Citrix ADC (formerly NetScaler) Platinum Edition Version 11.1

Citrix Systems Inc.
Common Criteria Security Target

Prepared By:
Acumen Security
2400 Research Blvd
Rockville, MD 20850

www.acumensecurity.net

Table Of Contents

1 Security Target Introduction 4

1.1 Security Target and TOE Reference 4

1.2 TOE Overview 4

1.3 TOE Description 4

1.3.1 TOE Evaluated Configuration 4

1.3.2 Physical Boundaries 5

1.3.3 Logical Boundaries 6

1.3.1 TOE Documentation 7

1.4 Excluded Functionality 8

2 Conformance Claims 10

2.1 CC Conformance 10

2.2 Protection Profile Conformance 10

2.3 Scheme Interpretations 10

2.4 Conformance Rationale 12

3 Security Problem Definition 13

3.1 Threats 13

3.2 Assumptions 14

3.3 Organizational Security Policy 15

4 Security Objectives 16

4.1 Security Objectives for the Operational Environment 16

5 Security Requirements 17

5.1 Conventions 17

5.2 TOE Security Functional Requirements 17

5.2.1 Class: Security Audit (FAU) 17

5.2.2 Class: Cryptographic Support (FCS) 20

5.2.3 Class: Identification and Authentication (FIA) 22

5.2.4 Class: Security Management (FMT) 24

5.2.5 Class: Protection of the TSF (FPT) 24

5.2.6 Class: TOE Access (FTA) 25

5.2.7 Class: Trusted Path/Channels (FTP) 26

5.3 TOE SFR Dependencies Rationale for SFRs 26

5.4 Security Assurance Requirements 26

6 TOE Summary Specification 28

6.1 Key Storage and Zeroization 34
Annex A: References 36

Revision History

Version	Date	Description
0.1	June 2018	Draft for review.
0.2	July 2018	Respond to vendor feedback
0.3	July 2018	Updates based on vendor feedback
0.4	August 2018	Updates based on internal review
0.5	August 2018	Updated based on vendor provided detail.
0.6	September 2018	Finalized based on vendor feedback
0.7	January 2019	Changed security function claims.
0.8	January 2019	Minor Fixes
0.9	February 2019	Quality/Editorial fixes
0.10	February 2019	Integrated new TDs
0.11	April 2019	Updated based on ECR comments and integrated new TDs
1.0	August 2019	Finalized for release
1.1	September 2019	Updated based on ECR comments.
1.2	September 2019	Updated based on ECR comments.

1 Security Target Introduction

1.1 Security Target and TOE Reference

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

Category	Identifier
ST Title	Citrix ADC (formerly NetScaler) Platinum Edition Version 11.1 – Common Criteria Security Target
ST Author	Acumen Security, LLC.
ST Version	1.2
TOE Identifier	Citrix ADC Platinum Edition Version 11.1
TOE Hardware Reference	For physical appliances: MPX 14030 FIPS, MPX 14060 FIPS, MPX 14080 FIPS
TOE Software Version	11.1 NDcPP branch Build 54.138
TOE Developer	Citrix Systems Inc.
Key Words	Network Device, Security Appliance

Table 1 Security Target Information

1.2 TOE Overview

The Citrix ADC (formerly NetScaler) is an Application Delivery Controller that accelerates application performance, enhances application availability with advanced Layer 4 – Layer 7 load balancing, secures applications from attacks, and lowers server expenses by offloading computationally intensive tasks. The TOE comprises Citrix ADC running on the following hardware appliances.

- MPX 14030 FIPS
- MPX 14060 FIPS
- MPX 14080 FIPS

Citrix MPX 14XXX FIPS appliances are network devices that combine Layer 4 - Layer 7 load balancing and content switching with application acceleration, data compression, static and dynamic content caching, SSL acceleration, network optimization, application performance monitoring, application visibility, and robust application security via an application firewall. The ADC appliance supports NIST-approved FIPS 140-2 algorithms.

1.3 TOE Description

1.3.1 TOE Evaluated Configuration

The TOE evaluated configuration consists of one of the MPX series appliances listed above. All three models of the MPX series appliance use an Intel(R) Xeon(R) E5-2630 v2 processor and a Cavium Octeon II CN6120 cryptographic processor. The TOE also supports (sometimes optionally) secure connectivity with several other IT environment devices as described in Table 2 below,

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Syslog server	Yes	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. The syslog server must support communications using TLS 1.1 or TLS 1.2.

Component	Required	Usage/Purpose Description for TOE performance
LDAP Server	Yes	The LDAP server is used for authentication of administrator credentials The LDAP server must support communications using TLS 1.1 or TLS 1.2.

Table 2 IT Environment Components

The following figure provides a visual depiction of an example of a typical TOE deployment. The TOE boundary is surrounded with **hashed red lines**.

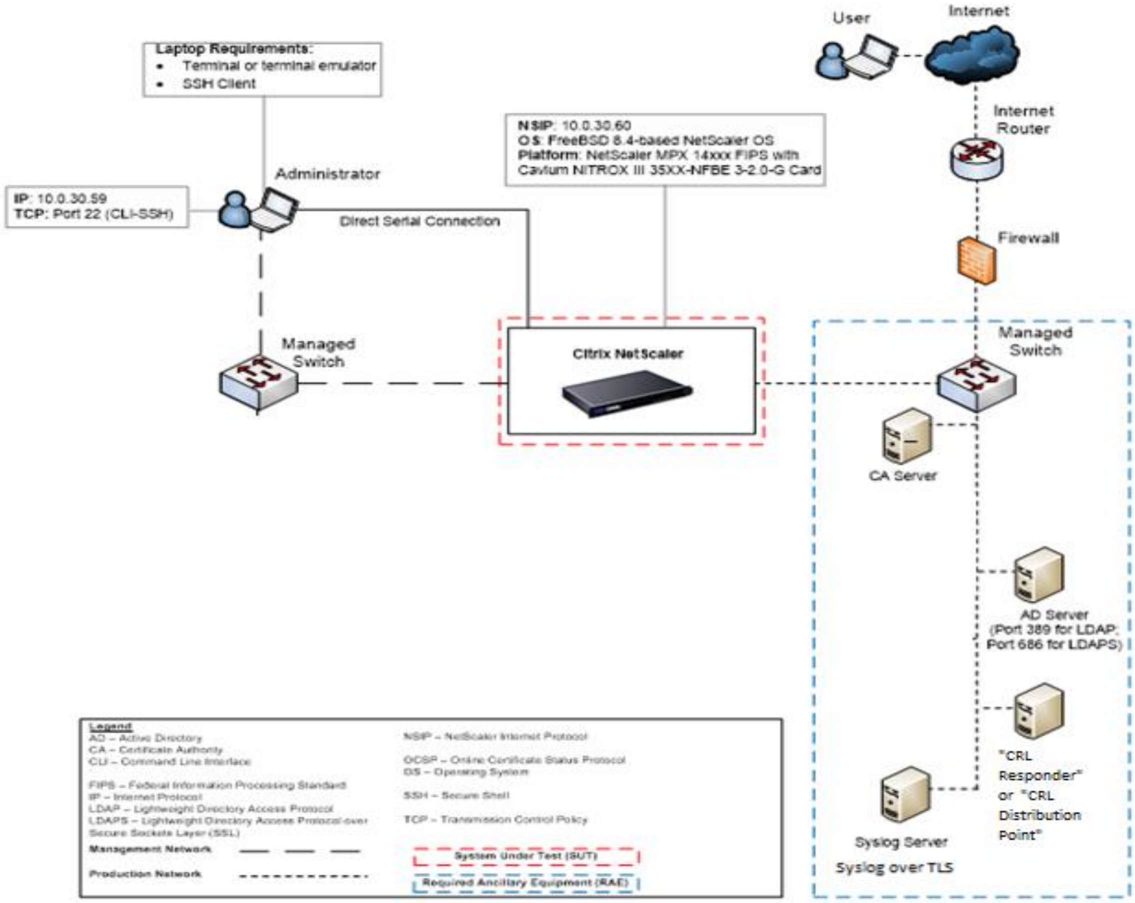
User
Internet
Laptop Requirements:
• Terminal or terminal emulator
• SSH Client
Internet Router
NSIP: 10.0.30.60
OS: FreeBSD 8.4-based NetScaler OS
Platform: NetScaler MPX 14xxx FIPS with Cavium NITROX III 35XX-NFBE 3-2.0-G Card
Administrator
IP: 10.0.30.59
TCP: Port 22 (CLI-SSH)
Direct Serial Connection
Firewall
Managed Switch
Citrix NetScaler
Managed Switch
CA Server
AD Server
(Port 389 for LDAP; Port 686 for LDAPS)
"CRL Responder" or "CRL Distribution Point"
Syslog Server
Syslog over TLS
Legend
AD – Active Directory
CA – Certificate Authority
CLI – Command Line Interface
FIPS – Federal Information Processing Standard
IP – Internet Protocol
LDAP – Lightweight Directory Access Protocol
LDAPS – Lightweight Directory Access Protocol over Secure Sockets Layer (SSL)
Management Network
Production Network
NSIP – NetScaler Internet Protocol
OCSP – Online Certificate Status Protocol
OS – Operating System
SSH – Secure Shell
TCP – Transmission Control Policy
System Under Test (SUT)
Required Ancillary Equipment (RAE)

Figure 1 Deployment Configuration of TOE

1.3.2 Physical Boundaries

The TOE is a hardware and software solution that is comprised of the security appliance models described above in Section 1.3. The TOE guidance documentation can be found at http://docs.citrix.com/en-us/netscaler/11-1.html#.

1.3.3 Logical Boundaries

The TOE is composed of the Citrix ADC OS running directly on the MPX appliance hardware. It is also comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

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

These security functions are discussed in detail in the sections below.

1.3.3.1 Security Audit

The TOE keeps local and remote audit records of security relevant events.

1.3.3.2 Cryptographic Support

The TOE provides cryptographic support for the SSH and TLS protocols. The related FIPS 140-2 validation details are provided in Table 3.

Algorithm	CAVP Cert #	Standard	Operation	SFR
NITROXIII CNN3560-NFBE-G Algorithms (CMVP Cert. #2850)				
RSA	1634	FIPS 186-4	Signature Verification	FCS_COP.1/SigGen
DRBG	680	SP 800-90A	Random Bit Generation	FCS_RBG_EXT.1
AES	20343 205	AES specified in ISO 18033-3 CBC specified in ISO 10116	TLS Encryption/Decryption DRBG Primitive	FCS_COP.1/DataEncryption
SHA	1780	ISO/IEC 10118-3:2004	Hashing	FCS_COP.1/Hash
HMAC	1233	ISO/IEC 9797-2:2011	Keyed-Hashing	FCS_COP.1/KeyedHash
Citrix FIPS Cryptographic Module Algorithms (CMVP Cert. #2988)				
RSA	2379	FIPS 186-4	Key Generation Signature Generation/Verification	FCS_CKM.1 FCS_COP.1/SigGen
ECDSA	1056	FIPS 186-4	Key Generation	FCS_CKM.1
DRBG	1417	SP 800-90A	Random Bit Generation	FCS_RBG_EXT.1
SHA	3626	ISO/IEC 10118-3:2004	Hashing	FCS_COP.1/Hash
HMAC	2923	ISO/IEC 9797-2:2011	Keyed-Hashing	FCS_COP.1/KeyedHash
AES	4397	AES specified in ISO 18033-3 CBC specified in ISO 10116 CTR specified in ISO 10116	SSH Encryption/ Decryption DRBG Primitive	FCS_COP.1/DataEncryption

Algorithm	CAVP Cert #	Standard	Operation	SFR
CVL (SP800-56A)	1106	SP 800-56A	Key Establishment	FCS_CKM.2

Table 3 CAVP Algorithm Testing References

1.3.3.3 Identification and Authentication

The TOE provides two types of authentication to provide a trusted means for Security Administrators and remote endpoints to interact: X.509v3 certificate-based authentication for remote devices and password-based or public-key authentication for Security Administrators. Device-level authentication allows the TOE to establish a secure communication channel with a remote endpoint.

Security Administrators can set a minimum length for passwords (between 4 and 127 characters). Additionally, the TOE detects and tracks consecutive unsuccessful remote authentication attempts and will prevent the offending attempts from authenticating when a Security Administrator defined threshold is reached.

1.3.3.4 Security management

The TOE enables secure local and remote management of its security functions, including:

- Local console CLI administration
- Remote CLI administration via SSHv2
- Administrator authentication using a local database
- Timed user lockout after multiple failed authentication attempts
- Password complexity enforcement
- Role Based Access Control - the TOE supports several types of administrative user roles. Collectively these sub-roles comprise the “Security Administrator”
- Configurable banners to be displayed at login
- Timeouts to terminate administrative sessions after a set period of inactivity
- Protection of secret keys and passwords

1.3.3.5 Protection of the TSF

The TOE ensures the authenticity and integrity of software updates through hash comparison and requires administrative intervention prior to the software updates being installed.

1.3.3.6 TOE Access

Prior to login, the TOE displays a banner with a message configurable by the Security Administrator. The TOE terminates user connections after an Authorized Administrator configurable amount of time.

1.3.3.7 Trusted Path Channels

The TOE uses TLS to provide a trusted channel between itself and remote syslog and LDAP servers.

The TOE uses SSH to provide a trusted path between itself and remote administrators.

1.3.1 TOE Documentation

- Common Criteria Evaluated Configuration Guide for ADC 11.1 Platinum Edition v1.1 [CCECG]
- Citrix ADC MPX, September 16, 2019
- NetScaler 11.1, September 13, 2019

1.4 Excluded Functionality

Hardware and software located in the TOE environment (see section 1.3.1) are not included in the scope of evaluations against this Security Target.

Only security functionality specified in the SFRs in section 5.2 (and the corresponding security functions in section 6) is covered by the scope of evaluation against this Security Target. Other product features or functionality are considered unevaluated, because they are not included in the scope of this Security Target:

- Web Logging
- Application Firewall
- Global Server Load Balancing (GSLB)
- AAA-TM Authentication
- External authentication methods: Kerberos, TACACS+, SAML, RADIUS
- Responder
- Rewrite (URL Transformation)
- Layer 3 Routing
- Vpath
- RISE
- High Availability
- CloudBridge
- CallHome
- Integrated Disk Caching
- General TLS VPN functionality
- Clientless VPN functionality
- SSL acceleration – SSL termination for application servers[1]
- AppFlow
- AppQoE
- BGP
- Cache Redirection
- Compression Control
- Content Accelerator
- Content Filtering
- Content Switching
- FEO
- OSPF
- LSN
- RDP Proxy
- RIP
- HTM Injection
- Http DoS Protection
- Integrated Caching
- Surge Protection
- ISIS
- Priority Queuing

[1] TLS used by the TSF is in scope and evaluated by FCS_TLSC_EXT.1.

- Reputation
- Sure Connect
- NetScaler Push

Additionally, the following features may not be used when the TOE is operated in a manner compliant with this Security Target:

- IPv6
- NTP based updates to the time
- Use of superuser privileges except as described in [CCECG]
- ADC GUI (HTTP/HTTPS), ADC Nitro API and ADM

2 Conformance Claims

2.1 CC Conformance

This TOE is conformant to:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 4, September 2012: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 4, September 2012: Part 3 conformant

2.2 Protection Profile Conformance

This TOE is conformant to:

- Collaborative Protection Profile for Network Devices, Version 2.0 + errata, 14 March 2018 [NDcPP2.0e].

2.3 Scheme Interpretations

The following NIAP Technical Decisions (TDs) apply to [NDcPP 2.0e]:

Identifier	Applicable	Exclusion Rationale (if applicable)
0425 – NIT Technical Decision for Cut-and-paste Error for Guidance AA	Yes	
0423 – NIT Technical Decision for Clarification about application of RfI#201726rev2	Yes	
0412 – NIT Technical Decision for FCS_SSHS_EXT.1.5 SFR and AA discrepancy	Yes	
0411 – NIT Technical Decision for FCS_SSHC_EXT.1.5, Test 1 - Server and client side seem to be confused	No	This TD addresses SSH Client functionality. The TOE does not support SSH Client functionality.
0410 – NIT technical decision for Redundant assurance activities associated with FAU_GEN.1	Yes	
0409 – NIT decision for Applicability of FIA_AFL.1 to key-based SSH authentication	Yes	
0408 – NIT Technical Decision for local vs. remote administrator accounts	Yes	
0407 – NIT Technical Decision for handling Certification of Cloud Deployments	Yes	
0402 – NIT Technical Decision for RSA-based FCS_CKM.2 Selection	Yes	
0401 – NIT Technical Decision for Reliance on external servers to meet SFRs	Yes	
0400 – NIT Technical Decision for FCS_CKM.2 and elliptic curve-based key establishment	Yes	
0399 – NIT Technical Decision for Manual installation of CRL (FIA_X509_EXT.2)	Yes	
0398 – NIT Technical Decision for	Yes	

FCS_SSH*EXT.1.1 RFCs for AES-CTR		
0397 – NIT Technical Decision for Fixing AES-CTR Mode Tests	Yes	
0396 – NIT Technical Decision for FCS_TLSC_EXT.1.1, Test 2	Yes	
0395 – NIT Technical Decision for Different Handling of TLS1.1 and TLS1.2	No	This TD addresses TLS Server functionality. The TOE does not support TLS Server functionality.
0394 – NIT Technical Decision for Audit of Management Activities related to Cryptographic Keys	Yes	
0343 – NIT Technical Decision for Updating FCS_IPSEC_EXT.1.14 Tests	No	This TD addresses IPsec functionality. The TOE does not support IPsec.
0342 – NIT Technical Decision for TLS and DTLS Server Tests	No	This TD addresses (D)TLS Server functionality. The TOE does not support (D)TLS Server functionality.
0341 – NIT Technical Decision for TLS wildcard checking	Yes	
0340 – NIT Technical Decision for Handling of the basicConstraints extension in CA and leaf certificates	Yes	
0339 – NIT Technical Decision for Making password-based authentication optional in FCS_SSHS_EXT.1.2	Yes	
0338 – NIT Technical Decision for Access Banner Verification	Yes	
0337 – NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6	Yes	
0336 – NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8	Yes	
0335 – NIT Technical Decision for FCS_DTLS Mandatory Cipher Suites	No	This TD addresses DTLS functionality. The TOE does not support DTLS.
0334 – NIT Technical Decision for Testing SSH when password-based authentication is not supported	No	This TD addresses SSH client functionality. The TOE does not claim FCS_SSHC_EXT.1.
0333 – NIT Technical Decision for Applicability of FIA_X509_EXT.3	Yes	
0324 – NIT Technical Decision for Correction of section numbers in SD Table 1	Yes	
0323 – NIT Technical Decision for DTLS server testing - Empty Certificate Authorities list	No	This TD addresses DTLS functionality. The TOE does not support DTLS.
0322 – NIT Technical Decision for TLS server testing - Empty Certificate Authorities list	No	This TD is associated with FCS_TLSS_EXT.2. The TOE does not include FCS_TLSS_EXT.2 functionality.
0321 – Protection of NTP communications	No	The TOE does not support an NTP server for automatic time updates.
0291 – NIT technical decision for DH14 and FCS_CKM.1	Yes	
0290 – NIT technical decision for physical interruption of trusted path/channel.	Yes	
0289 – NIT technical decision for	Yes	

FCS_TLSC_EXT.x.1 Test 5e		
0281 – NIT Technical Decision for Testing both thresholds for SSH rekey	Yes	
0262 – NIT Technical Decision for TLS server testing - Empty Certificate Authorities list	No	This TD has been archived
0260 – NIT Technical Decision for Typo in FCS_SSHS_EXT.1.4	No	This TD has been archived.
0259 – NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187	Yes	
0257 – NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4	Yes	
0256 – NIT Technical Decision for Handling of TLS connections with and without mutual authentication	No	This TD is associated with FCS_DTLSC_EXT.2/FCS_TLSC_EXT.2. The TOE does not include this functionality.
0228 – NIT Technical Decision for CA certificates - basicConstraints validation	Yes	

Table 4 TOE Technical Decisions

2.4 Conformance Rationale

This Security Target provides exact conformance to the Protection Profile(s) described in the conformance claims above. The security problem definition, security objectives and security requirements in this Security Target are all taken from the applicable Protection Profile(s) performing only operations defined there.

3 Security Problem Definition

The security problem definition has been taken from [NDcPP 2.0e] and is reproduced here for the convenience of the reader.

3.1 Threats

The following table lists the threats addressed by the TOE and the IT environment.

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 tunneling 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.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., 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.

Threat	Threat Definition
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_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include 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_FUNCTIONALITY_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.

Table 5 Threats

3.2 Assumptions

This section describes the assumptions made in identification of the threats and security requirements for network devices.

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 ND cPP. It is assumed that this protection will be covered by cPPs 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.
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.
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.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.

Table 6 Assumptions

3.3 Organizational Security Policy

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

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.

Table 7 Organizational Security Policies

4 Security Objectives

The security objectives have been taken from [NDcPP] and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the Operational Environment

The following table describes objectives for the Operational Environment.

Environment Security Objective	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.
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.
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.

Table 8 Security Objectives for the Operational Environment

5 Security Requirements

The individual security functional requirements are specified in the sections below.

The Evaluation Activities defined in [SD] describe actions that the evaluator will take in order to determine compliance of a particular TOE with the SFRs. The content of these Evaluation Activities will therefore provide more insight into deliverables required from TOE Developers.

5.1 Conventions

The conventions used in descriptions of the SFRs are as follows:

- Unaltered SFRs are stated in the form used in [CC2] or their extended component definition (ECD);
- Refinement made in the PP: the refinement text is indicated with bold text and strikethroughs;
- Selection: the selection values are indicated with underlined text
  - For example, "[selection: disclosure, modification, loss of use]" in [CC2] or an ECD might become "[disclosure]";
- Assignment: indicated with italicized text;
- Assignment completed within a selection: the completed assignment text is indicated with italicized and underlined text
  - e.g. "[selection: change_default, query, modify, delete, [assignment: other operations]]" in [CC2] or an ECD might become "[change_default, *select_tag*]";
- Iteration: indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").
- Extended SFRs are identified by having a label "EXT" at the end of the SFR name.
- Where operations were completed in the PP itself, the formatting used in the PP has been retained.

5.2 TOE Security Functional Requirements

The Security Functional Requirements for the TOE are adopted from [NDCPP v2.0e], with selections and assignments made for the TOE. These SFRs are stated in the sections below. Application notes from [NDCPP v2.0e] are included only where they clarify the meaning of the SFRs. For details of Assurance Activities, please refer to [NDCPP v2.0e]

5.2.1 Class: Security Audit (FAU)

5.2.1.1 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 shut-down of the audit functions;*
b) *All auditable events for the not specified level of audit; and*
c) *All administrative 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 9***.**

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 9

Requirement	Auditable Events	Additional Audit Record Contents
Mandatory SFRs		
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
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_RBG_EXT.1	None.	None.
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 identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	All management activities of TSF data.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.

Requirement	**Auditable Events**	**Additional Audit Record Contents**
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	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).
FTA_SSL_EXT.1 (if "terminate the session" is selected)	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.
Selection-Based SFRs		
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None.

Table 9 Auditable events

5.2.1.2 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.

5.2.1.3 FAU_STG_EXT.1 Protected Audit Event 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.

FAU_STG_EXT.1.3 The TSF shall [*overwrite previous audit records according to the following rule: [overwrite oldest record first]*] when the local storage space for audit data is full.

5.2.2 Class: Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 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;*

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

5.2.2.2 FCS_CKM.2 Cryptographic Key Establishment

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 meet 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”;*

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

5.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM_EXT.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 [single overwrite consisting of [zeroes];*
- *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 [*
    - *logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes];*
    - *instructs a part of the TSF to destroy the abstraction that represents the key]*

that meets the following: *No Standard*.

