National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

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)

Report Number: CCEVS-VR-07-0001

Dated: 9 February 2007

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Jerome F. Myers
David M. Dignan

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of 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) at EAL3 augmented with ALC_FLR. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 11 December 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.2, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 3 Augmented with ALC_FLR resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the Sniffer InfiniStream Enterprise which consists of 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 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.

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.

The Sniffer Enterprise Administrator 4.1 (MR2) 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.

The Sniffer Enterprise Visualizer 4.1 (MR2) Software (VISUALIZER) provides both canned reports and user created reports on statistical information about captured network traffic. 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.

1 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifier

Evaluation Identifiers for Sniffer InfiniStream Enterprise system	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme

Evaluation Identifiers for Sniffer InfiniStream Enterprise system	
TOE	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)
Protection Profile	N/A
Security Target	Network General Sniffer InfiniStream Enterprise Security Target, Version 9, dated January 17, 2007
Evaluation Technical Report	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) Evaluation Technical Report Document No. F3-0107-001, Dated 24 January 2007
Conformance Result	Part 2 conformant and EAL3 Part 3 conformant
Version of CC	CC Version 2.2 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on February 10, 2005
Version of CEM	CEM Version 2.2 and all applicable NIAP and International Interpretations effective on February 10, 2005
Sponsor	Network General 178 E. Tasman Drive, Suite 101 San Jose, CA 95134, USA
Developer	Network General 178 E. Tasman Drive, Suite 101 San Jose, CA 95134, USA
Evaluator(s)	**COACT Incorporated** Bob Roland Greg Beaver Ching Lee Nick Rojewski
Validator(s)	**NIAP CCEVS** Jerome F. Myers, David M. Dignan

1.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0426 – Content of PP Claims Rationale
I-0427 – Identification of Standards

International Interpretations

None

2 Security Policy

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.

2.1 Access Control Policy

Privacy Filtering
Sniffer InfiniStream Enterprise is a network management system that provides network measurements used for performance management and problem solving. 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.

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 (Network Users) 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.

ADMINSTRATOR Access Control
The ADMINISTRATOR enforces access control 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.

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.

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.

2.2 User Authentication
The TOE requires users to identify and authenticate themselves before accessing the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes (*role, associated domains)* associated with their user account that defines the functionality the user is allowed to perform.

2.3 Roles
The TOE defines and enforces six types of security roles: *Administrator, Network User, Root, Console, Monitor, and Regular Users.* These roles are managed within the TOE. The Sniffer Enterprise Administrator has the ability to define groups and other roles to assist in the management of access rights and privileges. The Capture Engine and Visualizer administrators have full access to and have the ability to create user accounts in their domains. Authorized Users are users that are authorized to use some TOE resources.

2.4 TOE Separation
The TOE ensures that all functions are invoked and succeed before the next function may proceed.

2.5 Security Function Strength of Function Claim
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.

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

3 Assumptions

The specific conditions listed in the following subsections are assumed to be met by the environment and operating conditions of the system. The assumptions are ordered into three groups. They are personnel assumptions, physical assumptions, and IT environment assumptions.

A) Personnel assumptions describe characteristics of personnel who are relevant to the system.

B) Physical environment assumptions describe characteristics of the non-IT environment that the system is deployed in.

C) IT environment assumptions describe the technology environment within which the TOE is operating.

3.1 Physical Assumptions

The results of the evaluation rely upon the assumption that the processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access.

3.2 IT Environment Assumptions

The results of the evaluation rely upon the following assumptions regarding the IT Environment.

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 following threats are addressed by the TOE and IT environment, respectively.

Threats Addressed by the TOE

The TOE addresses the following 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.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.

4 Clarification of Scope

The evaluation of the Sniffer InfiniStream Enterprise system covers the 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 evaluation does not make any statements about the adequacy or effectiveness of the Sniffer InfiniStream Enterprise system for its advertised usage in network management or forensics.

The underlying hardware and operating systems are not part of the TOE evaluation and the TOE relies upon their correct functionality to protect the TOE.

The data that threats are addressed by this TOE deal with threats due to misuse of the **retained** data streams. This is data that was captured off the backbone network. The TOE does not protect the original packets on the backbone.

