Network Chemistry RFprotect™ Distributed v6.1.2, RFprotect™ Sensor v6.1.22, and RFprotect™ Mobile v6.1.2

Security Target

Evaluation Assurance Level: EAL 2
Document Version: 1.0

Prepared for:

Network Chemistry, Inc.
1804 Embarcadero Road, Suite 201
Palo Alto, CA 94303
Phone: (650) 858-3120

http://www.networkchemistry.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2006-03-23	Nathan Lee	Initial draft.
0.2	2006-09-12	Christie Kummers	Updates to include new security functionality.
0.3	2007-01-22	Teresa MacArthur	Addressed first round of verdicts.
0.4	2007-03-28	Greg Milliken	Minor administrative changes.
1.0	2007-04-16	Amy Nicewick	Final revisions for submission to CB.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The subjects of evaluation are the Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2, and will hereafter be referred to as the TOE throughout this document. The TOE is a wireless intrusion detection and intrusion prevention system.

1.1 Overview

This ST contains the following sections to provide a mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish, or mitigate the defined threats:

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- TOE Security Environment (Section 3) – Describes the threats and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- IT Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, TOE and CC Identification and Conformance

Table 1 - ST, TOE, and CC Identification and Conformance

	Network Chemistry RFprotect™ v6.1.2, RFprotect™ Sensor v6.1.22, RFprotect™ Mobile v6.1.2 Security Target
ST Version	Version 1.0
Author	Corsec Security, Inc.
TOE Identification	Network Chemistry RFprotect™ v6.1.2 build 13, RFprotect™ Sensor v6.1.22, RFprotect™ Mobile v6.1.2 build 13
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3; CC Part 2 extended, CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted CEM as of September 6, 2006 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL 2
Keywords	Wireless IDS, Wireless IPS, IDS, IPS, Wireless, Intrusion Detection, Intrusion Prevention

1.3 Conventions, Acronyms, and Terminology

1.3.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for several operations to be performed on security requirements: assignment, refinement, selection, and iteration. All of these operations are used within this ST. These operations are presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parenthesis following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

1.3.2 Acronyms

The acronyms used within this ST are described in Section 9 – "Acronyms."

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the general capabilities and security requirements provided by the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

The Network Chemistry RFprotect suite is a wireless intrusion detection system (IDS) coupled with intrusion prevention functionality. This system uses wireless network Sensors to detect and respond to suspicious activity and to determine the impact of network attacks, based on collected forensic data. It analyzes the authorized wireless network, checking for and responding to identified vulnerabilities. Wireless intrusion prevention capabilities allow the RFprotect system to prevent "rogue" wireless stations (including wireless access points, wireless network clients, and ad-hoc wireless devices) from operating within the range of the product, and to neutralize threats after identification of an attack by terminating an attacker's wireless session.

2.2 Product Description

The product is a wireless intrusion detection and prevention system which uses wireless Sensors to collect information about target systems and networks. The system contains an analyzer component to support analysis of the data and to initiate actions in response to its findings.

There are three TOE components which combine to form the two evaluated TOE configurations. These three TOE components are:

- RFprotect Sensor
- RFprotect Server
- RFprotect Client

These TOE components can be instantiated on separate inter-dependent devices to form the first TOE configuration, or they can be combined onto one device (typically a mobile laptop workstation) to form the second TOE configuration (called *RFprotect Mobile*). RFprotect Mobile can operate independently of or in conjunction with standalone Sensors, Servers, and Clients.

2.2.1 RFprotect Sensor

The RFprotect Sensor is a self-contained appliance which is used to scan the channels defined in the 802.11 wireless networking specifications for unauthorized, malicious, or otherwise suspicious traffic, report its findings back to the RFprotect Server, and respond to unauthorized or undesirable network traffic as directed by the Server. It can detect all 802.11 wireless devices within the Sensor's scan range, as well as anomalies such as malformed network protocol headers and network traffic patterns which may indicate malicious probes, attacks, denial of service attempts, or other types of wireless network abuse.

Along with typical intrusion detection capabilities the RFprotect Sensor can also be used to respond to identified attacks or unauthorized network traffic by terminating or controlling the wireless connections of any wireless stations within its scanning range.

2.2.2 RFprotect Server

The RFprotect Server is a software package which is installed on standard server hardware and functions as the central management and analysis server for the RFprotect system. The Server provides scanning policies to the RFprotect Sensors deployed on the local network and receives wireless traffic reports from them. The Server stores the reports from all of the Sensors on the network and continuously analyzes the complete wireless traffic dataset. If the complete dataset indicates that suspicious or malicious activity is or may be occurring, the Server may be

configured to respond by instructing one or more Sensors to take appropriate actions to mitigate the threat. The Server allows authorized users to view events generated by the Sensors via the RFprotect Client software.

2.2.3 RFprotect Client

The RFprotect Client is a software package which is installed on standard Personal Computer (PC) hardware. It is used to manage the Server and the Sensors and to view reports on wireless network activity. The Client provides a Graphical User Interface (GUI) to manage users and their associated roles, system policies, and alarms associated with specific events. It also provides a means to view the status of all deployed Sensors and can display reports generated by the Server to provide summary information about attacks, activity graphs, and analysis of event trends.

2.2.4 RFprotect Mobile

The RFprotect Mobile software is made up of functionality from RFprotect Sensor, RFprotect Server and RFprotect Mobile Client. It is installed on a standard PC workstation, typically a laptop computer, to provide mobility. In the evaluated configuration of the RFprotect Mobile product, the Sensor functionality is provided by a wireless network adapter and the RFprotect Agent software module installed on the host laptop. The RFprotect Agent software that controls the wireless network adapter is included in the TOE, but the wireless network adapter hardware is not. The RFprotect Mobile configuration is architecturally similar to the separate Sensor, Server, and Client configuration; however, in the evaluated configuration, the RFprotect Mobile configuration communicates only with the local Sensor. Please see Figure 2 below for more information about this configuration.

2.3 TOE Boundaries and Scope

The TOE comprises both hardware and software. This section addresses what physical (hardware) and logical (software) components of the TOE are included in evaluation.

2.3.1 Physical Boundary

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment. The physical components that compose the TOE in the evaluated configuration are:

- The RFprotect Sensor

The following physical components are excluded from the TOE boundary, but are part of the Information Technology (IT) environment in the TOE's evaluated configuration:

- The computer hardware running the RFprotect Server software
- The computer hardware running the RFprotect Client software
- The computer hardware running the RFprotect Mobile software (including the 802.11 a/b/g wireless network adapter hardware)

In addition, the Packetyzer is not included as part of the TOE.

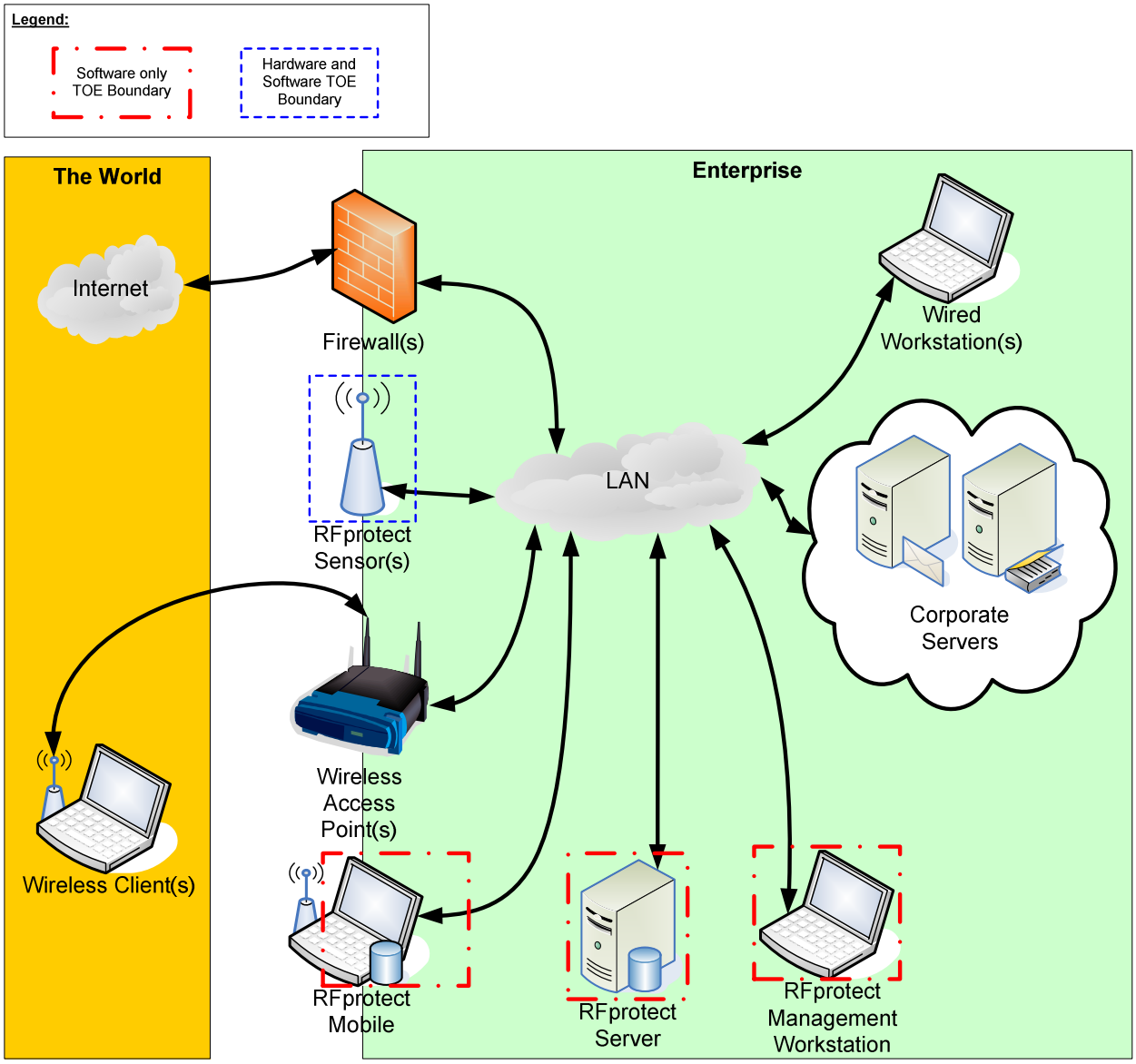

Figure 1 - Physical TOE Boundary

2.3.2 Logical Boundary

The logical boundaries of each of the components of the TOE are shown in Figure 2 below. The logical boundaries of the Server, Client, and Mobile TOE components include the RFprotect software components but not the underlying OS. The logical boundary of the Sensor includes the radio, the RFprotect software, and the underlying operating system.

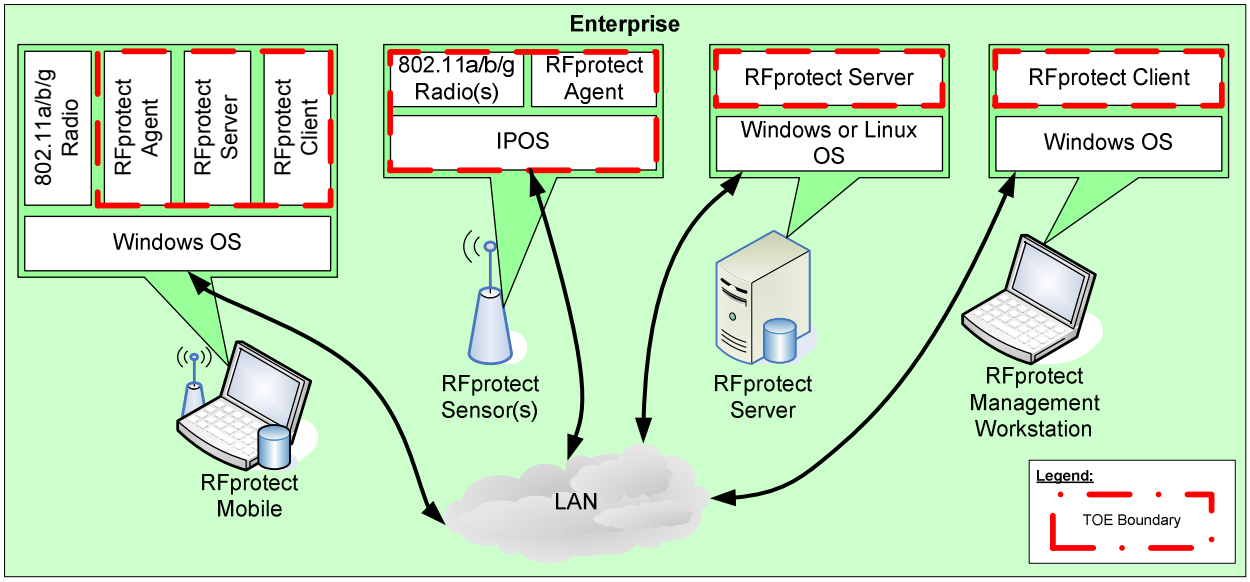

Figure 2 - TOE Logical Boundary

2.3.2.1 RFprotect Sensor

The ipOS 6.8 operating system used in the RFprotect Sensor is licensed from Ubicom, Inc. Ubicom also makes the IP3000 family processors used in the sensors. The Ubicom ipOS is the only OS supported by the hardware. Three models of sensors can be used: model ND-10, ND-20, and ND-30.

2.3.2.2 RFprotect Mobile

RFprotect Mobile is fitted with a Peripheral Component Interconnect (PCI) card as part of the TOE environment. This is currently a commercial-off-the-shelf card with the Atheros AR5004X chipset; however any Atheros chipset may be used to communicate with the modified version of the Atheros driver used in RFprotect Mobile.

The evaluated version of RFprotect Mobile may be installed on any of the following OSs:

- Windows XP Professional Service Pack 2
- Windows 2003 Server Service Pack 1

2.3.2.3 RFprotect Server

Any of the following OSs may be used for the evaluated version of the RFprotect Server platform:

- Windows (XP Professional Service Pack 2 or Windows 2003 Server Service Pack 1)
- Linux (Redhat Enterprise 9, Fedora Core 3, or SUSE Enterprise 9.1)

2.3.2.4 RFprotect Client

The OS for the evaluated version of RFprotect Client (on the Management Workstation) may be any of the following:

- Windows XP Professional Service Pack 2
- Windows 2003 Server Service Pack 1

The Logical Boundaries of the TOE embody security functions that it implements. These TOE security functions are usefully grouped under the following Security Function Classes:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- IDS Component Requirements

Please refer to Section 6.1 for descriptions of these Security Function Classes.

3 TOE Security Environment

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

- assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects,
- known and presumed threats countered by either the TOE or by the security environment,
- Organizational Security Policies (OSPs) with which the TOE must comply.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

3.1.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

3.1.2 Physical Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.1.3 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

3.1.4 Connectivity Assumption

A.CONNECT The TOE will be installed such that all network traffic will flow through the TOE.

3.2 Threats to Security

The following are threats identified for the TOE and the IT System the TOE monitors. The assumed level of expertise of the attacker for all the threats is unsophisticated.

3.2.1 TOE Threats

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

T.BLIND An attacker may blind the TOE by physically shielding or damaging TOE antennas.

T.MSQERADE A network attacker may attempt to imitate a client system in order to gain information about the vulnerabilities of the client system.

3.2.2 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity, thereby resulting in a threat to the IT system.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source, thereby resulting in a threat to the IT system.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources, thereby resulting in a threat to the IT system.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the TOE.

P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 TOE Security Objectives

The following are the TOE security objectives:

O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.

O.IDSCAN The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

O.IDSENS The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets.

O.IDANLZ The TOE must accept data from Sensors and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

O.RESPON The TOE must respond appropriately to analytical conclusions.

O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.

O.AUDITS The TOE must record audit records for data accesses and use of the System functions.

O.INTEGR The TOE must ensure the integrity of all audit and System data.

O.EXPORT When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the System data.

4.2 Security Objectives for the Environment

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

4.2.1 Non-IT Objectives

These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

OE.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

OE.INTROP The TOE is interoperable with the IT System it monitors.

4.2.2 IT Objectives

OE.TIME The IT Environment will provide reliable timestamps to the TOE.

OE.PROTECT The IT Environment will protect itself and the TOE from external interference or tampering.

5 IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE as well as Security Functional Requirements met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 2 identifies all SFRs implemented by the TOE.

Table 2 – TOE Security Functional Requirements

SFR ID	Description
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RVM.1(1)	Non-bypassability of the TSP
FPT_SEP.1(1)	TSF domain separation
FPT_STM.1(1)	Reliable time stamps
IDS_NDC.1	Network data collection
IDS_ANL.1	Analyzer analysis
IDS_RCT.1	Analyzer react
IDS_RDR.1	Restricted data review
IDS_STG.1	Guarantee of System data availability

Section 5.1 contains the functional components from the Common Criteria (CC) Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.1.

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

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

b) All auditable events, for the [*not specified*] level of audit; and

c) [*auditable events listed in Table 3*].

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other information*].

Dependencies: FPT_STM.1 Reliable time stamps

Table 3 – Auditable Events

Auditable Event
Alert unacknowledged by user
Alert deleted by user
Location record deleted
Location record moved
User logged on to database
All alerts from expert acknowledged
All alerts from expert unacknowledged
Expert alert acknowledged
Expert alert unacknowledged
Expert alert deleted
KnownStation record deleted
KnownStation record updated
Ignore status for known station changed
Cleared all events from event log
Database cleared by user
Built-in Sensor properties edited

Auditable Event
Station deleted
Notification record created
Notification record deleted
Notification record edited
License key removed
License key added
Report generated
Sensor properties edited
New StationTemplate record created/edited
Sensor template deleted
Sensor template enabled
Sensor template disabled
Sensor record created
Sensor record deleted
Sensor edited
Sensor enabled
Sensor disabled
User added to the Account Manager
User deleted from the Account Manager
New KnownStation record created

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*users with the SysDBA and/or Administrator roles*] with the capability to read [*all audit data*] from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2

The TSF shall be able to [*prevent*] unauthorised modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.1.2 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [u*ser ID, hashed password, user role*].

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1

The TSF shall allow [*user identification, access to online help*] on behalf of the user to be performed before the user is authenticated.

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.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1

The TSF shall allow [*access to online help*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

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

Dependencies: No dependencies

5.1.3 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*of System data collection, analysis, and reaction*] to [*authorised System administrators*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*query, modify, delete, clear*] the [*System data*] to [*the SysDBA and Administrator roles*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [*TSF data management and security function management*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*SysDBA, Administrator, Viewer*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.4 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1

The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between **Sensors and the Server** ~~separate parts of the TOE~~.

Dependencies: No dependencies

FPT_RVM.1(1) Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1(1).1

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

Dependencies: No dependencies

FPT_SEP.1(1) TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1(1).1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1(1).2

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

Dependencies: No dependencies

FPT_STM.1(1) Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1(1).1

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

Dependencies: No dependencies

5.1.5 Class IDS: IDS Functionality

IDS_NDC.1 Network data collection (EXP)

IDS_NDC.1.1

The System shall be able to collect the following information from the targeted network:

a) [*identification and authentication events, data accesses, service requests, network traffic, data introduction, detected known vulnerabilities, radio frequency characteristics and anomalies*]; and

b) [*no other events*]. (EXP)

IDS_NDC.1.2

At a minimum, the System shall collect and record the following information:

- Date and time of the event, type of event, and subject identity; and
- Specific service, Protocol, source address, and destination address. (EXP)

IDS_ANL.1 Analyzer analysis (EXP)

IDS_ANL.1.1

The System shall perform the following analysis function on all IDS data received:

a) [*statistical, signature*]; and

b) [*no other functions*]. (EXP)

IDS_ANL.1.2

The System shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) [*no other information*]. (EXP)

IDS_RCT.1 Analyzer react (EXP)

IDS_RCT.1.1

The System shall send an alarm to [*the authorized administrator via the RFprotect Console*] and [*create a System data record*] when an intrusion is detected. (EXP)

IDS_RDR.1 Restricted data review (EXP)

IDS_RDR.1.1

The System shall provide [*the SysDBA and/or Administrator roles*] with the capability to read [*all System data*] from the System data. (EXP)

IDS_RDR.1.2

The System shall provide the System data in a manner suitable for the user to interpret the information. (EXP)

IDS_RDR.1.3

The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access. (EXP)

IDS_STG.1 Guarantee of System data availability (EXP)

IDS_STG.1.1

The System shall protect the stored System data from unauthorized deletion. (EXP)

IDS_STG.1.2

The System shall protect the stored System data from unauthorized modification. (EXP)

IDS_STG.1.3

The System shall ensure that [*the previously recorded*] System data will be maintained when the following conditions occur: [*System data storage exhaustion*]. (EXP)

5.2 Security Functional Requirements on the IT Environment

This section specifies the SFRs for the TOE environment. This section organizes the SFRs by CC class. Table 4 identifies all SFRs implemented by the TOE environment and indicates the ST operations performed on each requirement.

Table 4 – TOE Environment SFRs

SFR ID	Description
FPT_RVM.1(2)	Non-bypassability of the TSP
FPT_SEP.1(2)	TSF domain separation
FPT_STM.1(2)	Reliable time stamps

5.2.1 Class FPT: Protection of the TSF

FPT_RVM.1(2) Non-bypassability of the TSP

FPT_RVM.1.1(2)

The *environment* shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1(2) TSF domain separation

FPT_SEP.1.1(2)

The *environment* shall maintain a security domain for **the RFprotect Server's, RFprotect Sensor's, and RFprotect Mobile's** execution that protects them from interference and tampering by untrusted subjects.

FPT_SEP.1.2(2)

The *environment* shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1(2) Reliable time stamps

FPT_STM.1.1(2)

The *environment of the RFprotect Server* shall be able to provide reliable time stamps for **the RFprotect Server's and RFprotect Sensor's** use.

5.3 Assurance Requirements

This section defines the EAL 2 assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are summarized in Table 5 below.

Table 5 – Assurance Requirements

Assurance Requirements	
Class ACM: Configuration management	ACM_CAP.2 Configuration items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

6 TOE Summary Specification

This section details how the TOE meets the functional and assurance requirements described in previous sections of this ST.

6.1 TOE Security Functions

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

Table 6 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_STM.1	Reliable time stamps
IDS Component Requirements	IDS_NDC.1	Network data collection
	IDS_ANL.1	Analyzer analysis
	IDS_RCT.1	Analyzer react
	IDS_RDR.1	Restricted data review
	IDS_STG.1	Guarantee of System data availability

6.1.1 Security Audit

The TOE generates two types of audit data; audit records which contain information regarding the administration and management of the TOE, and IDS event records which contain IDS information received from the sensors and

other local network devices[1]. This security function addresses the generation, storage and viewing of audit records. The separate TOE security function called "IDS Component Requirements" covers the generation, storage, and viewing of the IDS event records. IDS Event Records are discussed in Section 6.1.5.

The TOE administrators interact with the TOE through the RFprotect Console client software (hereafter referred to as the "Console") and the EngineManager[2] client software interfaces. Both TOE administrator interfaces are mechanisms for interacting with the RFprotect Server (hereafter referred to as the "Server") and as such all audited administrator actions made through either interface are recorded in the Server. The TOE creates an audit record when a TOE administrator causes any of the events in Table 3 above to occur. Audit records are stored within a database which is a subcomponent of the Server. Audit records include the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event[3]. TOE administrators do not have direct access to the database. TOE administrators can read audit records only through the TOE's administrative interfaces, and only when authenticated as described below. TOE administrators are never given write access to the audit records.

Only TOE administrators can read the audit data.

Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_STG.1

6.1.2 Identification and Authentication

This section describes the TOE controls on user access and the user attributes employed by the TOE to make access control decisions. TOE administrators can properly access the TOE in two ways; via the Console client or via the EngineManager client. TOE administrators do not directly access the Sensors. For both methods of access, the identification and authentication mechanism is provided by the Server. The Server stores a username, a hashed password (i.e. authentication data), and the role associated with the administrator (i.e. authorizations), for each TOE administrator. An administrator is authenticated when the hash of the password that has been entered matches the stored hashed password. No actions are allowed on behalf of the administrator prior to identification and authentication of an administrator. Any user attempting to interact with the TOE is presented only with a login screen until successful identification and authentication is completed. A role is assigned to an administrator when the administrator account is created. Login is not permitted if there is no associated role for the administrator.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.1, FIA_UID.1

6.1.3 Security Management

This section describes the role definition and role management functionalities of the TOE. The TOE maintains three (3) roles which are identified in FMT_SMR.1. The roles determine an administrator's level of access to security management functions provided by the TOE. These security management functions are the management of all audit and event records, management of access control, and management of IDS functions used to collect, react to, and analyze data. An administrator can be assigned one role from the list of available roles.

User attempts to manage TOE security functionality and change, query, modify, or delete security attributes originate at the Console or the EngineManager interfaces. All requests for services from either of these interfaces

[1] The TOE's "RogueCheck" function probes the local protected network to determine whether or not a rogue wireless access point is physically connected to the protected local area network. This probe involves communication with various network devices which form the infrastructure of the protected network, such as routers and switches.

[2] EngineManager is run locally on the Server and allows administrators to start, stop, and manage the Server engine.

[3] In some cases, "success" of an event is indicated by the existence of an audit record, and "failure" of an event is indicated by the non-existence of an audit record.

are passed to the Server, which mediates the access control to those functions. The Server makes the access control decision by comparing the administrator's role and the privilege requirement for the type of request made.

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

6.1.4 Protection of the TSF

The TOE provides several mechanisms for protecting its security functions. The TOE protects all TOE Security Function (TSF) data from disclosure when it is transmitted between Sensors and the Server by using direct protection via Network Chemistry's implementation of AES. The Sensors and Server are configured with a shared secret to validate their identity and protect their communications.

The TOE consists of four architecturally separate components that are listed below. Each physical TOE component ensures that security mechanisms cannot be bypassed; however, all TOE components rely on the TOE environment to enforce domain separation.

- RFprotect Server
- RFprotect Console
- RFprotect Sensor
- RFprotect Mobile

The RFprotect Server is a software application which runs on a standard server. This component of the TOE ensures that the security mechanisms cannot be bypassed. The security mechanisms cannot be bypassed because all management and configuration functions of the TOE are carried out only by Authorized TOE Users. All management and configuration operations are conducted in the context of an associated management session. This management session is established only after an administrator has successfully authenticated. Sessions ensure that all future communications within the context of that session are logically linked to the original authentication. All management and configuration operations are checked for conformance to the granted level of access and rejected if non-conformant. The management session is destroyed when the corresponding TOE User logs out of that session. No management functions can be executed by a non-authenticated administrator. This ensures that security protection enforcement functions are invoked and succeed before each function within the TSF scope of control is allowed to proceed.

Protection of the TOE from physical tampering is ensured by its environment. It is the responsibility of the administrator to ensure that the physical connections made to the TOE remain intact and unmodified. The Server runs on standard PC/server hardware on a general purpose operating system; the combination of Server application, the operating system, and the hardware and firmware provide all the services necessary to implement the Server-supported TSFs. The environment (that is, the hardware and operating system hosting the Server) maintains a security domain for the Server's own execution that protects it from interference and tampering by untrusted subjects. The underlying assumption regarding the operation of the Server is that it is maintained in a physically secure environment. Using kernel/user mode switching, the underlying OS controls the execution of each process and ensures that all the information used for management purposes is protected from direct access by any other process. Furthermore, in order to ensure the correct execution of each process, the OS protects each process's private information (executable code, data, and stack) from uncontrolled interferences from other processes. These features ensure that the TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

The RFprotect Console application does not directly enforce any security mechanisms; therefore non-bypassability is not applicable. The RFprotect Console operates in its own domain of execution provided by the underlying operating system and hardware (the environment), which is not part of the TOE.

The RFprotect Sensor is a software application which runs on a dedicated appliance with a proprietary operating system. It contains a wireless network interface which scans the available radio channels in promiscuous mode, *i.e.* it receives and analyses all network traffic which reaches its antennas on the channel which it is currently scanning. This component of the TOE enforces domain separation and ensures that the security mechanisms cannot be bypassed. The tight control of the ability to make configuration changes on the Server ensures that the Sensor

cannot be disabled by an attacker. The logic of wireless protocol processing on the Sensor ensures that all activities indicative of intrusions are reported to the Server; therefore, the sensor will detect and react to all appropriate network traffic and is non-bypassable. All management and configuration operations are conducted in the context of an associated management session. This management session is established only after an administrator has successfully authenticated to the Server and/or to the Sensor. No management functions can be executed by a non-authenticated administrator; this ensures that security protection enforcement functions are invoked and succeed before each function within the TSF scope of control is allowed to proceed. These mechanisms are linked deeply into the operating system (OS) access control, process management, and Transmission Control Protocol (TCP) session management mechanisms. These mechanisms operate correctly because they are protected by the Domain Separation mechanisms.

The RFprotect Mobile TOE component is a self-contained combination of the RFprotect Server software, the RFprotect Sensor software, and the RFprotect Console software running on a standard PC with a general purpose operating system. The Mobile component has a network interface operating in promiscuous mode, *i.e.* it receives and analyzes all network traffic. The Server software and the Console software are configured and implemented exactly as described above; the Sensor software is also configured and implemented as described above, except that the Sensor is not a self-contained appliance, but rather the Sensor software runs on a general purpose operating system.

The Server provides reliable timestamps for its own use. The Server receives time information from the local operating system.

TOE Security Functional Requirements Satisfied: FPT_ITT.1, FPT_RVM.1(1), FPT_SEP.1(1), FPT_STM.1(1)

6.1.5 IDS Component Requirements

The TOE provides intrusion detection functions that include collection of data from sensor and scanner functions as well as analysis functions found within the Server.

The Sensor is used to scan, monitor, and regulate local wireless networks. The Sensor can detect suspicious events by monitoring network traffic from visible network stations. The Sensor collects information about wireless events and sends this information back to the Server which then analyzes the data and generates IDS event records as necessary. The Server provides functionality to view collected IDS event records as well as to determine summary information.

6.1.5.1 Data Collection and Analysis by the RFprotect Sensor

The RFprotect Sensor's primary purpose is to scan various radio frequencies ("channels") via its built-in radio, receive data packets, perform pre-processing on those packets, and send the results to the Server.

The Sensor uses an adaptive algorithm to spend more time on the channels which are currently seeing traffic and less time on the channels that are not seeing traffic. The administrator specifies a default amount of time to spend watching each channel, and the Sensor then adapts this default time based on the traffic that is currently seen on various channels – channels with heavy traffic patterns will get more time, and channels with little traffic will get less time. When the Sensor sees a data packet on a channel, it collects and generates statistical data about the packet and transmits this information to the Server in bursts.

6.1.5.2 Data Collection and Analysis by the RFprotect Server

The RFprotect Server stores all the IDS event records generated by the sensors components of the TOE in a central location for analysis and viewing. The Server stores the IDS event records in a dedicated database. TOE administrators in appropriate roles can read and delete IDS event records through the Server. Alerts are generated and stored in the database for viewing via the RFprotect Console.

The RFprotect Console processes event data from the Server and displays it in a human readable format. It provides tools for sorting, scoring, and listing events.

TOE Security Functional Requirements Satisfied: IDS_NDC.1, IDS_ANL.1, IDS_RCT.1, IDS_RDR.1, IDS_STG.1

6.2 TOE Security Assurance Measures

EAL 2 was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL 2 level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 7 – Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_CAP.2	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 – Configuration Management
ADO_DEL.1	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 – Secure Delivery
ADO_IGS.1	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 - Installation Guide Supplement
ADV_FSP.1	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 – TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_HLD.1	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 – TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_RCR.1	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 – TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
AGD_ADM.1	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 Administrator Guidance Supplement
AGD_USR.1	[User Guides]
ATE_COV.1	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 – Functional Tests and Coverage
ATE_FUN.1	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 – Functional Tests and Coverage
ATE_IND.1	*Generated by Common Criteria Testing Laboratory*
AVA_SOF.1	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 – Vulnerability Assessment
AVA_VLA.1	Network Chemistry RFprotect Distributed v6.1.2, RFprotect Sensor v6.1.22, and RFprotect Mobile v6.1.2 – Vulnerability Assessment

6.2.1 ACM_CAP.2: Configuration Management Document

The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at Network Chemistry. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.2.2 ADO_DEL.1: Delivery and Operation Document

The Delivery and Operation document provides a description of the secure delivery procedures implemented by Network Chemistry to protect against TOE modification during product delivery. The Installation Documentation provided by Network Chemistry details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the TOE Users(s) on configuring the TOE and how they affect the TSF.

6.2.3 ADO_IGS.1: Installation Guidance, AGD_ADM.1: Administrator Guidance, AGD_USR.1: User Guidance

The installation guidance document provides the procedures necessary for the secure installation, generation, and start-up of the TOE for administrators and users of the TOE.

The administrator guidance documentation provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE.

The User Guidance documentation provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they need to be exercised.

6.2.4 ADV_FSP.1: Informal Functional Specification, ADV_HLD.1: High Level Design, ADV_RCR.1: Representation Correspondence.

The Network Chemistry design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Representation Correspondence demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

6.2.5 ATE_COV.1: Test Coverage Analysis, ATE_FUN.1: Functional Testing, ATE_IND.2: Independent Testing

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a

tester, are also provided in order to meet the assurance requirement Functional Testing. Independent Testing will be performed by EWA in order to determine whether the TOE behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests.

6.2.6 AVA_VLA.1: Vulnerability Analysis, AVA_SOF.1: Strength of Function Analysis

A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TOE Security Policy (TSP) and provide a list of identified vulnerabilities. Additionally, this document provides evidence of how the TOE is resistant to obvious attacks.

The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum Strength of Function (SOF) requirements.

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no protection profile claims for this security target.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target.

8.1.1 Security Objectives Rationale Relating to Threats

Table 8 demonstrates the mapping between the threats and the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat.

Table 8 – Relationship of Security Threats to Objectives

Threats \ Objectives		TOE												Environment						
		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.PROTECT	OE.TIME
Threats	T.COMINT	✓						✓	✓			✓							✓	
	T.COMDIS	✓						✓	✓				✓						✓	
	T.LOSSOF	✓						✓	✓			✓								
	T.NOHALT		✓	✓	✓			✓	✓											
	T.PRIVIL	✓						✓	✓											
	T.IMPCON						✓	✓	✓					✓						
	T.INFLUX									✓										
	T.FACCNT										✓									
	T.BLIND														✓					
	T.MSQERADE	✓						✓	✓				✓						✓	
	T.SCNCFG		✓																	
	T.SCNMLC		✓																	
	T.SCNVUL		✓																	
	T.FALACT					✓														
	T.FALREC				✓															
	T.FALASC				✓															
	T.MISUSE			✓							✓									
	T.INADVE			✓							✓									
	T.MISACT			✓							✓									

T.COMINT **An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.**

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the meeting of this policy by ensuring that the environment protects the TOE from bypass attacks.

T.COMDIS **An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.**

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the meeting of this policy by ensuring that the environment protects the TOE from bypass attacks.

T.LOSSOF **An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.**

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.NOHALT **An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.**

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.

T.PRIVIL **An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.**

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.IMPCON **An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.**

The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.

T.INFLUX **An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.**

The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

T.BLIND An attacker may blind the TOE by physically shielding or damaging TOE antennas.

The OE.PHYCAL objective counters this threat by requiring those responsible for the TOE to ensure that the TOE is protected from any physical attack.

T.MSQERADE A network attacker may attempt to imitate a client system in order to gain information about the vulnerabilities of the client system.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the meeting of this policy by ensuring that the environment protects the TOE from bypass attacks.

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a Scanner.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code. The ST will state whether this threat must be addressed by a Scanner.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability. The ST will state whether this threat must be addressed by a Scanner.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

T.MISUSE **Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.**

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.INADVE **Inadvertent activity and access may occur on an IT System the TOE monitors.**

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.MISACT **Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.**

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

8.1.2 Security Objectives Rationale Relating to Assumptions

Table 9 demonstrates the mapping between the threats and the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption.

Table 9 – Relationship of Security Assumptions to Objectives

Assumptions \ Objectives		TOE												Environment						
		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.PROTECT	OE.TIME
Assumptions	A.ACCESS																	✓		
	A.DYNMIC																✓	✓		
	A.ASCOPE																	✓		
	A.PROTCT														✓					
	A.LOCATE														✓					
	A.MANAGE																✓			
	A.NOEVIL													✓	✓	✓				
	A.NOTRUST														✓	✓				
	A.CONNECT			✓										✓						

A.ACCESS **The TOE has access to all the IT System data it needs to perform its functions.**

The OE.INTROP objective ensures the TOE has the needed access.

A.DYNMIC **The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.**

The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.

A.ASCOPE **The TOE is appropriately scalable to the IT System the TOE monitors.**

The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

A.PROTCT **The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.**

The OE.PHYCAL provides for the physical protection of the TOE hardware and software.

A.LOCATE **The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.**

The OE.PHYCAL provides for the physical protection of the TOE.

A.MANAGE **There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.**

The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

A.NOEVIL **The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.**

The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST **The TOE can only be accessed by authorized users.**

The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.CONNECT **The TOE will be installed such that all network traffic will flow through the TOE.**

The OE.INSTAL objective provides for the correct installation of the TOE. The O.IDSENS objective ensures that that TOE is installed in a way that will allow it to monitor and collect all relevant network data.

8.1.3 Security Objectives Rationale Relating to Policies

Table 10 demonstrates the mapping between the threats and the security objectives is complete. The following discussion provides detailed evidence of coverage for each policy.

Table 10 – Relationship of Security Policies to Objectives

Policies \ Objectives		TOE												Environment						
		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.PROTECT	OE.TIME
OSPs	P.DETECT		✓	✓							✓									✓
	P.ANALYZ				✓															
	P.MANAGE	✓					✓	✓	✓					✓		✓	✓			
	P.ACCESS	✓						✓	✓											
	P.ACCACT								✓		✓									✓
	P.INTGTY											✓								
	P.PROTCT									✓					✓				✓	

P.DETECT **Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.**

The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data. Where required these objectives are supported by OE.TIME, the objective that the environment provide reliable timestamps.

P.ANALYZ **Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.**

The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.

P.MANAGE **The TOE shall only be managed by authorized users.**

The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCESS **All data collected and produced by the TOE shall only be used for authorized purposes.**

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCACT **Users of the TOE shall be accountable for their actions within the IDS.**

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. Where required these objectives are supported by OE.TIME.

P.INTGTY **Data collected and produced by the TOE shall be protected from modification.**

The O.INTEGR objective ensures the protection of data from modification.

P. PROTCT **The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.**

The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the meeting of this policy by ensuring that the environment protects the TOE from external entities.

8.2 Security Functional Requirements Rationale

Table 11 and the following discussion provides detailed evidence of coverage for each security objective.

Table 11 – Relationship of Security Requirements to Objectives

	Objectives / Requirements	TOE												Env.	
		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	OE.PROTECT	OE.TIME
TOE	FAU_GEN.1										✓				
	FAU_SAR.1						✓								
	FAU_STG.1	✓						✓	✓	✓		✓			
	FIA_ATD.1								✓						
	FIA_UAU.1							✓	✓						
	FIA_UID.1							✓	✓						
	FMT_MOF.1	✓						✓	✓						
	FMT_MTD.1(1)	✓						✓	✓			✓			
	FMT_SMF.1	✓						✓	✓			✓			
	FMT_SMR.1								✓						
	FPT_ITT.1											✓	✓		
	FPT_RVM.1(1)	✓					✓		✓		✓	✓			
	FPT_SEP.1(1)	✓					✓		✓		✓	✓			
	FPT_STM.1(1)										✓				
	IDS_NDC.1		✓	✓											
	IDS_ANL.1				✓										

		TOE											Env.	
	IDS_RCT.1					✓								
	IDS_RDR.1						✓	✓	✓					
	IDS_STG.1	✓						✓	✓	✓		✓		
Env	FPT_RVM.1(2)												✓	
Env	FPT_SEP.1(2)												✓	
Env	FPT_STM.1(2)													✓

The following discussion provides detailed evidence of coverage for each security objective.

O.PROTCT **The TOE must protect itself from unauthorized modifications and access to its functions and data.**

The TOE is required to protect the audit data from deletion [FAU_STG.1]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure, or attack [IDS_STG.1]. The TOE should provide facilities to enable the authorized user to manage the TOE [FMT_SMF.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5)]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)].

O.IDSCAN **The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.**

A System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected must be defined in the ST [IDS_NDC.1].

O.IDSENS **The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.**

A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [IDS_NDC.1].

O.IDANLZ **The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).**

The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].

O.RESPON **The TOE must respond appropriately to analytical conclusions.**

The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].

O.EADMIN **The TOE must include a set of functions that allow effective management of its functions and data.**

The TOE must provide the ability to review the audit trail of the System [FAU_SAR.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)].

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion [FAU_STG.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE should provide facilities to enable the authorized user to manage the TOE [FMT_SMF.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5)].

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.1]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure, or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE should provide facilities to enable the authorized user to manage the TOE [FMT_SMF.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5)]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)].

O.OFLOWS The TOE must appropriately handle potential System data storage overflows.

The TOE is required to protect the audit data from unauthorized deletion [FAU_STG.1]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1].

O.AUDITS The TOE must record audit records for data accesses and use of the System functions.

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1(1)]. Time stamps associated with an audit record must be reliable [FPT_STM.1(1)].

O.INTEGR The TOE must ensure the integrity of all audit and System data.

The TOE is required to protect the audit data from deletion [FAU_STG.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. The TOE should provide facilities to enable the authorized user to manage the TOE [FMT_SMF.1]. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5)]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITT.1]. The TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)].

O.EXPORT **When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the System data.**

The TOE must protect all data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITT.1].

OE.TIME **The IT Environment will provide reliable timestamps to the TOE**

The IT environment of the Sensor is required to provide reliable timestamps to the Sensor [FPT_STM.1(2)]

OE.PROTECT **The IT environment will protect itself and the TOE from external interference or tampering.**

The IT environment must ensure that all functions to protect the data are not bypassed [FPT_RVM.1(2)]. The IT environment must protect the TOE from interference that would prevent it from performing its functions [FPT_SEP.1(2)].

8.3 Security Functional Requirement Refinement Rationale

FPT_ITT.1.1 was refined to more clearly describe the transmission of data within the TOE.

8.4 Security Assurance Requirements Rationale

EAL 2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL 2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.5 Rationale for Explicitly Stated Requirements

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

8.6 Rationale for Strength of Function

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial and Department of Defense (DoD) low robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in Section 4.

8.7 Dependency Rationale

This ST satisfies all the requirement dependencies of the Common Criteria. Table 12 Functional Requirement Dependencies lists each requirement from the ST with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 12 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met
FAU_GEN.1	FPT_STM.1	✓
FAU_SAR.1	FAU_GEN.1	✓
FAU_STG.1	FAU_GEN.1	✓
FIA_UAU.1	FIA_UID.1	✓
FMT_MOF.1	FMT_SMF.1 and FMT_SMR.1	✓
FMT_MTD.1(1)	FMT_SMF.1 and FMT_SMR.1	✓
FMT_MTD.1(2)	FMT_SMF.1 and FMT_SMR.1	✓
FMT_MTD.1(3)	FMT_SMF.1 and FMT_SMR.1	✓
FMT_MTD.1(4)	FMT_SMF.1 and FMT_SMR.1	✓
FMT_MTD.1(5)	FMT_SMF.1 and FMT_SMR.1	✓
FMT_SMR.1	FIA_UID.1	✓

8.8 TOE Summary Specification Rationale

8.8.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 13 identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism. For an analysis of the Strength of Function (SOF), please refer to Section 8.6.

Table 13 – Mapping of Security Functional Requirements to TOE Security Functions

TOE Security Function	SFR	Rationale
Security Audit	FAU_GEN.1	This requires that appropriate audit records are generated.
	FAU_SAR.1	This requires that the audit records are viewable only by authorized administrators.

TOE Security Function	SFR	Rationale
	FAU_STG.1	This requires that the audit records are protected from unauthorized deletion.
Identification and Authentication	FIA_ATD.1	This requires that the TOE stores information required to make identification and authentication decisions.
	FIA_UAU.1	These require that administrators must identify themselves and be authenticated before being allowed access to the TSF.
	FIA_UID.1	
Security Management	FMT_MOF.1	This requires that only authorized administrators can modify the behaviour of the security functions.
	FMT_MTD.1	This requires that only authorized administrators can modify security attributes.
	FMT_SMF.1	This requirement defines what management functions are available.
	FMT_SMR.1	This requirement defines the roles used for access control.
Protection of the TSF	FPT_ITT.1	This requirement protects the confidentiality and integrity of data flowing between physically distinct components of the TOE.
	FPT_RVM.1(1)	This requirement ensures the TSF are not bypassable.
	FPT_SEP.1(1)	This requirement ensures the TOE has a separate domain of operation.
	FPT_STM.1(1)	This requirement ensures the TOE provides reliable timestamps.
IDS Component Requirements	IDS_NDC.1	This requirement ensures that IDS data is gathered.
	IDS_ANL.1	This requirement ensures that IDS data is analyzed.
	IDS_RCT.1	This requirement ensures that IDS data is reacted to.
	IDS_RDR.1	This requirement ensures that IDS data can only be viewed by authorized administrators
	IDS_STG.1	This requirement ensures that IDS data is stored appropriately..

8.8.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL 2 was chosen to provide a basic level of independently assured security. The chosen assurance level is consistent with the postulated threat environment. Although the system may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond to this environment. Therefore, the threat of malicious attacks is considered to be not greater than moderate. At EAL 2, the system will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.8.2.1 Configuration Management

The Configuration Management documentation provides a description of tools used to control the configuration items and how they are used at Network Chemistry. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system describes the procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

8.8.2.2 Delivery and Operation

The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by Network Chemistry to protect against TOE modification during product delivery. The Installation Documentation provided by Network Chemistry details the procedures for installing the TOE and placing the TOE in a secure state. The Installation Documentation provides guidance to the administrators of the TOE regarding configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

8.8.2.3 Development

The Network Chemistry design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Descriptive High-Level Design
- Informal Representation Correspondence

8.8.2.4 Guidance Documentation

The Network Chemistry Guidance documentation provides administrator guidance on how to securely operate the TOE. The administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information for administration of the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. Network Chemistry provides single versions of documents which address the administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance

8.8.2.5 Tests

Three components make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Network Chemistry Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a

tester, are also provided. The Common Criteria Testing Laboratory generates and performs a separate test plan in order to independently verify the accuracy and completeness of the functional testing.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing
- Independent Testing

8.8.2.6 Vulnerability and TOE Strength of Function Analyses

A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

Corresponding CC Assurance Components:

- Strength of TOE Security Function analysis
- Vulnerability Analysis

8.9 Strength of Function

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL 2 assurance requirements. This SOF is sufficient to resist the threats identified in Section 3. Section 4 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information.

The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2 Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8.2 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements.

The relevant security function and security functional requirement which has probabilistic or permutational functions is FIA_UAU.1

9 Acronyms

Table 14 – Acronyms

Acronym	Definition
CC	Common Criteria
DoD	Department of Defense
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
IT	Information Technology
OS	Operating System
OSP	Organizational Security Policy
PC	Personal Computer
PCI	Peripheral Component Interconnect
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy