NetScout Systems, Inc.
nGeniusONE™ Unified Performance Management Platform (V5.2.1)
and
nGenius® InfiniStream® (V5.2.1)
Security Target

Version 1.0

March 6, 2015

Prepared for:

NetScout Systems, Inc.
310 Littleton Road
Westford, MA 01886-4105

Prepared By:

Ward Rosenberry

Rosenberry Associates Inc.
30 Newfield Street
N. Chelmsford, MA 01863

DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the nGeniusONE™ Unified Performance Management Platform (V5.2.1) and nGenius® InfiniStream® (V5.2.1).

This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS LIST

CC ..... **Common Criteria**
CDE ..... **Common Data Export**
CLA ..... **Command Line Administrator**
CLI ..... **Command Line Interface**
CSP ..... **Critical Security Parameter**
GB ..... **GigaByte**
GUI ..... **Graphical User Interface**
HMAC ..... **Hash based Message Authentication Code**
HTTPS ..... **HyperText Transfer Protocol over Secure Socket Layer**
I&A ..... **Identification and Authentication**
IP ..... **Internet Protocol**
IT ..... **Information Technology**
MAC ..... **Media Access Control**
MB ..... **MegaByte**
NDPP ..... **Protection Profile for Network Devices**
PM ..... **Performance Manager**
PP ..... **Protection Profile**
SFP ..... **Security Function Policy**
SSH ..... **Secure Shell**
ST ..... **Security Target**
TCP ..... **Transmission Control Protocol**
TLS ..... **Transport Layer Security**
TOE ..... **Target of Evaluation**
TSF ..... **TOE Security Function**
TSFI ..... **TSF Interface**
UDP ..... **User Datagram Protocol**

GLOSSARY

console – the TOE operating system command line interface.

local administration interface – the serial port on the nGeniusONE appliance accessing the appliance operating system command line and used for initial configuration.

maintenance interface – the remote console accessed using SSH which accesses the operating system command line on the nGeniusONE appliance or the nGenius InfiniStream appliance.

remote administration interface – the web interface on the nGeniusONE appliance used for routine day-to-day operations.

Security Administrators – nGeniusONE users with the role of System Administrator.

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the NetScout nGeniusONE™ Unified Performance Management Platform (V5.2.1) and nGenius® InfiniStream® (V5.2.1). The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1* and all international interpretations through July 2013. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

NetScout Systems, Inc. nGeniusONE™ Unified Performance Management Platform (V5.2.1) and nGenius® InfiniStream® (V5.2.1) Security Target, Version 1.0, March 6, 2015.

1.2 TOE Reference

nGeniusONE™ Unified Performance Management Platform (V5.2.1 build #789) and nGenius® InfiniStream® (V5.2.1 with the common criteria certified build).

1.3 TOE type

The TOE type is Network Device.

1.4 Conformance Claims

This TOE is conformant to the following CC specifications:

- Protection Profile for Network Devices (PP-ND), Version 1.1, June 8, 2012 including the Security Requirements for Network Devices Errata #2.
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1 Revision 4, September 2012.
    - Part 3 Conformant

1.5 TOE Overview

1.5.1 Usage and Major Security Features

The TOE consists of multiple software components that together provide an integrated network management application addressing key performance management disciplines:

- application and network monitoring
- network capacity planning, network troubleshooting
- fault detection

- service level management

The nGenius InfiniStream appliance passively and nonintrusively captures all network traffic and generates metrics to provide rich and detailed operational understanding of application and network performance in live production environments. It captures every transaction and session that makes up an application service in real-time and simultaneously extracts intelligence from Layer 2 through Layer 7. This information is used by the nGeniusONE platform to provide critical context so IT teams across network, application, telecom, server and security domains can work collaboratively. The correlated data is used to spot network and application issues, understand the impact of enabling services on applications, distinguish application and network brownouts, identify server issues and security breaches, provides insights for infrastructure optimization and planning, and identify other significant service delivery problems.

The nGeniusONE™ Unified Performance Management platform unifies application and network performance management providing a top-down view into any IP-based business services, including voice, video and data. Rather than look at individual elements in isolation, nGeniusONE provides an overarching view into the performance characteristics of all infrastructure and application components associated with service delivery. This platform combines real-time situational awareness, historical analysis, and multi-layered analytics capabilities. This unified perspective enables IT organizations to more effectively manage the health and availability of diverse application environments, improving the network and application teams' ability to proactively identify and triage performance issues, assess impact and quickly identify the root cause of problems.

nGeniusONE platform licensing provides a scalable "pay as you grow" model. As the monitoring footprint expands, additional licenses can be added, enabling the IT organization to only pay for the coverage required.

For current users of the nGenius Service Assurance Solution, each nGeniusONE deployment also includes licenses for nGenius Performance Manager and nGenius Service Delivery Manager. This allows users using the legacy analysis modules today to seamlessly migrate to nGeniusONE while still having access to familiar workflows and historical data. For the TOE, the both modules are enabled by licensing. These modules do not provide any additional security functionality or interfere with security functionality provided by the nGeniusONE server and nGenius InfiniStream base product.

This solution takes advantage of the same nGenius Intelligent Data Sources already deployed across a number of enterprise organizations. Many of these data sources can provide data to both the nGeniusONE platform and the previous generation nGenius Service Assurance Solution Analysis modules, preserving customer's long term investments in existing monitoring appliances.

To protect the integrity of these functions, the TOE provides the following security functionality:

Protected communications – The TOE protects communications with administrators, between distributed TOE components, and with servers it uses in the environment.

System monitoring – The TOE generates audit data and sends those data to an external syslog server to avoid loss of audit data.

Verifiable updates – The TOE helps ensure that any updates to the TOE software can be verified by the administrator to be unaltered and (optionally) from a trusted source.

Secure TOE administration – The TOE ensures that only administrators are able to log in and configure the TOE, and provides protections for logged-in administrators. The TOE also displays an advisory warning regarding use of the TOE.

Residual information clearing – The TOE ensures that any data contained in a protected resource (protected memory location) is not available when the resource is reallocated.

TOE security function self-test – The TOE performs self-tests on cryptographic algorithms and other security functions to ensure it is operating properly.

1.5.2 nGenius InfiniStream Hardware and Software

nGenius® InfiniStream® appliance is an intelligent deep packet capture and analysis appliance that delivers dedicated, always on, monitoring and continuous capture capabilities for real-time and back-in-time analysis. The appliance can be used with the nGeniusONE™ Unified Performance Management platform to analyze all packets traversing the network for rapid problem isolation and service delivery assurance.

The nGenius InfiniStream appliance hosts Adaptive Session Intelligence™ (ASI) technology, a high-performance deep packet inspection engine that analyzes network traffic in real-time and generates highly scalable metadata that enables a comprehensive view of service, network, application, and server performance across complex multi-tier, multi-domain service delivery environments.

The appliance performs local real-time granular Layer 4-7 data mining as traffic crosses the wire, eliminating the need for middleware and extensive backend processing while reducing management traffic loads. In addition, the appliance captures, indexes and stores packets crossing the wire for comprehensive deep-dive forensic analysis activities.

nGenius InfiniStream appliance, running on a customized Linux® operating system, is purpose-built for enabling pervasive visibility across enterprise networks and provides a foundation for extracting application and network performance metrics for the nGeniusONE platform.

Four nGenius InfiniStream 64-bit hardware configurations are supported; 7900 series, 6900 series, 4500 series, and 2900 series appliances. nGenius InfiniStream 32-bit appliances (69xxA and 69xxB) are not included in the evaluated configuration.

nGenius InfiniStream 7900 Series Appliances

The nGenius InfiniStream 7900 series appliance provides high capacity and flexibility through its unique modular design. Optimized for speed, performance, and resilience, the 7900 series appliance is expandable in 48TB increments with Extended Storage Units (ESU's) providing up to 144TB of storage per appliance. The nGenius InfiniStream 7900 series appliance is ideal for high capacity 10 Gigabit monitoring requirements such as data centers, high volume aggregation links and Service Provider environments that require vast storage capabilities for long-term back-in-time forensic analysis.

nGenius InfiniStream 6900 Series Appliances

The nGenius InfiniStream 6900 series appliance supports high density 1 Gigabit and 10 Gigabit interfaces and supports up to 16TB of storage capacity per appliance. Optimized for resilient

operations, the 6900 series appliance supports RAID storage with hot-swappable drives, as well as, redundant, hot-swappable power supplies. The nGenius InfiniStream 6900 series appliance is ideal for monitoring requirements at service aggregation points such as in the data center such as application server clusters, server farms, end of rack and service enabler monitoring environments that require storage capabilities for back-in-time forensic analysis.

nGenius InfiniStream 4500 Series Appliances

The nGenius InfiniStream 4500 series appliance supports high density 1 Gigabit and 10 Gigabit interfaces with support for 12TB storage and expandable to 60TB per appliance with the addition of an optional 48TB Extended Storage Unit (ESU). The appliance supports RAID storage with hot-swappable drives and redundant power with hot-swappable power supplies. Optimized for packet data processing, the nGenius InfiniStream 4500 series appliance is ideal for monitoring server farms and application server clusters in large data centers, and service enabler monitoring environments that require extensive packet data processing and high capacity storage disk for back-in-time forensic analysis.

nGenius InfiniStream 2900 Series Appliances

The nGenius InfiniStream 2900 series appliance is a small footprint appliance with storage capacity of 12TB. The appliance supports 1 Gigabit and 10 Gigabit interfaces and is designed to be deployed in remote offices, branch offices, or the network edge.

1.5.3 nGeniusONE Hardware and Software

The nGeniusONE server provides centralized management functionality to control and monitor nGenius InfiniStream appliances and manage configuration parameters within the nGeniusONE platform.

The nGeniusONE hardware server and software solution simplifies the deployment process by providing everything needed in a single pre-configured, pre-licensed solution. The factory pre-integrated hardware and software minimizes the tasks typically associated with installation, configuration and maintenance, and significantly reduces time required to deploy the nGeniusONE platform.

The nGeniusONE server hardware configuration features a dual six-core processor with 32 GB internal memory, 3 TB of hard disk capacity.

The nGeniusONE appliance provides statistics display, data mining, and reporting of network traffic captured by one or more managed InfiniStream appliances. The nGeniusONE appliance provides the mechanism to access one or more network traffic flows for analysis. It provides for the retrieval, analysis, and decode of captured traffic and allows the captured network traffic to be viewed graphically and statistically; it also identifies and diagnoses network problems. The nGeniusONE appliance includes a framework that enables intelligence modules to be added to the product to provide application protocol- or industry-specific traffic analysis.

The nGeniusONE appliance provides the ability to generate reports from analysis of the captured data.

nGeniusONE appliance functionality is accessed in the following ways:

- via a web browser executing on a client system using HTTPS (TLS) to protect the data being exchanged. Either of two equivalent interfaces may be chosen for use at log on: an HTML5 interface or a legacy Unified Management Console interface.
- via a remote terminal device using terminal software such as PuTTy or HyperTerminal. SSHv2 protects the data being exchanged.
- via a K/V/M or a local terminal device using terminal software such as PuTTy or HyperTerminal, with a direct connection to the local serial port using a null modem cable.

nGeniusONE platform provides advanced analysis capabilities for specialized data from pervasive nGenius Intelligent Data Sources. This system correlates components of a "service" into a unified view with a top level view that reveals service status.

nGeniusONE platform leverages the real-time data mining capabilities of NetScout's Adaptive Session Intelligence™ (ASI) technology to automate, accelerate and simplify the creation of a true representation of an end-to-end user data or voice session.

The nGeniusONE licensed applications rely on, but do not provide any security functions claimed in this security target.

1.5.4 Client Systems

Table 1 - Minimum Client System Hardware and Browser Requirements

Minimum Hardware Requirements	Browser Requirement
2 GHz processor 2 GB RAM 250 MB available disk space	Windows 7 — 32- and 64-bit, Ultimate, Professional, and Enterprise Windows Vista — Enterprise with SP1 Windows XP — Professional with SP2 and SP3 **Note**: nGeniusONE software is supported on: - Windows platforms configured with English, Japanese, Simplified Chinese and Korean language settings. (Refer to "Localization Requirements" in the nGeniusONE Administrator Guide) - Input of Unicode characters is not supported. - Windows 7 with UAC enabled JRE v1.7.45 (64-bit) Any of the following browsers: - Mozilla Firefox v19 or higher - Google Chrome v28 or higher - Internet Explorer v9.0 or higher **Note**: For users who perform a large number of configuration and monitoring activities, NetScout Systems recommends using Mozilla Firefox or Google Chrome. Light users, such as the Help Desk, network operators, and restricted users, can use Firefox, Chrome, or Internet Explorer. **Note**: Adobe Flash Player (32-bit) must be installed with the browser. The 64-bit version of Adobe Flash Player is not supported.

1.5.5 Physical Boundary

The physical boundary of the TOE includes:

A) One or more instances of an InfiniStream appliance which may be any of the following:

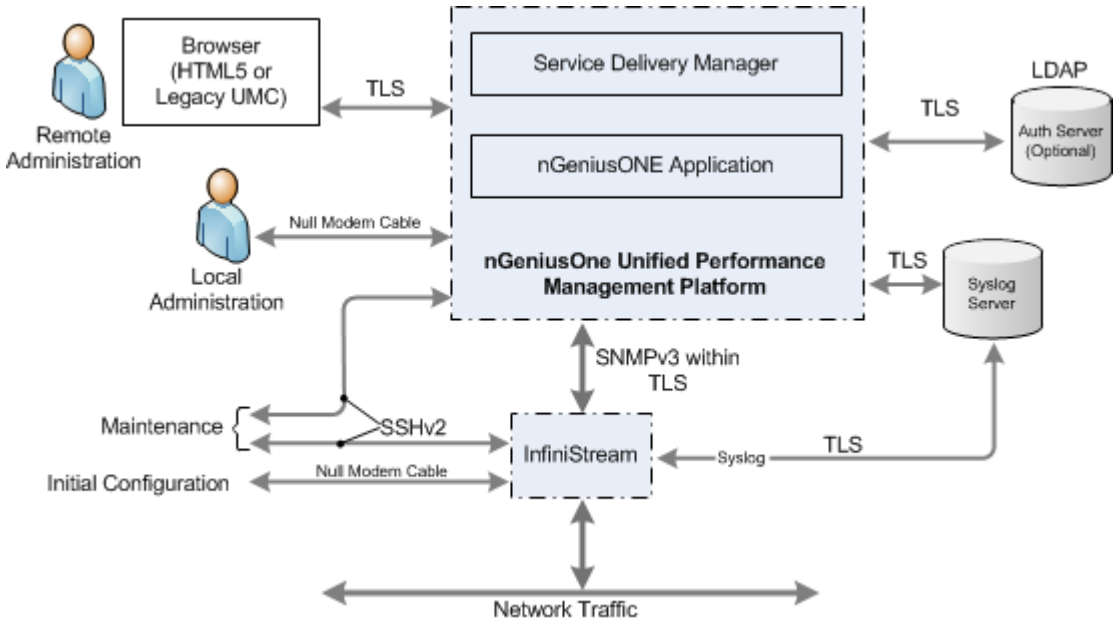
- nGenius InfiniStream 7900 Series
- nGenius InfiniStream 6900 Series
- nGenius InfiniStream 4500 Series
- nGenius InfiniStream 2900 Series

B) One instance of nGeniusONE Unified Performance Management Platform appliance that includes a licensed nSDM application.

C) Product Operating Manuals including *nGenius InfiniStream Administrator Guide* (Part Number 733-0549 Rev. A), *nGeniusONE™ Administrator Guide* (Part Number 733-0547 Rev. A), nGeniusONE™ online help version 5.2, *nGenius® Agent Administrator Guide for CDM v5.2.1* (Part Number 733-0528 Rev. A) and *Common Criteria Supplemental Guidance for nGeniusONE™ Unified Performance Management Platform (V5.2.1) and nGenius® InfiniStream® (V5.2.1)* (Part Number 733-0504 Rev A).

The major TOE components and the TOE boundary are shown in Figure 1.

Figure 1 - TOE Boundary



1.5.6 Logical Boundary

The TOE consists of a single nGeniusONE appliance and one or more managed nGenius InfiniStream appliances that together provide the required security functions.

1.5.6.1 Security Audit (FAU)

During operation, the TOE generates audit records for critical system and management events. The audit records are stored locally on the TOE where they can be viewed by all authorized users with appropriate privileges. A syslog server is required in operational environment for long term event storage.

1.5.6.2 Cryptographic Support (FCS)

The TOE includes FIPS 140-2 validated cryptographic modules and provides FIPS approved cryptography supporting key generation and destruction and the use of FIPS validated algorithms for protecting connections between TOE components, between the TOE and its users, and between the TOE and external services where required.

1.5.6.3 User Data Protection (FDP)

Full Residual Information Protection is provided as the TOE programmatically ensures that network packet payloads exiting the TOE contain only the intended data.

1.5.6.4 Identification and Authentication (FIA)

All users accessing the TOE are identified and authorized before they are granted access to any TOE security and management functions. User interfaces include a web-based remote administration interface, a local administration interface (a local serial port or K/V/M) that is also used for initial configuration of the nGeniusONE appliance, maintenance interfaces accessing the operating system command line using SSHv2 on both the nGeniusONE and nGenius InfiniStream appliances, and an initial configuration interface on the nGenius InfiniStream appliance. All interfaces require a user name and password before access is granted.

1.5.6.5 Security Management (FMT)

The TOE provides local and remote administrative access. The nGeniusONE appliance allows local administrative access used for initial configuration operations. The TOE web user interface is used for remote administrative access to perform day-to-day operations including user management, routine TOE configuration, and to use nGeniusONE product features.

SSHv2 access to the devices is provided for remote troubleshooting and maintenance.

1.5.6.6 Protection of the TSF (FPT)

The TOE provides a number of features to protect its functions from unauthorized use.

A suite of self tests executes during initial start-up to ensure the correct operation of TOE functions. Cryptography and other proven techniques protect passwords, cryptographic keys and other critical security parameters from access during entry, use and storage.

The TOE prevents reading of passwords, cryptographic keys and other critical security parameters using encrypted storage and other techniques. Time protocols synchronize time across all TOE components to prevent time based errors and exploits.

TOE users are instructed to validate software updates before they are installed by recalculating their SHA1 hash value and matching that to the published hash value. Users reject updates with un-matching hash values, preventing unauthorized software updates from being applied.

1.5.6.7 TOE Access (FTA)

Before users may access the TOE functions, they must acknowledge an administrator-specified advisory notice and consent warning message regarding use of the TOE. The TOE also monitors user sessions, enforcing session locking and logout on idle sessions.

1.5.6.8 Trusted Path/Channels (FTP)

The TOE uses FIPS validated cryptography for establishing trusted communication channels between the TOE and external entities.

- HTTPS over TLS protects user communications with the web user interface.
- SSHv2 protects user communications with remote troubleshooting and maintenance interfaces.
- TLS protects communication between distributed TOE components.
- TLS protects TOE communication with the syslog server and with the external LDAP server if external authentication is used.

1.6 Evaluated Configuration

1. Identification and authentication are performed locally by the TOE or externally by an LDAP server.
2. The nGeniusONE appliance is installed as a standalone Server. (It is not managed by a nGeniusONE global management server.)
3. TLS functionality is configured on the TOE to provide a trusted channel between the nGeniusONE appliance and individual nGenius InfiniStream appliances.
4. The following optional product components are not installed, configured or used: nGenius NewsStand for Remote Servers, Command Line Device Tools, Sniffer Analysis, and Standby Server.
5. nGenius InfiniStream appliances are configured to be managed by the nGeniusONE appliance using the CDM Agent Options to toggle the Performance Manager Console to ON.
6. HTTPS/SSL(TLS) is activated on the nGeniusONE platform and all connections from remote users to the nGeniusONE appliance web interface use HTTPS. (HTTP is not allowed for use.)
7. The Performance Manager Home Page, that is accessed via client software or the downloadable client application, is not evaluated and not allowed for use.
8. iDRAC6 (Integrated Dell Remote Access Controller) access, IPMI (Intelligent Platform Management Interface) access methods, RMM (remote management module), and the use of CLA (Command Line Administrator) and CDE (Common Data Export), are not allowed except for maintenance or troubleshooting purposes.

   Note: When accessing the TOE console either remotely using SSH or by using the local console connection, the TOE should be placed into maintenance mode immediately.

2. Security Problem Definition

2.1 Introduction

The Security Problem Definition (composed of organizational policies, threat statements, and assumption) has been drawn verbatim from the Security Requirements for Network Devices, Version 1.1, 8 June 2012 (NDPP). The NDPP offers additional information about the identified threats, but that has not been reproduced here and the NDPP should be consulted for those details.

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets, and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

2.2 Assumptions

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

Table 2 - Assumptions

Assumption Name	Assumption Definition
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.

2.3 Threats

The threats identified in the following table are addressed by the TOE and the Operational Environment.

Table 3 - Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, 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 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.

2.4 Organisational Security Policies

This section describes the Organizational Security Policy (OSP) that applies to the TOE. An OSP is a set of rules, practices, and procedures imposed by an organization to address its security needs.

Table 4 - Organizational Security Policy

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.

3. Security Objectives

The Security objectives have been drawn verbatim from the Security Requirements for Network Devices, Version 1.1, 8 June 2012 (NDPP). The NDPP offers additional information about the identified security objectives, but that has not been reproduced here and the NDPP should be consulted for those details.

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

3.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 5 - Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
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.

3.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 6 - Security Objectives of the Operational Environment

IT Environment Security Objective	IT Environment Security Objective Definition
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.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.

4. Extended Components Definition

The Security Target includes extended components listed below because the Protection Profile for Network Devices on which the TOE is based prescribes security objectives for the TOE that cannot be translated to Part 2 SFRs, or can be translated, but only with great difficulty based on components in CC Part 2. The extended components included in this security target are replicated directly from Protection Profile for Network Devices (NDPP), Version 1.1, June 8, 2012 with Errata 2.

Consult the NDPP for details regarding these extensions as they are not redefined here.

- FAU_STG_EXT.1: External Audit Trail Storage
- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_HTTPS_EXT.1 Explicit: HTTPS
- FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
- FCS_SSH_EXT.1: Explicit: SSH
- FCS_TLS_EXT.1: Explicit: TLS
- FIA_PMG_EXT.1: Password Management
- FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- 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_TST_EXT.1: TSF Testing
- FPT_TUD_EXT.1: Extended: Trusted Update
- FTA_SSL_EXT.1: TSF-initiated Session Locking

5. IT Security Requirements

This section defines the TOE Security Function Requirements (SFRs) and TOE Security Assurance Requirements (SARs) representing the security claims for the Target of Evaluation and to scope the evaluation effort.

The SFRs are drawn from the Protection Profile (PP): Security Requirements for Network Devices, Version 1.1, 8 June 2012 (NDPP) with Errata 2. Assignments and operations made within the PP are not identified (highlighted) here. Only the requirements and residual assignments and operations from the PP are completed here. The PP makes a number of refinements and completes operations made in the CC. Consult the CC and the PP for more information.

The SARs are also drawn from the NDPP Version 1.1 with Errata 2.

5.1 Conventions

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

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated with **bold** text and ~~strikethroughs~~, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined* text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

5.2 TOE Security Function Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from the Protection Profile for Network Devices which is based on Part 2 of the CC.

Table 7 - TOE Security Function Requirements

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User identity association
	FAU_STG_EXT.1: External Audit Trail Storage
FCS: 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_SSH_EXT.1: Explicit: SSH
	FCS_TLS_EXT.1: Explicit: TLS
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
FMT: 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
FPT: Protection of the TSF	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
	FPT_ITT.1: Basic Internal TSF Data Transfer Protection
	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM.1: Reliable Time Stamps
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update
FTA: 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
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1: Trusted Path

The security functional requirements are stated in the following subsections.

5.2.1 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 of the audit functions;

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

c) All administrative actions;

d) Specifically defined audit events listed in Table ~~1~~**8**.

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 ~~1~~**8**.

Table 8 - TOE Security Functional Requirements and Auditable Security Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU Security Audit		
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FCS_ Cryptographic Support		
FCS_CKM.1	None.	
FCS_CKM_EXT.4	None.	
FCS_COP.1(1)	None.	
FCS_COP.1(2)	None.	
FCS_COP.1(3)	None.	
FCS_COP.1(4)	None.	
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session	Reason for failure.
	Establishment/Termination of a HTTPS session.	Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1 (1)	None.	
FCS_RBG_EXT.1 (2)	None.	
FCS_SSH_EXT.1	Failure to establish an SSH session	Reason for failure.
	Establishment/Termination of an SSH session	Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_TLS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
	Establishment/Termination of a TLS session	Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP User Data Protection		
FDP_RIP.2	None.	
FIA Identification and Authentication		
FIA_PMG_EXT.1	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 mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FMT Security Management		
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.2	None.	
FPT Protection of the TSF		
FPT_SKP_EXT.1	None.	
FPT_APW_EXT.1	None.	
FPT_ITT.1	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.	
FTA TOE Access		
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.	
FTP Trusted Path/Channels		
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	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

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 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel implementing the TLS protocol.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1 The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with

- 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.

5.2.2.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.2.2.3 FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1(1) The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in *CBC* and cryptographic key sizes 128-bits and 256-bits that meets the following:

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

5.2.2.4 FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2) The TSF shall perform cryptographic signature services in accordance with a

1) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater,

that meets the following:

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

5.2.2.5 FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1(3) The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1, SHA-256 and message digest sizes 160, 256 bits that meet the following: FIPS Pub 180-3, "Secure Hash Standard."

5.2.2.6 FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1(4) The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-SHA-1, SHA-256 key size *160, 256 bits*, and message digest sizes 160, 256 bits that meet the following: FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."

5.2.2.7 FCS_HTTPS_EXT.1 Explicit: HTTPS

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.

5.2.2.8 FCS_RBG_EXT.1 (1) Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1(1) The TSF shall perform all random bit generation (RBG) services in accordance with SP 800-90 using CTR_DRBG (AES) seeded by an entropy source that accumulated entropy from a software-based noise source and a TSF-hardware-based noise source.

FCS_RBG_EXT.1.2(1) 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.

5.2.2.9 FCS_RBG_EXT.1 (2) Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1(2) The TSF shall perform all random bit generation (RBG) services in accordance with SP 800-90 using Hash_DRBG (SHA256) seeded by an entropy source that accumulated entropy from a software-based noise source and a TSF-hardware-based noise source.

FCS_RBG_EXT.1.2(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.

5.2.2.10 FCS_TLS_EXT.1 (1) Explicit: TLS

FCS_TLS_EXT.1.1 (1) The TSF shall implement one or more of the following protocols TLS 1.0 (RFC 2246) supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

5.2.2.11 FCS_TLS_EXT.1 (2) Explicit: TLS

FCS_TLS_EXT.1.1 (2) The TSF shall implement one or more of the following protocols TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246) supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

5.2.2.12 FCS_SSH_EXT.1 Explicit: SSH

FCS_SSH_EXT.1.1	The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and no other RFCs.
FCS_SSH_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_SSH_EXT.1.3	The TSF shall ensure that, as described in RFC 4253, packets greater than *256k* bytes in an SSH transport connection are dropped.
FCS_SSH_EXT.1.4	The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256 and no other algorithms.
FCS_SSH_EXT.1.5	The TSF shall ensure that the SSH transport implementation uses SSH_RSA, and no other public key algorithms as its public key algorithm(s).
FCS_SSH_EXT.1.6	The TSF shall ensure that data integrity algorithms used in SSH transport connection is hmac-sha1, hmac-sha1-96.
FCS_SSH_EXT.1.7	The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.2.3 User Data Protection (FDP)

5.2.3.1 FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to all objects.

5.2.4 Identification and Authentication (FIA)

5.2.4.1 FIA_PMG_EXT.1 Password Management

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: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", *"[", ":", ",", ".", "+", "<", ">", "?", "|", "]", "_", and ";"*.

2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater.

5.2.4.2 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
- *Respond to ICMP ping commands if enabled*.

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.

5.2.4.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

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

5.2.4.4 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.

5.2.5 Security Management (FMT)

5.2.5.1 FMT_MTD.1 Management of TSF Data

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

5.2.5.2 FMT_SMF.1 Specification of Management Functions

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

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using published hash capability prior to installing those updates;
- No other capabilities.

5.2.5.3 FMT_SMR.2 Restrictions on Security Roles

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 Protection of the TSF (FPT)

5.2.6.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

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

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

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

5.2.6.3 FPT_APW_EXT.1 Extended: 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.

5.2.6.4 FPT_STM.1 Reliable Time Stamps

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

5.2.6.5 FPT_TUD_EXT.1 Extended: Trusted Update

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 published hash prior to installing those updates.

5.2.6.6 FPT_TST_EXT.1: TSF Testing

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 TOE Access (FTA)

5.2.7.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, terminate the session after a Security Administrator-specified time period of inactivity.

5.2.7.2 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.

5.2.7.3 FTA_SSL.4 User-initiated Termination

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

5.2.7.4 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.

5.2.8 Trusted Path/Channels (FTP)

5.2.8.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall use 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 *authentication service, audit service*.

5.2.8.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall use SSH, TLS/HTTPS provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FTP_TRP.1.2 The TSF shall permit remote administrators 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 TOE Security Assurance Requirements

The TOE meets the assurance requirements specified by Protection Profile for Network Devices Version 1.1, June 8, 2012. These requirements are summarized in the following table.

Table 9 - Security Assurance Requirements

Assurance Class	Component ID
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

5.3.1 Development (ADV)

5.3.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.2d The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.2 Guidance Documents (AGD)

5.3.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.

AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-Cycle Support (ALC)

5.3.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Tests (ATE)

5.3.4.1 Independent Testing - Conformance (ATE_IND.1)

ATE_IND.1.1d The developer shall provide the TOE for testing.

ATE_IND.1.1c The TOE shall be suitable for testing

ATE_IND.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability Assessment (AVA)

5.3.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d The developer shall provide the TOE for testing..

AVA_VAN.1.1c The TOE shall be suitable for testing.

AVA_VAN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3e	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This section explains how the TOE provides the required security functions.

- Security Audit (FAU)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of the TSF (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

6.1 Security Audit (FAU)

The security capabilities described in this section satisfy the following security function requirements:

FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1,

The TOE logs start-up of the audit functions, TOE administrative operations and, the events listed in Table 8.

All TOE log messages except InfiniStream HTTPS messages include the following parameters: Priority (info, warning, error, fatal error), the time the message was generated, the user that triggered the audit event (if applicable), the user's IP address (if applicable) and the message description.

InfiniStream HTTPS messages contain date and time, originating IP Address, operation, status (success or failure), and reason code parameters.

The TOE consists of the nGeniusONE server and a separate nGenius InfiniStream server, with each server component generating and storing log messages using separate mechanisms.

To avoid losing log events when log files are rotated, a syslog server is configured as required by FAU_STG_EXT.1 to store logs over the long term. Most event messages are continuously copied to the syslog server whenever they are written to a local log. Messages generated by nGeniusONE for HTTPS communications with InfiniStream on port 8443 must be manually transferred to syslog. The Common Criteria supplemental guidance directs users to configure syslog and set to up a secure channel using TLS to protect data transferred on that channel from both the nGeniusONE and nGenius InfiniStream TOE components. TOE identification and authentication settings prevent unauthorized access to log files.

6.1.1 The nGeniusONE Message Logs

The nGeniusONE web-based remote administrative interface logs actions including authentication attempts, changes to server and device configuration, and all auditable administrative operations performed using this interface to the nGeniusONE message log that

may be viewed within the nGeniusONE Server Management application Message Log tab. After thirty one days the oldest messages are overwritten with new messages. Additionally, the complete set of UI related messages is stored for seven days in the /opt/NetScout/rtm/log/debuglog-*day*.txt file. These messages are written to the audit server for long term storage as they are received. Only authenticated users with the role of NETWKADMIN or SYSADMIN may view the logs using the TOE web UI.

6.1.2 The nGeniusONE and nGenius InfiniStream Console Logs

The nGeniusONE and nGenius InfiniStream consoles (operating system command line interfaces) are used by TOE administrators to perform initial configuration of system parameters including the server IP address and hostname, the DNS server IP address, and the system time and time zone settings. Initial configuration occurs using the local serial ports on both TOE components.

> **Note:** The nGeniusONE console accessed using the serial port is the TOE local administrative interface.

The consoles may also be accessed remotely using SSH for troubleshooting and maintenance purposes. These initial configuration actions along with all console authentication events are logged to system logs in **/opt/var/logs/secure, /opt/var/logs/messages,** and **/opt/var/logs/audit/audit.log**. By default, log entries are kept on the TOE for 2 days, after which the oldest log entries are overwritten with new log entries. Only authenticated users using a valid local account may view the logs. For long term storage, log entries are written to the audit server as they are generated.

TOE administrators must monitor the log consumption of disk space and make the best effort to manually offload log files to a secure location if the space used approaches 90 % of the available disk space in the **/opt** partition. If the local audit data store becomes full (the available disk space becomes exhausted), the system performance will degrade fatally, causing an uncontrolled shutdown. A system administrator will need to add disk space or move the disk to another system as a slave disk and manually move messages to a secure location to regain diskspace.

6.2 Cryptographic Support (FCS)

The security capabilities described in this section satisfy the following security function requirements:

> FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_HTTPS_EXT.1, FCS_RBG_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1

The TOE uses FIPS cryptography provided by the following FIPS-validated cryptographic libraries to communicate with users and other entities in the IT environment:

OpenSSL is built into the nGeniusONE server for use within TOE web interface HTTPS (TLS) and for TLS connections to syslog and for software update verification.

NSS (Network Security Service) is built into the nGeniusONE server to provide cryptography used for SSH and for communicating with InfiniStream servers and for communicating with an optional LDAP server if that is configured.

OpenSSL is built into the nGenius InfiniStream server for use within TLS when communicating with a managing nGeniusONE server and for TLS connections to syslog.

6.2.1 Key Generation

Table 10 describes the cryptographic keys that are used by the TOE to protect communication channels to external entities and between distributed TOE components.

Table 10 - TOE Cryptographic Key Usage Storage, and Destruction

Key or CSP	Key Generation / Establishment Method	Purpose or use	Storage	Zeroization
nGeniusONE Appliance Web Server Keys				
Web server RSA key pair	[ANSI X9.31] RSA	Authenticate to incoming web connections and provide RSA key exchange (SP-800-56B)	Maintained in web server key store (plaintext) and private key only in memory (plaintext) for key transfer	Private key zeroized from memory after key exchange. Key store is zeroized when updated keys replace expired key pair
Web Server Session key	TLS key agreement	Encrypt or decrypt web session traffic	Ephemeral, maintained in memory (plaintext) during use.	Zeroized at session termination.
nGeniusONE TOE Software Update Verification Key				
Software/Firmware load test RSA public key	Generated by manufacturing	Authenticate software/ firmware updates	Embedded in the TOE firmware as plaintext.	Never expire.
SSH keys on the nGeniusONE Appliance				
SSH session key (nGeniusONE server)	DH Key establishment	Encrypt or decrypt session traffic	Ephemeral, maintained in memory (plaintext) during use	Zeroized at session rekey or session termination

Key or CSP	Key Generation / Establishment Method	Purpose or use	Storage	Zeroization
SSH RSA key pair	[ANSI X9.31] RSA	Server Authentication	Maintained in sshd key store (plaintext) and in memory (plaintext) for session establishment	Zeroized from memory after session establishment. Key store is zeroized when updated keys replace expired key pair
SSH DH key pair	DH	Key Establishment	Ephemeral, maintained in memory (plaintext) during session establishment	Zeroized after session establishment
SSH keys on the nGenius InfiniStream Appliance				
SSH session key (nGenius InfiniStream server)	DH Key establishment	Encrypt or decrypt session traffic	Ephemeral, maintained in memory (plaintext) during use	Zeroized at session rekey or session termination
SSH RSA key	[ANSI X9.31] RSA	Server Authentication	Maintained in sshd key store (plaintext) and in memory (plaintext) for session establishment	Zeroized in memory after session establishment. Key store zeroized when updated keys replace expired key pair
SSH DH key	DH	Key Establishment	Ephemeral, maintained in memory (plaintext) during session establishment	Zeroized after session establishment
SNMP Channel within TLS keys on the nGeniusONE Appliance				

Key or CSP	Key Generation / Establishment Method	Purpose or use	Storage	Zeroization
SNMP channel session key on nGeniusONE server	[SP 800-90] DRBG	Encrypt or decrypt session traffic	Ephemeral, maintained in memory (plaintext) during use	Zeroized at session termination
SNMP Channel within TLS keys on the nGenius InfiniStream Appliance				
SNMP channel RSA key pair on nGenius InfiniStream	[ANSI X9.31] RSA	RSA key exchange	Maintained in key store (plaintext) and in memory (plaintext) for session establishment	Private key zeroized from memory after key transfer. Key store zeroized when updated keys replace expired key pair
SNMP channel session key on nGenius InfiniStream	RSA key exchange SP-800-56B	Encrypt or decrypt session traffic	Ephemeral, maintained in memory (plaintext) during use	Zeroized at session termination
Syslog TLS Channel keys on the nGenius InfiniStream Appliance				
InfiniStream TLS-syslog session key.	[SP 800-90] DRBG	Encrypt or decrypt session traffic	Ephemeral, maintained in memory (plaintext) during use	Zeroized at session termination.
Syslog TLS Channel keys on the nGeniusONE Appliance				
nGeniusONE TLS-syslog session key.	[SP 800-90] DRBG	Encrypt or decrypt session traffic	Ephemeral, maintained in memory (plaintext) during use	Zeroized at session termination.
LDAP TLS Channel keys on the nGeniusONE Appliance				
nGeniusONE TLS-LDAP session key.	[SP 800-90] DRBG	Encrypt or decrypt session traffic.	Ephemeral, maintained in memory (plaintext) during use	Zeroized at session termination.

The SSHv2 protocol uses RSA keys for client authentication and the Diffie-Hellman protocol for symmetric session key establishment. For use within HTTPS and TLS 1.0, the TOE generates RSA keys for server authentication and for use with RSA key establishment.

Symmetric keys and user passwords, are protected from viewing as the TOE does not provide an interface designed to view these critical security parameters.

Private keys and certificates are protected from viewing as these CSPs are maintained in the operating system that is accessible only to administrators who are trusted to follow and apply all administrator guidance in a trusted manner. Moreover the TOE must be placed into maintenance mode whenever the operating system is accessed.

RSA keys are generated in accordance with ANSI X9.31. When these key pairs are used for key establishment, they are used in accordance with NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes. No un-allowed options or operations described in the standard are used. Additionally, the TOE does not contain any extensions or processing that is not included in SP 800-56B.

The TOE satisfies the NIST SP 800-56B requirements without extensions. The following table specifically identifies the "should," "should not," and "shall not" statements from the publication indicating whether the TOE conforms to those statements and rationalizing any deviations.

Table 11 - NIST SP800-56B Conformance

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?	Rationale for deviation
5.6	Should	Yes	
5.9	shall not (first occurrence)	Yes	
5.9	shall not (second occurrence)	Yes	
6.1	should not	Yes	
6.1	should (first occurrence)	Yes	
6.1	should (second occurrence)	Yes	
6.1	should (third occurrence)	Yes	
6.1	should (fourth occurrence)	Yes	
6.1	shall not (first occurrence)	Yes	
6.1	shall not (second occurrence)	Yes	
6.2.3	Should	Yes	
6.5.1	Should	Yes	
6.5.2	Should	Yes	
6.5.2.1	Should	Yes	
6.6	shall not	Yes	
7.1.2	Should	Yes	
7.2.1.3	Should	Yes	

7.2.1.3	should not	Yes	
8	Should	Yes	
8.3.2	should not	Yes	

6.2.2 Key Zeroization

When keys are zeroized after use as described in Table 10, the zeroization function overwrites the key memory buffers with zeros. For key material maintained in key stores on disk, the disk location is overwritten 25 times with a final overwrite of zeros.

6.2.3 Cryptographic Operations

Cryptographic Operations (algorithms) are provided by the OpenSSL and NSS (Network Security Service) cryptographic modules. The following table describes the cryptographic operations and their use within the SSHv2 protocol.

Table 12 - SSHv2 Cryptography

Cryptographic Method	Purpose in SSHv2
RSA Digital Signatures	Server authentication.
Key Exchange (Diffie-Hellman)	Session establishment.
HMAC-SHA	Traffic integrity verification.
[SP 800-90] DRBG	Key material provisioning.
AES	Session traffic encryption.

The following table describes the cryptographic operations and their use within the TLS protocol. Note the TLS protocol may be used alone or within the HTTPS protocol.

Table 13 - TLS Cryptography

Cryptographic Method	Purpose in TLS
RSA Digital Signatures	Server authentication.
SP 800-56B RSA Key Exchange	Session establishment.
SHA	Traffic integrity verification.
[SP 800-90] DRBG	Key material provisioning.
AES	Session traffic encryption.

The following table lists all of the FIPS-validated algorithms implemented within the TOE. These algorithms are provided by the OpenSSL and NSS cryptographic modules included in the TOE.

Table 14 - TOE Cryptographic Algorithms

Function	Standard	Algorithm
Random Number Generation	[SP 800-90] DRBG (OpenSSL) [SP 800-90] DRBG (NSS)	DRBG CTR DRBG (AES) Hash_DRBG: (SHA-256)
Encryption / Decryption	[FIPS Pub 197]	AES 128/256 CBC, CTR
Message Digests	[FIPS Pub 180-3]	SHA-1, SHA-2 (256)
Keyed Hash	[FIPS Pub 198]	HMAC SHA-1, SHA-2 (256)
Digital Signature	RSA	RSA SigGen9.31, SigGenPKCS1.5, SigVer9.31, SigVerPKCS1.5

6.2.4 SSH Conformance to RFCs 4251, 4252, 4253, and 4254

The SSHV2 implementations on nGeniusONE server and the InfiniStream server conform to RFCs 4251, 4252, 4253, and 4254.

The SSH protocol supports SSH_RSA public key authentication and Linux password-based client authentication. The default configuration does not enable public key authentication. Diffie-Hellman support is limited to using group 14 keying material.

For compliance with RFC 4253, the TOE drops packets greater than 256k bytes. Independent implementations for client>server and server>client channel algorithms use AES-CBC-128 or AES-CBC-256 encryption and. hmac-sha1 or hmac-sha1-96 for packet integrity as negotiated during the handshake. Rekey is triggered after one hour or after 2^{28} packets have been transferred (whichever event occurs first).

6.2.5 TLS Conformance

The following five or optionally six TLS channels exist on the TOE:

- Two channels between the nGenius InfiniStream and nGeniusONE appliances (one to InfiniStream port 443 and another to InfiniStream port 8443.
- The channel between the nGenius InfiniStream appliance and the syslog server
- The channel between the nGeniusONE appliance and users accessing the TOE UI.
- The channel between the nGeniusONE appliance and syslog server.
- The channel between the nGeniusONE appliance and optional LDAP server.

In all cases, the TOE implements the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

The TLS implementation does not use md5 for integrity. The TLS Record Protocol and TLS Handshake Protocol are used for authentication and key negotiation. Client authentication is not used for any TLS channels. Note the channel between the nGenius InfiniStream and nGeniusONE appliances uses self-signed server certificates and relies on a strong community string within the embedded SNMP channel for authentication. TLS does not implement any extensions defined in RFC 3546.

6.2.6 HTTPS Conformance to RFC 2818

The TOE provides two HTTPS servers for establishing TLS communication channels:

- The nGeniusONE appliance HTTP server establishes a TLS communication channel between the appliance and users (clients) accessing the TOE UI.
- The nGenius InfiniStream appliance HTTP server establishes a TLS communication channel between the appliance and a managing nGeniusONE appliance.

In both cases when the server (httpd) receives a connection request, it waits for the TLS ClientHello message to begin the TLS handshake. When the TLS handshake has finished, the server waits for the client to initiate the first HTTP request. All HTTP data is sent and treated as TLS "application data". Normal HTTP behavior is followed.

6.3 User Data Protection (FDP)

The following description of network packet processing explains how the TOE satisfies FDP_RIP.2, Full Residual Information Protection.

After a packet is transmitted from the server, the server de-allocates the packet buffer, returning it to the buffer pool. When a new packet is to be sent, the server allocates a new buffer from the buffer pool and the server process writes the data items (as appropriate) into the buffer. In many cases, the packet data will fill (overwrite) the entire buffer and in these cases no additional buffer processing is needed to ensure the packet does not contain stale data. In other cases the packet payload does not fill the entire buffer and in these cases the server detects the packet buffer under-run and pads the unused remainder of the buffer with zeros before transmitting the packet.

6.4 Identification and Authentication (FIA)

The security capabilities described in this section satisfy the following security function requirements:

> FIA_PMG_EXT.1, FIA_UIA_EXT.1.1, FIA_UIA_EXT.1.2, FIA_UAU_EXT.2.1, FIA_UAU.7.1

The TOE offers the following interfaces for users to interact with the TOE and use TOE Features.

- Browser access to the TOE web interface for routine TOE operation.
- Local console access using hyper terminal and a null-modem cable or an LCD K/V/M for initial TOE configuration.
- Remote console access over an SSHv2 channel for troubleshooting and maintenance purposes.

For all TOE access methods, password feedback is obscured as follows:

- When web interface users enter passwords into the UI, feedback consists of dot characters.
- When local or remote console users log into the console, the system does not return any password feedback.

6.4.1 Remote user Web Access

Browser users access the nGeniusONE web user interface directly over HTTPS (TLS) and interact with nGeniusONE using HTML5 or interact with the legacy Unified Management Console over HTML. Users enter identification and authentication data (their user name and password) directly into the nGeniusONE web user identification and authentication interface.

Both of the above usage scenarios (HTML5 or Unified Management Console) provide the same product functionality. Equivalent functionality is provided by both access methods.

The TOE in its evaluated configuration displays a warning banner (consent box) for web users in accordance with FTA_TAB.1 before users may enter any authentication data (user name or password).

How the TOE handles authentication data depends on whether internal or external authentication is configured. When internal authentication is configured, the TOE looks up the user-provided username in the internal database and then compares a hash of the user-provided password to a hash of the password that is stored in the database. If the hashed passwords match, an authentication success message is generated and the user is allowed to access the TOE resources. If the hashed passwords do not match, an authentication failure message is generated and the login screen is returned to the user.

When external authentication is configured the TOE passes the user-provided username and password to the configured authentication server for authentication there. Authentication success or failure responses are returned to the nGeniusONE server which, in turn, grants or denies access to the TOE resources, and logging an authentication success or failure audit message. For the initial authentication success by a user using external authentication, the nGeniusONE server persists the username into the local database and assigns default roles associated with that authentication method. The administrator may change the role for specific users and that role is applied on subsequent authentications.

Users may initiate an ICMP ping to the IP address of the nGeniusONE server or the InfiniStream server and receive an ICMP response indicating the device is running on the network. The TOE components must be configured to respond to ICMP ping operations for such responses to be generated. Any other TSF-mediated action other than handling user authentication requests from unauthenticated users requires the user to be successfully identified and authenticated.

6.4.2 Console Access

The console may be accessed locally using hyper terminal on a PC with a null-modem cable or an LCD K/V/M for initial TOE configuration and maintenance activities or remotely over SSHv2 using a terminal program such as PuTTY. The TOE in its evaluated configuration displays a warning banner (consent box) for users in accordance with FTA_TAB.1

For local console access to nGeniusONE and nGenius InfiniStream, only local authentication is allowed. Users must have their own user accounts within the system which authenticates users by hashing the password entered and comparing the hash value to the locally stored password hash value. Authentication success or failure responses trigger the server to grant or deny access to the TOE resources. Additionally, an authentication success or failure audit message is logged in **/opt/var/logs/secure**.

6.5 Security Management (FMT)

The security capabilities described in this section satisfy the following security function requirements:

FMT_MTD.1, FMT_SMF.1, FMT_SMR.2.

The NDPP role of TOE Authorized Administrator has complete access to TOE functionality including managing user accounts.

The TOE provides the following pre-defined, non-editable administrative roles:

System Administrator has access to all user account management functions, all reporting functions, and some packet analysis functions. No other role may access user account management functions for other users.

Network Administrator accesses all packet analysis functions, all reporting functions, and system configuration functions including configuring external services such as DNS and NTP services.

Approver, Network Operator, and **Help Desk** roles may access various reporting functions, and varying (limited to no) packet analysis functions.

A **Custom** role is available and may contain any of the available privileges.

Together, the System Administrator and Network Administrator roles make up the TOE Authorized Administrator, accessing all TOE security management functions. Other roles are limited to non-security relevant TOE functions including viewing TOE reports.

6.6 Protection of the TSF (FPT)

The security capabilities described in this section satisfy the following security function requirements:

FPT_SKP_EXT.1, FPT_APW_EXT.1, FPT_ITT.1, FPT_STM.1, FPT_TUD_EXT.1, FPT_TST_EXT.1

All passwords used to access the TOE are stored in non-plaintext form such that users are prevented from reading them. Locally stored web user passwords are stored in SHA1 format. Local console passwords are stored in MD5 hash format.

Persistent cryptographic keys that are maintained in key stores in plaintext form are protected from casual viewing as the TOE does not provide a key store viewing utility while it is in operation. Symmetric keys exist only in memory which requires substantial effort to view. Administrators are considered trusted agents who would not undertake such an effort.

The nGeniusONE appliance and the InfiniStream appliance provide their own hardware clocks. By default, the nGeniusONE appliance relies on its own clock for time needs and uses the built-in NTP protocol to regulate the time for connected InfiniStream appliances. The TOE can also be configured to receive time from an external NTP server.

Changes to the system time trigger generation of audit messages indicating the old and new values for the time and the origin of the attempt (e.g., IP address). Security functions that make use of time are: cryptographic operations that use time and date information, audit record timestamps, and session inactivity timing for session locking and termination.

Manual TOE software updates are supported. A valid account on the NetScout Master Care Portal is required to use this service. The Common Criteria supplemental guidance directs users to ensure a valid Master Care Portal account exists for this purpose.

To prevent unauthorized or invalid software updates from being applied, TOE users are instructed to validate software updates before they are installed by calculating their SHA1 hash value and matching that to a corresponding published hash value. Users reject updates with un-matching hash values.

The nGeniusONE web interface displays the nGeniusONE server firmware version in the Server tab of the Server Management application.

The InfiniStream server firmware version is shown in the nGeniusONE web interface Device Configuration tab.

The following self-tests run on both the nGeniusONE server and the nGenius InfiniStream server during system start-up:

On power up or reset, the TOE conduct a series of internal tests (called a POST or power on self-test). The POST confirms that critical functions work before making the system available for use by applications. The ROM based POST program first tests the processor by conducting some operations for which the results are known and maintained in the program. The POST compares the calculated results to the stored results, passing on a match and failing on a mismatch.

The memory and disk drive configuration are read from the boot ROM. The POST memory test writes various data patterns into memory locations and reads them back to confirm that each memory location is functional. The test then interacts with every device in the machine looking for any failures. If any tests fail, the POST writes the failure indicator to the display and exits. When the POST ends successfully, the BIOS searches the various boot mechanisms (using the boot ordering maintained in ROM) for the operating system.

The operating system loads and then uses its configuration files to load the TOE software and any other utilities needed by the TOE. During this phase, FIPS cryptographic modules start and execute their POSTs which include software integrity tests, KATs (known answer tests) for cryptographic algorithms, PCTs (pairwise consistency tests) for asymmetric key pairs, and random bit and random number generator tests. A failure of any cryptographic module self-test causes the module to cease all use of cryptographic operations such that all data output is prevented. The tests are:

- The software integrity test is an HMAC-SHA1 verification of the binary code comprising the module executable.

- A KAT functions by encrypting a predetermined string with a symmetric encryption algorithm and an associated encryption key. The result must match the known answer or the test fails. Then a decryption is performed and that result must match the original string or the test fails.
- A PCT (a conditional test that runs only when asymmetric keys are generated) functions by using the private key of a key pair to transform a predetermined string. The result is compared to a known answer. The result must match the known answer or the test fails. Then the answer is transformed with the public key and that result must match the original string or the test fails.
- Random bit generator and random number generator tests (conditional tests that run only when random bits and random numbers are generated) confirm the generators are not "stuck" (providing the same number more than once in sequence).

If any tests fail, the module writes the failure indicator to a log file and all data output is halted from that module. As the self-tests completely exercise the cryptographic and other functionality underlying TOE security functions, all tests passing assures the TOE operator that the TOE security functions are operating correctly.

Errors that may result from these tests and the user actions for resolving them are provided in the Common Criteria supplemental guidance.

6.7 TOE Access (FTA)

The security capabilities described in this section satisfy the following security function requirements:

FTA_TAB.1.1, FTA_SSL_EXT.1.1, FTA_SSL.3.1, FTA_SSL.4.1.

TOE access is protected by using session management controls and procedures.

The TOE provides a warning banner called a consent box that must be addressed by interactive users accessing the TOE using the HTML5 and UMC web interfaces. A banner is also provided for the local and remote consoles on both the nGeniusONE and InfiniStream appliances. All TOE banners are disabled by default. The Common Criteria supplemental guidance provides instructions for enabling these protections.

Users logged into the TOE web interface or into the local or remote console on the nGeniusONE and InfiniStream server platforms are automatically logged out when idle sessions meet the administrator–specified period of inactivity. The Common Criteria supplemental guidance provides instructions for using the idle-session log termination functions.

Users logged into the any of the remote or local TOE interfaces have the ability to log off from their session. The web interfaces provide a log off function on the always-visible tool-bar portion of the UI. To log off from a local or remote console session, users enter an **exit** command. The Common Criteria supplemental guidance provides instructions logging on and off from TOE interfaces.

Supplemental Common Criteria guidance directs uses to disable telnet and HTTP access as these methods do not protect communications between users and the TOE.

6.8 Trusted Path/Channels (FTP)

The Trusted path/channels function satisfies the following security functional requirements:

- FTP_ITC.1: The TOE can be configured to use TLS to ensure that any authentication operations or exported audit records are readable only by the optional authentication server or the SYSLOG server respectively, so they are not subject to unauthorized disclosure or modification.
- FTP_TRP.1: The TOE provides TLS within HTTPS using an embedded FIPS validated cryptographic module and SSHv2 to support secure remote administration. TLS and SSHv2 protect remote sessions from unauthorized disclosure and modification using FIPS validated cryptographic algorithms. No unprotected remote administration channels exist.

The TOE provides trusted communication channels between itself and external entities and between distributed TOE components using TLS protocol.

TLS within HTTPS provides the following protections:

- Assured identification of server end points is provided by using CA issued certificates.
- Protection of the channel data from disclosure is provided by using AES encryption.
- Detection of modification of the channel data is provided by using SHA in TLS 1.0 integrity protection mechanisms.

SSH provides the following protections:

- Protection of the channel data from disclosure is provided by using AES encryption.
- Detection of modification of the channel data is provided by using HMAC-SHA integrity protection mechanisms.

Independent paths from each TOE component to an external audit server (syslog) are protected by TLS 1.0. The syslog server must support TLS 1.0 connections. These communication channels are initiated by the TOE security function.

- The nGeniusONE server logs and the logs generated from use of the nGeniusONE console for TOE configuration activities are transmitted over a TLS channel to an external syslog server.
- The nGenius InfiniStream logs generated from use of the InfiniStream console for TOE configuration activities are transmitted over a TLS channel to the external syslog server.

The path between the TOE and an external authentication server (if one is used) in the IT environment is protected by TLS 1.0. The authentication server must support TLS 1.0 connections. All authentication connections are initiated by the nGeniusONE platform (nGenius InfiniStream use of an external authentication server is handled by the nGeniusONE platform) so only a single protected path is required.

Communication channels for remote administrators accessing the TOE using a browser are protected by TLS1.0 within HTTPS. In this case, communication channels are initiated by the client side (browser) entities. Additionally, web users must provide valid identification (a

registered username) and authentication (a valid password) to access TOE services over the trusted communication channel.

Remote administrators may access the TOE console on the nGeniusONE server and the nGenius InfiniStream for troubleshooting and maintenance operations using the SSHv2 protocol. An SSHv2 client is required. Remote administrators initiate these communication channels and also must provide valid identification (a registered username) and authentication (a valid password or digital signature generated with a valid private key corresponding to a public key certificate maintained in the TOE) to access TOE services over the trusted communication channel.

The communication channel between distributed TOE components is protected by TLS 1.0 algorithms initiated using HTTPS. Authentication is enabled using strong SNMP community strings. The TLS channel wraps SNMP commands sent from the nGeniusONE server to the InfiniStream and InfiniStream responses to the nGeniusONE server. Initial configuration settings (client and server IP addresses) and strong community strings ensure that only the authorized nGeniusONE server is communicating with the InfiniStream server, and that commands to the InfiniStream server are pre-authorized by the I&A services on the nGeniusONE server. In this case, the TOE nGeniusONE server component initiates the communication channel.

7. Rationale

This chapter provides the rationale for the selection of the IT security requirements, IT security objectives, assumptions and threats. It demonstrates that mappings are complete between the threats, policies, and assumptions, and TOE security function requirements.

7.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 15 - Threats and Assumptions to Security Objectives Mapping

	O.PROTECTED_COMMUNICATIONS	O.VERIFIABLE_UPDATES	O.SYSTEM_MONITORING	O.DISPLAY_BANNER	O.TOE_ADMINISTRATION	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.TSF_SELF_TEST	OE.NO_GENERAL_PURPOSE	OE.PHYSICAL	OE.TRUSTED_ADMIN
A.NO_GENERAL_PURPOSE									X		
A.PHYSICAL										X	
A.TRUSTED_ADMIN											X
T.ADMIN_ERROR			X								
T.TSF_FAILURE								X			
T.UNDETECTED_ACTIONS			X								
T.UNAUTHORIZED_ACCESS	X		X		X		X				
T.UNAUTHORIZED_UPDATE		X									
T.USER_DATA_REUSE						X					
P.ACCESS_BANNER				X							

7.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat to security objectives mapping.

Table 16 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.ADMIN_ERROR	**O.SYSTEM_MONITORING.** The TOE will provide the capability to generate audit data and send those data to an external IT entity. This mitigates the threat that an incorrect configuration would be undetected as the TOE audits TOE configuration actions for review.

T.TYPE	Security Objectives Rationale
T.TSF_FAILURE	**O.TSF_SELF_TEST.** The TOE tests a subset of its security functionality to ensure it is operating properly. This mitigates the threat that security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	**O.SYSTEM_MONITORING.** The TOE will provide the capability to generate audit data and send those data to an external IT entity. This mitigates the threat that malicious remote users or external IT entities may take actions that adversely affect the security of the TOE.
T.UNAUTHORIZED_ACCESS	This threat is mitigated by the following objectives: **O.PROTECTED_COMMUNICATIONS**. The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities, preventing attackers from gaining access to the TOE or to TSF data using data transmitted across the network. **O.SYSTEM_MONITORING.** The TOE will provide the capability to generate audit data and send those data to an external IT entity assuring that unauthorized accesses will be detected. **O.TOE_ADMINISTRATION.** The TOE will provide mechanisms to ensure that only authorized administrators are able to log in and configure the TOE, and access security management functions assuring that unauthorized entities cannot access the TOE and reconfigure the TOE security functions. **O.SESSION_LOCK**. The TOE shall provide session locking mechanisms that mitigate the risk of unattended sessions being hijacked.
T.UNAUTHORIZED_UPDATE	**O.VERIFIABLE_UPDATES.** The TOE will ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source. This mitigates the threat of malicious updates intended to compromise TOE security features.
T.USER_DATA_REUSE	**O.RESIDUAL_INFORMATION_CLEARING.** The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated. This mitigates the threat that data would be erroneously sent to an unintended recipient.

7.1.2 Rationale Showing Assumptions to Environment Security Objectives

The following rationales ensure assumptions are satisfied using tracings to show that security objective *X* directly upholds assumption *Y* by restating the assumption.

7.1.2.1 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.

This Assumption is satisfied by ensuring that:

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.

7.1.2.2 A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

This Assumption is satisfied by ensuring that:

OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

7.1.2.3 A.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

This Assumption is satisfied by ensuring that:

OE.TRUSTED_ADMIN: TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

7.2 Security Function Requirements Rationale

7.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 17 - SFRs to Security Objectives Mapping

	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST	O.VERIFIABLE_UPDATES
FAU_GEN.1				X				
FAU_GEN.2				X				
FAU_STG_EXT.1				X				
FCS_CKM.1		X						
FCS_CKM_EXT.4		X						
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						X
FCS_COP.1(3)		X						X
FCS_COP.1(4)		X						
FCS_HTTPS_EXT.1		X						
FCS_RBG_EXT.1(1)		X						

	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST	O.VERIFIABLE_UPDATES
FCS_RBG_EXT.1(2)		X						
FCS_SSH_EXT.1		X						
FCS_TLS_EXT.1		X						
FDP_RIP.2			X					
FIA_PMG_EXT.1						X		
FIA_UIA_EXT.1						X		
FIA_UAU_EXT.2						X		
FIA_UAU.7						X		
FMT_MTD.1						X		
FMT_SMF.1						X		
FMT_SMR.2						X		
FPT_APW_EXT.1						X		
FPT_ITT.1		X						
FPT_SKP_EXT.1		X						
FPT_STM.1					X			
FPT_TST_EXT.1							X	
FPT_TUD_EXT.1								X
FTA_SSL.3				X		X		
FTA_SSL.4						X		
FTA_SSL_EXT.1				X		X		
FTA_TAB.1	X							
FTP_ITC.1		X						
FTP_TRP.1		X						

The following table provides the detail of TOE security objective(s).

Table 18 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.DISPLAY_BANNER	FTA_TAB.1 requires the TOE to display a consent banner to any user attempting to access the TOE user interfaces.
O.PROTECTED_COMMUNICATIONS	FCS_CKM.1: The TOE generates encryption keys to encrypt channels between the TOE and external entities. FCS_CKM_EXT.4: The TOE zeroizes secret cryptographic keys when they are no longer needed. FCS_COP.1(1): The TOE uses FIPS-validated AES for cryptographic operations. FCS_COP.1(2): The TOE uses FIPS-validated rDSA for cryptographic operations. FCS_COP.1(3): The TOE uses FIPS-validated SHA-1 andSHA-256 for cryptographic operations. FCS_COP.1(4): The TOE uses FIPS-validated HMAC SHA-1, for cryptographic operations. FCS_HTTPS_EXT.1.1 The TOE uses HTTPS with TLS to protect communications with remote administrators and users. FCS_RBG_EXT.1(1): The TOE is required to implement NIST- or FIPS-conformant Random Bit Generation in support of cryptographic protocols. FCS_RBG_EXT.1(2): The TOE is required to implement NIST- or FIPS-conformant Random Bit Generation in support of cryptographic protocols. FCS_TLS_EXT.1: The TOE uses mandatory cipher suites AES 128 or 256 to protect communications with remote administrators and users. FCS_SSH_EXT.1: The TOE uses SSHv2 to protect TOE communication with local administrators. FPT_ITT.1: The TOE uses TLS to communicate between distributed TOE components. FPT_SKP_EXT.1: The TOE maintains stored cryptographic keys and CSPs in non-human readable format. FTP_ITC.1: The TOE protects communication between itself and its external authentication and audit services from disclosure and modification. FTP_TRP.1: The TOE protect communication between itself and its administrators from disclosure and modification.
O.RESIDUAL_INFORMATION_CLEARING	FDP_RIP.2: The TOE zeroizes new buffers to ensure network packets do not contain stale data.
O.SESSION_LOCK	FTA_SSL.3: The TOE terminates remote sessions after an administrator defined period of inactivity to help prevent unauthorized access. FTA_SSL_EXT.1: The TOE terminates local sessions after an administrator defined period of inactivity to help prevent unauthorized access.
O.SYSTEM_MONITORING	FAU_GEN.1: The TOE generates audit events for security relevant activities on the TOE. FAU_GEN.2: The TOE associates audit events with users to ensure proper accountability. FAU_STG_EXT.1: The exports audit records to an external syslog server using a

Security Objective	SFR and Rationale
	trusted channel to protect the data from disclosure and modification. FPT_STM.1: The TOE generates reliable time stamps for use in audit records for proper accounting.
O.TOE_ADMINISTRATION	FIA_PMG_EXT.1: TOE administrators can configure password length and composition for increased strength of authentication. FIA_UAU.7: The TOE does not echo passwords being entered to prevent password disclosure. FIA_UAU_EXT.2: The TOE implements a local authentication mechanism and an optional external authentication mechanism. FIA_UIA_EXT.1: The TOE identifies and authenticates users before allowing them to access TOE security functions. FMT_MTD.1: The TOE restricts management of TSF data to TOE administrators. FMT_SMF.1: The TOE is provides management functions to ensure the TOE administrators can properly manage the TOE. FMT_SMR.2: The TOE maintains the role of Authorized Administrator role and provides additional administrative roles as needed. FPT_APW_EXT.1: The TOE stores passwords in non-human readable form to prevent administrators and others from reading them. FTA_SSL.3: The TOE terminates remote sessions after an administrator defined period of inactivity to prevent unauthorized TOE access. FTA_SSL.4: The TOE has a log out interface for users to terminate their sessions as needed to protect an open session from misuse by other users. FTA_SSL_EXT.1: The TOE is terminates local sessions after an administrator defined period of inactivity to prevent unauthorized TOE access.
O.TSF_SELF_TEST	FPT_TST_EXT.1: The TOE executes self-tests during start-up to ensure that the TOE security functions are operating correctly.
O.VERIFIABLE_UPDATES	FCS_COP.1(2): The TOE uses digital signatures to ensure the integrity of updates. FPT_TUD_EXT.1: The TOE provides software/firmware update functions and enables an administrator to initiate and verify updates before they are applied.

7.3 Requirements Dependency Rationale

The following table shows the security function requirement dependencies and the security assurance requirement dependencies are satisfied.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UIA_EXT.1
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and	FCS_COP.1(*) and FCS_CKM_EXT.4

ST Requirement	CC Dependencies	ST Dependencies
	FCS_CKM.4	
FCS_CKM_EXT.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1
FCS_COP.1(1)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(2)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(3)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(4)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_HTTPS_EXT.1	None	None
FCS_RBG_EXT.1(1)	None	None
FCS_RBG_EXT.1(2)	None	None
FCS_SSH_EXT.1	FCS_COP.1	FCS_COP.1(*)
FCS_TLS_EXT.1	FCS_COP.1	FCS_COP.1(*)
FDP_RIP.2	None	None
FIA_PMG_EXT.1	None	None
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1
FIA_UAU_EXT.2	None	None
FIA_UIA_EXT.1	None	None
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.2	FIA_UID.1	FIA_UIA_EXT.1
FPT_APW_EXT.1	None	None
FPT_ITT.1	None	None
FPT_SKP_EXT.1	None	None
FPT_STM.1	None	None
FPT_TST_EXT.1	None	None
FPT_TUD_EXT.1	None	None
FTA_SSL.3	None	None

ST Requirement	CC Dependencies	ST Dependencies
FTA_SSL.4	None	None
FTA_SSL_EXT.1	None	None
FTA_TAB.1	None	None
FTP_ITC.1	None	None
FTP_TRP.1	None	None
ADV_FSP.1	None	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.1
AGD_PRE.1	None	None
ALC_CMC.1	ALC_CMS.1	ALC_CMS.1
ALC_CMS.1	None	None
ATE_IND.1	ADV_FSP.1 and AGD_OPE.and AGD_PRE.1	ADV_FSP.1 and AGD_OPE.and AGD_PRE.1
AVA_VAN.1	ADV_FSP.1 and AGD_OPE.and AGD_PRE.1	ADV_FSP.1 and AGD_OPE.and AGD_PRE.1

7.4 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

Table 19 - SFRs to TOE Security Functions Mapping

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE access	Trusted path/channels
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_STG_EXT.1	X							
FCS_CKM.1		X						
FCS_CKM_EXT.4		X						
FCS_COP.1(1)		X						

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE access	Trusted path/channels
FCS_COP.1(2)		X						
FCS_COP.1(3)		X						
FCS_COP.1(4)		X						
FCS_HTTPS_EXT.1		X						
FCS_RBG_EXT.1(1)		X						
FCS_RBG_EXT.1(2)		X						
FCS_SSH_EXT.1		X						
FDP_RIP.2			X					
FIA_PMG_EXT.1				X				
FIA_UAU.7				X				
FIA_UAU_EXT.2				X				
FIA_UIA_EXT.1				X				
FMT_MTD.1					X			
FMT_SMF.1					X			
FMT_SMR.2					X			
FPT_APW_EXT.1						X		
FPT_ITT.1						X		
FPT_SKP_EXT.1						X		
FPT_STM.1						X		
FPT_TST_EXT.1						X		
FPT_TUD_EXT.1						X		
FTA_SSL.3							X	
FTA_SSL.4							X	
FTA_SSL_EXT.1							X	
FTA_TAB.1							X	
FTP_ITC.1								X
FTP_TRP.1								X

8. PP Claims Rationale

This ST is conformant to the Security Requirements for Network Devices, Version 1.1, 8 June 2012 (NDPP) – with the optional ITT, SSH, and TLS requirements.

The TOE is an Ethernet monitoring device which is a network device. This makes the NDPP claim valid and applicable.

As explained in section 2, Security Problem Definition, the Security Problem Definition of the NDPP has been copied verbatim into this ST.

As explained in section 3, Security Objectives, the Security Objectives of the NDPP have been copied verbatim into this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is drawn from verbatim from the NDPP.

Table 20 - TOE Security Functional Components

Requirement Class	Requirement Component	Source
FAU: Security audit	FAU_GEN.1: Audit Data Generation	NDPP
	FAU_GEN.2: User identity association	NDPP
	FAU_STG_EXT.1: External Audit Trail Storage	NDPP
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)	NDPP
	FCS_CKM_EXT.4: Cryptographic Key Zeroization	NDPP
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)	NDPP
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)	NDPP
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)	NDPP
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)	NDPP
	FCS_HTTPS_EXT.1 Explicit: HTTPS	NDPP
	FCS_RBG_EXT.1(1): Extended: Cryptographic Operation (Random Bit Generation)	NDPP
	FCS_RBG_EXT.1(2): Extended: Cryptographic Operation (Random Bit Generation)	NDPP
	FCS_SSH_EXT.1: Explicit: SSH	NDPP
	FCS_TLS_EXT.1: Explicit: TLS	NDPP
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection	NDPP
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management	NDPP
	FIA_UAU.7: Protected Authentication Feedback	NDPP
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism	NDPP
	FIA_UIA_EXT.1: User Identification and Authentication	NDPP

FMT: Security management	FMT_MTD.1: Management of TSF Data (for general TSF data)	NDPP
	FMT_SMF.1: Specification of Management Functions	NDPP
	FMT_SMR.2: Restrictions on Security Roles	NDPP
FPT: Protection of the TSF	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords	NDPP
	FPT_ITT.1: Basic Internal TSF Data Transfer Protection	NDPP
	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)	NDPP
	FPT_STM.1: Reliable Time Stamps	NDPP
	FPT_TST_EXT.1: TSF Testing	NDPP
	FPT_TUD_EXT.1: Extended: Trusted Update	NDPP
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination	NDPP
	FTA_SSL.4: User-initiated Termination	NDPP
	FTA_SSL_EXT.1: TSF-initiated Session Locking	NDPP
	FTA_TAB.1: Default TOE Access Banners	NDPP
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel	NDPP
	FTP_TRP.1: Trusted Path	NDPP