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

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

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

FCS_COP.1.1/SigGen 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) [2048 bits, 3072 bits],*

] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~

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 RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,*

].

5.2.2.6 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*.

5.2.2.7 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-512]* and cryptographic key sizes *[160 bits, 256 bits, 512 bits]* **and message digest sizes [*160, 256, 512*] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

5.2.2.8 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 [*[2] hardware-based noise source*] with a minimum of [*128 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

5.2.2.9 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*

].

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches the reference identifier per RFC 6125 section 6.

FCS_TLSC_EXT.1.3 The TSF shall only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall [*not establish the connection, [send an error/alert with the dropped connection]*].

FCS_TLSC_EXT.1.4 The TSF shall [*not present the Supported Elliptic Curves Extension*] in the Client Hello.

5.2.2.10 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) [*4251, 4252, 4253, 4254, 4344, 5656, 6668*].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [password-based].

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*262,144*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: *[aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr]*.

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [*ssh-rsa*] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses *[hmac-sha2-256, hmac-sha2-512]* as its data integrity MAC algorithm(s) and rejects all other MAC algorithms.

FCS_SSHS_EXT.1.7 The TSF shall ensure that *[ecdh-sha2-nistp256]* and *[ecdh-sha2-nistp384, ecdh-sha2-nistp521]* are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

5.2.3 Class: Identification and Authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*0 and 4,294,967,295*] 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 remote Administrator from successfully establishing remote session using any authentication method that involves a password until [the unlock account action] is taken by an Administrator; prevent the offending remote Administrator from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed*].

5.2.3.2 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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, [“~”, “`”, “-”, “ ”, “=”, “+”, “{”, “}”, “[”, “]”, “|”, “\”, “:”, “<”, “>”, “/”, “.”, “,”, “ ”]];

b) Minimum password length shall be configurable to [*4*] and [*127*]

5.2.3.3 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;
- [*[responses to ping or ARP]*]

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

5.2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

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

5.2.3.5 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.**

5.2.3.6 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 certificate path validation **supporting a minimum path length of three certificates**.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate 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 [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.

5.2.3.7 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*].

5.2.4 Class: Security Management (FMT)

5.2.4.1 FMT_MOF.1/ManualUpdate Management of security functions behavior

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

5.2.4.2 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 *Security Administrators***.**

5.2.4.3 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 the cryptographic functionality*
    - *Ability to re-enable an Administrator account;*
    - *Ability to set the time which is used for time-stamps;]*

].

5.2.4.4 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 the user 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.

5.2.5 Class: Protection of the TSF (FPT)

5.2.5.1 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

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

5.2.5.2 FPT_APW_EXT.1 Protection of Administrator Passwords

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

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

5.2.5.3 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*].

5.2.5.4 FPT_TST_EXT.1 TSF Testing

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

- *Memory (RAM) walk*
- *File integrity verification*
- *Citrix FIPS Cryptographic Module tests:*
  - *Integrity check*
  - *Algorithm known answer tests*
- *CNN3560-NFBE card*
  - *Integrity check*
  - *Algorithm known answer tests*

].

5.2.5.5 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 [*the most recently installed version of the TOE firmware/software*].

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.

5.2.6 Class: TOE Access (FTA)

5.2.6.1 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.

5.2.6.2 FTA_SSL.3 TSF-initiated Termination

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

5.2.6.3 FTA_SSL.4 User-initiated Termination

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

5.2.6.4 FTA_TAB.1 Default TOE Access Banners

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.

5.2.7 Class: Trusted Path/Channels (FTP)

5.2.7.1 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]** 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 *[export of audit logs to external audit server, authentication dialogue with authentication servers]*.

5.2.7.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin The TSF shall **be capable of using [*SSH*] 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 TOE SFR Dependencies Rationale for SFRs

The Collaborative Protection Profile for Network Devices contains all the requirements claimed in this Security Target. As such, SFR dependencies are not applicable since the PP has been approved.

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the Collaborative Protection Profile for Network Devices. The assurance requirements are summarized in the table below.

Assurance Class	Components	Components Description
Security Target	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_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance

	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

Table 10 Security Assurance Requirements

6 TOE Summary Specification

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

TOE SFR	Rationale
FAU_GEN.1 FAU_GEN.2	The TOE generates audit records for commands executed by Administrators using the CLI and for other security-related events as shown in Table 9. In general terms the audit records include the date and time of the event, type of event (including the selected options in the case of administrator commands), subject identity (if applicable), the outcome (success or failure) of the event, and (if connecting remotely) the IP address of the relevant IT entity. Other details specific to each event are indicated in Table 9. For the administrative task of managing cryptographic keys, the TOE identifies the relevant key in the following manner: • KEK – There is only a single KEK, so any KEK operation implicitly identifies the KEK. • X.509 Certificates – The administrator specifies a unique filename for the certificate. • SSH Host Key – There is only a single SSH host key so any SSH host key operations implicitly identifies the SSH host key. • SSH User Public Keys – The full public key is logged when it is added or removed from the authorized_keys file.
FAU_STG_EXT.1	Audit records are stored on the TOE in /var/log in the ns.log file. The TOE transmits audit records to an external syslog server as the audit records are generated. The channel to the syslog server is protected using TLS as specified in FTP_ITC.1. When the connection to the syslog server is down, the audit records are stored locally. When the connection to the syslog server comes back up, the TOE will resume transmission of audit records to the syslog server; however, it does not transmit audit records generated while the connection was down. The TOE stores 2,500KB of raw (uncompressed) audit records locally; however, actual physical storage space is less. The storage is segmented into the active ns.log file which is rotated when it reaches 100KB in size. The rotation process compresses the ns.log file and adds new audit records to a new ns.log file. If there are more than 25 compressed ns.log files, the TOE deletes the oldest file; effectively overwriting the previous audit records.
FCS_CKM.1 FCS_CKM.2	The TOE generates a 2048 bit RSA key that is used as the SSH host key on the TOE. This key is generated according to FIPS 186-4. The TOE generates P-256, P-384, and P-521 ECDH/ECDSA keys to perform Elliptic curve-based key establishment specified in FCS_SSHS_EXT.1.7 and SP 800-56A. These keys are generated according to FIPS 186-4. The TOE uses RSAES-PKCS1-v1_5 key transport as part of the TLS protocol. The TOE is the client/sender, so this operation does not involve RSA key generation. The relevant NIST CAVP certificate numbers are listed in Table 3.
FCS_CKM.4	See Table 12 in section 6.1.

<table>
<tr><td>FCS_COP.1/DataEncryption</td><td>The TOE supports encryption and decryptions using AES-128 and AES-256 in CBC and CTR modes.
The relevant NIST CAVP certificate numbers are listed in Table 3</td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE supports cryptographic signature services using the RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 or 3072 bits or greater, meeting FIPS PUB 186-4.
These RSA signature services are used in the TLS protocols as well as the SSH protocol (ssh-rsa).
The relevant NIST CAVP certificate numbers are listed in Table 3</td></tr>
<tr><td>FCS_COP.1/Hash</td><td>The TOE supports cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512.
SHA-1 and SHA-256 are used in digital signatures.
SHA-256 is used for update verification.
SHA-256, SHA-384 and SHA-512 are used in the SSH KDF.
SHA-1, SHA-256, and SHA-512 are used as HMAC primitives.
SHA-512 is used for password hashing.
The relevant NIST CAVP certificate numbers are listed in Table 3</td></tr>
<tr><td>FCS_COP.1/KeyedHash</td><td>The TOE supports the generation and verification of hash message authentication codes (HMACs) using HMAC-SHA-1, HMAC_SHA-256, and HMAC-SHA512. The details of each HMAC function is described below.
<table>
<tr><th></th><th>HMAC-SHA-1</th><th>HMAC-SHA-256</th><th>HMAC-SHA-512</th></tr>
<tr><td>Key Length</td><td>160 bits</td><td>256 bits</td><td>512 bits</td></tr>
<tr><td>Hash function</td><td>SHA-1</td><td>SHA-256</td><td>SHA-512</td></tr>
<tr><td>Block Size</td><td>512 bits</td><td>512 bits</td><td>1024 bits</td></tr>
<tr><td>Output MAC</td><td>160 bits</td><td>256 bits</td><td>512 bits</td></tr>
<tr><td>Uses</td><td>TLS KDF
TLS MAC</td><td>TLS KDF
SSH MAC</td><td>SSH MAC</td></tr>
</table>
The relevant NIST CAVP certificate numbers are listed in Table 3</td></tr>
<tr><td>FCS_RBG_EXT.1</td><td>The TOE also generates random bits using two SP 800-90A CTR_DRBGs, both using AES-256.
The CNN3560-NFBE DRBG is used to generate keys and random bits for TLS. It is seeded using one third party hardware-based noise source that is assumed to produce at least 24 bits of entropy per 64-bit sample. The DRBG is seeded with 6 samples from the noise source that contain at least 144 bits of entropy. The CNN3560-NFBE DRBG is used to generate keys for FCS_TLSC_EXT.1 which only uses 128-bit AES keys.
The Citrix FIPS DRBG is used to generate keys and random bits for all other uses. The DRBG is seeded using RDRAND (a third-party hardware-based noise source). The internal noise source is assumed to produces 0.5 bits of entropy per 1-bit sample. RDRAND performs internal post-processing and conditioning that results in an assumed min-entropy rate of 128-bits per 2816-bits output from RDRAND. The DRBG is seeded with 2944 bits of output from RDRAND that</td></tr>
</table>

	contains at least 256 bits of entropy. The Citrix FIPS DRBG is used to generate keys for FCS_SSHS_EXT.1. The relevant NIST CAVP certificate numbers are listed in Table 3
FCS_SSHS_EXT.1	The TOE implements SSHv2 (compliant with RFCs 4251, 4252, 4253, 4254, 4344, 5656, and 6668) for administrators to make remote connections to access the CLI (as an alternative to the use of the local console). The TOE supports both ssh-rsa public key-based and password-based authentication methods for SSH. When using public-key authentication methods, ssh-rsa public keys are stored in /var/pubkey/<username>.ssh/authorized_keys. The ssh-rsa private host key is stored in /nsconfig/ssh. When connecting over SSH, the ssh daemon looks up the relevant public key in the authorized_keys file. If a public key is present then it will be used for authentication, otherwise password-based authentication is used, passing the username and passphrase details to the PAM library to confirm their validity. If the authentication is successful, then the login process uses an exec system call to launch the CLI. SSH packets larger than 256KB (262,144 bytes) are dropped by the TOE. For SSH transport, the TOE uses aes128-cbc, aes256-cbc, aes128-ctr, or aes256-ctr to encrypt data. The data integrity algorithms used are hmac-sha2-256 and hmac-sha2-512. The TOE uses only ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521 as the SSH key exchange methods. The TOE automatically rekeys the connection after 1 hour has elapsed or 1 GB of data has been encrypted with an encryption key. The TOE initiates the rekey upon reaching either threshold (whichever is reached first).
FCS_TLSC_EXT.1	The TOE implements TLS versions 1.1 (RFC 4346) and 1.2 (RFC 5246) with the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite. The TOE automatically configures references identifiers based on the FQDN configured by the administrator to connect to the TLS server. When a FQDN has been configured, the TOE establishes reference identifiers of DNS-ID and CN-ID. When the TOE compares the reference identifies to the identifiers in the presented certificate, it will consider the identifiers matching if they are an exact match or if the presented identifier exactly matches with the exception of a wildcard in the left most position matching the left most position of the reference identifier. The TOE will use the SAN(s) in the presented certificate if present. The TOE will only use the CN if the certificate does not contain any SANs. The TOE does not support certificate pinning. The TOE will not establish the connection if the server certificate is invalid, if the presented identifier does not match, or if the CRL cannot be retrieved. The TOE does not present the Supported Elliptic Curves Extension (renamed Supported Groups Extension), because the TOE only supports RSA key transport.
FIA_AFL.1	The TOE is capable of tracking authentication failures for each of the claimed authentication mechanisms (local, SSH). The administrator can configure the maximum number of failed attempts using the CLI interface via the `set aaa parameter -maxloginAttempts <num> -failedLoginTimeout <seconds>` command. The configurable

	range is between 0 and 4,294,967,295 attempts (i.e. a 32-bit integer). When a user account has sequentially failed authentication the configured number of times, the account will be locked. If the `-failedLoginTimeout` is configured, then the user account will be unlocked when the specified number of seconds have elapsed since the locking mechanism was engaged. If the administrator is required to intervene to unlock an account, this is done using the CLI via the `unlock aaa user <username>` CLI command from the local console. Irrespective of whether an administrator intervened or whether the elapsed time occurred, when a locked account is unlocked, the failure counter associated with that user is reset to 0. If a user succeeds at authenticating before the locking mechanism has been enabled, the failure counter is reset to 0. If the lockout attempts is set to, for example, 5 attempts, then the user will be locked out after the 5th consecutive failed login attempt. This means that the 6th and subsequent attempts will fail to gain access to the TOE even if the credential being offered is correct. The TOE prevents a situation where all administrator accounts are locked out by allowing local access for accounts that are blocked from remotely authenticating to the TOE.
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 “ ”. The minimum password length is settable by the Authorized Administrator and can range from 4 to 127 characters.
FIA_UIA_EXT.1 FIA_UIA_EXT.2	Administrators access the TOE through the CLI, either using a local console or via a remote connection using SSH with an optional TLS tunnel. Identification and authentication is required for administrators before access is given to any of the TOE functions except for the display of the warning banner (as in FTA_TAB.1) or responses to ping or ARP. The local console supports username/password credentials. The SSH connection supports a username with a password or SSH public key authentication.
FIA_UAU.7	When a user enters their password at the local console then no characters are displayed on the console.
FIA_X509_EXT.1/Rev FIA_X509_EXT.2	The TOE performs X.509 certificate validation at the following points: • authentication of server X.509 certificates; • When certificates are loaded into the TOE, such as when importing CAs, certificate responses. In all scenarios, certificates are checked for several validation characteristics: • If the certificate ‘notAfter’ date is in the past, then this is an expired certificate which is considered invalid; • If the certificate ‘notBefore’ date is in the future, then this certificate is not yet valid which is considered invalid • The certificate chain must terminate with a trusted root CA certificate;

	• Server certificates consumed by the TOE TLS client must have a ‘serverAuthentication’ extendedKeyUsage purpose; • Client certificates consumed by the TOE TLS server must have a ‘clientAuthentication’ extendedKeyUsage purpose. A trusted root CA certificate is defined as any certificate loaded into the TOE trust store. All CA certificates must have, at a minimum, a basicConstraints extension with the CA flag set to TRUE. Certificate revocation checking is performed using CRLs. The TOE verifies the CA certificate used to sign the CRL has the CRLsign key usage bit set. If this bit is not set, the TOE considers this CRL invalid. As X.509 certificates are not used for either trusted updates or firmware integrity self-tests, the code-signing purpose is not checked for in the extendedKeyUsage. The TOE has a trust store where root CA and intermediate CA certificates can be stored. The trust store is not cached: if a certificate is deleted, it is immediately untrusted. If a certificate is added to the trust store, it is immediately trusted for its given scope. The X.509 certificates for each of the given scenarios are validated using the certificate path validation algorithm defined in RFC 5280, which can be summarized as follows: • The public key algorithm and parameters are checked • The current date/time is checked against the validity period revocation status is checked • Issuer name of X matches the subject name of X+1 • Name constraints are checked • Policy OIDs are checked • Policy constraints are checked; issuers are ensured to have CA signing bits • Path length is checked • Critical extensions are processed If, during the entire trust chain verification activity, any certificate under review fails a verification check, then the entire trust chain is deemed untrusted and the TLS connection is terminated.
FMT_MOF.1/ManualUpdate	The TOE restricts the ability to perform manual software updates to the Security Administrator role.
FMT_MTD.1/CoreData	The TOE does not allow administrators to perform any administrative actions prior to administrator login. Once the administrator has successfully been identified and authenticated, the TOE restricts the ability to manage TSF data to the Security Administrator role.
FMT_SMF.1	The TOE allows Security Administrators the ability to manage the following functions: • Ability to configure the access banner; • Ability to configure the session inactivity time before session termination; • Ability to update the TOE, and to verify the updates using hash comparison prior to installing those updates;

	• Ability to configure the authentication failure parameters for FIA_AFL.1; • Ability to configure the cryptographic functionality • Ability to re-enable an Administrator account; • Ability to set the time which is used for time-stamps All management functions are available from both the local console and remote SSH CLI.
FMT_SMR.2	The TOE maintains the Security Administrator role. This role maps to the ADC System User role. The TOE also supports a superuser role; however, this role may not be used in the evaluated configuration.
FPT_SKP_EXT.1	The TOE does not provide a CLI interface designed to permit the viewing of pre-shared keys, symmetric keys or private keys. The TOE does not utilize pre-shared keys. The TOE only stores symmetric keys in RAM and does not provide any interface for reading these keys. Private keys are protected from access by the use of file and API permissions. The filesystem permissions prevent administrators from reading the SSH hostkey. The API permission of the CNN3560-NFBE card prevent the reading of TLS private keys.
FPT_APW_EXT.1	The TOE does not store passwords in plaintext form and does not provide an interface to view passwords (plaintext or hashes). Administrator passwords are stored in hashed (SHA-512) form (after adding a random 64-bit salt to each password); and password strings contained in audit log entries are obscured with asterisks.
FPT_TST_EXT.1	The TOE automatically runs the following self-tests at power-up: • Memory (RAM) walk • File integrity verification using CRC32 • Citrix FIPS Cryptographic Module tests: ○ Integrity check ○ Algorithm known answer tests • CNN3560-NFBE card ○ Integrity check ○ Algorithm known answer tests If any failures are detected during the Memory walk, the TOE will take the memory module out of service and log the error. The TOE will continue to operate as long as one memory module remains operational. If any of the other self-tests fail, the TOE will enter an error state and not provide any cryptographic services. The self-tests demonstrate the TOE is operating correctly, because the integrity checks verify the executable code has not been modified and the algorithm known answer tests verify the hardware executing the instructions is operating correctly.
FPT_TUD_EXT.1	An Authorized Administrator can determine the current version of the TOE using the `show version` and `shell cat /tmp/aaad.debug` commands to display the software version identifier and the `show hardware` command to display the hardware model identifier. The version of the inactive firmware can be queried using the `show version -installedversion` command. The inactive version of firmware can be activated by rebooting the TOE.

	Updates to the TOE software are obtained by an Administrator by download from the Citrix website. Each update is accompanied by a hash value that is also published on the Citrix website: before applying any update, the administrator applies the OpenSSL hash tool on the appliance, using the SHA-256 hash function and verifying that the hash value obtained matches the value published for that item on the Citrix website. Provided that the hash value is correct the Administrator then applies the update.
FPT_STM_EXT.1	The TOE hardware provides a system clock, which is used for timestamps in audit log entries, to measure periods of inactivity during local and remote administrator sessions in order to determine when an inactive session is to be terminated, determine if certificates are valid, and determine the time-based SSH rekeying threshold. The Administrator must manually update the time to ensure accuracy of the system clock.
FTA_SSL_EXT.1 FTA_SSL.3	An Authorized Administrator can specify a maximum inactivity time period for both local and remote interactive sessions after which a session will be automatically terminated by the TOE.
FTA_SSL.4	An Administrator can choose to terminate their own interactive session from the CLI at any time using the 'logout' (or 'exit' or ctrl-d) command.
FTA_TAB.1	An Authorized Administrator can specify a banner message that is displayed at the beginning of each administrative user session, both local console and SSH CLI.
FTP_ITC.1	The TOE uses trusted channels based on TLS v1.1 and v1.2 (see FCS_TLSC_EXT.1) to communicate with external authentication servers and remote audit servers. These channels protect the communications from unauthorized disclosure or modification. The TOE initiates the connections to both server types.
FTP_TRP.1/Admin	The trusted path used for remote administrator connections is provided using SSH (see FCS_SSHS_EXT.1).

Table 11 TOE Summary Specification SFR Description

6.1 Key Storage and Zeroization

The following table describes the origin, storage and zeroization of keys as relevant to FCS_CKM.4 and FPT_SKP_EXT.1 provided by the TOE.

Key	Type	Origin	Storage/Protection	Zeroization
KEK	AES Key	Generated when needed from the Key Files	RAM	Automatically overwritten with zeros immediately after use.
Key Files	N/A – input to generate the KEK	Generated from passphrase combined with random data from the DRBG	ACL protected directory	These files are destroyed by instructing the underlying filesystem interface to delete the keyfiles.
EC Diffie Hellman private key	DH Key	TOE generated	RAM	Keys are overwritten with zeros at power cycle.
EC Diffie Hellman public key	DH Key	TOE generated	RAM	Keys are overwritten with zeros at power cycle.

Key	Type	Origin	Storage/Protection	Zeroization
SSH Private Key	RSA Private Key	TOE generated	ACL protected directory and encrypted using the KEK	Key is overwritten by zeros when the compliance declassify zeroize command is issued.
SSH Public Key	RSA Public Key	TOE generated	n/a - public	Key is overwritten by zeros when the compliance declassify zeroize command is issued.
SSH Session Key	AES Key	TOE generated	RAM	Keys are overwritten with zeros at power cycle.
TLS Session Encryption Key	AES Key	TOE generated	RAM	Keys are overwritten with zeros at power cycle.
TLS Session Integrity Key	HMAC Key	TOE generated	RAM	Keys are overwritten with zeros at power cycle.

Table 12 Key Storage & Zeroization

Non-volatile keys are overwritten with zeros using a single pass when the administrator disables FIPS/CC mode. As part of the disablement function, the device is power-cycled to zeroize keys and CSPs in volatile memory.

When the device is reverted to factory settings, all non-volatile keys are zeroized by overwriting with zeros using a single pass.

Annex A: References

The following documentation was used to prepare this ST:

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 4, CCMB-2012-09-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 4, CCMB-2012-09-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components April 2017, version 3.1, Revision 4, CCMB-2012-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated April 2017, version 3.1, Revision 4, CCMB-2012-09-004
[NDcPP]	Collaborative Protection Profile for Network Devices, Version 2.0 errata, March-2018.
[SD]	Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP, Version 2.0 errata, March-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
[800-56Ar2]	NIST Special Publication 800-56A Revision 2, May 2013, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[800-56B]	NIST Special Publication 800-56B Revision 1, September 2014, Recommendation for Pair-Wise 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 186-4]	FIPS PUB 186-4 Federal Information Processing Standards Publication: Digital Signature Standard (DSS), July 2013.
[FIPS PUB 198-1]	FIPS PUB 198-1 Federal Information Processing Standards Publication: The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90A]	NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015
[FIPS PUB 180-4]	FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), August 2015.
[RFC3526]	RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003.
[RFC2818]	RFC 2818, HTTP Over TLS, May 2000.
[RFC4251]	RFC 4251, The Secure Shell (SSH) Protocol Architecture, January 2006.
[RFC4252]	RFC 4252, The Secure Shell (SSH) Authentication Protocol, January 2006.
[RFC4253]	RFC 4253, The Secure Shell (SSH) Transport Layer Protocol, January 2006.
[RFC4254]	RFC 4254, The Secure Shell (SSH) Connection Protocol January 2006.
[RFC5647]	RFC 5647, AES Galois Counter Mode for the Secure Shell Transport Layer Protocol, August 2009.
[RFC6668]	RFC 6668, SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol, July 2012.
[RFC5246]	RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008.
[RFC4346]	RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1, April 2006.
[RFC3268]	RFC 3268, Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security

	(TLS), June 2002.
[RFC6125]	RFC 6125, Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS), March 2011.
[RFC5280]	RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.
[RFC6960]	RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013.
[RFC2986]	RFC 2986, PKCS #10: Certification Request Syntax Specification Version 1.7, November 2000.

Table 13 References