5 Architecture Information

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. The TOE is divided into four primary components, the CAPTURE ENGINE, the ADMINISTRATOR, the CONSOLE, and the VISUALISER.

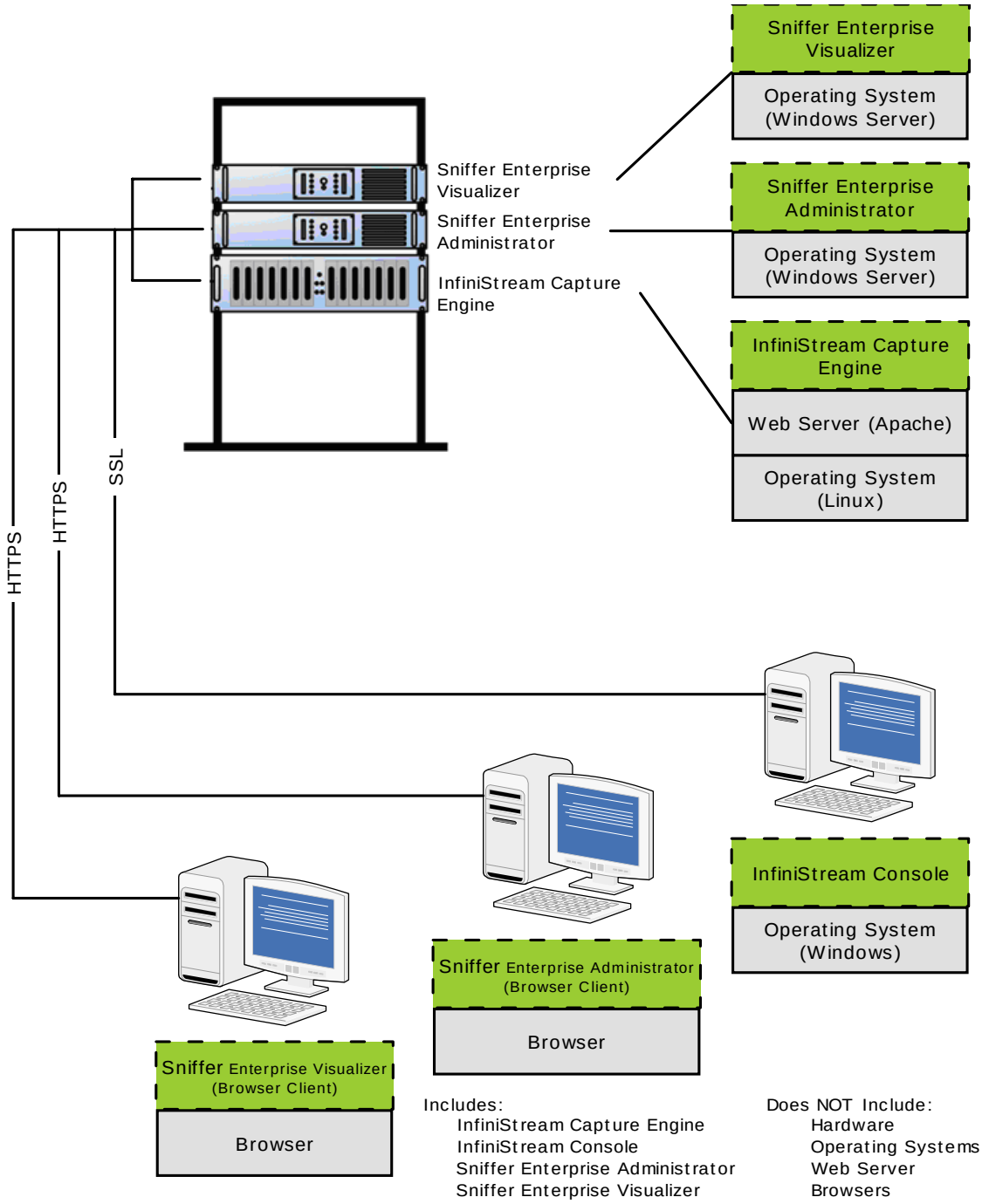

Figure 1 - Sniffer Infinistream Enterprise TOE Boundary

5.1 Evaluated Configuration

Table 2 - 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

Component	Version	Quantity
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 3 - 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	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)

	space CD-ROM Drive VGA color monitor with 1024x768 resolution 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.

5.2 Functionality Excluded from the Evaluation

A) Auditing

6 Product Delivery

The TOE delivery contains one set of Master CDs and related hard copy documents. Master CDs include installation CDs, Application CDs, and Documentation CDs.

The hard copy documentation includes:

Start Here – i420/i620 **(part of evaluation)**,
End User License **(part of evaluation)**,
Sniffer InfiniStream Release Notes **(part of evaluation)**,
Software Installation Booklet **(part of evaluation)**,
Network General Support Services Portfolio,
Network General Services Portfolio,
SUPER Micro Motherboard User's Manual,
Sniffer Enterprise Visualizer Release Note **(part of evaluation)**,
Sniffer Enterprise Visualizer Deployment Guide **(part of evaluation)**,
Sniffer Enterprise Visualizer Install Instructions Card **(part of evaluation)**,
NGC Global Services Advanced Operational Services Card,
NGC Global Services Core Operational Support Card,
SUPER Micro Motherboard User's Manual,
Administrator Release Note **(part of evaluation)**,
Network General Terms of Sale **(part of evaluation)**,
Network General Core Support,
Network General Advanced Support,
NG QA Checklist **(part of evaluation)**.

Note: The documents not listed as part of the evaluation are for general support services and motherboard reference for the appliances executing the evaluated software.

The documentation CDs contains the following documents:

10GbE Analyzer Image Recovery
10GbE Analyzer Expert Alarm Reference

10GbE Analyzer Installation Guide
10GbE Analyzer Regulatory Information
10GbE Analyzer Security Enhancements
10GbE Analyzer Users Guide
Application Intelligence Users Guide
Sniffer Distributed ATM Book Users Guide
Sniffer Distributed Getting Started Guide
Sniffer Distributed Hardware Installation Guide
Sniffer Distributed Reporter Users Guide
Sniffer Distributed Software Only Booklet
Sniffer Distributed Switch Expert Guide
Sniffer Distributed Upgrade Guide
Sniffer Distributed Users Guide
Sniffer Enterprise Administrator Installation Guide (part of evaluation)
Sniffer Enterprise Administrator Remote Reimage Procedures
Sniffer Enterprise Administrator Software-only Booklet (part of evaluation)
Sniffer Enterprise Administrator User Guide (part of evaluation)
Sniffer InfiniStream Installation and Administration Guide (part of evaluation)
Sniffer InfiniStream Installation Booklet (part of evaluation)
Sniffer InfiniStream Start Here (Model i120) (part of evaluation)
Sniffer InfiniStream Start Here (Model i420_Model i1620) (part of evaluation)
Sniffer InfiniStream Users Guide (part of evaluation)
Mobile Intelligence Operations
Sniffer MultiSegment Intelligence User Guide
Sniffer Portable ATM Adapter Reference Guide
Sniffer Portable Full Duplex Adapter Upgrade
Sniffer Portable Full Duplex Reference Guide
Sniffer Portable Gigabit Ethernet Reference Guide
Sniffer Portable Installation Guide
Sniffer Portable Reporter Users Guide
Sniffer Portable Snifferbook Reference Guide
Sniffer Portable Snifferbook Ultra Reference Guide
Sniffer Portable Switch Expert Guide
Sniffer Portable Users Guide
Sniffer Portable WAN Adapter Reference Guide
Sniffer Tool Collection Capture Format Converter Guide
Sniffer Tool Collection Focused Analysis Guide
Voice Intelligence Operations
Wireless Guide
VirusScan Best Practices
VirusScan Installation
VirusScan Product
VirusScan Quick Reference
Model APGB Getting Started
Model APGB Getting Started Guide
Model APGB Hardware Installation Guide
Model APGB Users Guide
Sniffer Enterprise NetVigil Quick Install
Sniffer Enterprise NetVigil Quick Start
Sniffer Enterprise NetVigil Reference Guide
Sniffer Enterprise NetVigil Troubleshooting

Sniffer Enterprise Visualizer Deployment Guide (part of evaluation)
Sniffer Enterprise Visualizer Installation Guide (part of evaluation)
Sniffer Enterprise Visualizer User Guide (part of evaluation)
SuperTAP Users Guide

Note: The documents highlighted above are part of the evaluated configuration. The remaining documentation is for other products manufactured by Network General.

Network General ships a second set of Master CDs and related documents to a fulfillment house for software installation and packaging of hardware appliances.

The software is installed and tested on the unit with the original Master CDs. They then install a second appliance from a replicated CD and compare the two installations to ensure the validity of the software images.

7 IT Product Testing

Testing was performed on October 19 through October 23 2006 at the COACT Laboratory in Columbia, MD. Two COACT employees performed the tests. During some pretest activities the CCTL identified a TOE vulnerability that needed to be fixed. The vendor made the appropriate changes to the TOE, placed the updated version into their configuration management system and manufacturing process, the updated version was delivered through the normal delivery channels and the updated version was installed and tested.

7.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of a Visualizer Appliance, an Administrator Appliance, a Capture Engine, a Console (PC w/ Windows XP), and a “Test” PC (Windows XP), connected through a Hub. Figure 2 shows the topology of the test bed configuration.

Figure 2 - Test Bed Configuration

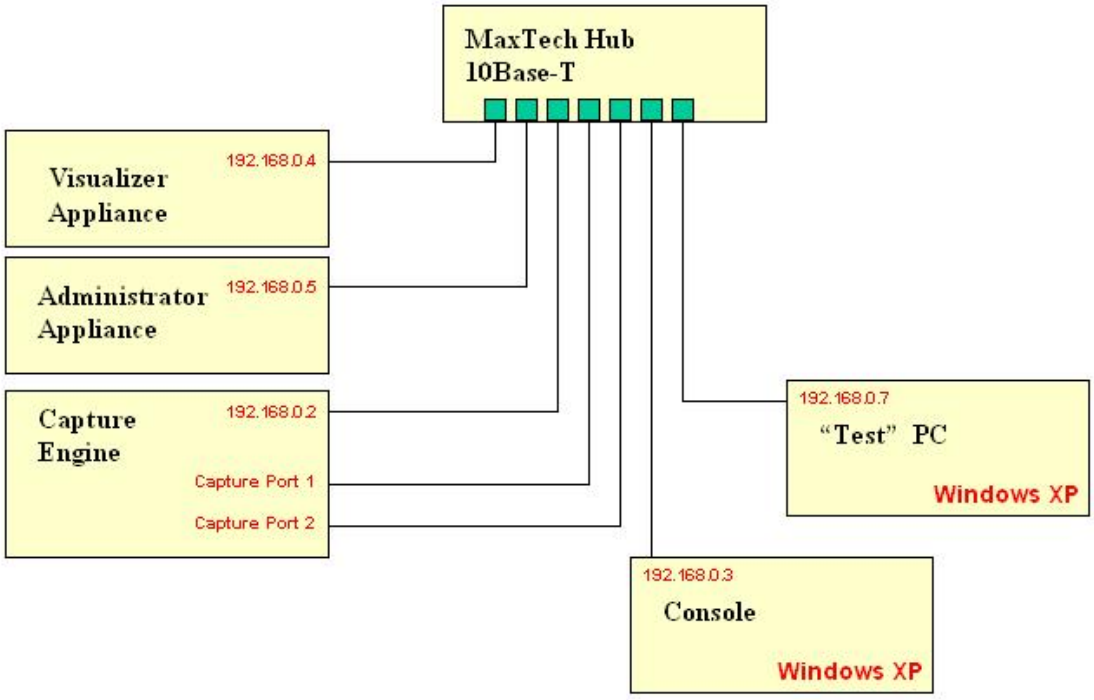

Table 4 - Test Configuration

Component	Description
Console Computer	Pentium 4, 2.80 GHz 512 MB RAM Microsoft Windows XP Professional Version 2002 Service Pack 2
"Test" Computer	Dell Latitude Laptop Pentium 3, 750 MHz 256 MB RAM Microsoft Windows XP Professional Version 2002 Service Pack 2 Nmap Win Version 1.3.1 Ethereal Version 0.9.16
Hub	MaxTech 10Base-T Hub
InfiniStream Sniffer Console	Version 3.0 Service Pack 1 (MR7)
InfiniStream Capture Engine	Version 3.0 Service Pack 1 (MR7)

Sniffer Enterprise Administrator	Version 4.1 (MR2)
Sniffer Enterprise Visualizer	Version 4.1 (MR2)

7.2 Functional Test Results

The evaluation team executed the entire developer test suite. All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the developer and CCTL proprietary report, Functional Test Report F3-0107-002, dated 24 January 2007.

7.3 Evaluator Independent Testing

The evaluation team performed an analysis of all of the developer tests to assess the level of developer testing corresponding to each of the TSFIs. The following tests were performed during independent functional testing:

1) Simulate a network failure in which the SEA loses communication with the ICE and SEV. Attempt to log on to the ICE and SEV. Restore the network connection and attempt to log on to the ICE and SEV.
2) Verify that the captured streams from the ICE that are sent to the Console are encrypted using SSL.
3) Verify that the Frame Slicing function operates correctly.
4) Verify that the Privacy Filtering function operates correctly.
5) The Visualizer statistical flow control policies will be tested.

The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests. All tests were performed satisfactorily and the results were as expected. The TOE passed all tests.

7.4 Evaluator Penetration Tests

The evaluators examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. While verifying the information found in the developer's vulnerability assessment, the evaluators conducted a search to verify that no additional obvious vulnerabilities existed for the TOE.

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluators made an assessment of the rationales provided by the developer indicating that the vulnerability was non-exploitable in the intended environment of the TOE. After performing a threat analysis on each of the vulnerabilities, the evaluators reached the same conclusion as was in the vendor analysis; i.e. further testing of those vulnerabilities was unnecessary.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities.

As a result of the evaluator's examination of the developer's vulnerability analysis and the independent search for obvious TOE vulnerabilities, the evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the vulnerabilities. The scope of evaluator analysis and testing included potential obvious vulnerabilities in the IT Environment that would be introduced as a result of the presence of the TOE. The following Penetration tests were performed by the evaluator:

#1 Have an unauthenticated user access the Console and attempt to reconfigure it.

#2 Attempt to access the Sniffer InfiniStream Administrator from a PC whose IP address is not in the SEA's access control list and reconfigure the Sniffer InfiniStream Administrator
#3 Perform a port scan on each individual TOE component and determine if any ports are open that would permit an intruder to access the TOE.

The test configuration is illustrated in Figure 2. It consisted of a Visualizer Appliance, an Administrator Appliance, a Capture Engine, a Console (PC w/ Windows XP), and a "Test" PC (Windows XP), connected through a Hub.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, COACT document F3-0107-003 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) Penetration Testing Report, dated 24 January 2007.

7.5 Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

8 RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 3 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the document Evaluation Technical Report for the Network General 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), F3-0107-001, Dated 24 January 2007 contains the verdicts of "PASS" for all the work units.

The evaluation determined that the product meets the requirements for EAL 3 augmented with ALC_FLR. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10. VALIDATOR COMMENTS

The Validator observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validator agrees that the CCTL presented appropriate rationales to support the evaluation results presented in

Evaluation Technical Report 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, and Sniffer Enterprise Visualizer 4.1 (MR2) Software). The Validator, concludes that the evaluation and Pass result for the ST and TOE are complete and correct.

Items of note: Prospective users of this product should read the "Minimum Hardware and Software Requirements" portion of this report carefully and thoroughly. Doing so will insure their respective environment is sufficient and will make optimum use of this application. Users should also be aware of SSL encryption and its possible effects on system performance. The InfiniStream User Guide on pages 38 – 39 presents the SSL encryption as an option and states that enabling the SSL encryption degrades the system performance and uses considerable system resources. Specific instructions to the administrator must be given to enable and keep the SSL encryption enabled in order to keep the TOE in the evaluated configuration."

11. Security Target

The Network General Sniffer InfiniStream Enterprise Security, Version 9, dated January 17, 2007, is incorporated here by reference.

12. List of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute for Standards Technology
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

13. Bibliography

The following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.2, dated January 2004
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000