NetScout Systems, Inc.
nGenius® InfiniStream® (V4.7 MR2),
nGenius® Performance Manager (V4.7 MR2),
and
nGenius® K2 (V4.7 MR2)
Security Target

Version 14.0

April 6, 2010

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

DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the NetScout nGenius InfiniStream (Version 4.7 MR2 which is build #4.70.603), nGenius Performance Manager (Version 4.7 MR2 which is build #4.70.352), and nGenius K2 (Version 4.7 MR2 which is build #4.70.352). 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.

REVISION HISTORY

Rev	Description
1.0	August 1, 2008, initial release
2.0	August 12, 2008, incorporated comments from NetScout internal review
3.0	November 5, 2008, incorporated updates for Software Version
4.0	November 7, 2008, incorporated comments from NetScout internal review
5.0	May 7, 2009, addressed Observation Reports and updated software version number
6.0	May 8, 2009, incorporated comments from NetScout internal review
7.0	May 15, 2009, incorporated comments from NetScout internal review
8.0	June 3, 2009, addressed Observation Reports
9.0	June 11, 2009, addressed Observation Reports
10.0	June 18, 2009, addressed Observation Report
11.0	October 9, 2009, addressed Observation Report of Development Evidence
12.0	December 3, 2009, updated product/version being evaluated
13.0	January 7, 2010, addressed Observation Report
14.0	April 6, 2010, included software build numbers

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS LIST

ACL .....Access Control List
CC .....Common Criteria
CDE ..... Common Data Export
CLA .....Command Line Administrator
CLI .....Command Line Interface
EAL3 .....Evaluation Assurance Level 3
GB ..... GigaByte
GUI ..... Graphical User Interface
HTTPS ..... HyperText Transfer Protocol over Secure Socket Layer
I&A .....Identification and Authentication
IP.....Internet Protocol
IT .....Information Technology
JRE .....Java Runtime Environment
MAC .....Media Access Control
MB .....MegaByte
MR.....Maintenance Release
PM .....Performance Manager
PP.....Protection Profile
SFP ..... Security Function Policy
ST.....Security Target
TCP..... Transmission Control Protocol
TOE .....Target of Evaluation
TSF ..... TOE Security Function
TSFI..... TSF Interface
UDP .....User Datagram Protocol
VLAN .....Virtual Local Area Network

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the NetScout nGenius InfiniStream (Version 4.7 MR2), nGenius Performance Manager (Version 4.7 MR2), and nGenius K2 (Version 4.7 MR2). 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 22, 2008. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

NetScout Systems, Inc. nGenius® InfiniStream® (V4.7 MR2), nGenius® Performance Manager (V4.7 MR2), and nGenius® K2 (V4.7 MR2) Security Target, Version 14.0, April 6, 2010.

1.2 TOE Reference

NetScout nGenius InfiniStream (Version 4.7 MR2 which is referring to nGenius InfiniStream 4.70.603), nGenius Performance Manager (Version 4.7 MR2 which is referring to nGenius Performance Manager 4.70.352), and nGenius K2 (Version 4.7 MR2 which is referring to nGenius K2 4.70.352).

1.3 Keywords

nGenius, Sniffer, InfiniStream, Enterprise Management, Capture Engine, Performance Manager, K2, Sniffer Analysis, data mining, frame slicing, capture ports, store, stream, selective recording, slice size, nGenius InfiniStream Appliance, InfiniStream Application, monitored element, service assurance, network management, network monitoring

1.4 TOE Overview

1.4.1 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 prevention
- service level management

The nGenius InfiniStream appliance is a continuous capture platform that records the packet-level details of enterprise traffic seen by monitoring network links. nGenius InfiniStream application is the software on this platform responsible for performing the capture and storage of the network traffic.

nGenius Performance Manager is a GUI-based management product that may be used to control and monitor the operation of the nGenius InfiniStream application as well as analyze the captured data. The captured data is used to provide efficient top-down KPI-to-Flow-to-Packet

[1]analysis and minimize mean time to resolution when network issues occur. The solutions also provide real-time performance monitoring and statistical monitoring of the enterprise network.

nGenius Performance Manager, and nGenius Performance Manager with nGenius K2, are both valid configurations of nGenius Performance Manager which provide various levels of analysis and reporting functionality. Only one is used operationally in each installation. All of the products share common functions which provide the complete set of security functions claimed in this document.

There is a single software installation for nGenius Performance Manager which includes optional modules which are by default disabled and can be enabled if a license is applied. The optional modules provide increased levels of analysis and reporting. These optional modules do not provide any additional security functionality or interfere with security functionality provided by the nGenius Performance Manager base product. nGenius K2 is an optional licensable nGenius Performance Manager module.

nGenius Performance Manager provides the ability to control and monitor the InfiniStream application, perform basic analysis of the captured data, and generate reports. nGenius K2 adds additional analysis functions including KPI alarms and specialized analysis of internal threats[2]. . Sniffer Intelligence modules provide specialized analysis functions for distinct application protocols or industries; these modules do not provide any additional security functions.

In support of these functions, the TOE provides the following security functionality:

- Capture and storage of network traffic
- Restricted access to the captured data to protect the contents of that data from unauthorised users
- Management functionality to enable administrators to configure the security functions
- Identification and Authentication (I&A) to provide user-based privileges to the users of the system

1.4.2 TOE type

The TOE type is Network Management.

1.4.3 Required Non-TOE Hardware/Software/Firmware

The individual TOE components execute on different platforms and therefore have different required hardware and software to support them.

In addition, the management product is accessed remotely from client systems using a browser. The requirements for the client systems are also specified.

---

[1] KPI-to-Flow-to-Packet is the term used to describe the workflow process for how an nGenius Performance Management Solution user can navigate from a high-level alert based on key performance indicators (KPIs) to the relevant flow-based content and then to the actual packet-level information.

[2] Specialized analysis of internal threats provided by nGenius Security Manager is not claimed as TOE security functionality in this Security Target.

1.4.3.1 nGenius InfiniStream

The nGenius InfiniStream application executes on a dedicated server running a NetScout customized and hardened Linux distribution based on Fedora Core 6 based on kernel 2.6.22. The required hardware and software to support the nGenius InfiniStream application is specified in the following table. To accommodate new, former, and existing customers of either NetScout or Network General (a company acquired by NetScout), this application may be executed on hardware falling into three categories:

1. Legacy NetScout hardware – hardware that NetScout customers purchased prior to the acquisition of Network General
2. Legacy Network General hardware – hardware purchased from Network General prior to the acquisition by NetScout
3. Current hardware – hardware supported for new systems

Table 1 - Minimum InfiniStream Hardware and Operating System Requirements

Category	Minimum Hardware Requirements	Operating System Requirements
Legacy NetScout	Intel Xeon processors with 1 MB integrated Advanced Transfer Cache at 3.20 GHz, 533 MHz FSB, dual on board 10/100/1000 Mbps LAN ports with Intel 7501 chip set, 16 GB ECC, registered DDR PC 2100 at 266 MHz (133 x 2), 6 PCI-X (2 @ 133 MHz) slots with 3 separate buses. 200 GB ATA/133 Drive (OS and applications) 3Ware 9500 SATA High Performance RAID 4 x 300GB SATA Drives (data storage) 2 x 10/100/100 Ethernet ports	NetScout customized and hardened Linux distribution based on Fedora Core 6 based on kernel 2.6.22. Net-SNMP v. 5.0.9
Legacy Network General	Intel Dual Core Xeon 5100 processor at 3.0 GHz, 1333 MHz FSB, dual on board LAN ports, with Intel 5000 chip set, 16GB FBD 533 MHz SDRAM, 1 PCI-Express (x8) and 2 (133 MHz) PCI-X slots. 1 x 250 GB SATA Drives (OS and applications) Areca PCI-Express SATA II RAID Controller 5 x 250GB SATA Drives (data storage) 4 x 10/100/100 Ethernet ports	NetScout customized and hardened Linux distribution based on Fedora Core 6 based on kernel 2.6.22. Net-SNMP v. 5.0.9
Current Hardware	Intel Xeon Processor with Intel Extended Memory 64-bit Techno1ogy at 3.8 GHz, 800 1MHz FSB, dual on board 10/100/1000 Mbps LAN ports, with Intel E7520 Chipset, 16GB DDR2 400 SDRAM, 1 PCI-Express (x8) and 5 PCI-X slots (3 @ 133MHz) 2 x 80 GB SATA Drives (OS and applications) LSI/Dell PERC RAID Controller, or 3Ware 9550 SATA RAID Controller 5 x 250GB SATA Drives (data storage) 2 x 10/100/100 Ethernet ports	NetScout customized and hardened Linux distribution based on Fedora Core 6 based on kernel 2.6.22. Net-SNMP v. 5.0.9

1.4.3.2 nGenius Performance Manager

The management product (whichever one is used for any specific installation) executes on a dedicated system running Linux, Solaris or Windows. The required hardware and software is

specified in the following table (the requirements are the same for all three management products).

Table 2 - Minimum Management System Hardware and Software Requirements

Operating System	Minimum Hardware Requirements	Software Requirements
Linux	Two Dual-Core Xeon processors 5130 or better; 2.00 GHz, 1333 MHz FSB, 4 MB L2 Cache 4 GB DDR-2 RAM with swap space equal to twice the capacity of physical memory 5 x 300 GB or 6 x 250 GB hard drives; RAID 5; Ultra 320 SCSI, SATA, or SAS CD-ROM drive (DVD-ROM drive recommended) 100/1000 Ethernet adapter Dual, redundant power supplies	Red Hat Linux ES 4.0 Update 4 (English) with the following package selections: • Desktops – X Window System (in Details, select all 42 items) – GNOME Desktop Environment (accept defaults, 41/44 items) • Applications – Editors (in Details, select only vim-enhanced, nedit, emacs) – Graphical Internet (in Details, select only FireFox) – Text-based Internet (in Details, select only elinks) – Office/Productivity (in Details, select only ggv, gpdf, andtetex-xdvi) – Authoring and Publishing (full package, 12 items) • Servers – Server Configuration Tools (in Details, select all except redhat-config-httpd, redhat-switch-mail, and redhat-switch-mail-gnome) – Windows File Server (full package, 3 items) – Legacy Network Server (in Details, select only rwho, rusers) • Development – Development Tool (accept defaults, 57/75 packages) – Legacy Software development (full package, 6 items) • System select – Administration Tools (full package,12 items) – System Tools (in Details, select all except tn5250, x3270-x11, festival) – Printing Support (in Details, select all except hpoj) • Miscellaneous – No selections JRE v1.5.0_10 JBoss Application Server (version 4.0.4GA) Apache Web Server (version 2.0.63) Sybase DBMS (version 10.0.1.3488)
Solaris	Two Dual-Core Xeon processors 5130 or better; 2.00 GHz, 1333 MHz FSB, 4 MB L2 Cache 4 GB DDR-2 RAM with swap space equal to twice the capacity of physical memory 5 x 300 GB or 6 x 250 GB hard drives; RAID 5; Ultra 320 SCSI, SATA, or SAS; NTFS formatted	Solaris v8 or v9 (English, Japanese) with patches required for Java Runtime Environment (JRE) v1.5.0_10 JRE v1.5.0_10 JBoss Application Server (version 4.0.4GA) Apache Web Server (version 2.0.63) Sybase DBMS (version 10.0.1.3488)

Operating System	Minimum Hardware Requirements	Software Requirements
	CD-ROM drive (DVD-ROM drive recommended) 100/1000 Ethernet adapter Dual, redundant power supplies	
Windows	Two Dual-Core Xeon processors 5130 or better; 2.00 GHz, 1333 MHz FSB, 4 MB L2 Cache 4 GB DDR-2 RAM with swap space equal to twice the capacity of physical memory 5 x 300 GB or 6 x 250 GB hard drives; RAID 5; Ultra 320 SCSI, SATA, or SAS CD-ROM drive (DVD-ROM drive recommended) 100/1000 Ethernet adapter Dual, redundant power supplies	Windows 2003 — Standard or Enterprise with Service Pack 1 (English, Japanese, Simplified Chinese) OR Windows 2003 R2 — Standard or Enterprise (English, Japanese, Simplified Chinese) JRE v1.5.0_10 DirectX 8.1 or higher JBoss Application Server (version 4.0.4GA) Apache Web Server (version 2.0.63) Sybase DBMS (version 10.0.1.3488)

1.4.3.3 Client Systems

Table 3 - Minimum Client System Hardware and Browser Requirements

Minimum Hardware Requirements	Browser Requirement
800 MHz processor 512 MB RAM 250 MB available disk space	JRE v1.5.0_10

1.5 TOE Description

The TOE is a set of software components executed on Linux, Solaris, and/or Windows platforms. The TOE is a network capture and analysis tool intended for use in enterprise environments. The individual components are described in more detail in the following sections.

In the remainder of this document, the term MANAGEMENT is used to describe the common functionality provided by nGenius Performance Manager, or nGenius Performance Manager with nGenius K2. Whenever reference is made to a capability not common to all these products, a more product-specific reference is used.

The MANAGEMENT component provides the mechanism for user interaction with the operational TOE (capturing traffic is transparent to users).

1.5.1 TOE Component Descriptions

1.5.1.1 nGenius InfiniStream

The nGenius InfiniStream application (InfiniStream application) captures a continuous flow of network traffic for each network interface. Stored network traffic can be searched using custom search criteria. Additionally, using Selective Recording or Monitor Element Groups it is possible to omit unwanted network packets from storage during the capture process.

The InfiniStream application executes on a Linux operating system server. The hardware, Linux operating system and 3rd party software are excluded from the TOE. The server this component executes on must be dedicated to this application; no software other than that required by the TOE is installed.

1.5.1.2 nGenius Performance Manager

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

Performance Manager provides centralized management functionality to control and monitor InfiniStream application instances, control and monitor InfiniStream appliances and manage configuration parameters within Performance Manager.

Performance Manager provides the ability to generate reports from analysis of the captured data.

Performance Manager functionality is accessed via a web browser executing on a client system. HTTPS is used in order to protect the data being exchanged.[3]

The Performance Manager application executes on a Linux, Solaris, or Windows server. The hardware, operating system, and all 3rd party software are excluded from the TOE. The server this component executes on must be dedicated to this application; no software other than that required by the TOE is installed.

1.5.1.3 nGenius Performance Manager with nGenius K2

nGenius Performance Manager with nGenius K2 (K2) is a management system including all the Performance Manager capabilities as well as providing additional analytic analysis capabilities to monitor the health of critical business services, additional analytic analysis of potential internal network threats,[4] and early warning of anomalous changes in application and network performance.

The K2 application executes on a Linux, Solaris, or Windows server. The hardware, operating system, and all 3rd party software are excluded from the TOE. The server this component executes on must be dedicated to this application; no software other than that required by the TOE is installed.

1.5.2 Physical Boundary

The physical boundary of the TOE includes:

---

[3] HTTPS is part of the operational environment and is not being evaluated.

[4] The specialized analysis of internal threats provided by nGenius Security Manager is not claimed as TOE security functionality in this Security Target.

A) One or more instances of the InfiniStream application, each executing on a system dedicated to this purpose

B) One instance of MANAGEMENT, executing on a system dedicated to this purpose. This element may be Performance Manager, or K2 because they provide the same security functionality.

C) Product Operating Manuals including nGenius InfiniStream Hardware Installation and Administration Guide(Part Number 293-2142 Rev. C), nGenius Performance Manager Installation Guide (Part Number 293-2212 Rev. A), nGenius Performance Manager Online Help version 4.7 MR2, and NetScout's Guide to Configure the Common Criteria Evaluated Configuration (Part Number 733-0157 Rev. A TBD)

Note specifically that the hardware, operating system, and all 3rd party software on each of the systems are excluded from the TOE boundary.

1.5.3 Logical Boundary

The TOE consists of software applications that execute on at least 2 different hardware platforms. These software applications provide audit generation, identification and authentication, security management, and user data protection.

1.5.3.1 Audit Generation

During operation, the TOE generates audit records for system and management events. The audit records are stored on the MANAGEMENT system. The audit record generated can be viewed by all authorised users of the MANAGEMENT system.

1.5.3.2 Identification and Authentication

When users first access the TOE via a web browser, they must provide credentials for Identification and Authentication (I&A) before access is granted to any further TOE capabilities. The TOE validates the credentials against the configured credentials. Upon successful login, security attributes are associated with the user session to control its access.

1.5.3.3 Security Management

The TOE provides management functions directly related to the secure operation of its components and management functions that ensure the strict limitations of access to stored captured network traffic. The TOE provides mechanisms to configure user credentials, user permissions and user access to network traffic. Management functionality is limited to users that have been granted permissions to perform these functions.

1.5.3.4 User Data Protection

The TOE provides user data protection by limiting the data that is captured and limiting individual user access to that data.

Two Selective Recording mechanisms may be configured to limit the data that is stored. Selective Recording per application allows organizations to specify exactly which application protocols they are not interested in capturing so data associated with application protocol is discarded. The Selective Recording slice size provides the mechanism to restrict the amount of

bytes captured per packet. By setting the slice size to a low value, the captured data can be limited to information which does not contain sensitive information.

Users can be restricted from accessing data captured from specific InfiniStream application interfaces via Monitored Element Group Restrictions. A Monitored Element Group is a grouping any element that the InfiniStream Application can monitor. A single InfiniStream appliance may have many physical ports and logical interfaces, each of which is an individual monitored element.

1.6 Evaluated Configuration

1. Identification and authentication are performed locally by the TOE.
2. The MANAGEMENT product is installed as a Standalone Server.
3. SNMPv3 functionality provided by the operational environment is used to provide a channel between MANAGEMENT and individual InfiniStream application instances.
4. The following optional product components are not installed: nGenius NewsStand for Remote Servers, nGenius Command Line Interface (CLI), nGenius Command Line Administrator (CLA), nGenius Common Data Export (CDE), Command Line Device Tools, Sniffer Analysis, and Standby Server.
5. The serviceManager.userAccountLockup.enabled configuration parameter is set to True to force accounts to be locked out for a specified period of time after the configured number of consecutive authentication failures has occurred.
6. The “Change Config Server Address” option in the InfiniStream is set to the IP address of the Managing Performance Manager, forcing authentication to be performed by Performance Manager. Administrators are procedurally prohibited from using the InfiniStream local console except for setting the “Change Config Server Address” option and the access list.
7. HTTPS/SSL is activated on the MANAGEMENT platform and all connections from remote users to the MANAGEMENT use HTTPS. HTTPS/SSL is provided by the operational environment and beyond the boundary of the TOE being evaluated.
8. Access List Security is configured on all InfiniStream application instances to limit the systems that may remotely access the InfiniStream application instances.

2. Conformance Claims

2.1 Common Criteria Conformance

The TOE and the ST is conformant with the Common Criteria (CC) Version 3.1, functional requirements (Part 2) Version 3.1 Revision 2 conformant, and assurance requirements (Part 3) Version 3.1 Revision 2 conformant for EAL3 augmented by ALC_FLR.1 (Basic Flaw Remediation).

2.2 Protection Profile Conformance

The TOE does not claim conformance to any registered Protection Profile.

2.3 Security Requirement Packages

The TOE does not claim conformance to any registered Security Requirement Packages.

3. Security Problem Definition

3.1 Introduction

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*.

3.2 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 4 - Assumptions

A.Type	Description
A.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
A.FIREWALL	The TOE will be located behind a firewall and an Access Control List (ACL) will be created on the router between the TOE and the rest of the network to provide network security.
A.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance and specific organisational security policies.
A.NETWORK	There will be a network that supports communication between distributed components of the TOE. This network functions properly.
A.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

3.3 Threats

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

Table 5 - Threats

T.Type	TOE Threats
T.COMDIS	A user may access data under TOE control they are not authorised to view by bypassing a security mechanism.
T.COMINT	An unauthorised user may attempt to compromise the integrity of the data collected by the TOE by bypassing a security mechanism.
T.COMMS	An unauthorised user may attempt to access TOE and user data during transmission from one TOE component to another TOE component.
T.LOSSOF	An unauthorised user may attempt to remove, alter, or destroy data collected by the TOE.
T.MISCFG	An unauthorised user may change the configuration of the TOE causing the collection of data to change from its originally configured intention.
T.NOHALT	An unauthorised user may attempt to compromise the continuity of the TOE's data collection functionality by halting execution of the TOE.

T.Type	TOE Threats
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be modified.
T.UNAUTHACCESS	An authorised user may attempt to gain access to TOE and user data without proper authorization.
T.UNSECURE_ENVIRONMENT	An unathorised user may attempt to access the server to which the TOE resides or the router that transmits communication between TOE components.

3.4 Organisational Security Policies

There are no Organisational Security Policies identified for this TOE.

4. Security Objectives

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*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 6 - Security Objectives for the TOE

O.Type	Security Objective
O.AUDIT	The TOE will provide the capability to detect, create and review records of security-relevant events.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorised use.
O.SELECT	The TOE provides a means to select only certain network traffic or certain types of network traffic is captured and stored.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
O.TRUNCATE	The TOE provides a means to truncate network traffic before it is captured so that sensitive information is not stored or revealed to TOE users.

4.2 Security Objectives for the Operational Environment

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

Table 7 - Security Objectives of the IT Environment

OE.Type	IT Environment Security Objective
OE.COMM	The IT Environment will protect communication between distributed components of the TOE from disclosure.
OE.ENVIRON	The Administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
OE.INFO_STORAGE	The IT Environment will provide secure storage for system data generated by the TOE.
OE.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
OE.NETWORK	The Administrator will install and configure a network that supports communication between the distributed TOE components. The administrator will ensure that this network functions properly.
OE.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.
OE.OS_PROTECTION	The IT Environment will support TOE self-protection by maintaining a domain for its own execution and domains for separate application processes that protects itself and the application processes from external interference, tampering, or unauthorised disclosure through its own interfaces.
OE.TIME_STAMP	The Operational Environment will provide reliable time stamps for accountability purposes.

5. Extended Components Definition

5.1 Extended Security Functional Components

No extended components are included in this document.

5.2 Extended Security Assurance Components

No extended components are included in this document.

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

a) Start-up and shutdown of the audit functions[5];

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

c) *no other auditable events*.

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, *the additional information specified in the Details column of the following table*.

SFR	Audit Event Type	Details
FAU_GEN.1	None	
FAU_GEN.2	None	
FDP_ACC.1	Data uploaded from InfiniStream application	
FDP_ACF.1	Data uploaded from InfiniStream	

[5] Audit messages are always enabled. There is no explicit message indicating Start-up and shutdown of the audit functions as they cannot be disabled.

SFR	Audit Event Type	Details
	application	
FDP_IFC.1	None	
FDP_IFF.1	None	
FIA_AFL.1	Reaching the threshold for unsuccessful authentication attempts	Userid supplied
FIA_ATD.1	None	
FIA_SOS.1	None	
FIA_UAU.2	Successful logins Unsuccessful logins	Userid supplied
FIA_UAU.7	None	
FIA_UID.2	Successful logins Unsuccessful logins	Userid supplied
FIA_USB.1	None	
FMT_MOF.1	Configuration Change	
FMT_MSA.1	None	
FMT_MSA.3	None	
FMT_MTD.1	None	
FMT_SMF.1	None	
FMT_SMR.1	None	

6.1.1.2 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.

6.1.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide *all authorised users* with the capability to read *all audit information* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the *User Data Access Security Policy* on *authorised users, captured data, viewing.*

6.1.2.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the *User Data Access Security Policy* to objects based on the following:

A) *Subjects: Authorised users*

B) *Objects: Captured data of a specific application protocol*

C) *Subject Security Attributes: Monitored Element Group Restriction, User slice size*

D) *Object Security Attributes: Monitored Element Group*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Authorised user is allowed to view captured data of a Monitored Element Group if they do not have a Monitored Element Group Restriction. The amount of data displayed for each captured packet is limited by the User slice size.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *if no Monitored Element Group Restrictions are associated with a user, the user has access to all interfaces*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *no further rules*.

6.1.2.3 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce *information flow control SFP* on *subjects: Monitored Elements, information: network packets, operation: store network packet*.

6.1.2.4 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce *information flow control SFP* based on the following types of subject and information security attributes:

A) *Subjects: Monitored Element*

B) *Subject Security Attributes: Capture Port Status, Selective Recording per application, Selective Recording Slice Size*

C) *Information: Network packet*

D) *Information Security Attributes:*

1) Presumed IP Addresses

2) Presumed MAC Addresses

3) Presumed Protocol

4) Presumed TCP Ports

5) Presumed UDP Ports

6) *Or any combination of the above.*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

A) *if the Capture Port Status is ON then the received network data packets will be stored per the Selective Recording slice size specified by application protocol.*

B) *if the Selective Recording per application is set to FULL then the all the received data packets for that application protocol will be stored.*

C) *if the Selective Recording per application is set to a numerical value then data packets will be stored per the Selective Recording slice size specified by application protocol.*

FDP_IFF.1.3 The TSF shall enforce the *additional information flow control rules:*

A) *The amount of data from a network packet that is stored is limited by the Selective Recording Slice Size.*

B) *If both the Global Settings Selective Recording Slice Size and the Interface specific Selective Recording Slice Size are configured is the lesser Slice Size specified is stored.*

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: *no explicit rules*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *If the Selective Recording per application is set to NONE instead of the default of FULL, no traffic for that application protocol is captured*.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an administrator-configurable positive integer within *the range of 1 to 31* unsuccessful authentication attempts occur related to *attempted logins to MANAGEMENT*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall *prevent login using that account for the configured amount of time*.

6.1.3.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: *user ID, password, roles, Monitored Element Group restrictions, User slice size*.

6.1.3.3 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet *the following rules:*

1. *A minimum length of 8 characters.*
2. *At least one numeric value.*

6.1.3.4 FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.5 FIA_UAU.7 Protected Authentication Feedback

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

6.1.3.6 FIA_UID.2 User Identification Before any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.7 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user:

1. *user ID*
2. *roles*
3. *Monitored Element Group restrictions*
4. *User slice size*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

1. *The user ID is the value associated with the username supplied for a successful login.*
2. *The roles define the set of privileges associated with each user account that has this role associated.*
3. *The Monitored Element Group restrictions are configured for the user account.*
4. *The Selective Recording User Slice Size can be an explicitly configured value for each user account except for the System Administrator role where it is automatically and irrevocably set to Full Packet.*

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *the security attributes do not change during a session.*

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to activate, deactivate the functions *selective recording per application protocol* to *authorised user associated with the Network Administrator role.*

6.1.4.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the *User Data Access Security Policy and information flow control SFP* to restrict the ability to query, modify, delete, *create* the security attributes *specified in the following table* to *authorised roles with the privilege specified in the following table.*

Table 8 - Security Attribute Management Details

Security Attribute	Applicable Operations	Required Roles
Capture Port Status	Query, Modify	Network Administrator
Monitored Element Group	Query	Approver, Helpdesk, Network Administrator, Network Operator, or System Administrator
	Modify (associating interfaces with Monitored Element Groups)	Approver, Network Administrator
Monitored Element Group Restriction	Query	Approver, Helpdesk, Network Administrator, Network Operator, or System Administrator
	Modify (restricting or unrestricting Monitored Element Groups from	System Administrator

Security Attribute	Applicable Operations	Required Roles
	user accounts)	
Password	Modify	System Administrator
	Modify (the user's own password)	n/a
Roles	Query	Approver, Helpdesk, Network Administrator, Network Operator, or System Administrator
	Modify (roles associated with user accounts)	System Administrator
User ID	Create, Query, Modify, Delete	System Administrator
User Slice Size	Query	Approver, Helpdesk, Network Administrator, Network Operator, or System Administrator
	Modify	System Administrator

Application Note: Users are restricted to modifying information for their own user account if they have any associated Monitored Element Group Restrictions.

6.1.4.3 FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1(1) The TSF shall enforce the *information flow control SFP* to provide permissive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the *no users* to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1(2) The TSF shall enforce the *User Data Access control SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the *no users* to specify alternative initial values to override the default values when an object or information is created.

6.1.4.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1 The TSF shall restrict the ability to query, modify, delete, or *create* the *TSF data specified in the following table* to *authorised roles with the privilege specified in the following table*.

Table 9 - TSF Data Management Details

TSF Data	Definition	Applicable Operations	Required Role
Global Settings Selective Recording per application	Active/deactivate recording of a specific protocol for all InfiniStream application instances managed by MANAGEMENT	Query	Approver, System Administrator, or Network Administrator
		Modify	Network Administrator
Global Settings capture slice size	Specify capture slice size for all InfiniStream application instances managed by MANAGEMENT	Query	Approver, System Administrator, or Network Administrator
		Modify	Network Administrator

TSF Data	Definition	Applicable Operations	Required Role
Interface Specific Slice Size	Specify Capture slice size for Interfaces managed by MANAGEMENT	Query	Network Administrator
		Modify	Network Administrator
Monitored Element Group interface set up	Grouping of interfaces to be included within a Monitored Element Group	Create, Modify, Delete	System Administrator
		Query	Approver, Helpdesk, Network Administrator, Network Operator, or System Administrator
Role Privileges	Maintain Privileges associated to predefined user roles	Query, Modify	System Administrator
Configure # of failed attempts before lock out	Maintain counter of sequential authentication failures. If the credentials are not valid, the user is prompted to enter the credentials again. If the user ID is valid but the password is not, the counter of sequential authentication failures for the user ID is also incremented.	Query, Modify	System Administrator
Configure Time out period after failed log in timeout	If the threshold value for consecutive authentication failures is reached, the user account is locked for the configured amount of time after which the counter is reset.	Modify, query	System Administrator
Message Log	Non-network management audit logs	Query	Approver, Helpdesk, Network Administrator, Network Operator, or System Administrator
		Modify	System Administrator, or Network Administrator

6.1.4.5 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *managing user accounts, configuring capture ports, managing Monitored Element Groups*.

6.1.4.6 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *Approver, Helpdesk, Network Administrator, Network Operator, and System Administrator*

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL3 augmented by ALC_FLR.1 (Basic Flaw Remediation). These requirements are summarized in the following table.

Table 10 - EAL3+ Assurance Requirements

Assurance Class	Component ID
Development	ADV_ARC.1
	ADV_FSP.3
	ADV_TDS.2
Guidance Documents	AGD_OPE.1
	AGD_PRE.1
Life-Cycle Support	ALC_CMC.3
	ALC_CMS.3
	ALC_DEL.1
	ALC_DVS.1
	ALC_FLR.1
	ALC_LCD.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	AVA_VAN.2

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 11 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied by the IT Environment (OE.TIME_STAMP)
FAU_GEN.2	No other components.	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by FIA_UID.2
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FDP_ACC.1	No other components.	FDP_ACF.1	Satisfied
FDP_ACF.1	No other components.	FDP_ACC.1, FMT_MSA.3	Satisfied Satisfied
FDP_IFC.1	No other components.	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components.	FDP_IFC.1, FMT_MSA.3	Satisfied Satisfied
FIA_AFL.1	No other components.	FIA_UAU.1	Satisfied by FIA_UID.2
FIA_ATD.1	No other components.	None	n/a
FIA_SOS.1	No other components.	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UAU.7	No other components.	FIA_UAU.1	Satisfied by FIA_UAU.2
FIA_UID.2	FIA_UID.1	None	n/a

FIA_USB.1	No other components.	FIA_ATD.1	Satisfied
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MSA.1	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied Satisfied Satisfied
FMT_MSA.3 (1) and (2)	No other components.	FMT_MSA.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2

7. TOE Summary Specification

7.1 Security Functions

7.1.1 Audit Generation

The MANAGEMENT application generates and stores audit event records for the following security relevant events:

1. Start-up of the MANAGEMENT application. This event is equivalent to the start of the audit function.
2. Controlled shutdown of the MANAGEMENT application. Since the audit function cannot be stopped independently of the application, this event is equivalent to stopping the audit function.
3. Successful login attempts.
4. Logouts.
5. Unsuccessful login attempts (the record includes the user ID string input by the user).
6. Upload of captured data to the MANAGEMENT application.

All audit event records include the date and time of the event and the type of event. The subject identity (user ID) is included when applicable. Read access of message logs (audit records) is granted to all authorised users of the MANAGEMENT application.

7.1.2 Identification and Authentication

When a user opens a browser to the MANAGEMENT system, the user is prompted to enter their user ID and password. Until the I&A function completes successfully, no access to any other function is available.

When the password is entered, only asterisks are displayed. The MANAGEMENT system performs the I&A function by validating the credentials presented. If the credentials are valid, the following security attributes are bound to the session:

1. User ID
2. User privileges, based on the union of any privileges configured for each role associated with the user account
3. Monitored Element Group restrictions
4. Selective Recording User Slice Size can be an explicitly configured value for the each user account except for the System Administrator role where it is automatically and irrevocably set to Full Packet

The user is then presented with the opening GUI for user sessions. The counter of sequential authentication failures for the user ID is also reset to 0.

If the credentials are not valid, the user is prompted to enter the credentials again. If the user ID is valid but the password is not, the counter of sequential authentication failures for the user ID is also incremented. If the threshold value for consecutive authentication failures is reached, the user account is locked for the configured amount of time and the counter is reset to 0.

7.1.3 Security Management

The MANAGEMENT application provides security management functions to authorised users. The user privileges bound to a user's session define the management functions available to each user. The privileges associated with each of the user's associated roles are joined to define the set of privileges for the session.

The User Setup privilege is required to configure the set of privileges associated with each defined role.

The Global Settings privilege is required to configure Global Settings for specifying the traffic types (application protocols) to be captured and (for each protocol) the slice size.

The Monitored Element Group privilege is required to add to or delete interfaces from the set of Monitored Element Groups. The list of Monitored Element Groups may be viewed if the user has the Monitored Element Group or User Accounts privilege.

The Device Configuration privilege is required to view or modify the following InfiniStream application interface parameters:

1. Status (enabled or disabled)
2. Monitored Element Group
3. Interface Capture Slice Size

The User Accounts privilege is required to create, query, modify, or delete userids. That same privilege is required to manage the following per-user attributes:

1. Password
2. Monitored Element Group restriction (the default is none)
3. Associated role(s); if more than one role is associated with a user, the user privileges consist of all privileges assigned to any of the associated roles.
4. User Slice Size; by default, users with the Network Administrator role assigned have visibility to the full slice size. Users with the System Administrator role are not allowed to do any on-demand data capture. Users with the Approver, Network Operator or Helpdesk roles can decode up to 64bytes of the packet.

If a user account has a Monitored Element Group restriction, the user is considered to be a "restricted user;" if a restricted user has the User Accounts privilege, that user may only modify parameters for its own account.

All users may change their own password. Whenever a password is changed, the TOE enforces the following rules:

1. The password must be at least 8 characters.
2. At least one numeric value must be included.

7.1.4 User Data Protection

The MANAGEMENT application limits user access to the network traffic captured by InfiniStream application instances. Raw traffic is captured and saved on the InfiniStream appliances, then retrieved by the MANAGEMENT application. For efficient analysis by the

MANAGEMENT application, the InfiniStream application instances also summarize the captured data; the summarized information is periodically retrieved by the MANAGEMENT application. User access restriction checking is always performed by the MANAGEMENT application. The confidentiality of data exchanged between the MANAGEMENT application and InfiniStream application instances is assured by cryptographic functionality and protocols provided by the operational environment.

The following mechanisms are used to limit what information is captured and what subset of that information is available to individual users.

1. Only InfiniStream application interfaces that are enabled capture network traffic.
2. The Network traffic application protocols captured are determined by the Global Settings.
3. Each network packet that is captured is limited by the Selective Recording Slice Size. , The slice size is the lesser of the Selective Recording Global Settings capture slice size and the Interface capture slice size.
4. Captured traffic is only available to users without Monitored Element Group restrictions to a Monitored Element Group including the desired InfiniStream application interface. If no Monitored Element Group restrictions are associated with a role, that role has access to all interfaces.

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

8.1 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 12 - Threats and Assumptions to Security Objectives Mapping

	O.AUDIT	O.MANAGE	O.SELECT	O.TOE_ACCESS	O.TRUNCATE	OE.COMM	OE.ENVIRON	OE.INFO_STORAGE	OE.INSTALL	OE.NETWORK	OE.NOEVILADMIN	OE.OS_PROTECTION	OE.TIME_STAMP
A.ENVIRON							X						
A.FIREWALL									X				
A.INSTALL									X				
A.NETWORK										X			
A.NOEVILADMIN											X		
T.COMDIS			X		X							X	
T.COMINT								X					
T.COMMS						X							
T.LOSSOF								X					
T.MISCFG		X											
T.NOHALT						X	X						
T.TSF_ COMPROMISE		X										X	
T.UNAUTHACCESS	X			X		X							X
T.UNSECURE_ENVIR ONMENT									X				

8.1.1 Rationale Showing Threats to Security Objectives

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

Table 13 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.COMDIS	**O.TRUNCATE** helps to mitigate this threat by providing a means to limit the

T.TYPE	Security Objectives Rationale
	number of bytes captured for each data packet thereby never capturing sensitive payload data. **O.SELECT** helps mitigate this threat by providing a means to select only certain network traffic that can be captured. **OE.OS_PROTECTION** contributes to countering this threat by ensuring that the OS can protect itself from users within its control. If the OS could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the executable code of the TOE.
T.COMINT	**OE.INFO_STORAGE** contributes to mitigating this threat by controlling modification of data.
T.COMMS	**OE.COMM** contributes to mitigating this threat by specifying that the environment will protect communications between TOE components thereby limiting access to TOE and user data during transmission.
T.LOSSOF	**OE.INFO_STORAGE** contributes to mitigating this threat by controlling deletion of system data records. **O.MANAGE** contributes to mitigating this threat by providing the mechanism that only allows users with appropriate privileges the ability to delete information collected by the TOE**.** **O.TOE_ACCESS** contributes to mitigating this threat by providing the mechanism that limits access to information collected by the TOE to authorised users.
T.MISCFG	**O.MANAGE** contributes to mitigating this threat by providing the mechanism that only allows users with appropriate privileges the ability to configure the TOE.
T.NOHALT	**OE.ENVIRON** contributes to countering this threat by specifying that the administrator must install the TOE in a physically secure environment with limited access. **OE.COMM** contributes to countering this threat by limited the communication channels and specifying that the environment will protect communications between TOE components.
T.TSF_COMPROMISE	**O.MANAGE** is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions. **OE.OS_PROTECTION** contributes to countering this threat by ensuring that the OS can protect itself from users within its control. If the OS could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the executable code of the TOE.
T.UNAUTHACCESS	**O.AUDIT**contributes to mitigating this threat by auditing actions performed by authorised users and provides visibility of audit logs. **O.TOE_ACCESS** mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorised users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of an unauthorised user attempting to login and masquerade as an authorised user. **OE.COMM** mitigates this threat by protecting TSF data from disclosure when it is transferred between distributed components of the TOE. **OE.TIME_STAMP** contributes to mitigating this threat by providing a time stamp that can be included in the audit records.
T.UNSECURE_ENVIRONMENT	**OE.INSTALL** explains how firewall separation of TOE components contributes to security of communication.

8.1.2 Rationale Showing Assumptions to Environment Security Objectives

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

Table 14 - Assumptions to Security Objectives Rationale

A.TYPE	Environment Security Objective Rationale
A.ENVIRON	**OE.ENVIRON** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.FIREWALL	**OE.INSTALL** addresses this assumption by requiring the administrator to configure per guidance documentation. The guidance instructs the Administrator to configure a firewall and create an ACL.
A.INSTALL	**OE.INSTALL** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.NETWORK	**OE.NETWORK** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.NOEVILADMIN	**OE.NOEVILADMIN** addresses this assumption by restating it as an objective for the Administrator to satisfy.

8.2 Security Requirements Rationale

8.2.1 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 15 - SFRs to Security Objectives Mapping

	O.AUDIT	O.MANAGE	O.SELECT	O.TOE_ACCESS	O.TRUNCATE
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAR.1	X				
FDP_ACC.1				X	
FDP_ACF.1				X	
FDP_IFC.1			X		X
FDP_IFF.1			X		X
FIA_AFL.1				X	
FIA_ATD.1				X	
FIA_SOS.1				X	
FIA_UAU.2				X	
FIA_UAU.7				X	
FIA_UID.2				X	
FIA_USB.1				X	
FMT_MOF.1		X			
FMT_MSA.1		X			
FMT_MSA.3		X			
FMT_MTD.1		X			
FMT_SMF.1		X			

	O.AUDIT	O.MANAGE	O.SELECT	O.TOE_ACCESS	O.TRUNCATE
FMT_SMR.1		X			

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

Table 16 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.AUDIT	**FAU_GEN.1** defines the events that will cause audit records to be generated. **FAU_GEN.2** requires that the audit records include the userid of the user causing the event to occur. **FAU_SAR.1** allows visibility to audit logs to all authorised users.
O.MANAGE	**FMT_MOF.1** requires that the ability to use particular TOE capabilities be restricted to the users with appropriate permissions. **FMT_MSA.1** requires that the ability to perform operations on security attributes be restricted to users with appropriate permissions. **FMT_MSA.3 (1) and (2)** defines appropriate default security attributes. **FMT_MTD.1** requires that the ability to manipulate TOE content is restricted to users with appropriate role assignment. **FMT_SMF.1** defines the specific security management functions to be supported. **FMT_SMR.1** maintains the five predefined user roles and associates users to those roles.
O.SELECT	**FDP_IFC.1** defines an information flow control policy to monitored elements **FDP_IFF.1**defines the selection of what network traffic or what type of network traffic is to be captured based on attributes selected.
O.TOE_ACCESS	**FIA_AFL.1** requires the TOE to lock out accounts experiencing an administrator configured number of failed authentication attempts, which mitigates against brute force password attacks. **FIA_ATD.1** defines the attributes of users, including a user ID that is used by the TOE to determine a user's identity and enforce what type of access the user has to the TOE (e.g., the TOE associates a user ID with any permissions they have). **FIA_SOS.1** defines the minimum password requirements for the TOE. **FIA_UID.2** requires that a user be identified to the TOE in order to access to anything. **FIA_UAU.2** requires that a user be authenticated by the TOE before accessing anything. **FIA_UAU.7** provides that the authentication data provided by the user is not echoed back in plaintext, thus serving to protect that data. **FIA_USB.1** defines the security attributes bound to a session when I&A is successful. **FDP_ACC.1 and FDP_ACF.1** define security policies based on subject and object attributes and allowed operations to access information protected by the TOE.
O.TRUNCATE	**FDP_IFC.1** defines an information flow control policy to monitored elements. **FDP_IFF.1** defines the amount of network traffic that is to be captured and stored based on a selectable number of bytes per data packet, preventing the capturing of sensitive data.

8.2.2 Security Assurance Requirements Rationale

8.2.2.1 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL3+ from part 3 of the Common Criteria.

8.3 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 17 - SFRs to TOE Security Functions Mapping

	Audit Generation	Identification and Authentication	Security Management	User Data Protection
FAU_GEN.1	X			
FAU_GEN.2	X			
FAU_SAR.1	X			
FDP_ACC.1				X
FDP_ACF.1				X
FDP_IFC.1				X
FDP_IFF.1				X
FIA_AFL.1		X		
FIA_ATD.1		X		
FIA_SOS.1			X	
FIA_UAU.2		X		
FIA_UAU.7		X		
FIA_UID.2		X		
FIA_USB.1		X		
FMT_MOF.1			X	
FMT_MSA.1			X	
FMT_MSA.3(1)			X	
FMT_MSA.3(2)			X	
FMT_MTD.1			X	

	Audit Generation	Identification and Authentication	Security Management	User Data Protection
FMT_SMF.1			X	
FMT_SMR.1			X	

Table 18 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1	**Audit Generation** – The SF restates the audit event records that are generated along with their contents.
FAU_GEN.2	**Audit Generation** – Audit event records include the user ID of the user that caused the event to occur (when applicable).
FAU_SAR.1	**Audit Generation-** Ability to review audit log by all authorised users.
FDP_ACC.1	**User Data Protection –** User access to captured data is restricted.
FDP_ACF.1	**User Data Protection -** User access to captured data is restricted by Monitored Element Group Restrictions.
FDP_IFC.1	**User Data Protection –** Capturing of network traffic is restricted.
FDP_IFF.1	**User Data Protection -** Capturing of network traffic is restricted by the status of the Selective Recording per application setting and the Slice Size.
FIA_AFL.1	**Identification and Authentication** – Repeated authentication failures result in the user account being locked out for a period of time.
FIA_ATD.1	**Identification and Authentication** – User Security attributes including password, monitored element group restrictions, user slice size, and role(s) are maintained and tied to the user id.
FIA_SOS.1	**Security Management** – All configured passwords must adhere to the strength of secret requirements.
FIA_UAU.2	**Identification and Authentication** – Successful authentication is required before users gain access to any other functions.
FIA_UAU.7	**Identification and Authentication** – Only asterisks are displayed while the password is being entered.
FIA_UID.2	**Identification and Authentication** - Successful identification is required before users gain access to any other functions.
FIA_USB.1	**Identification and Authentication** – Upon successful identification, the specified security attributes are bound to the user session.
FMT_MOF.1	**Security Management** – Roles with the privilege to configure Global Settings may disable and enable this function.
FMT_MSA.1	**Security Management** - Users with the required privilege may perform the operations on the specified security attributes.
FMT_MSA.3(1)	**Security Management** - Users with the user permission to manage user accounts may change the assigned attributes. The default values are permissive because all traffic is captured.
FMT_MSA.3(2)	**Security Management** - Users with the user permission to configure capture ports may change the assigned attributes. The default values are restrictive because user slice size is defined based on user role assignment.
FMT_MTD.1	**Security Management** - Users with the required privilege may perform the operations on the specified TSF data.

SFR	SF and Rationale
FMT_SMF.1	**Security Management** – The administrative interface includes the ability to manage user accounts, Monitored Elements Groups, and Selective Recording per application.
FMT_SMR.1	**Security Management** – The five predefined roles are maintained. Users are associated to a predefined role.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Section 7.4 Protection Profile Rationale.