Symantec Corporation
SSL Visibility Appliance

Models: SV1800-C, SV1800-F, SV1800B-C, SV1800B-F, SV2800, SV2800B, SV3800, SV3800B, SV-3800B-20
Software Version: 3.10.2.1-21-FIPS140

Symantec SSL Visibility Appliance NDPP Security Target

Document Version: 1.3

Contact Information

Americas:
Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
www.symantec.com

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Purpose

The Security Target (ST) is divided into eight sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Security Requirements (Section 5) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 7) - Presents the rationale for the SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 8) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	Symantec SSL Visibility Appliance NDPP Security Target
ST Version	Version 1.3
ST Author	Symantec Corporation
ST Publication Date	February 8, 2017
TOE Reference	Symantec SSL Visibility Appliance
TOE Software Version	3.10.2.1-21-FIPS140
TOE Hardware Version	SV1800-C, SV1800-F, SV1800B-C, SV1800B-F, SV2800, SV2800B, SV3800, SV3800B, SV-3800B-20
TOE developer	Symantec Corporation

1.3 Product Overview

The Symantec SSL Visibility Appliance is a high performance transparent proxy for Secure Socket Layer (SSL) network communications. It enables a variety of applications to access the plaintext (that is, the original unencrypted data) in SSL encrypted connections, and has been designed for security and network appliance manufacturers, enterprise IT organizations and system integrators. Without compromising any aspect of enterprise policies or government compliance, the SSL Visibility Appliance lets network appliances be deployed with highly granular flow analysis while maintaining line rate performance. Additionally, the SSL Visibility Appliance will not interfere with plaintext traffic transversing the network.

1.4 TOE Overview

The TOE is the Symantec SSL Visibility Appliance, hardware models SV1800-C, SV1800-F, SV1800B-C, SV1800B-F, SV2800, SV2800B, SV3800, SV3800B, SV-3800B-20, running Software Version: 3.10.2.1-21-FIPS140 and is a hardware and software TOE. The Symantec SSL Visibility Appliance is an integral component to any encrypted management strategy, and offers complete visibility into encrypted traffic without requiring the re-architecting of the network infrastructure. The SSL Visibility Appliance lets you add SSL inspection capabilities to your network security architecture and close the security visibility loophole created by encrypted traffic.

The SSL Visibility Appliance provides a complete solution to the problem of dealing with threats contained within encrypted SSL traffic. A single SSL Visibility Appliance can be deployed to detect and inspect all SSL traffic that may pose a threat, and can pass the decrypted content to one or more network security appliances which can record or block any threats. The ability to feed "inspected" traffic to more than one associated security appliance ensures that SSL traffic only as to be decrypted and then re-encrypted once as it crosses the network. The SSL Visibility Appliance is designed to work alongside existing security devices such as Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Data Loss Prevention systems (DLP), Network Forensic appliances, and so on. It provides a non-encrypted version of SSL traffic to the associated appliance while maintaining an end to end SSL connection between the client and server involved in the session.

Unlike most other SSL proxy devices, the SSL Visibility Appliance does not rely on the TCP destination port number being used by a session to determine if it is using SSL or not. The SSL Visibility Appliance uses deep packet inspection (DPI) to identify SSL flows. This ensures that it can find and inspect any SSL traffic in the network, even if the traffic is using non standard port numbers. The SSL Visibility Appliance incorporates flow processing hardware and cryptographic acceleration hardware, enabling it to forward non SSL traffic at multi-Gigabit/s rates, while offering industry-leading transparent proxy performance (that is, decrypting and re-encrypting) for SSL traffic.

This product is a networked appliance. This evaluation focuses on the management plane functionality provided by the product; consistent with the Network Device Protection Profile (NDPP).

1.4.1 TOE Environment

There are three basic connectivity modes that define how the TOE is connected to the network. These modes are identified as:

- Active-Inline
- Passive-Inline
- Passive-Tap

The Active/Passive designation refers to the associated IT environment security appliance and how it behaves. The Inline/Tap designation refers to how the TOE is connected to the network. An "Active" associated IT environment security appliance processes traffic from the TOE and then returns the traffic to the TOE, while a "Passive" appliance simply consumes traffic from the TOE.

The TOE itself can be either "Inline," or a TAP, which is connected to a network span or tap port. The following figures show the modes of operation.

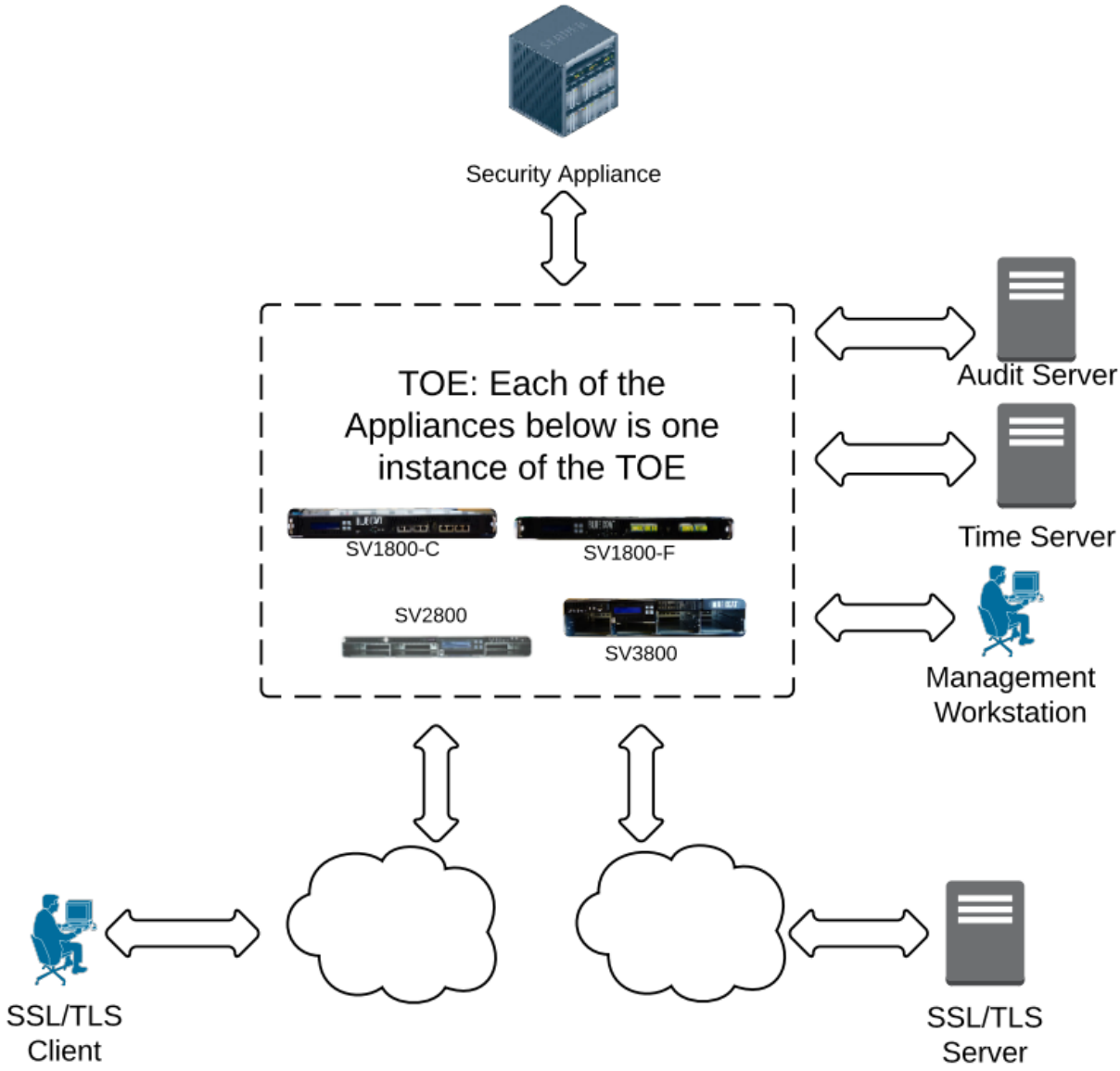

Figure 1 Passive Inline Mode

In Passive-Inline mode, network traffic flows through the TOE only, a copy of the network traffic is sent to the attached IT environment security appliance. A typical example of this type of deployment would be an IDS or Forensic appliance attached to the TOE.

