Network General Sniffer InfiniStream Enterprise Security Target

January 17, 2007

Version 9

About Network General Corporation

Network General™ is a leading provider of IT management solutions designed to integrate and simplify IT management and troubleshooting across IT domains, assuring the delivery of IT services. The Network General portfolio consists of innovative software solutions and intelligent appliances that monitor and manage all elements of the IT infrastructure including network devices, applications, and servers, while simultaneously delivering a correlated view of the health of the business service. Network General's solutions provide IT professionals with an end-to-end correlated view of the performance and availability of critical business services and the underlying network infrastructure. For more information on Network General, a privately-held company based in San Jose, California, dial +1-408-571-5000 or go to www.networkgeneral.com.

DOCUMENT INTRODUCTION

Prepared By:

COACT, Inc.
9140 Guilford Road, Suite N
Columbia, Maryland 21046-2587

Prepared For:

Network General
178 E. Tasman Drive, Suite 101
San Jose, CA 95134, USA

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Sniffer InfiniStream Enterprise V3.0 Service Pack 1 (MR7). 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	
	January 26, 2006	Initial Release
1	January 30, 2006	Address evaluation comments
2	May 15, 2006	Address Policy 10 comments
3	July 19, 2006	Remove audit, other corrections
4	July 21, 2006	Updated figure 1
5	August 11, 2006	Remove fail-over, other corrections
6	August 14, 2006	Tables were updated to complete the removal of fail-over & Clarified difference between Admin/Root
7	October 16, 2006	Minor corrections, clarified stream access control granularity
8	November 22, 2006	Replaced COACT Logo with Network General Logo, minor corrections.
9	January 17, 2007	Removed Draft Watermark.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CC ..... Common Criteria
EAL2 ..... Evaluation Assurance Level 2
IT ..... Information Technology
NIAP ..... National Information Assurance Partnership
PP ..... Protection Profile
SF ..... Security Function
SFP ..... Security Function Policy
SOF ..... Strength of Function
ST ..... Security Target
TOE ..... Target of Evaluation
TSC ..... TSF Scope of Control
TSF ..... TOE Security Functions
TSFI ..... TSF Interface
TSP ..... TOE Security Policy

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Sniffer InfiniStream Enterprise (Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Console Software, Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Capture Engine Software, Sniffer Enterprise Administrator 4.1 (MR2) Software, Sniffer Enterprise Visualizer 4.1 (MR2) Software). The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.2*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all international interpretations through February 10, 2006. National Information Assurance Partnership (NIAP) interpretations have been selectively incorporated. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Network General Sniffer InfiniStream Enterprise Security Target, revision number 9, dated January 17, 2007

1.2 TOE Reference

Sniffer InfiniStream Enterprise (Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Console Software, Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Capture Engine Software, Sniffer Enterprise Administrator 4.1 (MR2) Software, Sniffer Enterprise Visualizer 4.1 (MR2) Software)

1.3 Evaluation Assurance Level

EAL3 (Evaluation Assurance Level 3) augmented by ALC_FLR.1 from the *Common Criteria for Information Technology Security Evaluation, Version 2.2*.

1.4 Keywords

Sniffer, InfiniStream, Enterprise Management, Capture Engine, Enterprise Administrator, Enterprise Visualizer, data mining, frame slicing, Capture Ports, store, stream.

1.5 TOE Overview

This Security Target defines the requirements for the Sniffer InfiniStream Enterprise system, which consists of four components, the InfiniStream Capture Engine (ICE) v3.0 Service Pack 1 (MR7), the Sniffer Enterprise Administrator (ADMINISTRATOR) v4.1 (MR2), the Sniffer InfiniStream Console (CONSOLE) v3.0 Service Pack 1 (MR7), and the Sniffer Enterprise Visualizer (VISUALIZER) v4.1 (MR2).

The TOE is a network management system that is capable of capturing and storing network traffic used for network(s) monitoring, network(s) performance measurements and management and network(s) problem solving. The TOE provides user GUIs that can display the captured information or a subset of the captured information in graphical and statistical representations. The displayed information can be tailored to show the gathered information in a variety of methods, such as date/time, LAN segment, IP pair, TCP/UDP port, or a combination of these methods. The TOE is capable of providing real-time analysis, point-in-time analysis, back-in-time analysis and historical analysis of captured network traffic.

The TOE consists of four components, the CAPTURE ENGINE, the ADMINISTRATOR, the CONSOLE, and a VISUALIZER. The CAPTURE ENGINE component captures the network traffic, the ADMINISTRATOR manages the CAPTURE ENGINE and VISUALIZER, the CONSOLE is the user interface into the system, and the VISUALIZER provides both canned and user created reporting capabilities.

The TOE is capable of limiting the amount of bytes captured for each data packet and can also be tailored to capture only specific network traffic based on, IP address, MAC address, protocol, TCP port, UDP port and VLAN ID.

1.5.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the Sniffer InfiniStream Enterprise (Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Console Software, Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Capture Engine Software, and Sniffer Enterprise Administrator 4.1 (MR2) Software, Sniffer Enterprise Visualizer 4.1 (MR2) Software) to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.6 Common Criteria Conformance

The Sniffer InfiniStream Enterprise (Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Console Software, Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Capture Engine Software, Sniffer Enterprise Administrator 4.1 (MR2) Software, Sniffer Enterprise Visualizer 4.1 (MR2) Software) is compliant with the Common Criteria (CC) Version 2.2, functional requirements (Part 2) extended and assurance requirements (Part 3) augmented for EAL3.

1.7 Protection Profile Conformance

The Sniffer InfiniStream Enterprise (Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Console Software, Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Capture Engine Software, Sniffer Enterprise Administrator 4.1 (MR2) Software, Sniffer Enterprise Visualizer 4.1 (MR2) Software) does not claim conformance to any registered Protection Profile.

1.8 Conventions

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 letters in parentheses following the component or element (e.g., FAU_ARP.1a).

1.9 Terminology

CAPTURE – the act of capturing network traffic via a Capture Port.

CAPTURE PORT – An InfiniStream Capture Engine network interface operating in promiscuous mode to capture all network traffic.

CAPTURE FILTER – A filter that specifies what type of network traffic that will be captured.

FRAME SLICING – The process of uniformly truncating all selected frames to a specific length measured from the beginning of the frame.

PRIVACY FILTER – A filter that limits access to each data packet that has been captured and stored based on byte count.

RESOURCES – Either a Capture Engine or a VISUALIZER.

STREAM – The network traffic that is stored after being captured from a single Capture Port, filtered, and frame sliced. Streams are FIFO buffers that store captured traffic up to the size limits of the storage on the InfiniStream Capture Engine.

OPEN STREAM – A stream that has been selected by a user and is available for analysis.

MINED STREAM – Same as open stream.

STORE – The proprietary Capture Engine file system that provides persistent storage for all captured packet data and statistics.

MINING PORT– Interface used to manage, configure, and access the CAPTURE ENGINE.

CHAPTER 2

2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Version

Sniffer InfiniStream Enterprise is comprised of the following components, each with its own specific version: Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Console Software, Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Capture Engine Software, Sniffer Enterprise Administrator 4.1 (MR2) Software, and Sniffer Enterprise Visualizer 4.1 (MR2) Software.

2.2 Sniffer InfiniStream Enterprise (TOE) Description

The Sniffer InfiniStream Enterprise is a set of software components executed on Linux and Windows platforms. The TOE is comprised of four parts: the Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Console Software, the Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Capture Engine Software, Sniffer Enterprise Administrator 4.1 (MR2) Software (interface to Sniffer InfiniStream 3.0 Service Pack 1 (MR7)), the Sniffer Enterprise Visualizer 4.1 (MR2) Software (interface to Sniffer InfiniStream 3.0 Service Pack 1 (MR7)). Sniffer InfiniStream Enterprise collectively 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.

2.2.1 Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Console Software

The Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Console Software (CONSOLE) provides statistics display, data mining, and Expert analysis of network traffic captured by the Sniffer InfiniStream Capture Engine. The CONSOLE provides the mechanism to connect to an InfiniStream Capture Engine(s) and select one or more network traffic flows, called streams, for analysis. Once the CONSOLE is connected to a Capture Engine, the CONSOLE allows for the retrieval, analysis, and decode of captured traffic. The CONSOLE allows the captured streams to be viewed graphically and statistically, and analyzed using the Expert Analyzer. The Expert Analyzer identifies and diagnoses network problems and saves mined data to capture files, which are stored on the Console.

The CONSOLE application executes on any Windows 2000, Windows XP, or Windows 2003 platforms. The hardware, Windows operating system, and all 3rd party software are excluded from the TOE. The CONSOLE application runs on a general purpose workstation platform that does not need to be dedicated to this application.

