348, P-521)</td><td>FCS_TLSS_EXT.1</td><td>HTTPS Remote Administration</td></tr>
<tr><td>ECC (P-256, P-348, P-521)</td><td>FCS_TLSS_EXT.2</td><td>Distributed TOE communication</td></tr>
<tr><td>FFC</td><td>FCS_TLSC_EXT.1</td><td>LDAP over TLS</td></tr>
<tr><td>FFC</td><td>FCS_TLSC_EXT.2</td><td>Syslog over TLS
Distributed TOE communication</td></tr>
<tr><td>FFC</td><td>FCS_TLSS_EXT.1</td><td>HTTPS Remote Administration</td></tr>
<tr><td>FFC</td><td>FCS_TLSS_EXT.2</td><td>Distributed TOE communication</td></tr>
</table>
</td></tr>
<tr><td>FCS_CKM.4</td><td>The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs). See Table 18 for more information on the key destruction.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>The TOE provides symmetric encryption and decryption capabilities using AES in CBC and GCM mode (128, 256 bits) as described in ISO 18033-3 and ISO 10116. AES is implemented in TLS.</td></tr>
</table>

TOE SFRs	How the SFR is Met
	Through the implementation of the FIPS validated cryptographic module, the TOE provides AES encryption and decryption in support of TLS for secure communications.
FCS_COP.1/SigGen	The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 4096 as specified in FIPS PUB 186-4, “Digital Signature Standard”. Through the implementation of the FIPS validated cryptographic module, the TOE provides cryptographic signatures in support of TLS for secure communications. Management of the cryptographic algorithms is provided through the GUI with auditing of those commands. The TOE provides the RSA option in support of TLS key establishment.
FCS_COP.1/Hash	The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in ISO/IEC 10118-3:2004. Through the implementation of the FIPS validated cryptographic module, the TOE provides Secure Hash Standard (SHS) hashing in support of TLS, for secure communications. Management of the cryptographic algorithms is provided through the GUI with auditing of those commands.
FCS_COP.1/KeyedHash	The TOE provides keyed-hashing message authentication services using HMAC-SHA1 HMAC-SHA-256, and HMAC-SHA-384, with key sizes 160, 256 and 384-bits, and message digest sizes 160, 256, and 384-bits as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”. Through the implementation of the FIPS validated cryptographic module, the TOE provides SHS hashing and HMAC message authentication in support TLS for secure communications. Management of the cryptographic algorithms is provided through the GUI with auditing of those commands. SHS hashing and HMAC message authentication (SHA-1) is used in the establishment of TLS/HTTPS sessions.
FCS_HTTPS_EXT.1	The TOE implements HTTPS over TLS as specified in RFC 2818 and FCS_TLSS_EXT.1. The TSF HTTPS implementation authenticates the TOE to the remote client with an X.509 certificate. System Administrators manage the TOE identity certificates using the TOE GUI. The TSF HTTPS implementation performs server based authentication using a server X.509v3 certificate to establish the TLS session. The TSF HTTPS implementation does not require client authentication at the TLS level but presents the Web interface logon page for administrative users to authenticate using their name and password.

TOE SFRs	How the SFR is Met
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG) seeded by a hardware-based entropy source within the TOE. The DRBG is seeded with a minimum of 256 bits of full entropy, which is at least equal to the greatest security strength of the keys and hashes that the DRBG will generate.
FCS_TLSC_EXT.1 FCS_TLSC_EXT.2	The TOE uses TLS clients for: • Transmitting syslog over TLS. • Interconnections among distributed TOE components. • Connecting to LDAP servers over TLS. The TLS clients of each TOE component support mutual authentication (FCS_TLSC_EXT.2) for connections to the syslog server (FTP_ITC.1), and for interconnections between distributed TOE components (FPT_ITT.1). Mutual authentication is not supported for TLS connections to LDAP servers (FTP_ITC.1). The TOE only supports TLSv1.1 and TLSv1.2 with AES 128 or 256 bit symmetric ciphers in CBC and GCM modes, in conjunction with SHA, RSA, ECDHE (NIST curves supported are secp256r1, secp384r1, and secp521r1) and ECDSA. By default all the Supported Elliptic Curves Extension options are presented in the Client Hello and this behavior is not configurable. The following TLS cipher suites are implemented by the TOE in CC mode: • Ciphersuites relevant to FTP_ITC and FCS_TLSC_EXT.2, for syslog over TLS (client only, from each TOE component) are listed in section 5.3.3.11 of this document. • Ciphersuites relevant to FPT_ITT, FCS_TLSC_EXT.2, and FCS_TLSS_EXT.2 (client and server, where each TOE component can operate as the client and/or server) are as listed in sections 5.3.3.11 and 5.3.3.13 of this document. • Ciphersuites relevant to FTP_ITC and FCS_TLSC_EXT.1 for LDAP over TLS (client only, from the SMC TOE component only) are listed in section 5.3.3.10 of this document. While the FOM (see section 7.2) supports additional cipher suites (for example, RSA_3DES_EDE_CBC_SHA, RSA_DES_CBC_SHA, RSA_RC4_128_MD5, RSA_RC4_128_SHA, etc.), they are all disabled while operating in CC mode. If the remote TLS server does not support TLSv1.1 or TLSv1.2, the TLS connection will fail. When in CC mode and the TOE acts as a TLS client (e.g., connection to the syslog server), the TOE will verify the server Common Name (CN) and/or Subject Alternative Name (SAN) against the reference identity. When an IP address is used as the reference identifier the TOE converts the text representations (dotted-decimal notation) of the locally-stored

TOE SFRs	How the SFR is Met
	IP address and the IP addresses found in the CN to binary (hex-based) representations in network byte order, enforcing the canonical format per RFC 3986. Use of wildcards is not supported for any TLS connections (to syslog servers or LDAP servers, or between TOE components). In any case (connection to a syslog or LDAP servers, or connections among TOE components), if verification fails, the TLS connection will not be established. Certificate pinning is not supported. The key agreement parameters of the server key exchange message are specified in the RFC 5246 (section 7.4.3) for TLSv1.2 and RFC 4346 (section 7.4.3) for TLSv1.1. The TOE conforms to both RFCs.
FCS_TLSS_EXT.1 FCS_TLSS_EXT.2	An authorized administrator can initiate inbound TLSv1.1 and TLSv1.2 connections using the web based GUI for remote administration of the TOE. Any session where the client offers the following in the client hello: SSL 2.0, SSL 3.0 and TLS 1.0 will be rejected by the TOE's TLS server. Using the below TLS_RSA ciphers the RSA public key is used for authentication and key exchange. The TLS servers of each TOE component support mutual authentication (FCS_TLSS_EXT.2) for interconnections between distributed TOE components (FPT_ITT.1). Mutual authentication is not supported for TLS connections used for remote administration (FTP_TRP.1). When a TLS session is initiated between two TOE components, the server side of the TLS session will check the client certificate and if the SAN within the client certificate does not match the expected identifier on the server, the connection will be rejected by the server. The TOE supports TLSv1.1 and TLSv1.2 with AES 128 or 256 bit symmetric ciphers in CBC and GCM modes, in conjunction with SHA, RSA, ECDHE (NIST curves supported are secp256r1, secp384r1, and secp521r1) and ECDSA. The TOE will use secp521r1 if supported by the client, otherwise secp384r1, and lastly secp256r1. The following TLS cipher suites are implemented by the TOE in CC mode: • Ciphersuites relevant to FPT_ITT, FCS_TLSC_EXT.2, and FCS_TLSS_EXT.2 (client and server) are as listed in sections 5.3.3.11 and 5.3.3.13 of this document. • Ciphersuites relevant to FTP_TRP.1 and FCS_TLSS_EXT.1 (server only) are as listed in section 5.3.3.12 of this document. While the FOM (see section 7.2) supports additional cipher suites (for example, RSA_3DES_EDE_CBC_SHA, RSA_DES_CBC_SHA, RSA_RC4_128_MD5, RSA_RC4_128_SHA, etc.), they are all disabled while operating in CC mode. If the remote TLS client does not support TLSv1.1 or TLSv1.2 the TLS connections will fail and the administrators will not establish a HTTPS web-based session with the TOE.

TOE SFRs	How the SFR is Met
	The key agreement parameters of the server key exchange message are specified in the RFC 5246 (section 7.4.3) for TLSv1.2 and RFC 4346 (section 7.4.3) for TLSv1.1. The TOE conforms to both RFCs.
FIA_AFL.1	The administrator can configure the maximum number of failed login attempts (configurable from 1-99 consecutive failed attempts) before the account is locked. Accounts that become locked by this feature will remain locked for an administratively defined number of minutes (configurable from 1-60 minutes). By default this feature is disabled. The predefined ‘admin’ account on each appliance is exempt from being locked out, but in the CC-evaluated configuration that account is disabled. All remote administration is performed via the SMC using non-default administrative accounts on the SMC (local accounts or LDAP accounts), and no remote authentication is permitted to any other TOE component. If all non-default remote administration accounts become locked due to consecutive failed login attempts, the default ‘sysadmin’ account (which can only login via console and is exempt from lockout) can unlock the default ‘admin’ account and the default ‘admin’ account can be used to unlock any locally stored (not LDAP) remote administrative account.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: [“!”, “@”, “#”, “$”, “%”,“(“, “)”, [“<”, “>”, “.”, “?”, “/”, “’”, “””, “\”, “|”, “:”, “;”, “`”, “~”, “-“, “_”, “+”, “=”, “{”, “}”, “[“, and “]”. Minimum password length is settable by the Authorized Administrator, and support passwords of 15 characters or greater (from 8 to 30 characters). Password composition rules specifying the types and number of required characters that comprise the password are settable by the Authorized Administrator.
FIA_UIA_EXT.1	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for acknowledging the pre-login warning banner. The TOE mediates all administrative actions through its GUI and CLI. Once a potential administrative user attempts to access the TOE through either a directly connected console or remotely through TLS, the TOE prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. In this distributed TOE all remote administration is performed via the WebUI (GUI) of the SMC. The default ‘admin’ remote administration account is disabled on all TOE components and only the SMC has non-default remote administrative accounts (defined locally, and/or as LDAP accounts). Each non-SMC (FC, FS, and UDPD) TOE

TOE SFRs	How the SFR is Met
	component continues to have a remotely accessible login page, but all remote login attempts will fail because the only existing remote account (the default 'admin' account) is disabled. Every TOE component (SMC, FC, FS, and UDPD) allow local console login using the default 'sysadmin' account.
FIA_UAU_EXT.2	The TOE provides a local password based authentication mechanism at its console CLI and its remote GUI. The TOE also supports AAA LDAP authentication at its GUI. The administrator authentication policies include authentication to the local user database or, optionally for the GUI, redirection to a remote authentication server (LDAP over TLS). Interfaces can be configured to try one or more remote authentication servers, and then fail back to the local user database if the remote authentication servers are inaccessible. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via TLS. At initial login in the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and password is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console none of the typed characters are echoed in the password field, and at the HTTPS/TLS GUI, the password field displays only '*' characters so that the password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.
FIA_X509_EXT.1/ITT	When the distributed components initiate TLS connections to each other the client validates the server's certificates during session establishment and validate those certificates against the locally stored root certificate. Revocation checking (neither CRL nor OCSP checking) is not performed for the TLS connection between TOE components. The extendedKeyUsage field is validated according to the following rules - Server certificates have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field and the Client certificates have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. Checking is done for the 'basicConstraints' extension and the 'cA' flag to determine whether they are present and set to TRUE. If they are not, the CA certificate is not accepted as a trust anchor.

TOE SFRs	How the SFR is Met
FIA_X509_EXT.1/Rev FIA_X509_EXT.2 FIA_X509_EXT.3	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections. The certificate validation checking takes place during the TLS session setup. The TOE can generate a RSA key pair that can be embedded in a Certificate Signing Request (CSR) created by the TOE. The CSR can be generated at the UI. The administrator can then download the CSR from the GUI and provide the CSR to the CA for the CSR to sign and issue a certificate. Once the certificate has been issued, the administrator can import the X.509v3 certificate into the TOE. All certificate management for all TOE components is managed via the GUI of SMC. More than one certificate from one or more CAs on the TOE can be stored and used by TOE. For example, one certificate from one CA could be used for TLS connections to syslog or LDAP server, while another certificate from another CA could be used for TLS connections to another syslog or LDAP server. The physical security of the TOE (A.PHYSICAL_PROTECTION) protects the switch and the certificates from being tampered with or deleted. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE. Certificate revocation checking is supported by the TOE through use of OCSP and CRL when the TOE is validating server certificates when initiating outbound TLS connections to syslog and LDAP servers (for FTP_ITC only). Certificate validation includes verification of the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The local CA certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensure that the key usage extension is present. In all use cases (syslog-over-TLS and LDAP-over-TLS, whether using CRL or OCSP) if the connection to determine the certificate validity cannot be established, the TOE will not accept the certificate.
FMT_MOF.1/ManualUpdate	Manual software updates can only be initiated by the authorized administrator through the SMC GUI. Updates for all TOE components are managed through the GUI of SMC. All update files are first uploaded by an administrator to the SMC, then an SMC administrator manually initiates installing of updates to each appliance (SMC, FC, FS, and UDPD). When updating appliances other than the SMC itself, the update files are transmitted from the SMC to each other TOE component over the same TLS connection used for all other distributed TOE (FPT_ITT.1) communications.
FMT_MTD.1/CoreData	The TOE restricts the access to manage TSF data that can affect the security functions of the TOE to Security Administrators (i.e., administrator roles). The TSF data here includes user accounts and roles, login banner, inactivity timeout values, password length settings,

TOE SFRs	How the SFR is Met
	TOE updates, X.509 certificates, audit records, and audit server information. Access to TSF data is disallowed for all non-administrative users because all accounts are administrative accounts. Each TOE component contains a trust store of X.509v3 certificates. The trust store contains certificates for the local TOE component, and certificates for all other TOE components with which the local component communicates, and certificates for remote syslog servers. The trust store on the SMC additionally contains X.509v3 certificates of remote LDAP servers. Access to trust store data on each component is restricted to authorized administrators only. Remote administrators using the SMC WebUI can manage trust stores on each TOE component via the SMC WebUI. Local 'sysadmin' accounts on each appliance could regenerate a new self-signed X.509v3 device certificate, but doing so would break communication with other TOE components and would result in removing that component from the TOE.
FMT_MTD.1/CryptoKeys	The TOE restricts the access to manage cryptographic keys to Security Administrators (i.e., administrator roles). Ability to manage cryptographic keys is disallowed for all non-administrative users because all accounts are administrative accounts. Each TOE component contains its own set of cryptographic keys. Key regeneration/replacement/removal can be performed for any appliance via the SMC WebUIe.
FMT_SMF.1	The TOE includes the functions necessary to administer the TOE locally and remotely. Most TOE administrative actions are performed via the WebUI/GUI of the SMC (Stealthwatch Management Console), but each TOE component also has a local serial console interface through which some administrative actions can be performed. Each TOE component has an active WebUI accessible via TLS, but the SMC is the only TOE component that allows login via its WebUI. The following administrative actions are performed via the SMC WebUI: • Configuring the pre-login access banner. The banner for each TOE component is configured separately, and each TOE component uses a single banner for its local console and for its remote WebUI. • Configuring session inactivity time limits. The same idle timeout values apply to the WebUI and console interfaces. • Management and verification of software updates for each TOE component. Additionally, the local console of each appliance can be used to verify the running version, but the local console cannot be used to install updates. • Configuration of authentication failure parameters for FIA_AFL.1.

TOE SFRs	How the SFR is Met
	• Configuring audit behavior such as adding/removing syslog servers. • Configuring cryptographic functionality, such as enabling CC mode and FIPS mode, and enabling file integrity checking. • Configuring interactions between TOE components such as removing/deleting a managed TOE component, or rebooting a TOE component. • Configuring the reference identifier for peers such as adding IP addresses for syslog servers, and adding FQDN or IP addresses for LDAP servers. • Managing the trust store of each TOE component, importing trust anchors, and importing certificates of multiple TOE components, syslog servers, and LDAP servers. The following administrative actions are performed via the local console on each appliance: • Setting the time and date used for time-stamps. • Changing administrator passwords. • Verifying the TOE version.
FMT_SMR.2	The TOE platform maintains both privileged and semi-privileged administrator roles. The terms “Authorized Administrator” and "Security Administrator" are used interchangeable in this ST to refer to any user that has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. The assigned role determines the functions the user can perform; hence the authorized administrator with the appropriate privileges.
FPT_SKP_EXT.1	The TOE stores all private keys (associated with local X.509v3 certificates), and pre-shared/symmetric keys (associated with LDAP servers) such that they are not readable by administrators. The keys are stored in plaintext but there are no administrative interfaces that allow viewing of any stored keys.
FPT_APW_EXT.1	TOE ensures that plaintext user passwords will not be disclosed, even to administrators. There are no administrative interfaces that allow viewing of stored passwords; there is no viewable configuration file and no viewable password file; when changing passwords the old password is not displayed in any form (plaintext or otherwise) and the new password is obscured with asterisks as it’s being typed; passwords are obscured by asterisks during login via WebUI and are not echoed at all (the cursor at the password prompt does not move) when logging via the console; passwords are not written to audit records.

TOE SFRs	How the SFR is Met
FPT_ITT.1	The distributed components of the TOE communicate with each other using TLSv1.2. The SMC (Stealthwatch Management Console) communicates with each other appliance (FC, FS, and UDPD), and the TLS sessions can be initiated in either direction. During most TOE activity the managed components (FC, FS, and UDPD) initiate the mutually-authenticated TLS (FCS_TLSC_EXT.2) connections to the SMC (FCS_TLSS_EXT.2) to query the SMC for any updates (configuration updates and software updates). The SMC will initiate mutually-authenticated TLS connections (FCS_TLSC_EXT.2) with other components (FCS_TLSS_EXT.2) when an SMC administrator initiates a query for data stored on another component (e.g. to query for network flow data) for the purpose of displaying query results/reports to the SMC administrator.
FPT_STM_EXT.1	The TOE provides a source of date and time information in the form of a software clock, which it uses for writing timestamps to audit messages (FAU_GEN.1), for tracking session idle time (FTA_SSL_EXT.1 and FTA_SSL.3), for unlocking accounts after consecutive failed login attempts (FIA_AFL.1), and for verifying validity times of X.509v3 certificates (FIA_X509_EXT.1). When each TOE component boots, it will set its software clock to match the hardware clock of the underlying server. All Stealthwatch appliances operate in the UTC time zone and the time zone is not configurable, so the hardware clock of the underlying system must also be set to UTC. The software clock on each TOE component can be manually set by the 'sysadmin' account via the console.
FPT_TST_EXT.1	The TOE components include a number of built in diagnostic tests that are run during start-up to determine whether the TOE is operating properly. The crypto module within the TOE runs power-on self-tests including known answer tests (KATs). The following self-tests are executed: AES encryption/decryption KAT, RSA pairwise consistency and sign/verify KAT, SHA hash KATs, HMAC-SHA hash KATs, and DRBG KATs. When any crypto-dependent service (such as the TLS web server) initiates startup of the crypto module and any self-test fails during the startup of the crypto module the crypto module returns an error to the service and the service will fail to start. The crypto module will not enter an operational state if any of its self-tests fail, thus the requesting service will also fail to start, and the TOE will not enter a fully operational state. The TOE will remain in a state where all crypto-dependent services remain disabled (all TLS services: remote administration, inter-TSF communication, syslog-over-TLS, and LDAP-over-TLS), so the only interactive interface available will be via the local serial console for troubleshooting purposes. When a crypto-dependent service initiates startup of the crypto module and all cryptographic self-tests pass during the startup of the crypto module the crypto module returns a successful response to the service and the

TOE SFRs	How the SFR is Met
	services continue to load. The TOE runs SHA-256 integrity tests daily to verify the integrity of the kernel, and all binaries and libraries. If the hash verification fails, the TOE will generate an audit message indicating which file changed. The virtual appliance forms of TOE components perform the same self-tests as the physical appliances. These tests (periodically reverifying the integrity of the software files, periodically reverifying the permissions of those files, and verifying the correct operation of cryptographic operations prior to the TOE becoming operational) are sufficient to demonstrate that the TSF is operating correctly.
FPT_TUD_EXT.1	An Authorized Administrator can query the software version running on the TOE (on each TOE component) and can initiate software updates to each TOE component. The software version can be queried in multiple ways: the version running on every TOE component can be queried via the SMC WebUI, and the console interface of each individual TOE component can be used to view the running version on that component. When software updates are made available by Cisco, an administrator can download the update from Cisco, verify the integrity of the files using SHA-512 checksum verification on a local system, and install those updates to the TOE. To satisfy the NDcPP requirements, the integrity of update files for each TOE component are verified on a non-TOE workstation/server prior to being uploaded to the SMC. If the calculated checksum does not match the expected checksum, the administrator will not upload the file to SMC, but will instead download the file again from the original source on Cisco.com, and if the checksum does not match again, the administrator will contact Cisco Stealthwatch Support. Updates for all TOE components are first uploaded to the SMC by an SMC administrator via the SMC WebUI/GUI then using the same interface the SMC administrator initiates installation of the software updates to each TOE component until all TOE components have been updated to the same version. Updates for all TOE components other than SMC itself (FC, FS, UDPD) are transferred from the SMC to other TOE components over the same TLS channel that's used for all other FPT_ITT.1 communications.
FTA_SSL_EXT.1 FTA_SSL.3	TOE administrators can configure maximum inactivity times individually for both local and remote administrative sessions. These settings are not immediately activated for the current session, changes to inactivity limits are enforced for new sessions. If a local user session is inactive for a configured period of time, the session will be terminated, and re-authentication is required to start a new session. If a remote user session is inactive for the configured idle time limit, the session will be terminated and will require authentication

TOE SFRs	How the SFR is Met
	to establish a new session. The configurable idle timeout value is the same for local and remote sessions, and configured individually for each appliance via the SMC GUI: Central Management > Appliance Manager > General > Protected Sessions Time-Out. The configurable inactivity timeout range for local console sessions and remote sessions is from 2 to 1440 minutes.
FTA_SSL.4	Administrators able to logout of all local and remote administrative sessions. From the local console, the administrator selects “Exit”. From the GUI, the administrator clicks “Logout”.
FTA_TAB.1	The TOE displays a privileged Administrator specified banner on the CLI management interface and on the WebUI prior to allowing any administrative access to the TOE. The banner configured for each appliance (all configured via the SMC WebUI) is displayed prior to login at that appliance’s local console and prior to login at that appliance’s WebUI. Note that once the managed appliances (FC, FS, or UDPD) are in their CC evaluated configuration, authentication to each of their WebUI is effectively disabled since the local ‘admin’ account on those appliances is disabled and no remote (LDAP) authentication will be enabled, but the login banner continues to be displayed prior displaying the login prompt, and failed authentication attempts are logged.
FTP_ITC.1	The TOE protects communications between itself and remote audit servers using TLS. This provides a secure channel to transmit the syslog messages. The TOE protects communications between itself and AAA (LDAP) servers are secured using TLS.
FTP_TRP.1/Admin	All remote administrative communications take place over a secure encrypted TLS (HTTPS) session, allowing remote administrators to initiate TLS (HTTPS) communications with the TOE. TLSv1.1 and TLSv1.2 are supported, using the ciphersuites and RFCs listed under FCS_TLSS_EXT.1, and the RFC listed in FCS_HTTPS_EXT.1.
FTP_TRP.1/Join	During installation of the TOE the SMC is configured first, then other appliances are joined to the SMC and after successful registration those appliances are managed via the SMC. When TOE components are joined to the SMC, the administrator installing the non-SMC appliance (FC, FS, or UDPD) inputs the IP address or DNS-resolvable hostname of the SMC, then the new appliance initiates a TLS session to the SMC. This initial TLS session used for joining is authenticated using a valid SMC administrator username and password that is manually entered by the administrator performing the initial configuration of the new appliance. If authentication succeeds, the SMC and the joining appliance exchange X.509 certificates, and the initial TLS session is closed. All subsequent connections between the TOE components also

TOE SFRs	How the SFR is Met
	use TLS, but use X.509 certificate-based authentication in accordance with FPT_ITT.1 and FIA_X509_EXT.1/ITT. No supplemental support is required from the operational environment to secure the TLS connections between the SMC and other TOE components that are being joined to the SMC. If attempts to join Stealthwatch appliances to an SMC fail: • No FPT_ITT.1 TLS session (using certificate-based authentication per FIA_X509_EXT.1/ITT) can be established between the devices, and thus no TSF data can be exchanged between the devices until registration successfully completes. • If the connection failed due to network connectivity error, resolve the connectivity, and reattempt joining. • If the connection fails due to incorrect information provided by the administrator of the joining component (e.g. incorrect hostname/IP address of the SMC, or incorrect account name or password for the SMC), correct the information, and reattempt joining.

7 SUPPLEMENTAL TOE SUMMARY SPECIFICATION INFORMATION

7.1 Key Destruction

The following table describes the key destruction referenced by FCS_CKM_EXT.4 provided by the TOE.

Table 18: TOE Key Destruction

Name	Generation/ Algorithm	Purpose	Storage Location	Destruction Summary
RSA public/private keys	DRBG	Identity certificates for TOE components for TLS.	Private Key – hard disk (plaintext) and RAM (plain text) Public Key – hard disk (plaintext) and RAM (plain text)	Private Key - destroyed when certificates are deleted by administrators. Public Key - are deleted from hard disk when the certificates are deleted by administrators.
Diffie-Hellman Key Pairs	DRBG	Key agreement for TLS sessions.	RAM (plain text)	Keys in RAM are destroyed upon resetting (i.e., terminating all sessions) or rebooting.
RSA public/private keys	RSA	Used for TLS sessions.	Hard disk (plain text)/RAM (plain text)	Private Key - The private key is destroyed when the SMC and other appliances regenerate new CSRs, which results in generating new key pairs.
TLS Session Keys	DH / DRBG Algorithm: AES	Used for HTTPS sessions.	RAM (plain text)	Keys in RAM are destroyed upon rebooting the TOE.
Passwords	User generated	Critical security parameters used to authenticate administrators.	Hard disk (Hashed with SHA-512 and salt value)	Passwords are not stored in plaintext. Only the hashed of the passwords and a 32-bit nonces are stored.
Pre-shared keys / secrets	User generated	Critical security parameters used to authenticate to LDAP servers.	Hard disk	Stored in plaintext. Pre-shared keys and secrets are destroyed when deleted or replaced by administrators.
Certificates of Certificate Authorities (CAs)	DRBG	Necessary to verify certificates issued by the CA. Install the CA's certificate prior to installing subordinate certificates.	Hard disk (plain text) and RAM (plain text)	CA certificates are destroyed from hard disk when the CA certificates are deleted by the administrators. CA certificates in RAM will be destroyed upon rebooting the TOE.
PRNG Seed Key	Entropy	Seed key for DRBG	RAM (plain text)	Seed keys are destroyed and overwritten with the generation of new seed

7.2 CAVP Certificate Equivalence

The TOE models, processors, and cryptographic modules included in the evaluation are shown in the following table. The cryptographic module used in all TOE platforms is the CiscoSSL FOM 6.2. The table below (Table 19) lists the CPU for which the FOM has been validated, and the TOE component on which each CPU is used. Where the CiscoSSL FOM was validated as software, the processor is identified along with the operating system and hypervisor in the operational environment of the validated FOM. The table on the following page (Table 20) lists the CAVP certificate numbers for each cryptographic module for each applicable SFR.

Table 19: Processors Within the TOE

CAVP #	Processor	TOE Appliance / Platform
A402	Intel Xeon Gold 6130 (Skylake)	ST-SMC2210-k9, ST-FC4210-k9, ST-FC5210E, ST-FC5210D
A403	Intel Xeon Gold 5118 (Skylake)	ST-FS3210-k9, ST-FS4210-k9, ST-UDP2210-k9
A400	Intel Xeon Bronze 3106 (Skylake)	ST-FS1210-k9
A397	Intel Xeon E5-2609 v4 (Broadwell)	ST-FS1200-K9
A404	Intel Xeon E5-2650 v4 (Broadwell)	ST-FS2200-K9, ST-FS3200-K9, ST-FS4200-K9, ST-UDP2200-K9
A406	Intel Xeon E5-2680 v3 (Haswell)	ST-SMC2200-K9, ST-FC4200-K9
A401	Intel Xeon E5-2680 v4 (Broadwell)	ST-FC5200E
A405	Intel Xeon E5-2695 v3 (Haswell)	ST-FC5200D
A399[1]	Intel Xeon Gold 6128 (Skylake) w/ Linux 4 on ESXi 6	Cisco UCS C220-M5, or UCS C240-M5 (with any of: L-ST-SMC-VE-K9, L-ST-FC-VE-K9, L-ST-FS-VE-K9, and L-ST-UDP-VE-K9)
A391	Intel Xeon E5-2609 v4 (Broadwell) w/Linux 4 on ESXi 6	Cisco UCS C220-M4, or UCS C240-M4 (with any of: L-ST-SMC-VE-K9, L-ST-FC-VE-K9, L-ST-FS-VE-K9, and L-ST-UDP-VE-K9)

[1] While tested on the Intel Xeon Gold 6130 (Skylake), Intel Xeon Gold 6128 (Skylake) may also be used as part of the evaluated configuration.

Table 20: CAVP Validation Numbers

Algorithm	SFR	CAVP Validation Number
AES CBC 128/256 GCM 128/256	FCS_COP.1/DataEncryption	As identified for each CPU and TOE component listed in the previous table.
DSA	FCS_CKM.1	
RSA 4096 bit Sig Gen & Verify Key Gen	FCS_COP.1/SigGen FCS_CKM.1	
ECDSA curves P-256, P-384, and P-521 Sig Gen & Verify Key Gen and Verify	FCS_COP.1/SigGen FCS_CKM.1	
Hashing SHA-1, SHA-256, SHA-384, SHA-512	FCS_COP.1/Hash	
Keyed Hash HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	FCS_COP.1/KeyedHash	
DRBG CTR_DRBG (AES)	FCS_RBG_EXT.1	
CVL KAS ECC/FCC	FCS_CKM.2	

Americas Headquarters:

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

8 ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 21: References

Identifier	Description
[CC_PART1]	• Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-001
[CC_PART2]	• Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-002
[CC_PART3]	• Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-003
[CEM]	• Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-004
[NDcPP]	• collaborative Protection Profile for Network Devices, version 2.1, 24-September-2018
[800-38A]	• NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	• NIST Special Publication 800-56A Rev 2, May 2013 • Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[800-56B]	• NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 • Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	• FIPS PUB 140-2 Federal Information Processing Standards Publication • Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-2]	• FIPS PUB 186-2 Federal Information Processing Standards Publication 2000 January 27
[FIPS PUB 186-3]	• FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 186-4]	• FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS) July 2013
[FIPS PUB 198-1]	• Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[NIST SP 800-90A Rev 1]	• NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2015
[FIPS PUB 180-3]	• FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008

9 ANNEX B: SFR TOE COMPONENTS MAPPING

This TOE is a distributed TOE consistent with Use Case 3 as defined in the NDcPP. The following mapping shows which SFRs are supported by which TOE components:

Table 22: Distributed TOE SFR Mapping

Requirement	Description	SFR Enforcement Component	Audit Generation Component
FAU_GEN.1	Audit Data Generation	All	All
FAU_GEN.2	User Identity Association	All	N/A
FAU_GEN_EXT.1	Security Audit Generation	All	N/A
FAU_STG_EXT.1	Protected Audit Event Storage	All	N/A
FAU_STG_EXT.3	Protected Local Audit Event Storage for Distributed TOEs	All	N/A
FCO_CPC_EXT.1	Communication Partner Control	All	All
FCS_CKM.1	Cryptographic Key Generation	All	N/A
FCS_CKM.2	Cryptographic Key Establishment	All	N/A
FCS_CKM.4	Cryptographic Key Destruction	All	N/A
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)	All	N/A
FCS_COP.1/SigGen	Cryptographic Operation (Signature Verification)	All	N/A
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)	All	N/A
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)	All	N/A
FCS_HTTPS_EXT.1	Protocol Feature Dependent	SMC only	SMC only
FCS_RBG_EXT.1	Random Bit Generation	All	N/A
FCS_TLSC_EXT.1	TLS Client Protocol	SMC only	SMC only
FCS_TLSC_EXT.2	TLS Client Protocol with authentication	All	All
FCS_TLSS_EXT.1	TLS Server Protocol	SMC only	SMC only
FCS_TLSS_EXT.2	TLS Server Protocol with Mutual Authentication	All	All
FIA_AFL.1	Authentication Failure Management	SMC only	SMC only
FIA_PMG_EXT.1	Password Management	All	N/A
FIA_UIA_EXT.1	User Identification and Authentication	All	All

FIA_UAU_EXT.2	Password-based Authentication Mechanism	All	All
FIA_UAU.7	Protected Authentication Feedback	All	N/A
FIA_X509_EXT.1/ITT FIA_X509_EXT.1/Rev	X.509 Certification Validation	All	All
FIA_X509_EXT.2	X.509 Certificate Authentication	All	N/A
FIA_X509_EXT.3	Certificate Requests	All	N/A
FMT_MOF.1/ManualUpdate	Trusted Update - Management of Security Functions behaviour	SMC only	SMC only
FMT_MTD.1/CoreData	Management of TSF Data	All	All
FMT_MTD.1/CryptoKeys	Management of TSF Data	SMC only	N/A
FMT_SMF.1	Specification of Management Functions	All	All
FMT_SMR.2	Restrictions on Security Roles	All	N/A
FPT_APW_EXT.1	Protection of Administrator Passwords	All	N/A
FPT_ITT.1	Basic internal TSF data transfer protection	All	All
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)	All	N/A
FPT_STM_EXT.1	Reliable Time Stamps	All	All
FPT_TST_EXT.1	Testing (Extended)	All	N/A
FPT_TUD_EXT.1	Trusted Update	All	All
FTA_SSL_EXT.1	TSF-Initiated Session Locking	All	All
FTA_SSL.3	TSF-initiated Termination	SMC only	SMC only
FTA_SSL.4	User-Initiated Termination	All	All
FTA_TAB.1	Default TOE Access Banner	All	N/A
FTP_ITC.1	Inter-TSF Trusted Channel	All	All
FTP_TRP.1/Admin	Trusted Path	SMC only	SMC only
FTP_TRP.1/Join	Trusted Path	All	All