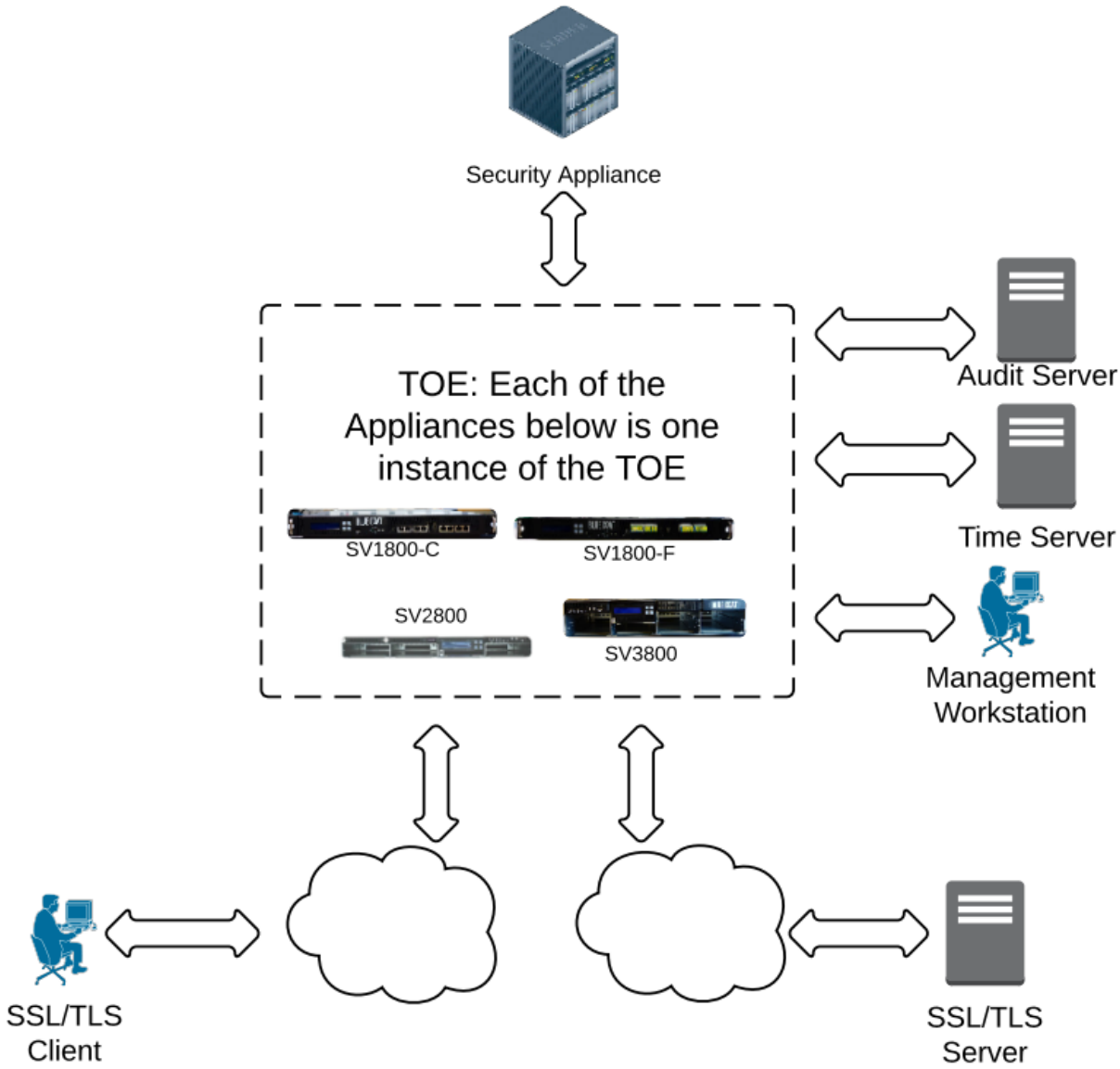

Figure 2 Active Inline Mode

In Active-Inline mode, network traffic flows through both the TOE and the attached IT environment security appliance. A typical example of this type of deployment would be an IPS attached to the TOE.