2.2.2 Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Capture Engine Software

The Sniffer InfiniStream 3.0 Service Pack 1 (MR7) Capture Engine Software application (CAPTURE ENGINE) captures a continuous flow of network traffic, called a stream, for each Capture Port and saves the captured stream to disk. Once saved, the stream can be searched, or mined, using custom search criteria. Additionally, using capture filters it is possible to filter unwanted network packets from the stream during the capture process. The CAPTURE ENGINE supports the following network ports: Capture Ports (up to 8), Mining Port and Technician Port. The Capture Ports are high-performance interfaces that

operate in promiscuous mode and capture network traffic from gigabit or Fast Ethernet segments; the transmit function of these adapters is disabled. The Mining Port is used to communicate with the InfiniStream Sniffer Console. The Technician Port is not used in the evaluated configuration.

The CAPTURE ENGINE 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.

2.2.3 Sniffer Enterprise Administrator 4.1 (MR2) Software

The Sniffer Enterprise Administrator Software (ADMINISTRATOR) provides centralized management, administration, and security for CAPTURE ENGINE and the Sniffer Enterprise Visualizer. ADMINISTRATOR provides single sign-on capabilities; multiple resource configuration management; central authentication; role based administration; and tracking and enforcement of access rights, alarms, and data replication and redundancy.

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

2.2.4 Sniffer Enterprise Visualizer 4.1 (MR2) Software

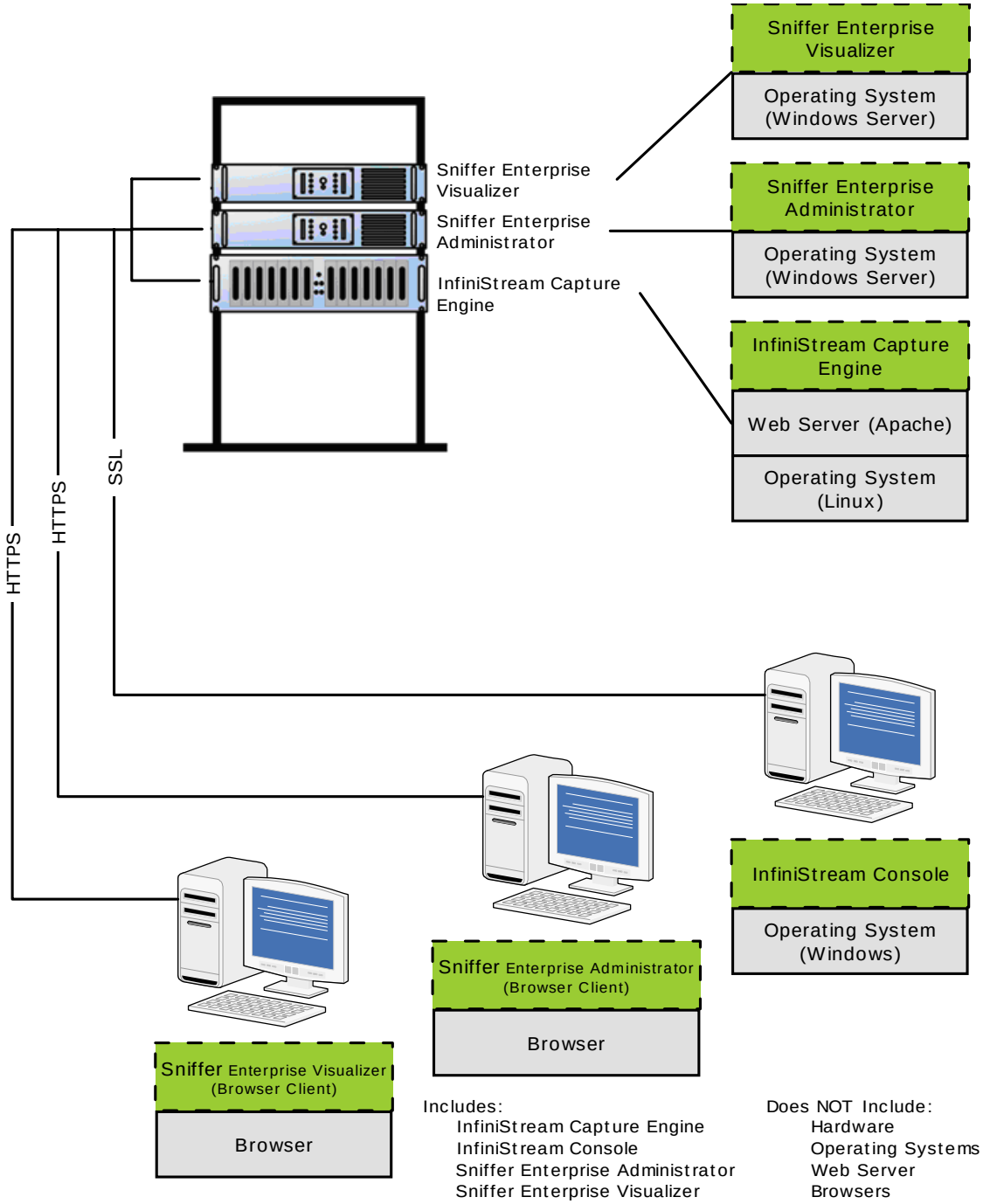
The Sniffer Enterprise Visualizer Software (VISUALIZER) provides both canned reports and user created reports on statistical information about captured network traffic. The VISUALIZER maintains two roles, administrator and user, but has no other security relevant functionality with regards to the TOE. It is included in the TOE because it is an integral part of the Sniffer Enterprise system.

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

2.3 Physical Boundary

The TOE is a set of software applications that execute on Linux and Windows platforms. The TOE is divided into four primary components, the CAPTURE ENGINE, the ADMINISTRATOR, the CONSOLE, and the VISUALISER.

Figure 1 - Physical Boundary



2.4 Logical Boundary

The TOE consists of four software applications that execute on four different hardware platforms. These four software applications provide identification and authentication, capture filtering, frame slicing, privacy filtering, security management, user data protection, and self-protection.

2.4.1 TSF Data

Identification and Authentication on the components is performed using the following TSF (authentication) data: user ID and password.

The TOE maintains the following roles:

A) Sniffer Enterprise Administrator

1) Administrator - access to all management functions.

2) NetworkUser - no management access and the ability to connect to a configured list of resources.

B) InfiniStream Capture Engine

1) Root – the primary administrative role with unrestricted access to all data and functionality, including Linux “root” privileges on the CAPTURE ENGINE, access to CAPTURE ENGINE configuration utilities, and immunity from Privacy Filters during data mining activities.

2) Admin – a secondary administrative role with access to capture data and statistics but with administrative access limited to the CONSOLE’S administrative functions.

3) Console – a non-administrative role with access limited to capture data mining and statistics.

4) Monitor – a non-administrative role with access limited to capture data statistics.

C) Sniffer Enterprise Visualizer

1) Administrator - access to all management functions except user management (this function is performed on Sniffer Enterprise Administrator).

2) Regular User - no management access and full access to statistics.

3) Monitor - access the Visualizer Dashboard only.

The TOE maintains a domain mapping for CAPTURE ENGINES and VISUALIZERS. The domains are groupings of those resources for ease of associating access permissions to users.

Each user ID has the following TSF data associated with it: role and associated domains.

The TOE maintains a list of IP addresses that are permitted to operate as CONSOLES. When a CONSOLE communicates with another component, the communication is rejected if the originating address is not included in the list.

Capture filters specify what network traffic is filtered. Frame slicing rules specify the amount of data from each network packet that is stored. Privacy filters specify the amount of data in stored network packets that may be mined.

2.4.2 Security Attributes

For each user, the per-component-type role and associated domains determine access privileges.

Captured network traffic has the following security attributes that are dynamically determined:

1) *Presumed Virtual Circuit*
2) *Presumed IP Address*
3) *Presumed MAC Address*
4) *Presumed Protocol*
5) *Presumed TCP Port*
6) *Presumed UDP Port*
7) *Presumed VLAN ID*

2.4.3 User Data

The TOE is a network management tool that captures and stores network traffic (streams) used for monitoring network performance and network problem solving. This captured and stored traffic has no real meaning to the TSF but is protected by the TSF by limiting what is captured, what is accessed and by whom.

2.4.4 Rationale for Non-Bypassability and Separation

The TOE is a set of applications that execute on top of an underlying system that includes hardware and software required for operation. Therefore responsibility for non-bypassability and separation are split between the TOE and IT Environment.

The TOE provides strictly controlled functionality to the users within the TSC. By limiting the functionality, the TSF is protected from corruption or compromise from users within the TSC. The TOE interfaces are separated into 2 categories – security enforcing and security supporting. Security enforcing interfaces invoke the TSF and ensure that all enforcement functions complete successfully before allowing the user invoked action to proceed. Security supporting interfaces are designed and implemented such that the TSF cannot be interfered with via those interfaces (i.e., they cannot manipulate TSF data or affect the behaviour of the TSF). Multiple simultaneous users are supported, and the TOE associates distinct attributes and privileges with each process/user to restrict their access appropriately. Multiple sessions are instantiated as separate operating system processes and it is the responsibility of the OS to ensure non-interference between the processes.

The OS and hardware support non-bypassability by ensuring access to protected resources passes through the TOE, or is limited to access within the OS scope of control according to the security policies stated for the OS. The hardware and OS provide separate process spaces in which the TOE executes; these process spaces are protected from interference from other processes except through the defined TOE interfaces.

2.5 Evaluated Configuration

The evaluated configuration of the TOE is described in the following table.

Table 1 - Evaluated Configuration

Component	Version	Quantity
InfiniStream Sniffer Console	3.0 Service Pack 1 (MR7)	1 or more
InfiniStream Capture Engine	3.0 Service Pack 1 (MR7)	1 or more
Sniffer Enterprise Administrator	4.1 (MR2)	1
Sniffer Enterprise Visualizer	4.1 (MR2)	1 or more

The following table summarizes the minimum hardware and software requirements for each of the TOE components.

Table 2 - Minimum Hardware and Software Requirements

Component	Minimum Hardware Requirements	Minimum Software Requirements
Sniffer Enterprise Administrator	2.0 GHz Dual Xeon Processor 512K DDR SDRAM 146GB Ultra 320 SCSI Drive Standard Ethernet Gigabit 100/1000 with Intel Dual Port Gigabit Ethernet (10/100/1000)	Windows 2003 Standard Edition Service Pack 1 Tomcat Web Server v5.0.28 MySQL Database v5.0.18 Sniffer Enterprise Administrator v4.1 (MR2)
Sniffer Enterprise Visualizer	3.2Ghz Dual Xeon Processors 2 GB PC 1600 DDR SDRAM 800 MHz Front-side bus speed 1 MB Internal cache 2 x 147 GB 10K RPM Disks configured in RAID 0 as C: Drive	Windows Server 2003 Standard Edition SQL Server 2000 Standard Edition Tomcat Web server v5.0.28 and Servlet Engine Axis for Web services Adobe SVG Viewer v3.0.3 Sniffer Enterprise Visualizer v4.1 (MR2)
InfiniStream Capture Engine	Dual Intel Xeon processors with 1 MB integrated Advanced Transfer Cache up to 3.20 GHz, 533 MHz FSB, dual on board 10/100/1000 Mbps LAN ports with Intel 7501 chipset, up to 16 GB ECC, registered DDR PC 2100 at 266 MHz (133 x 2), 6 PCI-X (2 @ 133 MHz) slots with 3 separate buses. 1 76 GB SCSI Drive 1 – 300 GB Serial SATA Drive 1 10/100/100 Port for Mining 2 – 10/100/100 ports	Red Hat Linux 9 Apache Web Server v. 2.0.40 Net-SNMP v. 5.0.9 InfiniStream Capture Engine v3.0 Service Pack 1 (MR7)
InfiniStream Sniffer Console	Intel 1.2GHz Pentium 4 or higher, or Intel 1.2GHz Celeron or higher, or AMD Athlon running at 1.2GHz or higher 1 GB RAM 1GB or more of free hard disk space CD-ROM Drive VGA color monitor with 1024x768 resolution	Microsoft Windows® 2000 Professional with Service Pack 4, or Microsoft Windows XP Professional Edition with Service Pack 2 InfiniStream Sniffer Console v3.0 Service Pack 1 (MR7)

	Network adapter card with 10/100 Ethernet or Gigabit interface	

The following configuration options must be used in the evaluated configuration:

A) SSL is used to provide secure communication between the TOE components.

B) Each CAPTURE ENGINE's "fail-over to local authentication" functionality must be disabled.

2.6 Functionality Excluded from the Evaluation

A) Auditing

CHAPTER 3

3. Security Environment

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 3 - 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.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance and specific organizational 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.
A.PLATFORM	The Administrator will ensure that the platforms used to host the TOE conform to the hardware and software outlined in the administrator guidance.

3.3 Threats

The threats identified in the following subsections are addressed by the TOE and the IT environment.

Table 4 - Threats

T.Type	TOE Threats
T.UNAUTHACCESS	An authorized user may attempt to gain access to TOE and user data without proper authorization.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be modified.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected by the TOE by bypassing a security mechanism
T.COMDIS	An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected by the TOE.

T.Type	TOE Threats
T.MISCFG	An unauthorized user may change the configuration of the TOE causing the collection of data to change from its originally configured intention.
T.MODIFY	The integrity of information collected by the TOE may be compromised due to unauthorized access or destruction of the TOE data.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the TOE's data collection functionality by halting execution of the TOE.
T.COMMS	An unauthorized user may attempt to access TOE and user data during transmission from one TOE component to another TOE component.

3.4 Organisational Security Policies

No OSPs are defined by this ST.

CHAPTER 4

4. Security Objectives

This section identifies the security objectives of the TOE, the TOE's IT environment and the TOE's non-IT environment. The security objectives identify the responsibilities of the TOE, the TOE's IT environment, and the TOE's non-IT environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the IT environment are designated as *OE.objective*. Objectives that apply to the non-IT environment are designated with an *ON.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 5 - Security Objectives for the TOE

O.Type	Security Objective
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 unauthorized use.
O.PARTIAL_SELF_PROTECT	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
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 captured, stored or revealed to TOE users. .(Frame Slicing)
O.SELECT	The TOE provides a means to select only certain network traffic or certain types of network traffic is captured and stored. (Capture Filter)
O.PRIVACY	The TOE provides a means to truncate mined network traffic so that sensitive information is not revealed to TOE users.(Privacy Filter)
O.EXPORT	The TOE provides a means to export mined network traffic to the IT Environment for follow-on analysis.

4.2 Security Objectives for the IT Environment

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

Table 6 - 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.INFO_STORAGE	The IT Environment will provide secure storage for system data generated by the TOE.
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 unauthorized disclosure through its own interfaces.

4.3 Security Objectives for the Non-IT Environment

The TOE's Non-IT environment must satisfy the following objectives.

Table 7 - Security Objectives for the Non-IT Environment

ON.Type	Security Objectives for the Non-IT Environment
ON.ENVIRON	The Administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
ON.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
ON.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.
ON.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.
ON.PLATFORM	The Administrator will ensure that the platforms used to host the TOE conform to the hardware and software outlined in the administrator guidance.

CHAPTER 5

5. IT 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.

5.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.2* with the exception of completed operations.

5.1.1 User Data Protection (FDP)

5.1.1.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1a The TSF shall enforce the [assignment: *VISUALIZER Access Security Policy*] on [assignment: *VISUALIZER users (X=Administrator, O=Administrator and Regular User roles, Z=All roles, objects as described in the table, operations as described in the table*].

Table 8 - VISUALIZER SP Detail

Object Type	View	Edit	Purge	Define	Set	Create	Delete	Add	Configure
Database Purge Settings		X							
Instant Purge Setting									X
Critical Entities							X	X	
Application Groups						X	X	X	
Client subnets				X					X
Address Groups						X			
Virtual Circuit Groups					X	X		X	
Interfaces									X
Reports	O		X	O					
Dashboard Views	Z			O					

FDP_ACC.1.1b The TSF shall enforce the [assignment: *ADMINISTRATOR Access Security Policy*] on [assignment: *ADMINISTRATOR users, objects see below, operations see below]*.

A) Subjects – ADMINISTRATOR Administrators, NetworkUsers or other non-administrative roles created by the ADMINISTRATOR administrator

B) Objects – Object types as specified in the table below.

C) Operations – Operations are specific to the object type, as specified in the following table (X = operations performed by Administrators only, O = operations performed by both administrators and NetworkUsers and other non-administrative roles created by administrators).

Table 9 - ADMINISTRATOR/RESOURCE SP Objects and Operations

Object Type	Clone	View	Connect	Filter	Save	Print	End	Export	Create	Edit	Set Permissions	Delete	Add	Configure	Sort	Add Destinations	Delete Destinations
Resources	X	O										X	X	X			
Resource List		O															
System Summary		X															
Report						X		X									
Active User		X	O				O										
Change Other User Password					X					X							
Change Your Own Password					O					O							
User Roles									X	X	X						
User List		O				X		X		X							
Users										X		X	X				
Resource Compliance Reports		X															
Domains		O									X	X	X				
Domain List															X		
Alarm Summary		X															
Alarm Monitor		X		X													
Alarm Forwarder																X	X
Alarm Severity														X			
Alarm Automation		X										X	X	X			

FDP_ACC.1.1c The TSF shall enforce the [assignment: *CAPTURE ENGINE Access Security Policy*] on [assignment: *subjects see table below, objects see table below, operations see table below*].

Table 10 - Capture Engine User Roles

Role	Associated operations	Objects
Monitor	Analyze statistical data.	Captured data
Console	Monitor role operations, and mine sliced frames.	Captured data
Admin	Console role operations; create and configure data streams;	Captured data
Root	Admin role operations, mine unsliced frames.	Captured data
Admin, Root	Configure	Capture Engine
Admin, Root	Configure	Roles
Admin, Root	Create	Alerts
Root	Mine frames without privacy filters being applied	Streams

5.1.1.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1a The TSF shall enforce the [assignment: *VISUALIZER Access Security Policy*] to objects based on the following [assignment: *subjects*: *Visualizer users; subject security attributes: role, associated domains; objects: as listed in the table in FDP_ACC.1a; object security attributes: domain*]

FDP_ACF.1.2a The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*assignment: on a VISUALIZER that is a member of the associated domains,*

A) *Operations are permitted according to the table in FDP_ACC.1a]*.

FDP_ACF.1.3a The TSF shall explicitly authorize access of subjects to objects based on the following additional rules [assignment: *the subject role is Administrator]*.

FDP_ACF1.4a The TSF shall explicitly deny access of subjects to objects based on the [assignment: *VISUALIZER does not belong to the associated domains*].

FDP_ACF.1.1b The TSF shall enforce the [assignment: *ADMINISTRATOR Access Security Policy*] to objects based on the following [assignment:

A) *Subjects: ADMINISTRATOR users*

B) *Objects: As listed in Table above*

C) *Subject Security Attributes: role*

D) *Object Security Attributes: None]*.

FDP_ACF.1.2b The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *user is allowed to perform operations on objects as listed in the table in FDP_ACC.1b]*.

FDP_ACF.1.3b The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment*: no further rules*].

FDP_ACF.1.4b The TSF shall explicitly deny access of subjects to objects based on the [assignment: *none*].

FDP_ACF.1.1c The TSF shall enforce the [assignment: *CAPTURE ENGINE Access Security Policy*] to objects based on the following [assignment:

A) *Subjects: root, admin, console, and monitor*

B) *Objects: Captured data, Capture Engine, Roles, Alerts, Streams*

C) *Subject Security Attributes: role, associated domains*

D) *Object Security Attributes: domain]*.

FDP_ACF.1.2c The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *on a CAPTURE ENGINE that is a member of the associated domains,*

A) *Operations are permitted according to the table in FDP_ACC.1c;*

B) *The amount of captured data accessed per stored network packet is limited by privacy filters].*

FDP_ACF.1.3c The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment*: no further rules*].

FDP_ACF.1.4c The TSF shall explicitly deny access of subjects to objects based on the [assignment: *CAPTURE ENGINE does not belong to the associated domains*].

5.1.1.3 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the [assignment: *CAPTURE ENGINE Access Security Policy*] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export user data without user data's associated security attributes.

5.1.1.4 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1a The TSF shall enforce the [assignment: *Stream information flow control SFP*] on [assignment: *subjects: Capture Ports, information: network packets, operation: store network packet*].

FDP_IFC.1.1b The TSF shall enforce the [assignment: *VISUALIZER Statistic flow control policy*] on [assignment: *subjects: Capture Ports, information: network packets, operations: collection of statistics on Capture Engine and transmission of collected statistics to VISUALIZER*].

5.1.1.5 FDP_IFF.1-NIAP-0407 Simple Security Attributes

FDP_IFF.1.1-NIAP-0407a The TSF shall enforce the [assignment: *Stream information flow control SFP*] based on the following types of subject and information security attributes: [assignment:

A) *Subjects: Capture Port*

B) *Subject Security Attributes: Capture Port ID*

C) *Information: Network packet*

D) *Information Security Attributes:*

1) Presumed IP Address

2) Presumed MAC Address

3) Presumed Protocol

4) Presumed TCP Port

5) Presumed UDP Port

6) Presumed VLAN ID

7) *Or any combination of the above]*.

FDP_IFF.1.2-NIAP-0407a The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *if the subject and information security attributes do not match a configured capture filter, the network packet is stored*].

FDP_IFF.1.3-NIAP-0407a The TSF shall enforce the following information flow control rules: [selection: no additional information flow control SFP rules]

FDP_IFF.1.4-NIAP-0407a The TSF shall provide the following [selection: [assignment: *the amount of data from a network packet that is stored may be limited by a frame slicing rule*]].

FDP_IFF.1.5-NIAP-0407a The TSF shall explicitly authorise an information flow based upon the following rules: [selection: [assignment: *default is no Capture Filter SFP*].

FDP_IFF.1.6-NIAP-0407a The TSF shall explicitly deny an information flow based upon the following rules: [selection: no explicit denial rules].

FDP_IFF.1.1b-NIAP-0407b The TSF shall enforce the [*VISUALIZER Statistic flow control policy*] based on the following types of subject and information security attributes: [assignment:

A) *Subjects: Capture Port*

B) *Subject Security Attributes: Capture Port ID*

C) *Information: Network packet*

D) *Information Security Attributes:*

1) *Presumed Virtual Circuit*

2) *Presumed Source IP address*

3) *Presumed Destination IP address*

4) *Presumed Protocol]*.

FDP_IFF.1.2b-NIAP-0407b The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *if the subject and information security attributes match a defined VISUALIZER policy, the statistics are updated with the information from the subject and information]*.

FDP_IFF.1.3b-NIAP-0407b The TSF shall enforce the following information flow control rules [selection: no additional information flow control SFP rules*]*.

FDP_IFF.1.4b-NIAP-0407b The TSF shall provide the following [selection: no additional SFP capabilities]

FDP_IFF.1.5-NIAP-0407b The TSF shall explicitly authorise an information flow based upon the following rules: [selection: no explicit authorise rules].

FDP_IFF.1.6-NIAP-0407b The TSF shall explicitly deny an information flow based upon the following rules: [selection: [assignment: *default is no VISUALIZER data flow*].

5.1.2 Identification and Authentication (FIA)

5.1.2.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *user ID, password, assigned domain*].

5.1.2.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a minimum 6 character password length including at least one digit [0-9]*].

5.1.2.3 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions found below*] on behalf of the user to be performed before the user is authenticated.

A) *InfiniStream Console*

1) *Access to open capture stream files located on the local CONSOLE for decoding and analysis*

2) *Selection of a component to connect to*

B) *Sniffer Enterprise Administrator*

1) *None*

C) *InfiniStream Capture Engine*

1) *None*

D) *Sniffer Enterprise Visualizer*

1) *None*

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

5.1.2.4 FIA_UAU.7 Protected Authentication Feedback

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

5.1.2.5 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow [assignment: *list-of TSF mediated actions found below*] on behalf of the user to be performed before the user is identified.

A) *InfiniStream Console*

1) *Selection of a component to connect to*

B) *Sniffer Enterprise Administrator*

1) *None*

C) *InfiniStream Capture Engine*

1) *None*

D) *Sniffer Enterprise Visualizer*

1) *None*

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

5.1.3 Security Management (FMT)

5.1.3.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: *capture filter, privacy filtering, frame slicing*] to [assignment: *root and administrator*].

5.1.3.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment: *VISUALIZER access security policy, ADMINISTRATOR access security policy, and CAPTURE ENGINE access security policy*] to restrict the ability to [selection: query, modify, delete, [assignment: *add*]] the security attributes [assignment: *described below*] to [assignment: *described below*].

A) *Sniffer Enterprise Administrator*
   1) *Resource IP address to Administrator*
   2) *Resource DNS name to Administrator*
   3) *VISUALIZER Roles to Administrator*
   4) *CAPTURE ENGINE Roles to Administrator*
   5) *Domain Assignments to Administrator*

B) *InfiniStream Capture Engine*
   1) *Capture Filtering to Admin and Root*
   2) *Privacy Filtering to Root*

C) *InfiniStream Console*
   1) *None*

D) *Sniffer Enterprise Visualizer*
   1) *None*

5.1.3.3 FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the [assignment: *Stream information flow control SFP*] to provide [selection: permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *root and CAPTURE ENGINE administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1a The TSF shall enforce the [assignment: *VISUALIZER Statistic information flow control SFP*] to provide [selection: restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2a The TSF shall allow the [assignment: *VISUALIZER administrator*] to specify alternative initial values to override the default values when an object or information is created.

5.1.3.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: *create*]] the [assignment: *user ID, password, domain, role on ADMINISTRATOR]* to *[assignment: administrator*].

5.1.3.5 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: *creating roles, creating user accounts, assigning users to roles, assigning passwords, access control, privacy filtering, session establishment, capture filtering*].

5.1.3.6 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [assignment*: the authorized identified roles as described below*].

D) *InfiniStream Console*

1) *None*

E) *Sniffer Enterprise Administrator*

1) *Administrator*

2) *NetworkUser*

F) *InfiniStream Capture Engine*

1) *Admin*

2) *Root*

3) *Monitor*

4) *Console*

G) *Sniffer Enterprise Visualizer*

1) *Administrator*

2) *Regular User*

3) *Monitor*

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

5.1.4 Protection of the TSF (FPT)

5.1.4.1 FPT_RVM_SFT.1 Non-Bypassability of the TSP for Software TOEs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM that can be addressed by the TOE. See FPT_RVM_OS (levied on the IT Environment) for the remaining functionality.

FPT_RVM_SFT.1.1: The TSF, when invoked shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed

5.1.4.2 FPT_SEP_SFT.1 TSF Domain Separation for Software TOEs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP that can be addressed by the TOE. See FPT_SEP_OS (levied on the IT Environment) for the remaining functionality.