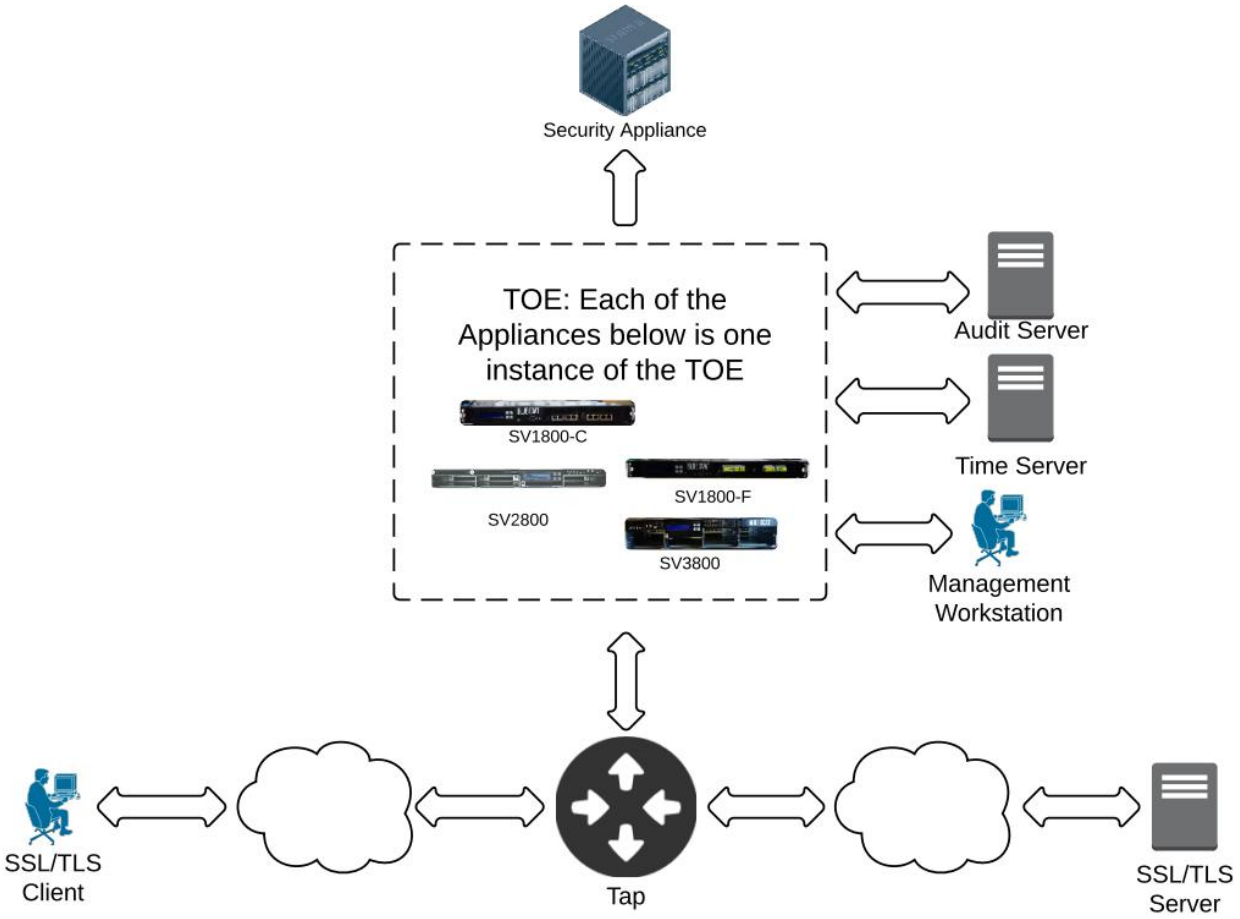

Figure 3 Passive Tap Mode

In Passive-Tap mode, network traffic does not flow through the TOE or the attached IT environment security appliance. The TOE receives a copy of traffic in the network from a TAP device and this traffic is sent to the attached IT environment security appliance. A typical example of this type of deployment would be an IDS or Forensic appliance attached to the TOE, which is in turn attached to a TAP or SPAN port.

In support of these modes of operation, the TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment.

Table 2 IT Environment

Component	Required?	Usage/Purpose
Management Workstation	Yes	This workstation provides the connection to the TOE for administration and management. The Management workstation may either be directly connected to the TOE or connected over the network via a TLS connection.
Time Server	No	The TOE optionally supports the use of an NTP server for time maintenance.

Component	Required?	Usage/Purpose
Audit Server	No	The TOE optionally sends a copy of the audit records to an external server. The connection to the audit server is a TLS-protected connection.
Security Appliance	No	This is the security device that is paired with the TOE to provide network protective services. Typically deployed devices may include: IPS, IDS, and Network Forensic devices.
Tap	No	This IT environment device provides passive connectivity when the TOE is configured in Passive-Tap mode.
Application Servers	No	These are servers deployed on the network for which the TOE is deployed.
Network Clients	No	These are clients of the servers deployed on the network for which the TOE is deployed.
Symantec Network Modules (SV2800, SV2800B, SV3800, SV3800B, and SV3800B-20 only)	Yes	On the SV2800, SV2800B, SV3800, SV3800B, and 3800B-20, a network module is required to inspect SSL/TLS traffic sent to a Security Appliance and allow policy enforcement between a Client and Application Server when deployed inline. Network modules come in different configurations including 10/100/1000Base-T, 10/100/1000Base-SX, 10GBase-SR, and 10GBase-LR.

1.5 TOE Description

This section addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

The TOE boundary comprises the SSL Visibility Appliance and Software Version: 3.10.2.1-21-FIPS140 installed on the SV1800B-C, SV1800B-F, SV2800B, SV3800B amd SV-3800B-20 appliances. The TOE appliances run software that differs only in platform-specific configuration data, which describes the intended hardware platform to the OS. Differences between TOE models allow for different capacity, performance, and scalability options, as described below.

Table 3 TOE Model Comparison

	SV1800-C/F and SV1800B-C/F	SV2800 and SV2800B	SV3800 and SV3800B	SV3800B-20
Total Packet Processing Capability	8 Gbps	20 Gbps	40 Gbps	40 Gbps
SSL Inspection Throughput	1.5 Gbps	2.5 Gbps	4 Gbps	9 Gbps

	SV1800-C/F and SV1800B-C/F	SV2800 and SV2800B	SV3800 and SV3800B	SV3800B-20
Concurrent SSL Flow States	100,000	200,000	400,000	800,000
New Full Handshake SSL Sessions	7,500 per second	10,500 per second	12,500 per second	30,000 per second
Power Supplies	1+1 Redundant 450W	1+1 Redundant 750W	1+1 Redundant 750W	1+1 Redundant 750W
Management Interfaces	2 x RJ45*	2 x RJ45*	2 x RJ45*	2 x RJ45*
Dimensions (in.) HxWxD	1.75 x 17 x 20	1.75 x 17.5 x 29	3.5 x 17.5 x 29	3.5 x 17.5 x 29

*Note: Only 1 RJ45 interface may be configured at a time. The other interface is non-operational.

1.5.1.1 TOE Software and Hardware

The TOE is a software and hardware TOE. For the evaluated configuration, the TOE software must be installed and run on one of the following hardware configurations:

- SV1800-C
- SV1800-F
- SV2800
- SV3800
- SV1800B-C
- SV1800B-F
- SV2800B
- SV3800B
- SV3800B-20

Each hardware model may be purchased with one of two licenses, a permanent license or a "Try-and-Buy" license (good for 60 days). The SKU used to purchase the appliance is based on the applied license. The following table identifies the SKUs (also referred to as hardware versions) associated with each hardware model.

Table 4 Hardware SKUs

Hardware Model	License	SKU/Version #
SV1800-C	Permanent License	090-03061
SV1800-F	Permanent License	090-03062
SV2800	Permanent License	090-03063
SV3800	Permanent License	090-03064
SV1800B-C	Permanent License	090-03547
SV1800B-F	Permanent License	090-03548

Hardware Model	License	SKU/Version #
SV2800B	Permanent License	090-03549
SV3800B	Permanent License	090-03550
SV3800B-20	Permanent License	090-03551

1.5.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- Symantec SSL Visibility Appliance Guidance Document, 3.10.2.1-21-FIPS140, version 1.6

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 5 and 6 of this ST. The logical scope also provides the description of the security features of the TOE. The SFRs implemented by the TOE are usefully grouped under the following Security Function Classes.

1.5.2.1 Security Audit

The TOE generates audit records for security relevant actions of the authorized administrators accessing the TOE via the WebUI and CLD; these records are stored in the System Event Log. The TOE records the identity of the administrator responsible for the log event, where applicable. All logs can be optionally sent to a remote audit server via a mutually authenticated TLS 1.1 or 1.2 secure channel (TLS provided by the TOE's cryptographic algorithms).

1.5.2.2 Cryptographic Support

The Cryptographic Support of the TSF function provides cryptographic functions to WebUI and CLD sessions between an administrator's management workstation and the TOE. The cryptographic operations necessary to support this TSF are provided by the Symantec proprietary cryptographic module (Symantec SSL Visibility Appliance Crypto Library). Transport Layer Security (TLS) is used to secure these communications sessions. In addition, the TOE provides a variety of cryptographic algorithms for its own use.

1.5.2.3 User Data Protection

Network packets are written into memory buffers exclusively used for packet processing. When a network packet is received by the TOE, network packets are written into 2048-bit memory buffers exclusively used for packet processing. The contents of the memory buffers include packet data and meta data. The metadata provides a mapping of packets to memory location. Packet data is not written to the areas of memory specified by the metadata as having contained packet data. Once the area of data allocated to packet data is completely used. The hardware release the buffer for reuse and the metadata will begin pointing to the previously used sections of the buffer. Only the data that is pointed to by the metadata is used. No packet data not pointed to by the metadata ever used. This ensures any user data that was previously present, is no longer available in the memory buffer for intentional or unintentional reuse. This guarantees that there is no residual data from the memory buffer's previous contents and therefore no potential for residual data its way into a new packet.

1.5.2.4 Identification and Authentication

The TOE requires administrative users to be authenticated prior to allowing access to any TOE administrative functionality. The Identification and Authentication TSF[1] ensures that only legitimate administrators can gain access to the configuration settings and management settings of the TOE. Administrators must log in with a valid user name and password before the TOE will permit the administrators to manage the TOE. The TOE requires administrators to use strong passwords. No feedback is presented to Administrators when they are entering their passwords at the login prompt when directly connected to the TOE via a serial connection or using a keyboard and monitor.

1.5.2.5 Security Management

The TOE provides a feature-rich WebUI and CLD for administrators to manage the security functions, configuration, and other features of the TOE. The Security Management function specifies user roles with defined access for the management of the TOE components.

1.5.2.6 Protection of the TSF

The TOE invokes a set of self tests each time the TOE is powered on to ensure that the TSF operates correctly. The TOE implements TLS for protection of the WebUI. TLS protects data transfer and leverages cryptographic capabilities to prevent replay attacks. The TOE also provides a reliable timestamp for its own use. A digital signature is used to verify all software updates that are applied to the TOE. The TOE prevents an administrator from reading plaintext keys or passwords by encrypting this data in a secure store using the AES[2] algorithm.

1.5.2.7 TOE Access

The TOE terminates local and remote management sessions after an administrator-configurable time period of inactivity. The TOE also provides administrator's the capability to manually terminate the session prior to the inactivity timeout. After an administrator's session is terminated, the administrator must log in again to regain access to TOE functionality. A login banner is displayed for users at the login screen of the Management Console and at the login prompt of the CLD.

1.5.2.8 Trusted Path/Channels

The cryptographic functionality of the TOE provides the TOE the ability to create trusted paths and trusted channels. The TOE implements a trusted channel using TLS between itself and a remote server in order to protect the audit logs as they are being sent to the server. Additionally, the TOE provides trusted paths between administrators and the WebUI via TLS/HTTPS. The management communication channels between the TOE and a remote entity are distinct from other communication channels and provide mutual identification and authentication. In addition, the communications are protected from modification and disclosure.

[1] TSF – TOE Security Functionality

[2] AES – Advanced Encryption Standard

2. Conformance Claims

2.1 CC and Protection Profile Conformance Claim

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 7.1.

Table 5 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 extended; CC Part 3 conformant.
PP Identification	Exact Conformance[3] to Security Requirements for Network Devices v1.1 (NDPP) plus the Security Requirements for Network Devices Errata #3.

[3] Exact Conformance is a type of Strict Conformance such that the set of SFRs and the SPD/Objectives are exactly as presented within the accepted NDPP without changes.

3. Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[4] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE.

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[5] and user data saved on the TOE. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 6 below lists the applicable threats.

Table 6 Threats

Name	Description
T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to

[4] IT – Information Technology

[5] TSF – TOE Security Functionality

Name	Description
	the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. Table 7 below lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

Table 7 Organizational Security Policies

Name	Description
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.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 8 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 8 Assumptions

Name	Description
A.NO_GENERAL_PURPOSE	It is assumed that 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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4. Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This section identifies the security objectives for the TOE.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 9 Security Objectives for the TOE

Name	Description
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the Administrator to be unaltered and (optionally) from a trusted source.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 10 IT Security Objectives

Name	Description

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.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives 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 11 Non-IT Security Objectives

Name	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5. Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 5.1.

5.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Assignments and selections made by NDPP and Network Devices Errata #3 to CC Part 2 are shown in *italicized* text.
- Refinement additions made by NDPP and Network Devices Errata #3 to CC Part 2 are shown in *underlined italicized* text.
- Refinement deletions made by NDPP and Network Devices Errata #3 to CC Part 2 are shown in ~~*struckthrough italicized*~~ text.
- Assignments made by the ST to NDPP and Network Devices Errata #3 are shown in **bold** text.
- Selections made by the ST to NDPP and Network Devices Errata #3 are shown in ***bold italicized*** text.
- Refinement additions made by the ST to NDPP and Network Devices Errata #3 are shown in **underlined bold** text.
- Refinement deletions made by the ST to NDPP and Network Devices Errata #3 are shown in ~~**struckthrough bold**~~ text.
- Extended Functional and Assurance Requirements are identified using "_EXT" at the end of the short name. Note: All extended components are derived directly from [NDPP]
- Iterations are identified by appending a number in parentheses following the component title. For example, FAU_GEN.1(1) Audit Data Generation would be the first iteration and FAU_GEN.1(2) Audit Data Generation would be the second iteration.

5.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 12 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 12 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	X	X		
FAU_GEN.2	User Identity Association				
FAU_STG_EXT.1	External Audit Trail Storage	X			
FCS_CKM.1	Cryptographic Key Generation (for Asymmetric Keys)	X		X	
FCS_CKM_EXT.4	Cryptographic Key Zeroization				
FCS_COP.1(1)	Cryptographic Operation (for Data Encryption/Decryption)	X	X	X	X

Name	Description	S	A	R	I
FCS_COP.1(2)	Cryptographic Operation (for Cryptographic Signature)	X		X	X
FCS_COP.1(3)	Cryptographic Operation (for Cryptographic Hashing)	X	X	X	X
FCS_COP.1(4)	Cryptographic Operation (for Keyed-Hash Message Authentication)	X	X	X	X
FCS_HTTPS_EXT.1	Explicit: HTTPS				
FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)	X			
FCS_TLS_EXT.1	Explicit: TLS	X			
FDP_RIP.2	Full Residual Information Protection	X			
FIA_PMG_EXT.1	Password Management				
FIA_UAU.7	Protected Authentication Feedback		X		
FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism	X	X		
FIA_UIA_EXT.1	User Identification and Authentication	X	X		
FMT_MTD.1	Management of TSF data (for General TSF Data)	X	X		X
FMT_SMF.1	Specification of Management Functions	X	X		
FMT_SMR.2	Restrictions on Security Roles	X	X		
FPT_APW_EXT.1	Extended: Protection of Administrator Passwords				
FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all Symmetric Keys)				
FPT_STM.1	Reliable Time Stamps				
FPT_TST_EXT.1	TSF testing				
FPT_TUD_EXT.1	Extended: Trusted Update	X			
FTA_SSL.3	TSF-initiated Termination		X	X	
FTA_SSL.4	User-initiated Termination				
FTA_SSL_EXT.1	TSF-initiated session locking	X			
FTA_TAB.1	Default TOE access banners			X	
FTP_ITC.1	Inter-TSF Trust Channel	X	X	X	
FTP_TRP.1	Trusted Path	X	X	X	

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

5.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps
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 administrative actions;*
d) *Specifically defined auditable events listed in Table 13.*

Table 13 Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	Start-up and shutdown of the audit functions	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM_EXT.4	None.	None.
FCS_COP.1(1)	None.	None.
FCS_COP.1(2)	None.	None.
FCS_COP.1(3)	None.	None.
FCS_COP.1(4)	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session. Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None.	None.
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication	Origin of the attempt (e.g., IP address).

Requirement	Auditable Events	Additional Audit Record Contents
	mechanism.	
FIA_UAU.7	None.	None.
FMT_MTD.1	None.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	None.	None.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
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 attempts.
FTP_TRP.1	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	Identification of the claimed user identity.

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 PP/ST, *information specified in column three of Table 13*.

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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.

FAU_STG_EXT.1 External audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FTP_ITC.1 Inter-TSF trusted channel

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 implementing the ***TLS*** protocol.

5.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

Refinement: The TSF shall generate *asymmetric* cryptographic keys *used for key establishment* in accordance with ~~*a specified cryptographic key generation algorithm*~~

- ***NIST[6] Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;***
- ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***

and specified cryptographic key sizes *equivalent to, or greater than, a symmetric key strength of 112 bits* ~~*that meet the following: list of standards*~~.

FCS_CKM_EXT.4 Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM_EXT.4.1

The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

FCS_COP.1(1) Cryptographic operation (for data encryption/decryption)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(1).1

Refinement: The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES operating in* ***CBC mode*** and cryptographic key sizes *128-bits and 256-bits,* and ***no other key sizes*** that meets the following:

- *FIPS PUB 197, "Advanced Encryption Standard (AES)"*
- ***NIST SP 800-38A***

[6] NIST – National Institute of Standards and Technology

FCS_COP.1(2) Cryptographic operation (for cryptographic signature)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(2).1

Refinement: The TSF shall perform *cryptographic signature services* in accordance with a ~~*specified cryptographic algorithm*~~ ***RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater*** ~~*and cryptographic key sizes*~~ that meets the following:

Case: RSA Digital Signature Algorithm

- ***FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard"***

FCS_COP.1(3) Cryptographic operation (for cryptographic hashing)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(3).1

Refinement: The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm ***SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*** and *message digest* ~~*cryptographic key*~~ sizes ***160, 224, 256, 384, 512*** *bits* that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

Application Note: The message digests above are not applicable for each algorithm. The message digest sizes are applicable as follows, SHA-1: 160 bits, SHA-224: 224 bits, SHA-256: 256 bits, SHA-384: 384 bits, and SHA-512: 512 bits.

FCS_COP.1(4) Cryptographic operation (for keyed-hash message authentication)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(4).1

Refinement: The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm *HMAC-**SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512**, key size **160, 224, 256, 384, 512 bits***, and *message digest* ~~*cryptographic key*~~ sizes **160, 224, 256, 384, 512** *bits* that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code"*, and *FIPS Pub 180-3, "Secure Hash Standard"*.

Application Note: The key sizes and message digests above are not applicable for each algorithm. The keys sizes and message digests are applicable as follows, HMAC-SHA1: 160 bits, HMAC-SHA224: 224 bits, HMAC-SHA256: 256 bit, HMAC-SHA384: 384 bits, and HMAC-SHA512: 512 bits.

FCS_HTTPS_EXT.1 Explicit: HTTPS
Hierarchical to: No other components.
Dependencies: FCS_TLS_EXT.1

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 as specified in FCS_TLS_EXT.1.

FCS_RBG_EXT.1 Extended: Cryptographic operation (Random bit generation)
Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1

The TSF shall perform all random bit generation (RBG) services in accordance with ***NIST Special Publication 800-90 using CTR_DRBG (AES)*** seeded by an entropy source that accumulated entropy from ***a TSF-hardware-based noise source***.

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded with a minimum of ***256 bits*** of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

FCS_TLS_EXT.1 Explicit: TLS

Hierarchical to: No other components.

Dependencies: FCS_COP.1(1) Cryptographic operation (for data encryption/decryption)
FCS_COP.1(2) Cryptographic operation (for cryptographic signatures)
FCS_COP.1(3) Cryptographic operation (for cryptographic hashing)

FCS_TLS_EXT.1.1

The TSF shall implement one or more of the following protocols ***TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*** supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA
~~TLS_RSA_WITH_AES_256_CBC_SHA~~
~~TLS_DHE_RSA_WITH_AES_128_CBC_~~
~~TLS_DHE_RSA_WITH_AES_256_CBC_SHA~~

Optional Ciphersuites:

TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

5.2.3 Class FDP: User Data Protection

FDP_RIP.2 Full Residual Information Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.2.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***deallocation of the resource from*** all objects.

5.2.4 Class FIA: Identification and Authentication

FIA_PMG_EXT.1 Password management

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_PMG_EXT.1.1

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

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: ***"!", "@", "#", "$", "%", "^", "&", "*", "(", ")",*** **comma, quotation mark, underscore, tab, space**;
2. Minimum password length shall settable by the Administrator, and support passwords of 15 characters or greater.

FIA_UIA_EXT.1 User identification and authentication

Hierarchical to: No other components.

Dependencies: FTA_TAB.1 Default TOE access banners

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 actions on behalf of that administrative user.

FIA_UAU_EXT.2 Extended: Password-based authentication mechanism

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU_EXT.2.1

The TSF shall provide a local password-based authentication mechanism, ***none*** to perform administrative user authentication.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1

FIA_UAU.7.1

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

5.2.5 Class FMT: Security Management

FMT_MTD.1 Management of TSF data (for general TSF data)
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1

The TSF shall restrict the ability to *manage* the *TSF data* to *the Security Administrators*.

FMT_SMF.1 Specification of management functions
Hierarchical to: No other components.
Dependencies: No dependencies.

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 update the TOE, and to verify the updates using* ***digital signature*** *capability prior to installing those updates;*
- ***Ability to configure the cryptographic functionality.***

FMT_SMR.2 Restrictions on security roles
Hierarchical to: FMT_SMR.1 Security roles
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.2.1

The TSF shall maintain the roles:

- *Authorized 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

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

are satisfied.

5.2.6 Class FPT: Protection of the TSF

FPT_SKP_EXT.1 Extended: Protection of TSF data (for reading of all symmetric keys)
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_SKP_EXT.1.1
The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

FPT_APW_EXT.1 Extended: Protection of administrator passwords
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_APW_EXT.1.1
The TSF shall store passwords in non-plaintext form.
FPT_APW_EXT.1.2
The TSF shall prevent reading of the plaintext passwords.

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps *for its own use*.

FPT_TUD_EXT.1 Extended: Trusted update
Hierarchical to: No other components.
Dependencies: [FCS_COP.1(2) Cryptographic operation (for cryptographic signature)]
FPT_TUD_EXT.1.1
The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.
FPT_TUD_EXT.1.2
The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.
FPT_TUD_EXT.1.3
The TSF shall provide a means to verify firmware/software updates to the TOE using a ***digital signature mechanism*** prior to installing those updates.

FPT_TST_EXT.1 TSF testing
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_TST_EXT.1.1
The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

5.2.7 Class FTA: TOE Access

FTA_SSL_EXT.1 TSF-initiated session locking
Hierarchical to: No other components.
Dependencies: No dependencies.
FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, ***terminate the session*** after a Security Administrator-specified time period of inactivity.