FPT_SEP_SFT.1.1: The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_SFT.1.2: The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5 TOE Access (FTA)

5.1.5.1 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: *CONSOLE IP Address*].

5.2 Security Requirements for the IT Environment

5.2.1 User Data Protection (FDP)

5.2.1.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the *IT Environment SFP* on

A) Subjects: IT Environment users;

B) Objects:

1) InfiniStream Capture Engine stream files;

2) Sniffer Enterprise Visualizer database;

3) Sniffer Enterprise Administrator database;

C) Operations: read, write, delete.

5.2.1.2 FDP_ACF.1 Security Attribute Based Access Control

Application Note: This SFR addresses interactions between the subjects and objects via IT Environment (non-TOE) interfaces. Interactions that occur through the TOE interfaces are addressed by the SFRs levied upon the TOE.

FDP_ACF.1.1 The TSF shall enforce the *IT Environment SFP* to objects based on the following:

A) InfiniStream Capture Engine users: superuser privilege;

B) Sniffer Enterprise Visualizer users: administrator privilege;

C) Sniffer Enterprise Administrator users: administrator privilege;

D) InfiniStream Capture Engine stream files: none;

E) Sniffer Enterprise Visualizer database: none;

F) Sniffer Enterprise Administrator database: none.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *the rules specified in the following table.*

Table 11 - IT Environment SFP Permitted Operations

Platform	Privilege	CAPTURE ENGINE Stream Files	VISUALIZER Database	ADMINISTRATOR Database
CAPTURE ENGINE	Superuser	Read, Delete	n/a	n/a
	Not superuser	None	n/a	n/a
VISUALIZER	Administrator	n/a	Read, Write, Delete	n/a
	Not Administrator	n/a	None	n/a
ADMINISTRATOR	Administrator	n/a	n/a	Read, Write, Delete
	Not Administrator	n/a	n/a	None

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no additional rules*.

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

5.2.2 Protection of the TOE

5.2.2.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 **Refinement:** The **IT Environment** shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

5.2.2.2 FPT_RVM_OS.1 Non-Bypassability of the TSP for OSs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM supplied by the OS and hardware in support of the overall FPT_RVM functionality. See FPT_RVM_SFT (levied on the TOE) for the remaining functionality.

FPT_RVM_OS.1.1 The security functions of the host OS shall ensure that host OS security policy enforcement functions are invoked and succeed before each function within the scope of control of the host OS is allowed to proceed.

5.2.2.3 Domain separation for OSs (FPT_SEP_OS)

FPT_SEP_OS.1 TSF Domain Separation for OSs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP supplied by the OS and hardware in support of the overall FPT_SEP functionality. See FPT_SEP_SFT (levied on the TOE) for the remaining functionality.

FPT_SEP_OS.1.1 The security functions of the host OS shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OS.

FPT_SEP_OS.1.2 The security functions of the host OS shall enforce separation between the security domains of subjects in the scope of control of the host OS.

5.3 Security Assurance Requirements

The TOE meets the assurance requirements for EAL3+. The augmentation is ALC_FLR.1. These requirements are summarised in the following table.

Table 12 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.3	Configuration Items and Authorization Controls
Configuration Management	ACM_SCP.1	TOE Configuration Management Coverage
Delivery and Operation	ADO_DEL.1	Delivery Procedures
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.2	Security Enforcing High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Life-Cycle Support	ALC_DVS.1	Identification of Security Measures
Life-Cycle Support	ALC_FLR.1	Flaw Remediation
Tests	ATE_COV.2	Analysis of Coverage
Tests	ATE_DTP.1	Testing High Level Design
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_MSU.1	Examination of Guidance
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

5.4 Strength of Function for the TOE

The only probabilistic or permutational mechanism in the product is the password mechanism used to authenticate users (FIA_SOS.1). The SOF for this mechanism is SOF-Basic. This SOF is appropriate for the intended environment of the TOE with threat agents of low attack potential.

5.5 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies.

5.5.1 TOE Security Functional Component Hierarchies and Dependencies

The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 13 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FDP_ACC.1a	N/A	FDP_ACF.1a	Satisfied
FDP_ACC.1b	N/A	FDP_ACF.1b	Satisfied
FDP_ACC.1c	N/A	FDP_ACF.1c	Satisfied
FDP_ACF.1a	N/A	FDP_ACC.1	Satisfied by FDP_ACC.1a
FDP_ACF.1b	N/A	FDP_ACC.1	Satisfied by FDP_ACC.1b
FDP_ACF.1c	N/A	FDP_ACC.1	Satisfied by FDP_ACC.1c
FDP_ETC.1	N/A	FDP_ACC.1c	Satisfied
FDP_IFC.1a	N/A	FDP_IFF.1	Satisfied by FDP_IFF.1-NIAP-0407a
FDP_IFC.1b	N/A	FDP_IFF.1	Satisfied by FDP_IFF.1-NIAP-0407b
FDP_IFF.1-NIAP0407a	N/A	FDP_IFC.1 FMT_MSA.3	Satisfied by FDP_IFC.1a Satisfied by FMT_MSA.3
FDP_IFF.1-NIAP0407b	N/A	FDP_IFC.1 FMT_MSA.3	Satisfied by FDP_IFC.1b Satisfied by FMT_MSA.3a
FIA_ATD.1	N/A	N/A	N/A
FIA_SOS.1	N/A	N/A	N/A
FIA_UAU.1	N/A	FIA_UID.1	Satisfied
FIA_UAU.7	N/A	FIA_UAU.1	Satisfied
FIA_UID.1	N/A	N/A	N/A
FMT_MOF.1	N/A	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_MSA.1	N/A	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied Satisfied
FMT_MSA.3	N/A	FMT_MSA.1 FMT_SMR.1	Satisfied Satisfied
FMT_MSA.3a	N/A	FMT_MSA.1 FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	N/A	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	N/A	N/A	N/A
FMT_SMR.1	N/A	FIA_UID.1	Satisfied
FPT_RVM.SFT.1	N/A	N/A	Satisfied
FPT_SEP_SFT.1	N/A	N/A	Satisfied
FTA_TSE.1	N/A	N/A	N/A

5.5.2 IT Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified IT Environment SFRs include the appropriate hierarchy and dependencies.

The following table lists the IT Environment SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 14 - IT Environment SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FDP_ACC.1	None	FDP_ACF.1	Satisfied
FDP_ACF.1	None	FDP_ACC.1, FMT_MSA.3	Satisfied Not addressed per PD-0091
FPT_ITT.1	None	None	N/A

SFR	Hierarchical To	Dependency	Rationale
FPT_RVM_OS.1	None	None	N/A
FPT_SEP_OS.1	None	None	N/A

CHAPTER 6

6. TOE Summary Specification

6.1 Security Functions

6.1.1 Identification and Authentication

During normal operations the Sniffer InfiniStream Enterprise uses the I&A functions of the ADMNISTRATOR. The CONSOLE is the primary interface into the CAPTURE ENGINE. A user selects a stream of captured data and is prompted to enter user ID and password to the CAPTURE ENGINE containing the selected stream. The user ID and password is transmitted to the CAPTURE ENGINE and the CAPTURE ENGINE redirects the user ID and password to the ADMINISTRATOR assigned to manage that CAPTURE ENGINE. The ADMINISTRATOR performs the I&A function and if successful notifies the CAPTURE ENGINE with role information and allows the connection between the CONSOLE and CAPTURE ENGINE to continue. The same process is followed for log in attempts to the VISUALIZER.

If a CAPTURE ENGINE fails to receive a response to an authentication request from the ADMINISTRATOR, the CAPTURE ENGINE fails to login the user.

If a VISUALIZER fails to receive a response to an authentication request from the ADMINISTRATOR, the VISUALIZER fails to login the user.

6.1.2 Security Management

The Sniffer InfiniStream Enterprise system performs 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 system limits the access and operations of certain features of the product, limits access to user data, maintains and manages roles, and performs this by managing security attributes associated with users, user data, and specifying default values for certain security attributes necessary for the secure execution of security policies.

The Sniffer InfiniStream Enterprise system maintains user roles throughout all TOE components with the exception of the CONSOLE application. The CAPTURE ENGINE maintains the roles Root, Admin, Console, and Monitor. The ADMINISTRATOR maintains the roles Administrator and NetworkUser. The VISUALIZER maintains the roles Administrator, Regular User, and Monitor. The administrative, including root, roles are separate and distinct and offer separate security privileges for the TOE components. The user roles are separate yet are intertwined throughout the TOE components. For example, a NetworkUser on the ADMINISTRATOR could be assigned an administrative, Console, or Monitor role on a CAPTURE ENGINE and/or an administrative or user role on the VISUALIZER.

6.1.2.1 ADMINISTRATOR

The ADMINISTRATOR performs role management for the CAPTURE ENGINE and the VISUALIZER. Role management is also performed by the ADMINISTRATOR for access to ADMINISTRATOR functions. There are three roles associated with the ADMINISTRATOR; administrator, NetworkUser, and any other role created by the administrator. The administrator role is used to perform administrative and management

functions for the ADMINISTRATOR. The NetworkUser role is the default role for all non-administrative users. For customer specific reasons the administrator may create other roles as required. The NetworkUser role has no access to ADMINISTRATOR administrative or management functions. The NetworkUser role is strictly limited to functions that allow viewing or access to resources or viewing and filtering alarms for the resources they are authorized to view, access, and filter.

6.1.2.2 CAPTURE ENGINE

The CAPTURE ENGINE maintains four roles: Root, Admin, Console, and Monitor. The Root and Admin roles are administrative. The root role has unrestricted access to all data and functionality, including Linux "root" privileges on the CAPTURE ENGINE, access to CAPTURE ENGINE configuration utilities, and immunity from Privacy Filters during data mining activities. The Admin role has access to capture data and statistics but with administrative access limited to the CONSOLE'S administrative functions. The Console and Monitor roles are non-administrative. The Console role has access to the mined captured data and statistics, while the Monitor role is limited to statistical information derived from the captured network data. Access control for Console roles to captured data is at the granularity of each CAPTURE ENGINE (i.e., a user has access to all or none of the streams on each CAPTURE ENGINE).

6.1.2.3 VISUALIZER

The VISUALIZER maintains three roles: Administrator, Regular User, and Monitor. The Administrator role has administrative and management privileges. Both the Administrator and Regular User roles have access to all reporting functions. The Monitor user has access to the dashboard only. In the evaluated configuration all user management functions are performed on the ADMINISTRATOR component.

6.1.2.4 CONSOLE

There are no roles maintained by the CONSOLE, although the CONSOLE recognizes roles. CONSOLE GUIs reflect this by disabling functions that are not authorized for specific roles.

6.1.3 Access Control

6.1.3.1 Privacy Filtering

Sniffer InfiniStream Enterprise is a network management system that provides network measurements used for performance management and problem solving. It also provides security functionality in that it can be used for forensic analysis of captured network traffic. There is the potential that it can also be used for malicious and abusive purposes. Because of the potential for abuse, privacy filtering is used to limit the amount of pay-load data that can be viewed by authorized users of the system. Privacy filtering restricts the number of bytes (from 1 to 1514) that can be viewed by an authorized user. Restricting the byte count that can be viewed ensures that the payload of the data packet cannot be viewed, yet provides enough information from the headers of the packet data to ensure useful analysis of network traffic can be complete and thorough. Role based access control also plays a part in providing further assurance. Monitor users cannot access the raw data. Only Console users, Administrative users, and Root users can access the raw data. Privacy filtering restricts the Console users by limiting the 'depth'

of the data packet that can be viewed. It is assumed that Administrative and Root users are beyond reproach and will not abuse the system. Organizations must make their own policy decisions regarding what can be viewed and what cannot be viewed. Privacy filtering restricts the number of bytes that can be viewed by a Console user. A dependable privacy filter also relies on proper identification and authentication, domain and stream id assignments attributes. Identification and authentication, domain assignments, and stream id assignments restrict console user access to only network traffic that they are authorized to view. Privacy filtering increases the restriction by limiting the 'depth' of data packets that can be viewed by Console users. Console users have the capability of saving these open streams to the Console hard drive. Therefore customer organizations must determine the sensitivity of the streams and plan protections accordingly.

6.1.3.2 ADMINISTRATOR/RESOURCE Access Control

The CONSOLE is the primary user interface into the Sniffer InfiniStream Enterprise system. Console users (root, administrator, console, and monitor users) attempt to log into a resource (CAPTURE ENGINE or Visualizer) and the resource re-directs the login attempt to the ADMINISTRATOR. Once identified and authenticated, the non-administrative and non-root (NetworkUsers) users are presented with a screen showing the resource list (VISUALIZER, CAPTURE ENGINE and stream ID that the user is authorized to access. This decision is based on the resource IP address or DNS name and the network users assigned domain and the stream ID. CONSOLE users are able to export data from the CAPTURE ENGINE and VISUALIZER that they are able to view.

6.1.3.3 ADMINSTRATOR Access Control

The ADMINISTRATOR enforces access control on itself by restricting access to objects and operations to objects contained in the ADMINISTRATOR. This is described in the table with FDP_ACC.1b. Users assigned root or administrative roles have access to all objects and may perform all operations. Users assigned to console or monitor roles have limited access to certain objects with limited operation capabilities.

6.1.3.4 CAPTURE ENGINE Access Control

The CAPTURE ENGINE enforces access control on streams by restricting access to steams and operations to streams contained in the CAPTURE ENGINE. The Root and Administrator roles have full access to all streams and can perform all operations on streams. Monitor users are restricted to statistical information while Console users have the same access as Monitor users but have the additional capability of viewing the data packets. In addition, the Root and Administrator roles have full administrative capabilities of the CAPTURE ENGINE. This is described in the table for FDP_ACC.1c.

6.1.3.5 VISUALIZER Access Control

The VISUALIZER enforces access control on statistical information by restricting access to its reports based on the role of the user. Monitor users are only able to access the predefined dashboard views. Regular users may access the dashboard views as well as reports. Administrators may access all the dashboard and report information as well as configure the system for data collection.

6.1.4 Session Establishment

The CONSOLE is the primary user interface into the Sniffer InfiniStream Enterprise system. Console users attempt to connect to a CAPTURE ENGINE. The CAPTURE ENGINE prompts the user (via CONSOLE) for a user ID and password and forwards the information to the ADMINISTRATOR for validation. The CONSOLE IP address must be resident in ADMINISTRATOR or the ADMINISTRATOR will reject the login attempt before attempting to identify and authenticate the user.

6.1.5 Capture Filter

Sniffer InfiniStream Enterprise is a network management system that provides network measurements used for performance management and problem solving by capturing and providing the tools to analyze the captured traffic. Different organizations have different requirements. Some organizations may wish to capture all network traffic and others may wish to capture only a subset of the network traffic. In special circumstances the capture is targeted. Capture filter allows organizations to specify exactly what type of traffic they are interested in capturing. Capture filter uses the IP address, MAC address, Protocol, TCP port, UDP port, or VLAN ID or combinations in order to filter in wanted traffic. Organizations should be careful as Capture Filter applies to specific network traffic being captured. All other network traffic not fitting the filter is lost.

6.1.6 Frame Slicing

Frame slicing normally provides optimization on the amount of network traffic that is captured but it does have security implications. Organizations must make policy decisions on the 'depth' of data packets captured. Frame slicing provides the mechanism to restrict the amount of bytes captured (64, 128, 256, 512, 768 or 1024). These bytes count provide enough data packet header information to make reasonable analysis possible on network performance issues and network problem solving decisions while not capturing the data packet payload. The default is full packet capture. Frame slicing provides the means necessary to capture only packet header information using the Capture Port ID and specifying the byte count required. Again, organizations should be careful as Frame Slicing limits the capture to packet header information and data packet payloads are lost.

6.1.7 VISUALIZER Statistics

The VISUALIZER is used for reporting on statistical information derived from captured network traffic from Capture Engines. The statistical information is generated on a Capture Engine capture port basis. Only the VISUALIZER administrator can initiate the collection of the statistical data by defining a matrix that contains a virtual circuit ID, a data collection time interval, and the Capture Engine capture port id. This statistical data is transmitted to the VISUALIZER from the Capture Engine and is available to all users with proper authorization to that VISUALIZER. This statistical data is network performance information, which is used to track network performance, track baselines and deviations from baselines, and to track trends that may be useful by customer organizations for determining future network growth. The customer organization is expected to determine the sensitivity of this statistical information and plan accordingly

for its protection. The statistical data is exported to a 3rd party database and is not protected by the TOE.

6.1.8 Self Protection

The TOE protects itself from bypass and interference via interfaces within its scope of control. The TOE includes interfaces that invoke other security functions (security enforcing) as well as those that do not invoke any other security function (security supporting). The security supporting interfaces are designed and implemented such that they do not have any access to TSF data and may not interfere with or bypass security functionality of the TOE. Security enforcing interfaces are designed and implemented such that all security policies are enforced. The TOE does not utilize shared memory, which helps to preclude interference from entities outside the TOE scope of control.

Multiple simultaneous users are supported, and the TOE associates distinct attributes and privileges with each process/user to restrict their access appropriately. Multiple sessions are instantiated as separate operating system processes and it is the responsibility of the It Environment to ensure non-interference between the processes.

6.2 Strength of Function

The claimed strength of function is SOF-basic. The Identification and Security function is a probabilistic function in the password mechanism. SOF-basic is appropriate for the intended use of the TOE in environments with threat agents with low attack potential.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profile.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profile.

CHAPTER 8

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 15 - Threats and Assumptions to Security Objectives Mapping

	O.MANAGE	O.PARTIAL_SELF_PROTECT	O.TOE_ACCESS	O.TRUNCATE	O.SELECT	O.PRIVACY	O.EXPORT	OE.INFO_STORAGE	OE.COMM	OE.OS_PROTECTION	ON.ENVIRON	ON.INSTALL	ON.NETWORK	ON.NOEVILADMIN	ON.PLATFORM
T. UNAUTHACCESS			X						X						
T.TSF_ COMPROMISE	X	X								X					
T.COMINT								X							
T.COMDIS		X		X	X	X	X			X					
T.LOSSOF								X							
T.MISCFG	X														
T.MODIFY	X		X												
T.NOHALT									X		X				
T.COMMS									X						
A.ENVIRON											X				
A.INSTALL												X			
A.NETWORK													X		
A.NOEVILADMIN														X	
A.PLATFORM															X

8.1.1 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.UNAUTHACCESS	**O.TOE_ACCESS** mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. **OE.COMM** mitigates this threat by protecting TSF data from disclosure when it is transferred between distributed components of the TOE.
T.COMINT	**OE.INFO_STORAGE** contributes to mitigating this threat by controlling modification of system data records.
T.TSF_COMPROMISE	**O.PARTIAL_SELF_PROTECTION** contributes to countering this threat by ensuring that the TSF can protect itself from users within the TSC. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control. Ensuring that the TSF is always invoked is also critical to the mitigation of this threat. **O.MANAGE** is necessary because an access control policy is not specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions. **OE.OS_SELF_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.COMDIS	**O.TRUNCATE** helps to mitigate this threat by providing a means to limit the 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. **O.PRIVACY** helps to mitigate this threat by providing a means to limit the number of bytes that can be accessed for each data packet that resides in store. **O.EXPORT** helps mitigate this threat by providing a controlled mechanism for exporting limited amounts of data. **O.PARTIAL_SELF_PROTECTION** contributes to countering this threat by ensuring that the TSF can protect itself from users within the TSC. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control. Ensuring that the TSF is always invoked is also critical to the mitigation of this threat. **OE.OS_SELF_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.LOSSOF	**OE.INFO_STORAGE** contributes to mitigating this threat by controlling deletion of system data records.
T.MISCFG	**O.MANAGE** contributes to mitigating this threat by providing the mechanism that only allows users with administrator and root privileges the ability to configure the TOE.
T.MODIFY	**O.MANAGE** contributes to mitigating this threat by providing the mechanism that only allows users with administrator and root 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 authorized users.

T.TYPE	Security Objectives Rationale
T.NOHALT	**ON.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 specifying that the environment will protect communications between TOE components thereby limiting access through communication channels.
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.

8.1.2 Rationale Showing Assumptions to Environment Security Objectives

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

Table 17 - Assumptions to Security Objectives Rationale

A.TYPE	Environment Security Objective Rationale
A.ENVIRON	**ON.ENVIRON** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.INSTALL	**ON.INSTALL** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.NETWORK	**ON.NETWORK** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.NOEVILADMIN	**ON.NOEVILADMIN** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.PLATFORM	**ON.PLATFORM** 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 18 - SFRs to Security Objectives Mapping

	O.MANAGE	O.PARTIAL_SELF_PROTECTION	O.TOE_ACCESS	O.TRUNCATE	O.SELECT	O.PRIVACY	O.EXPORT
FDP_ACC.1			X			X	
FDP_ACF.1			X			X	
FIA_ATD.1			X				
FDP_ETC.1							X
FDP_IFC.1				X	X		
FDP_IFF.1-NIAP-0407				X	X		
FIA_SOS.1			X				

	O.MANAGE	O.PARTIAL_SELF_PROTECTION	O.TOE_ACCESS	O.TRUNCATE	O.SELECT	O.PRIVACY	O.EXPORT
FIA_UAU.1			X				
FIA_UAU.7			X				
FIA_UID.1			X				
FMT_MOF.1	X						
FMT_MSA.1	X						
FMT_MSA.3	X						
FMT_MTD.1	X						
FMT_SMF.1	X						
FMT_SMR.1	X						
FPT_RVM_SFT.1		X					
FPT_SEP_SFT.1		X					
FTA_TSE.1			X				

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

Table 19 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.MANAGE	**FMT_MOF.1** requires that the ability to use particular TOE capabilities be restricted to the Administrator. **FMT_MSA.1** requires that the ability to perform operations on security attributes be restricted to particular roles. **FMT_MSA.3** ensures that the default values assigned to security attributes are restrictive. **FMT_MTD.1** requires that the ability to manipulate TOE content is restricted to Administrators. **FMT_SMF.1** defines the specific security management functions to be supported. **FMT_SMR.1** defines the specific security roles to be supported.
O.PARTIAL_SELF_PROTECTION	**FPT_SEP_SFT.1** ensures the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. The explicitly specified version was used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment. **FPT_RVM_SFT.1** ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and objects that are within the TSC. Without this non-bypassability requirement, the TSF could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to TOE resources (including TSF data and executable code) regardless of the defined policies.
O.TOE_ACCESS	**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 role(s) they may assume). **FIA_SOS.1** defines the minimum password requirements for the TOE. **FIA_UID.1** requires that a user be identified to the TOE in order to access anything.

Security Objective	SFR and Rationale
	FIA_UAU.1 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. **FDP_ACC.1 and FDP_ACF.1** define security policies based on subject and object attributes and allowed operations to access components of the TOE and information protected by the TOE. **FTA_TSE.1** limits access to TOE components based on proper IP address of the TOE CONSOLE.
O.TRUNCATE	**FDP_IFC.1** defines an information flow control policy to users on network traffic. **FDP_IFF.1-NIAP-0407** 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. It also specifies the rules for inclusion of network traffic in VISUALIZER statistics.
O.SELECT	**FDP_IFC.1** defines an information flow control policy to users on network traffic. **FDP_IFF.1-NIAP-0407** defines the selection of what network traffic or what type of network traffic is to be captured based on attributes selected.
O.PRIVACY	**FDP_ACC.1c** defines an access control policy to users on captured traffic. **FDP_ACF.1c** specifies who can access what captured traffic and the amount of captured traffic based on a specified byte count of each data packet.
O.EXPORT	**FDP_ETC.1** defines a mechanism to export mined data received from a Capture Engine.

8.2.2 Rationale for Security Functional Requirements of the IT Environment Objectives

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

The following table identifies for each SFR, the IT Environment security objective(s) that meets the objective.

Table 20 - IT Environment Security Objectives to SFR Mapping

	OE.INFO_STORAGE	OE.COMM	OE.OS_PROTECTION
FDP_ACC.1	X		
FDP_ACF.1	X		
FPT_ITT.1		X	
FPT_RVM_OS.1			X
FPT_SEP_OS.1			X

The following table provides the rational for the SFRs of the IT Environment security objective(s).

Table 21 - Security Objectives to SFR Rationale Detail

IT Environment Security Objective	SFR and Rationale
OE.INFO_ STORAGE	**FDP_ACC.1** and **FDP_ACF.1** restrict the ability to read, write and delete captured network traffic and configuration information.
OE.COMM	**FPT_ITT.1** protects traffic sent between the distributed TOE components.
OE.OS_ PROTECTION	**FPT_SEP_OS.1** ensures the OS provides a separate domain for itself and individual application processes that protects them from untrusted users. The explicitly specified version was used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment. **FPT_RVM_OS.1** ensures that the OS makes policy decisions on all interfaces that perform operations on subjects and objects that are within the scope of the OS control. Without this non-bypassability requirement, the OS could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to unauthorized resources regardless of the defined policies.

8.2.3 Security Assurance Requirements Rationale

8.2.3.1 TOE Security Assurance Requirements Rationale

The TOE meets the assurance requirements for EAL3 and is augmented by ALC_FLR.1. The following table provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 22 - Assurance Measures

Component ID	Rationale
ACM_CAP.3	Sniffer InfiniStream Enterprise ACM_CAP.3 Configuration Management, Sniffer InfiniStream Enterprise NIAP Evidence List Procedure, QMS, Information & Change Control The following Configuration Management procedures are described in this documentation: Use of the CM tool for revision control. Use of documented procedures for product builds. Use of document procedures for product test. Use of documented procedures for release to Fulfilment Center. Use of documented procedures for distribution to customers. List of configuration items and evidence that the items are maintained by the CM tool.
ACM_SCP.1	Sniffer InfiniStream Enterprise NIAP Evidence List The documentation contains lists of the items tracked by the CM revision Control tool. These items include the TOE implementation as well as the evidence used in the CC evaluation.
ADO_DEL.1	Sniffer InfiniStream Enterprise ADO_DEL.1 Delivery Procedures Procedure, QMS, Information & Change Control This document includes descriptions of the process used to create copies of the TOE and the procedures used to ensure consistent delivery of the TOE.

Component ID	Rationale
ADO_IGS.1	Sniffer Enterprise Visualizer Version 4.1 Installation Guide, Sniffer Enterprise Administrator Version 4.1 User Guide, Sniffer Enterprise Administrator Version 4.1 Installation Guide, Sniffer InfiniStream Version 3.0 SP1 User's Guide, Sniffer InfiniStream Version 3.0 SP1 Hardware Installation and Administration Guide, Sniffer InfiniStream Version 3.0 Software Installation Booklet These documents describe the procedures necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1	Sniffer InfiniStream Enterprise ADV_FSP.1 Functional Specification These documents provide the purpose and method of use of all external TSF interfaces and completely represent the TSF.
ADV_HLD.2	Sniffer InfiniStream Enterprise ADV_HLD.2 Security Enforcing High Level Design These documents describe the high level design. They contain representation of the TSF in terms of subsystems, identifying the TSP-enforcing subsystems, and describe the security functions. All subsystem interfaces are identified and the externally visible ones are noted. The purpose and method of use of all interfaces to the TSF subsystems are described.
ADV_RCR.1	Sniffer InfiniStream Enterprise ADV_RCR.1 Informal Correspondence Demonstration The correspondence between the TOE security functions and the high level design subsystems is described in these documents.
AGD_ADM.1	Sniffer Enterprise Visualizer Version 4.1 User Guide, Sniffer Enterprise Visualizer Version 4.1 Installation Guide, Sniffer Enterprise Administrator Version 4.1 User Guide, Sniffer Enterprise Administrator Version 4.1 Installation Guide, Sniffer InfiniStream Version 3.0 SP1 User's Guide, Sniffer InfiniStream Version 3.0 SP1 Hardware Installation and Administration Guide, Sniffer InfiniStream Version 3.0 Software Installation Booklet, Sniffer InfiniStream Version 3.0 Start Here Model i120 Sniffer InfiniStream Version 3.0 Start Here Model i120_Model i1620 Guidance to administrators is effectively supported by the listed documentation for this requirement.
AGD_USR.1	Sniffer Enterprise Visualizer Version 4.1 User Guide, Sniffer Enterprise Visualizer Version 4.1 Installation Guide, Sniffer Enterprise Administrator Version 4.1 User Guide, Sniffer Enterprise Administrator Version 4.1 Installation Guide, Sniffer InfiniStream Version 3.0 SP1 User's Guide, Sniffer InfiniStream Version 3.0 Software Installation Booklet, Sniffer InfiniStream Version 3.0 Start Here Model i120 Sniffer InfiniStream Version 3.0 Start Here Model i120_Model i1620 Guidance to non-administrator users is effectively supported by the documentation for this requirement.

Component ID	Rationale
ALC_DVS.1	Employee Proprietary Information and Inventions Agreement, Sniffer InfiniStream Enterprise ALC_DVS.1 Life Cycle Support, Network General Corporation Mutual Non-Disclosure Agreement Code of Business Ethics & Conduct Sniffer InfiniStream Enterprise ACM_CAP.3 Configuration Management The documentation of development security documentation that describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_FLR.1	ClearQuest Defect Tracking Release usage guidelines These documents describe well defined life-cycle model for all the steps of the TOE development, including flaw remediation procedures and policies, correct use of tools and techniques and the security measures used to protect the development environment.
ATE_COV.2	Sniffer InfiniStream Enterprise ATE_COV.2 Test Coverage These documents describe the functional and penetration tests performed and their results.
ATE_DPT.1	Sniffer InfiniStream Enterprise ATE_DPT.1 Depth Analysis These documents describe the functional and penetration tests performed and their results.
ATE_FUN.1	Sniffer InfiniStream Enterprise ATE_FUN Test Plan, Sniffer InfiniStream Enterprise ATE_FUN Test Procedures These documents describe the functional and penetration tests performed and their results
ATE_IND.2	Sniffer InfiniStream Enterprise ATE_FUN Test Plan, Sniffer InfiniStream Enterprise ATE_FUN Test Procedures These documents describe the functional and penetration tests performed and their results
AVA_MSU.1	Sniffer Enterprise Visualizer Version 4.1 User Guide, Sniffer Enterprise Visualizer Version 4.1 Installation Guide, Sniffer Enterprise Administrator Version 4.1 User Guide, Sniffer Enterprise Administrator Version 4.1 Installation Guide, Sniffer InfiniStream Version 3.0 SP1 User's Guide, Sniffer InfiniStream Version 3.0 SP1 Hardware Installation and Administration Guide, Sniffer InfiniStream Version 3.0 Software Installation Booklet, Sniffer InfiniStream Version 3.0 Start Here Model i120 Sniffer InfiniStream Version 3.0 Start Here Model i120_Model i1620 Guidance is effectively supported by the listed documentation for this requirement.
AVA_SOF.1	Sniffer InfiniStream Enterprise Strength of Function AVA_SOF These documents include strength of function analysis to support the SOF-basic claim. The analysis includes identifying the TOE password space and the probability of a password being compromised.

Component ID	Rationale
AVA_VLA.1	Sniffer InfiniStream Enterprise Vulnerability Analysis Network General Corporation: OS Hardening Procedures These documents describe the vulnerability analysis performed and the results of the analysis.

8.2.3.2 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.

C) The ALC_FLR.1 augmentation was chosen to provide a mechanism for addressing product flaws during the product lifecycle.

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 23 - SFRs to TOE Security Functions Mapping

	I&A	Security Management	Access Control	Session Establishment	Capture Filter	Frame Slicing	VISUALIZER Statistics	Self Protection
FDP_ACC.1			X					
FDP_ACF.1			X					
FDP_ETC.1			X					
FDP_IFC.1a					X	X		
FDP_IFF.1-NIAP-0407a					X	X		
FDP_IFC.1b							X	
FDP_IFF.1-NIAP-0407b							X	
FIA_ATD.1	X							
FIA_SOS.1	X							
FIA_UAU.1	X							
FIA_UAU.7	X							
FIA_UID.1	X							
FMT_MOF.1		X						
FMT_MSA.1		X						

	I&A	Security Management	Access Control	Session Establishment	Capture Filter	Frame Slicing	VISUALIZER Statistics	Self Protection
FMT_MSA.3		X						
FMT_MTD.1		X						
FMT_SMF.1		X						
FMT_SMR.1		X						
FPT_RVM_SFT.1								X
FPT_SEP_SFT.1								X
FTA_TSE.1				X				

Table 24 - SFR to SF Rationale

SFR	SF and Rationale
FDP_ACC.1	The **Access Control** security function predefines access policies to TOE components and information protected by the TOE based on roles, objects and operations that are allowed to be performed.
FDP_ACF.1	The **Access Control** security function defines access to TOE components and information protected by the TOE to authorized roles based on attributes assigned to roles and information.
FDP_ETC.1	The **Access Control** security function includes the ability to export data from the CAPTURE ENGINE that the authorized user is able to view.
FDP_IFC.1a	The **Capture Filter** and **Frame Slicing** security functions define policies levied on network traffic and capture operations.
FDP_IFF.1-NIAP-0407a	The **Capture Filter** and **Frame Slicing** security functions control the capture of network traffic based on attributes assigned to information and policies configured in the TOE.
FDP_IFC.1b	The **VISUALIZER Statistics** security function defines policies levied on the network traffic and statistics collection.
FDP_IFF.1-NIAP-0407b	The **VISUALIZER Statistics** security function controls the statistics collection for network traffic based on attributes assigned to information.
FIA_ATD.1	The **Identification and authentication** security function maintains attributes assigned to individual users. Access to TOE components and information protected by the TOE are controlled by these attributes.
FIA_SOS.1	The **Identification and Authentication** security function provides a mechanism that ensures that passwords are a minimum length.
FIA_UAU.1	The **Identification and Authentication** security function allows minimum TOE security functions to be performed before the user is authenticated. The security functions are identification and authentication.
FIA_UAU.7	The **Identification and Authentication** security function obscures the password as it is being entered.
FIA_UID.1	The **Identification and Authentication** security function only allows the identification security function to be performed before a user is identified.
FMT_MOF.1	The **Security Management** security function restricts the ability of modifying the capture filter and privacy filtering functions to administrator and root users.
FMT_MSA.1	The **Security Management** security function restricts the ability of modifying all security attributes to the administrator and root users.
FMT_MTD.1	The **Security Management** security function only allows ADMINISTRATOR Administrator users to control user related information and assign domains.

SFR	SF and Rationale
FMT_MSA.3	The **Security Management** security function only allows the administrator and root users of the TOE to specify alternative values for the default values used in Frame Slicing and Capture Filter.
FMT_SMF.1	The **Security Management** security function manages all aspects of the specified security functions as detailed in the FMT_SMF SFR.
FMT_SMR.1	The **Security Management** security function maintains all authorized roles and can associate users with roles.
FPT_RVM_SFT.1	The **Self Protection** security function addresses non-bypassability of the TSF via interfaces within the TSC.
FPT_SEP_SFT.1	The **Self Protection** security function addresses non-interference with the TSF via interfaces within the TSC.
FTA_TSE.1	The **Session Establishment** security function will allow or deny TOE access based on the IP address of the CONSOLE. The IP address of the CONSOLE must match the IP address for that CONSOLE inserted in the ADMINISTRATOR by the Administrator during initial and subsequent configuration of the TOE. If the IP address of the CONSOLE does not match the IP address as specified in the ADMINISTRATOR the connection is denied.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.