FTA_SSL.3 TSF-initiated termination
Hierarchical to: No other components.
Dependencies: No dependencies.
FTA_SSL.3.1

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

FTA_SSL.4 User-initiated termination
Hierarchical to: No other components.
Dependencies: No dependencies.
FTA_SSL.4.1

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

FTA_TAB.1 Default TOE access banners
Hierarchical to: No other components.
Dependencies: No dependencies.
FTA_TAB.1.1

Refinement: Before establishing *an administrative* user session, the TSF shall display *a Security Administrator-specified* advisory *notice and consent* warning message regarding ~~*unauthorized*~~ use of the TOE.

5.2.8 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel
Hierarchical to: No other components.
Dependencies: No dependencies.
FTP_ITC.1.1

Refinement: The TSF shall *use* **TLS** *to* provide a *trusted* communication channel between itself and *authorized IT entities supporting the following capabilities: audit server* ~~*another trusted IT product*~~ that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~*modification or*~~ disclosure *and detection of modification of the channel data*.

FTP_ITC.1.2

The TSF shall permit *the TSF, or the authorized IT entities* ~~*another trusted IT product*~~ to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for **the audit server**.

FTP_TRP.1 Trusted path
Hierarchical to: No other components.
Dependencies: No dependencies.
FTP_TRP.1.1

Refinement: The TSF shall *use* **TLS/HTTPS to** provide a *trusted* communication path between itself and *remote administrators* ~~*users*~~ 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 detection of modification of the communicated data*.

FTP_TRP.1.2

Refinement: The TSF shall permit *remote administrators* ~~*users*~~ to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for *initial administrator authentication and all remote administrative actions*.

5.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3.

Table 14 below summarizes the requirements.

Table 14 NDPP Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	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_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.1 Labeling of the TOE
	ALC_CMS.1 TOE CM Coverage
Class ADV: Development	ADV_FSP.1 Basic functional specification
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_IND.1 Independent testing – conformance
Class AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

6. TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

6.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 15 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	External Audit Trail Storage
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation (for Asymmetric Keys)
	FCS_CKM_EXT.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (for Data Encryption/Decryption)
	FCS_COP.1(2)	Cryptographic Operation (for Cryptographic Signature)
	FCS_COP.1(3)	Cryptographic Operation (for Cryptographic Hashing)
	FCS_COP.1(4)	Cryptographic Operation (for Keyed-Hash Message Authentication)
	FCS_HTTPS_EXT.1	Explicit: HTTPS
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
	FCS_TLS_EXT.1	Explicit: TLS
User Data Protection	FDP_RIP.2	Full Residual Information Protection
Identification and Authentication	FIA_PMG_EXT.1	Password Management
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism

TOE Security Function	SFR ID	Description
	FIA_UIA_EXT.1	User Identification and Authentication
Security Management	FMT_MTD.1	Management of TSF data (for General TSF Data)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
Protection of the TSF	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all Symmetric Keys)
	FPT_STM.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF testing
	FPT_TUD_EXT.1	Extended: Trusted Update
TOE Access	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_SSL_EXT.1	TSF-initiated session locking
	FTA_TAB.1	Default TOE access banners
Trusted path/channels	FTP_ITC.1	Inter-TSF Trust Channel
	FTP_TRP.1	Trusted Path

6.1.1 Security Audit

The Security Audit function provides the TOE with the functionality of generating audit records. As administrators manage and configure the TOE, their activities are tracked and recorded as audit records and are stored in the TOE's file system. The resulting audit records can be examined to determine which security relevant activities took place and who (i.e., which user) is responsible for those activities. (FAU_GEN.1, FAU_GEN.2)

The TOE provides auditing of all administrator actions and of all events explicitly listed in Table 13 that occur within the WebUI and CLD administrative interfaces. For audit events that result from actions of identified users, the TOE associates the action with the user who took the action in the logs.

The Audit Log entries contain at a minimum the following fields:

- Date and time of the event
- Type of event
- Identity of the subject
- Outcome of the event

Additional fields will be found in addition to these fields for those events that explicitly require additional information as defined in the "Additional Audit Record Contents" column of Table 13**.** **(**FAU_GEN.1)

The TOE supports the TLS and HTTPS protocols and will record administrator session establishment failures, successful session establishment, and session termination events to the audit log. Session establishment failure can occur if invalid or incorrect authentication credentials are submitted.

By default, the TOE is configured to store 1GB of data before it will begin to overwrite the earliest audited events. The TOE provides the ability to securely transmit a copy of the audit logs to an external audit server using TLS. The entire Audit Log is sent encrypted using TLS to the audit server where the Audit Logs contents can be verified and viewed (FAU_STG_EXT.1). The audit logs are stored in the TOE operating system and are protected with file permissions from unauthorized access.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1

6.1.2 Cryptographic Support

Cryptographic operations necessary to support TLS, HTTPS, encryption, decryption, hashing, signature generation, signature verification, key derivation, asymmetric seed generation and key generation are provided by the TOE's Symantec proprietary cryptographic module (Symantec SSL Visibility Appliance Crypto Library) (FCS_CKM.1, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1, FCS_HTTPS_EXT.1, FCS_TLS_EXT.1). The TOE uses TLS and HTTPS (via TLS) to protect communications. TLS is also used to provide a trusted channel during audit log transmissions from the TOE. HTTPS (via TLS) is used to provide a trusted path for administrator management connections to the WebUI (FCS_HTTPS_EXT.1, FCS_TLS_EXT.1). The TOE uses symmetric AES keys to encrypt and decrypt data. These symmetric keys are generated/established via the TLS protocol (FCS_TLS_EXT.1). The TOE also provides HMAC[7]-SHA[8] and SHS[9] to support TOE cryptographic functionality (FCS_COP.1(3)).

The TOE uses the following symmetric algorithms to encrypt and decrypt data, AES-128-CBC and AES-256-CBC (FCS_COP.1(1)). The TOE also uses the following MACs and hashes to support TOE cryptographic functionality HMAC[10]-SHA[11] and SHS[12] (FCS_COP.1(3)).

The TOE's cryptographic module includes self-tests for the supported FIPS-approved algorithms. For a complete list and description of the self-tests performed by the TOE, please section 6.1.6.

The TOE's cryptographic module is capable of generating cryptographic keys that provide at least 112 bits of symmetric key strength, in accordance with FIPS standards. The TOE implements a CTR_DRBG (using AES-256) to generate symmetric keys and to provide seeding material to asymmetric generation functions. The TOE implements finite field cryptography (FFC) Diffie-Hellman (DH) key pair generation in accordance with section 5.6.1 of NIST Special Publication 800-56A providing at least 112 bits of key

[7] HMAC – (keyed-) Hashed Message Authentication Code

[8] SHA – Secure Hash Algorithm

[9] SHS – Secure Hash Standard

[10] HMAC – (keyed-) Hashed Message Authentication Code

[11] SHA – Secure Hash Algorithm

[12] SHS – Secure Hash Standard

strength. The DH key pair is used for key establishment in accordance with the FFC sections of NIST Special Publication 800-56A. The TOE implements RSA 186-3 key pair generation in accordance with section 6.3 of NIST Special Publication 800-56B providing at least 112 bits of key strength. The RSA key pair is used for key establishment in accordance with section 6.2 of NIST Special Publication 800-56B. (FCS_CKM.1)

Cryptographic keys stored internally are protected in a secure store by an AES-256 bit key encryption key (KEK).

The TOE can use AES 128 and 256-bit keys when processing HTTPS/TLS requests depending on the capabilities of the client. When establishing a session, the client and server use the standard TLS handshake protocol, which involves exchanging the server's certificate and then the client returning an encrypted pre-master secret. The client and server then use the pre-master-secret to generate keys known only to the client and server. These keys are used to encrypt all future messages between the client and server. TLS/HTTPS is used for management sessions via the WebUI. TLS is used to protect communications with a remote audit server.

The TOE supports the following mandatory TLS ciphersuite (FCS_HTTPS_EXT.1, FCS_TLS_EXT.1):

- TLS_RSA_WITH_AES_128_CBC_SHA

The TOE also supports the following optional TLS ciphersuites (FCS_HTTPS_EXT.1, FCS_TLS_EXT.1):

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

The TOE's cryptographic module supports the following algorithms:

- AES key sizes of 128 bits and 256 bits
- AES modes of CBC
- rDSA with key sizes of 2048 bit and greater
- DH with public key sizes of 2048 bit and greater
- SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512
- HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512

The TOE provides zeroization techniques for all plaintext and private keys. TLS session keys reside in volatile memory only and never stored persistently. The contents of volatile memory are lost immediately (overwritten with zeros) when power is removed or the TOE is restarted; therefore, TLS session keys are considered zeroized when the TOE is restarted or shutdown. (FCS_CKM_EXT.4)

Keys stored in the secure store can be zeroized by performing a factory default reset. When the factory default reset is performed, the key encrypting the secure store is overwritten with zeros, effectively making any encrypted information in the secure store inaccessible. Also as part of the factory default reset, the entire disk is overwritten with zeros. After the factory default reset has been triggered during the boot process, no additional commands can be given until the reset has been completed. This prevents an attacker from influencing the zeroization procedure.

Each of the TOE cryptographic algorithms have been CAVP tested. The following table identifies each of the CAVP algorithm certificates associated with each algorithm:

Table 16 Cryptographic Algorithm Certificates

Algorithm	Certificate Number
AES (FCS_COP.1(1))	3195, 3496, and 4106
RSA (FCS_CKM.1, FCS_COP.1(2))	1238, 1625, 1794, and 2222
ECDSA (FCS_COP.1(2))	584, 711, and 931
SHS (FCS_COP.1(3))	2642, 2885, and 3378
HMAC-SHS (FCS_COP.1(4))	2013, 2230, and 2682
DRBG (FCS_RBG_EXT.1)	669, 886, and 1233

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1, FCS_HTTPS_EXT.1, FCS_TLS_EXT.1.

6.1.3 User Data Protection

The TOE enforces the User Data Protection TSF on user data by ensuring that the buffer area used by previous network packets is made unavailable during the buffer allocation process. When a network packet is received by the TOE, network packets are written into 2048-bit memory buffers exclusively used for packet processing. The contents of the memory buffers include packet data and meta data. The metadata provides a mapping of packets to memory location. Packet data is not written to the areas of memory specified by the metadata as having contained packet data. Once the area of data allocated to packet data is completely used. The hardware release the buffer for reuse and the metadata will begin pointing to the previously used sections of the buffer. Only the data that is pointed to by the metadata is used. No packet data not pointed to by the metadata ever used. This ensures any user data that was previously present, is no longer available in the memory buffer for intentional or unintentional reuse. This guarantees that there is no residual data from the memory buffer's previous contents and therefore no potential for residual data its way into a new packet.

TOE Security Functional Requirements Satisfied: FDP_RIP.2.

6.1.4 Identification and Authentication

The TOE provides mechanisms for authenticating administrators connecting to the TOE through the WebUI and CLD (FIA_UAU_EXT.2).

Administrator authentication is enforced through the use of a password. Authorized Administrators can configure the password to be at least a minimum password length of fifteen (15) characters. Valid passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: !, @, #, $, %, ^, <, &, *, (,), *comma (,), quotation mark ("), underscore (_), tab (\t), and space ( )*. (FIA_PMG_EXT.1, FIA_UAU_EXT.2)

All forms of authentication for the WebUI are secured using a trusted path or trusted channel depending on the authentication mechanism in use. Use of the CLD requires direct physical acces to the TOE. The CLD only accepts credentials via a keyboard and monitor or serial connection. The WebUI only accepts credentials via HTTPS (over TLS) (FIA_UAU_EXT.2).

There is no feedback presented to Administrators when they are entering their passwords at the login prompt of the CLD (FIA_UAU.7).

Unauthenticated users only have access to read the displayed warning banner before authenticating successfully with the TOE and establish a secure TLS session. While the TOE access banner is displayed to all Users before authentication, it is read-only and cannot be modified by an unauthenticated User (and in fact is not modifiable from the login screen at all). The secure TLS session only provides access for the unauthenticated Administrator to authenticate and there are no other services for unauthenticated users (FIA_UIA_EXT.1).

TOE Security Functional Requirements Satisfied: FIA_PMG_EXT.1, FIA_UIA_EXT.1, FIA_UAU_EXT.2, FIA_UAU.7.

6.1.5 Security Management

Security management specifies how the TOE manages several aspects of the TSF including TSF data and security functions. TSF data includes configuration data of the TSF and audit data, cryptographic functionality and information, hosts, dashboards and analytics, and administrator accounts. The TOE provides authorized administrators with the WebUI to easily manage the security functions and TSF data of the TOE. The WebUI can be used to configure the cryptographic functionality available on the TOE, update the TOE, and verify the updates via digital signatures (for more information on trusted updates, see section 6.1.6). Security management functionality is available to administrators over the CLD as well. (FMT_MTD.1, FMT_SMF.1, FMT_SMR.2).

The TOE defines the following authorized roles. Collectively, these are considered the TOE "Authorized Administrator:"

- "Manage Appliance" – This role is meant for system and network administrators. Settings which may be edited and viewed by this role, include, management network interface settings, system time, SNMP, login banner, remote logging, Symantec software licenses, and administrative user accounts. This role may also view the appliance system log and platform statistics.
- "Manage Policy" – This role is meant for corporate policy/compliance administrators. Setting which may be edited and viewed by this role, include, information flow policies. This role may view the PKI store, SSL session log, as well as the appliance and information flow policies statistics to verify that the configured policies work correctly.

TOE Security Functional Requirements Satisfied: FMT_MTD.1, FMT_SMF.1, FMT_SMR.2.

6.1.6 Protection of the TSF

The TOE provides TLS and TLS/HTTPS to protect TSF data from disclosure and to detect modification of TSF data while in transit between the TOE and External IT entities, including, the Audit Server and remote management workstations..

The TOE does not allow any Administrator to read plaintext passwords stored on the TOE (TOE administrator passwords), since all passwords are stored in encrypted form using an AES-256-bit key (FPT_APW_EXT.1). The TOE also prevents symmetric and private keys from being read by storing keys in encrypted form using an AES-256-bit key. The encrypting AES-256-bit key is stored in internally-allocated data structure. The TOE's OS safeguards memory and process space from unauthorized access. Because there is no direct access to memory, and passwords, private keys, and other CSPs are stored in

encrypted form, there is no potential for an all-powerful Administrator to directly read plaintext CSPs from memory (FPT_SKP_EXT.1/FPT_APW_EXT.1).

The TOE generates its own time stamps that originate from a system hardware clock. Administrators may change the time through the WebUI and configure the TOE to use an NTP server (FPT_STM.1). These timestamps are used to provide the time associated with audit logs.

Administrators can find the current version of TOE software by going to the home page of the WebUI or using the `version` command through the CLD. The TOE also provides a feature to update the TOE software. When a TOE software upgrade is initiated by an administrator, an integrity test public key (RSA 2048-bit SHA-256) is used to verify the digital signature of the new TOE software before it is installed. The integrity test public key resides on the TOE's hard disk. Failure to verify the integrity of the downloaded TOE software will result in an error and the administrator will be unable to proceed with the upgrade. Candidate updates are downloaded from Symantec's website (https://bto.bluecoat.com/download), which is the authorized source that signs these images. Access to the images requires an account with the site. All images are digitally signed by Symantec so they can be verified during the upgrade process (FPT_TUD_EXT.1).

At power up, the TOE runs a suite of self-tests that check for the correct operation of the cryptographic functionality provided by the TOE. All TOE appliances run these tests on startup. The TOE first performs an integrity test on the TOE software, guaranteeing that there have been no modifications, malicious or otherwise, to the TOE software. (FPT_TST_EXT.1)

The TOE proceeds to test its software implementation of cryptographic functionality through a series of known answer tests (KATs) and pairwise consistency tests, which exercise and verify the operation of the TOE's cryptographic services. Successfully completing the KATs and pairwise consistency tests provides evidence that the TOE is operating correctly. Any errors encountered during the software implementation self-tests will cause the TOE to enter a critical error state and require administrator intervention.

The TOE performs the following Power On Self Tests (POST):

- Software integrity tests check critical O/S components and appliance software binaries using RSA signature verification (2048 bit, SHA-256)
- AES encrypt/decrypt known answer tests (KAT) on software bulk ciphers (128 bit, CBC mode)
- AES encrypt/decrypt known answer tests (KAT) on software bulk ciphers (128 bit, GCM mode)
- AES encrypt/decrypt known answer tests (KAT) on software bulk ciphers (128 bit, CFB128 mode)
- Triple-DES encrypt/decrypt known answer tests (KAT) on software bulk ciphers (keying option 1)
- RSA known answer tests (KAT) on software signature operations (sign and verify) using the following digests (2048 bit PKCS#1 1.5)
    - SHA-1 (verify only)
    - SHA-224
    - SHA-256
    - SHA-384
    - SHA-512
- RSA known answer tests (KAT) on both NFPs hardware signature operations (sign and verify) using the following digests (2048 bit)
    - SHA-1 (verify only)
    - SHA-224

  - SHA-256
  - SHA-384
  - SHA-512
- RSA known answer tests (KAT) on both NFPs hardware based encryption using 2048-bit (encrypt and decrypt)
- RSA known answer tests (KAT) on software based encryption using 2048-bit (encrypt and decrypt)
- HMAC known answer tests (KAT) on software using the following digests
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- SHA known answer tests (KAT) on software hash for the following
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- SP 800-90A CTR DRBG known answer test (KAT)
- TRNG duplicate and zero output tests
- ECDSA known answer tests (KAT) (P-256, K-233 and SHA512)

All POSTs are run automatically at start-up. If an error is encountered, the TOE enters an error state and powers off (FPT_TST_EXT.1). This sufficient ensures that the TOE is operating correctly.

TOE Security Functional Requirements Satisfied: FPT_APW_EXT.1, FPT_SKP_EXT.1, FPT_STM.1, FPT_TST_EXT.1, FPT_TUD_EXT.1.

6.1.7 TOE Access

The TOE terminates local and remote management sessions after an Administrator configurable time period of inactivity has elapsed (FTA_SSL_EXT.1, FTA_SSL.3). Local sessions must be initiated by accessing the CLD via the serial port or using a keyboard and monitor. Remote sessions may be initiated by WebUI using HTTPS via TLS. Administrators may also terminate their sessions voluntarily (FTA_SSL.4). Users must log in again to regain access to TOE management capabilities. At the login screen Administrators are shown an advisory notice and consent warning message regarding unauthorized use of the TOE. The message is shown to users of both the WebUI and the CLD (FTA_TAB.1).

TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_SSL.4, FTA_SSL_EXT.1, FTA_TAB.1.

6.1.8 Trusted Path/Channels

The TOE provides a trusted path between the TOE management interfaces and remote TOE administrators. This interface is the WebUI over TLS/HTTPS. The protocols and the cryptography implemented by the TOE provide adequate defense against unauthorized disclosure and provide for the detection of modification of TSF data while it is being communicated (FTP_TRP.1).

Additionally, the TOE provides a trusted channel between the TOE and the trusted IT entities used for the audit servers. The TOE protects audit log traffic by encrypting it with a secure TLS tunnel. The TLS channel prevents unauthorized disclosure and detection of modification for all audit data (FTP_ITC.1).

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.1.

7. Rationale

7.1 Conformance Claims Rationale

This Security Target conforms to Part 2 extended and Part 3 conformant of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 4. This ST conforms to the NDPP.

7.1.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the following Protection Profile:

- Security Requirements for Network Devices v1.1 (NDPP) plus the Security Requirements for Network Devices Errata #3

7.1.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target are exactly reproduced from the Assumptions, Threats, and Organization Security Policies specified in the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1 plus Errata #3 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 are exactly reproduced from the Security Objectives specified in the NDPPv1.1 plus Errata #3 for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

7.1.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target are exactly reproduced from the Security Functional Requirements specified in the NDPPv1.1, for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in section 4.3 of the NDPPv1.1.

7.1.4 Variance Between the PP and this ST

In some instances changes were made in this ST from the NDPP. All of these changes are documented below with a rationale for the change.

- An Application Note in the NDPP states that the word "manage" in FMT_MTD.1 is the default requirement for management of TSF data. Other iterations are possible.
- The ST was modified to conform to Security Requirements for Network Devices Errata #3.

7.1.5 Security Assurance Requirements Rationale

This ST maintains exact conformance to NDPP, including the assurance requirements listed in section 4.3 of NDPP. This target was chosen to ensure that the TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks.

7.1.6 Dependency Rationale

The NDPPv1.1 and NDPP Errata#3 contain all the requirements claimed in this Security Target. The order of precedence followed in case of duplicate requirements is as follows - NDPP Errata#3 > NDPPv1.1. As such the dependencies are not applicable since the PP have been approved.

8. Acronyms

This section describes the acronyms used throughout this document.

Table 17 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CC	Common Criteria
CFB	Cipher Feedback
CLD	Command Line Diagnostics
CSP	Critical Security Parameter
CTR	Counter mode
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ECDHE	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
HMAC	Hashed Message Authentication Code
HTTPS	Hypertext Transfer Secure Protocol
KAT	Known Answer Test
KEK	Key Encryption Key
NDPP	Network Device Protection Profile
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PBKDF	Password Based Key Derivation Function
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
POST	Power On Self Test
SAR	Security Assurance Requirement
SFR	Security Functional Requirement

Acronym	Definition
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality