

**nCircle™  
IP360™ Vulnerability  
Management System V6.3.4  
Vulnerability and Exposure Manager  
(VnE 1000 and VnE 3000)  
Device Profiler  
(DP 1000 and DP 2000)  
nTellec™ 2000**

**Security Target**

Version 2.1  
May 11, 2005

Prepared for:



nCircle™ Network Security, Inc.  
101 Second Street Suite 400  
San Francisco, CA 94105

Prepared by:



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

## Table of Contents

---

<b>TABLE OF CONTENTS</b>	<b>2</b>
<b>LIST OF TABLES</b>	<b>5</b>
<b>LIST OF FIGURES</b>	<b>5</b>
<b>1 SECURITY TARGET INTRODUCTION</b>	<b>6</b>
1.1 Security Target, TOE and CC Identification	6
1.2 Conformance Claims	7
1.3 Strength of Environment	7
1.4 Conventions, Acronyms and Terminology	7
1.4.1 Conventions	7
1.4.2 Acronyms and Terminology	8
<b>2 TOE DESCRIPTION</b>	<b>9</b>
2.1 Product Type	9
2.2 Product Description	9
2.2.1 VnE Manager	10
2.2.2 Device Profiler	10
2.2.3 nTellect™	11
2.3 TOE Boundaries and Scope	11
2.3.1 Physical Boundary	11
2.3.2 Logical Boundary	15
2.3.2.1 Audit	15
2.3.2.2 Identification and Authentication	15
2.3.2.3 Security Management	15
2.3.2.4 Protection of the TSF	16
2.3.2.5 TOE Access	16
2.3.3 Scope	16
2.4 TOE Security Functional Policies (SFP)	18
2.4.1 Restricted User SFP (RU_SFP)	18
<b>3 TOE SECURITY ENVIRONMENT</b>	<b>19</b>
3.1 Secure Usage Assumptions	19
3.2 Threats to Security	19
3.2.1 Threats Addressed by the TOE	19

<b>4</b>	<b>SECURITY OBJECTIVES</b>	<b>21</b>
4.1	Security Objectives for the TOE	21
4.2	Security Objectives for the TOE Environment	21
<b>5</b>	<b>SECURITY REQUIREMENTS</b>	<b>22</b>
<b>5.1</b>	<b>TOE Security Functional Requirements</b>	<b>22</b>
5.1.1	Security Audit	22
5.1.1.1	FAU_GEN.1 Audit data generation	22
5.1.1.2	FAU_SAR.1 Audit review	23
5.1.1.3	FAU_SAR.3 Selectable Audit review	23
5.1.1.4	FAU_STG.1 Security audit event storage	24
5.1.2	Identification and Authentication	24
5.1.2.1	FIA_AFL.1 Authentication Failure	24
5.1.2.2	FIA_ATD.1 User Attribute Definition	24
5.1.2.3	FIA_UAU.2 User Authentication	25
5.1.2.4	FIA_UID.2 User Identification	25
5.1.3	Security Management	25
5.1.3.1	FMT_MOF.1 Management of functions in TSF	25
5.1.3.2	FMT_MTD .1 Management of TSF Data	26
5.1.3.3	FMT_SMF.1 Specification of Management Functions	26
5.1.3.4	FMT_SMR .1 Security Management Role	27
5.1.4	Protection of the TSF	27
5.1.4.1	FPT_RVM.1 Non-bypassability of the TSP	27
5.1.4.2	FPT_STM.1 Time Stamps	27
5.1.5	TOE Access	27
5.1.5.1	FTA_SSL.3 TSF-Initiated Termination	27
<b>5.2</b>	<b>TOE Environmental Security Functional Requirements</b>	<b>27</b>
5.2.1	Protection of the TSF	27
5.2.1.1	FPT_STM.1 Time Stamps	27
<b>5.3</b>	<b>TOE Security Assurance Requirements</b>	<b>28</b>
<b>6</b>	<b>TOE SUMMARY SPECIFICATION</b>	<b>29</b>
<b>6.1</b>	<b>TOE Security Functions</b>	<b>29</b>
6.1.1	Security Audit (FAU)	29
6.1.1.1	Audit Re view	29
6.1.1.2	Security Audit Event Storage	30
6.1.2	Identification and Authentication (FIA)	30
6.1.2.1	Authentication Failure	31
6.1.2.2	User Attribute Definition	31
6.1.2.3	User Authentication and Identification	31
6.1.3	Security Management (FMT)	32
6.1.4	Protection of the TSF (FPT)	33
6.1.5	TOE Access (FTA)	34
<b>6.2</b>	<b>TOE Security Assurance Measures</b>	<b>35</b>
<b>7</b>	<b>PROTECTION PROFILE CLAIMS</b>	<b>36</b>

<b>8</b>	<b>RATIONALE</b>	<b>37</b>
8.1	Security Objectives Rationale	37
8.2	Security Functional Requirements Rationale	40
8.3	Rational For Refinements of Security Functional Requirements	43
8.4	Security Assurance Requirements Rationale	44
8.5	Dependency Rationale	46
8.6	TOE Summary Specification Rationale	47
8.7	Strength of Function Rationale	49
<b>9</b>	<b>ACRONYMS AND TERMS</b>	<b>50</b>

## List of Tables

---

TABLE 1 ST AND TOE IDENTIFICATION	6
TABLE 2 COMMUNICATIONS DONE USING OPENSLL	10
TABLE 3 EVALUATED VERSIONS OF THE TOE COMPONENTS	11
TABLE 4 VNE MANAGER TECHNICAL SPECIFICATIONS	12
TABLE 5 DP TECHNICAL SPECIFICATIONS	13
TABLE 6 NTELLECT™ TECHNICAL SPECIFICATIONS	13
TABLE 7 LIST OF COMPONENTS NOT INCLUDED IN THE TOE	15
TABLE 8 LIST OF SUPPORTED BROWSERS FOR THE IP360™	16
TABLE 9 FUNCTIONAL REQUIREMENTS FOR THE TOE MAPPED TO ST OPERATIONS	22
TABLE 10 AUDIT EVENTS	23
TABLE 11 AUDIT RECORDS	23
TABLE 12 USER SECURITY ATTRIBUTES	25
TABLE 13 VNE GUI ADMINISTRATIVE INTERFACE FUNCTIONS	25
TABLE 14 VNE CLI ADMINISTRATIVE INTERFACE FUNCTIONS	26
TABLE 15 DP/NTELLECT™ CLI ADMINISTRATIVE INTERFACE FUNCTIONS	26
TABLE 16 FUNCTIONAL REQUIREMENTS FOR THE TOE MAPPED TO ST OPERATIONS	27
TABLE 17 ASSURANCE MEASURES MAPPING TO SECURITY ASSURANCE REQUIREMENTS (SARS)	35
TABLE 18 SECURITY ENVIRONMENT VS. OBJECTIVES	37
TABLE 19 MAPPING OF FUNCTIONAL REQUIREMENTS TO OBJECTIVES	40
TABLE 20 FUNCTIONAL REQUIREMENTS DEPENDENCIES	46
TABLE 21 MAPPING OF SECURITY FUNCTIONAL REQUIREMENTS TO TOE SECURITY FUNCTIONS	47

## List of Figures

---

FIGURE 1 VNE MANAGER .....	12
FIGURE 2 DEVICE PROFILER.....	12
FIGURE 3 NTELLECT™.....	13
FIGURE 4 NCIRCLE™ APPLIANCES SIMILARITIES .....	13
FIGURE 5 CONFIGURATION 1 OF PHYSICAL BOUNDARY .....	14
FIGURE 6 CONFIGURATION 2 OF PHYSICAL BOUNDARY .....	14

# 1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE) identification, ST conventions, ST conformance claims and the ST organization. The Target of Evaluation is the nCircle™ IP360™ Vulnerability Management System V6.3.4.

The IP360™ Vulnerability Management System V6.3.4 is a Vulnerability Management system that monitors a network and assesses in real-time the vulnerabilities of the IP enabled devices that are linked to it. More detail about the TOE is provided in section 2.

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to 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.
- Security Environment (Section 3) – Describes the threats and assumptions that pertain to the TOE and the TOE environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its supporting environment.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE.
- 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 and Terms (Section 9) – Defines the acronyms and terms used within this ST.

## 1.1 Security Target, TOE and CC Identification

**Table 1 ST and TOE Identification**

<b>ST Title</b>	nCircle™ IP360™ Vulnerability Management System V6.3.4 Vulnerability and Exposure Manager (VnE 1000 and VnE 3000) Device Profiler (DP 1000 and DP 2000) nTelect™ 2000 Security Target
<b>ST Version</b>	2.1
<b>ST Date</b>	May 11, 2005
<b>TOE Identification</b>	nCircle™ IP360™ Vulnerability Management System V6.3.4 Vulnerability and Exposure Manager (VnE 1000 and VnE 3000) Device Profiler (DP 1000 and DP 2000) nTelect™ 2000
<b>Common Criteria (CC) Identification</b>	Common Criteria for Information Technology Security Evaluation, Version 2.2 r256, January 2004; Parts 2 and 3 (aligned with ISO/IEC 15408:2004)  International Common Criteria interpretations through kick-off meeting date 10/07/2004 have been incorporated and are identified as follows: None.

<b>Assurance Level</b>	Evaluation Assurance Level (EAL) 3
<b>Keywords</b>	VnE, Device Profiler, Vulnerability Assessment,
<b>Author</b>	Corsec Security, Inc.

The Target of Evaluation (TOE) is hereafter referred to as the nCircle™ IP360™ Vulnerability Management System V6.3.4.

## 1.2 Conformance Claims

The TOE is CC Version 2.2r256 Part 2 and Part 3 conformant plus applicable interpretations, and conformance to Evaluation Assurance Level 3 is claimed.

## 1.3 Strength of Environment

The nCircle™ IP360™ Vulnerability Management System V6.3.4 hereafter called IP360™, safely identifies network vulnerabilities early enough to allow a measurable and structured proactive protection approach of digital assets.

The IP360™ is designed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.

The IP360™ must be protected from physical attacks i.e. access to the facility housing the system must be monitored and restricted to authorized users. All components of the TOE will be protected by restricting physical access to these components to only the TOE users.

The TOE Components are required to remain physically connected to the targeted network in order to maintain network assessment functionalities.

To ensure that the design of the IT networks is acknowledged and that the risks to the target environment are adequately addressed, the assurance requirements for EAL3, and the minimum strength of function, SOF-basic, were chosen.

## 1.4 Conventions, Acronyms and Terminology

### 1.4.1 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 is/are used within this ST. These operations are presented in the same manner in which they appear in Part 2 and 3 of the CC with the following exceptions:

- A) Changes based upon Interpretations are identified using ***red bolded italicized text***
- B) Completed assignment statements are identified using [*italicized text within brackets*]
- C) Completed selection statements are identified using *underlined italicized text*
- D) Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSE-Data~~) and should be considered as a refinement
- E) 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.

## **1.4.2 Acronyms and Terminology**

Please refer to section 9 for a complete list of the acronyms and terms used within this ST.



## 2 TOE Description

This section describes the TOE as an aid to understanding the general capabilities and security requirements provided by the TOE. The TOE description provides the context for the evaluation, in other words the boundary of evaluation detailing what specifically is being evaluated and what is outside the scope of evaluation.

### 2.1 Product Type

The IP360™ is a Vulnerability Management system that monitors a network and assesses in real time the vulnerabilities of the IP enabled devices that are linked to it.

The IP360™ consists of the three physical components listed below

- Vulnerability and Exposures Manager (VnE)
- Device Profiler (DP)
- nTellec™ (which is an optional component)

This evaluation addresses the two configurations of the IP360™ listed below

- Configuration 1 includes one VnE, one Device Profiler, and one nTellec™.
- Configuration 2 includes one VnE and one Device Profiler.

The nTellec™ is an optional component of the IP360™ that, if added, improves the overall vulnerability assessment of the targeted network by mitigating the number of false positives alerts from Cisco's Secure IDS product.

The VnE, DP and nTellec™ are IP enabled devices that work individually and together. The vulnerability assessment provided by the IP360™ relies on the collaboration of the VnE, DP, and nTellec™ (if included in the configuration). The IP360™ collects information about a specific network and identifies IP enabled devices on that network that could have vulnerabilities to known attacks.

### 2.2 Product Description

The components of the IP360™ work together to provide a service to collect information about a specific network and identify IP enabled devices on that network that could have vulnerabilities to known attacks. The two network assessment appliances, the Device Profiler and nTellec™ gather information or communicate with IP enabled devices and communicate with the VnE to push or pull needed information. The VnE and Device Profiler are present in all configurations of the TOE; the nTellec™ is an optional component that adds additional analysis capabilities. The Device Profiler's role is to continuously scan the targeted network infrastructure. In the scanning process, the Device Profiler continually discovers new IP enabled devices and applications on the network. The Device profiler then indicates to the VnE, in real time, what vulnerabilities have been identified on which devices. The vulnerability information is uploaded continuously, in real time, into the nTellec™ via the VnE.

The nTellec™ analyzes attack events based upon known network attacks and the known configurations of the IP-enabled devices on the network in such a way that false positives are reduced.

The nTellec™'s role is to proactively utilize the collected vulnerability information as a proactive resource in its task of analyzing attack events received from specific IP enabled devices on the targeted network. The nTellec™ analyzes attack events based upon known network attacks and the known configurations of the IP-enabled devices on the network in such a way that false positives are reduced. The nTellec™ seals the analysis of each attack event by tagging it appropriately before archiving it. Therefore the resources allocated to address attacks are always proportional to the validity of the attack. When an nTellec™ is not present, this additional nTellec™-specific vulnerability analysis is not performed by the TOE. In addition to storing the findings of the Device Profiler in its database or uploading them into the nTellec™ RAM, the VnE uses the findings of the Device Profiler to build a report, to educate the administrator and the restricted user (as determined by the RU\_SFP) on the state of vulnerabilities that are present in the network.

The IP360™ Vulnerability Management System v6.3.4 utilizes OpenSSL to protect inter-system communications as well as communication between the system and some IT environmental components. As of yet, OpenSSL is not a FIPS 140-2 validated crypto module; thus, no CC claims have been made about the product's cryptographic capabilities or protection of data when transmitted between separate parts of the system.

Table 2 details all the communications that are done using OpenSSL. In Table 2, a check mark indicates that the communication between the applicable devices is done using OpenSSL, no check mark indicates that the communication between the applicable devices is not done using OpenSSL and the communications that are not applicable are colored in black.

**Table 2 Communications Done Using OpenSSL**

	VnE	DP	nTellec™	NTP Server	Software Repository	VnE GUI Workstation	DP CLI Workstation	nTellec™ CLI Workstation	VnE CLI Workstation	IP Enabled Devices
VnE		v	v		v	v				
DP	v									
nTellec™	v									

The appliance is carefully designed to protect itself from tampering or bypass by untrusted code and users. The maintenance of a security domain for the appliance that protects it from interference and tampering by untrusted subjects and non-bypassability of the security policies are done by the hardware and the underlying hardened operating system. The components of the appliance mutually trust each other; the trusted software applications that mediate access to various objects within the appliance ensure proper domain separation.

### 2.2.1 VnE Manager

The VnE Manager is the central management tool for the IP360™ and, as such, has many functions.

**Central Data Repository:** The VnE primarily serves as a central data repository for both the DP and the nTellec™ in Configuration 1 and only the DP in Configuration 2. In this role, the VnE is passive, receiving connections instead of initiating them.

**Alerts:** The VnE stores all alert configurations and manages all alerts. All alerts (SNMP traps and SMTP messages) are issued from the VnE, based on user-defined alert definitions, system alert definitions, and the vulnerability and attack data submitted by the DP. Typically alerts are just informational.

**User Interface:** The VnE serves as the IP360™'s interface to the end-user, accessible via a web browser, using Transport Layer Security (TLS). Users can access network profile and attack data, and administrators can configure all appliances and the networks assigned to them.

### 2.2.2 Device Profiler

The Device Profiler is configured to continually profile a section, or sections, of network space specified in blocks of IP addresses. As such, several steps are involved in this process.

**Host Discovery:** While scanning the targeted network, the DP discovers which IP addresses in its assigned range have live devices attached to them. In other words, it detects all the IP enabled devices that are linked to the targeted network.

**Application Detection:** Besides discovering IP enabled devices, the DP performs application detection on the open ports it found while performing port scans.

**Operating System Classification:** After performing application detection, the DP categorizes the IP enabled devices found on the network by operating system.

**Vulnerability Assessment:** After gathering enough information about the IP enabled devices on the network and the network itself, the DP performs a quantification of the vulnerability.

**Reports Findings to the VnE:** While performing a continuous scanning of the targeted network, the DP reports in real-time its vulnerability findings. The reported information is stored in the VnE database.

### 2.2.3 nTellec™

As a continuous process, vulnerability information discovered by the Device Profiler (DP) is transferred to the VnE. After being stored in the database of the VnE, the vulnerability information is downloaded by the nTellec™ from the VnE. The vulnerability information is then used by the nTellec™ as a tool to analyze the information received from other IP enabled devices in the targeted network. The purpose of adding the nTellec™ into the configuration is to help decrease false positives and tag attack events appropriately before archiving them. The nTellec™ seals the analysis of each attack event by tagging it appropriately before archiving it. Therefore the resources allocated to address attacks are always proportional to the validity of the attack.

As such, the two main purposes of the nTellec™ are listed below:

- Greatly decrease false positives
- Appropriately tag each attack event before archiving it

## 2.3 TOE Boundaries and Scope

### 2.3.1 Physical Boundary

The physical boundary of Configuration 1 includes

- The VnE – Hardware, software, and operating system
- The Device Profiler – Hardware, software, and operating system
- The nTellec™ – Hardware, software, and operating system

The physical boundary of Configuration 2 includes

- The VnE – Hardware, software, and operating system
- The Device Profiler – Hardware, software, and operating system

Details of each evaluated component of the TOE are shown in Table 3.

**Table 3 Evaluated Versions of the TOE Components**

TOE Component	Operating System	Software Version	Hardware	Other Information
VnE	FreeBSD v4.7	nCircle™ IP360™ Vulnerability Management System V6.3.4	VnE 1000 and VnE 3000	The FreeBSD Operating system was customized to fit VnE functionalities
Device Profiler	FreeBSD 4.9	nCircle™ IP360™ Vulnerability Management System V6.3.4	DP 1000 and DP 2000	The FreeBSD Operating system was customized to fit DP functionalities
nTellec™	FreeBSD 4.9	nCircle™ IP360™ Vulnerability Management System V6.3.4	nTellec™ 2000	The FreeBSD Operating system was customized to fit nTellec™ functionalities

The TOE components run different versions of a modified and hardened FreeBSD. The FreeBSD Operating System was customized to fit the functionalities of the TOE components.

The VnE is produced at two performance levels, the VnE 1000 and the VnE 3000. Both VnE appliances provide the same functionality; they differ only in network throughput and performance, because of different CPUs, RAM capacity, number of disk drives, and number of network ports. As such, the VnE 1000 and the VnE 3000 will be referenced as VnE throughout the ST. All of the non-essential processes that are part of the FreeBSD operating system have been removed, and there is no method of accessing the operating system directly.

Figure 1 shows a picture of the VnE and Table 4 lists the technical specifications of both the VnE 1000 and VnE 3000.



**Figure 1 VnE Manager**

**Table 4 VnE Manager Technical Specifications**

	<b>Network Ports</b>
VnE 1000	3 integrated auto-negotiate 10/100/1000 Ethernet ports
VnE 3000	3 integrated auto-negotiate 10/100/1000 Ethernet ports

The Device Profiler appliance is produced at two performance levels, the DP 1000 and the DP 2000. Both DP appliances provide the same functionality; they differ only in network throughput and performance, because of different CPUs and RAM capacity. As such, both the DP 1000 and DP 2000 will be referenced as DP throughout the ST. All of the non-essential processes that are part of the FreeBSD operating system have been removed, and there is no method of accessing the operating system directly.

Figure 2 shows a picture of the DP and Table 5 lists technical specifications of both the DP 1000 and the DP 2000.



**Figure 2 Device Profiler**

**Table 5 DP Technical Specifications**

	<b>Network Ports</b>
DP 1000	3 integrated auto-negotiate 10/100 Ethernet ports
DP 2000	3 integrated auto-negotiate 10/100 Ethernet ports

The nTellec™ appliance is only produced at one performance level. The nTellec™ leverages the exact same hardware as the DP2000. All of the non-essential processes that are part of the FreeBSD operating system have been removed, and there is no method of accessing the operating system directly.

Figure 3 shows a picture of the nTellec™ and Table 6 lists its technical specifications.

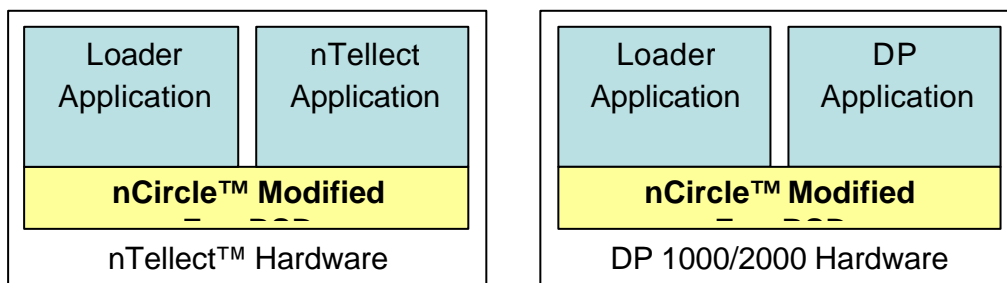


**Figure 3 nTellec™**

**Table 6 nTellec™ Technical Specifications**

	<b>Network Ports</b>
nTellec™	3 integrated auto-negotiate 10/100 Ethernet ports

As mentioned and detailed earlier, this evaluation focuses on two configurations – configuration 1 is shown in Figure 5 – configuration 2 is shown in Figure 6. These two TOE configurations are detailed as two configurations and not two separate TOE boundaries because of the similarities between the Device Profiler and the nTellec™ (see Figure 4). The DP and nTellec™ appliance run the same operating system and the same set of communication applications run to enable communication with the VnE. In fact, there is only one application that is different between the two appliances, which focus on the actual communication with other IP enabled devices on the target network. All other functionality that relates to the security functions claimed in this Security Target is implemented in the executables that are identical between the two appliance types.



**Figure 4 nCircle™ Appliances Similarities**

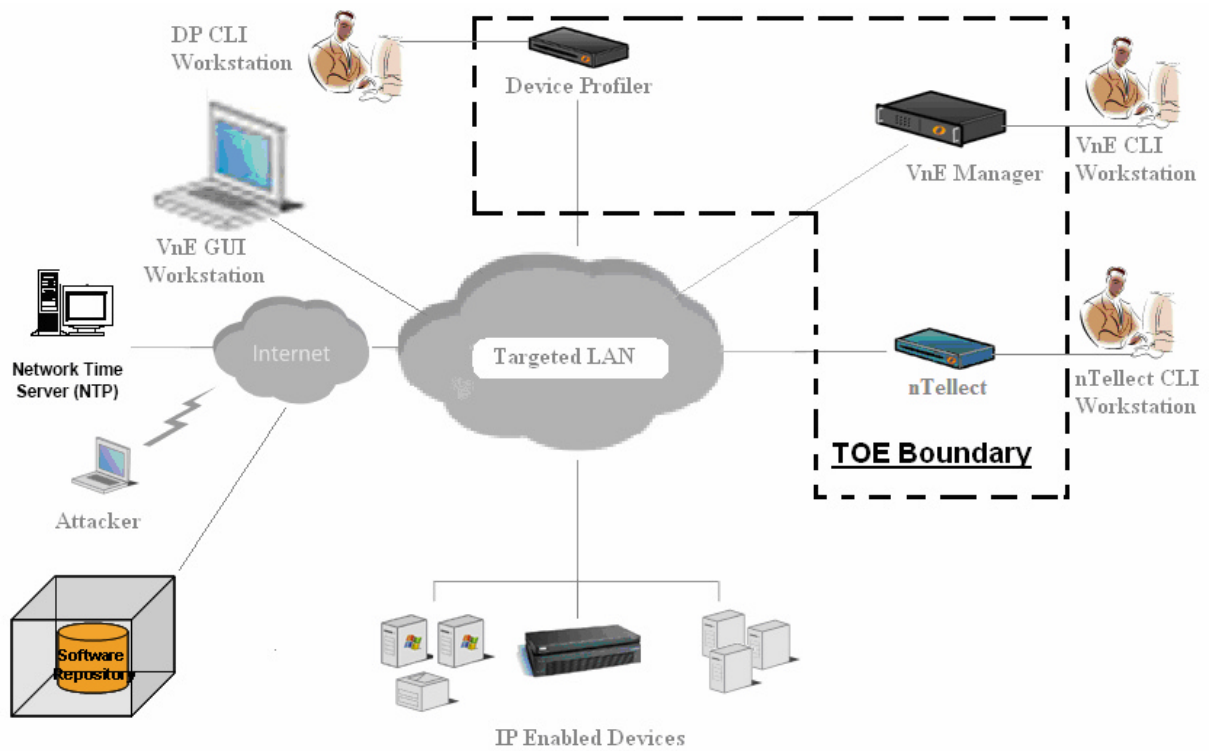


Figure 5 Configuration 1 of Physical Boundary

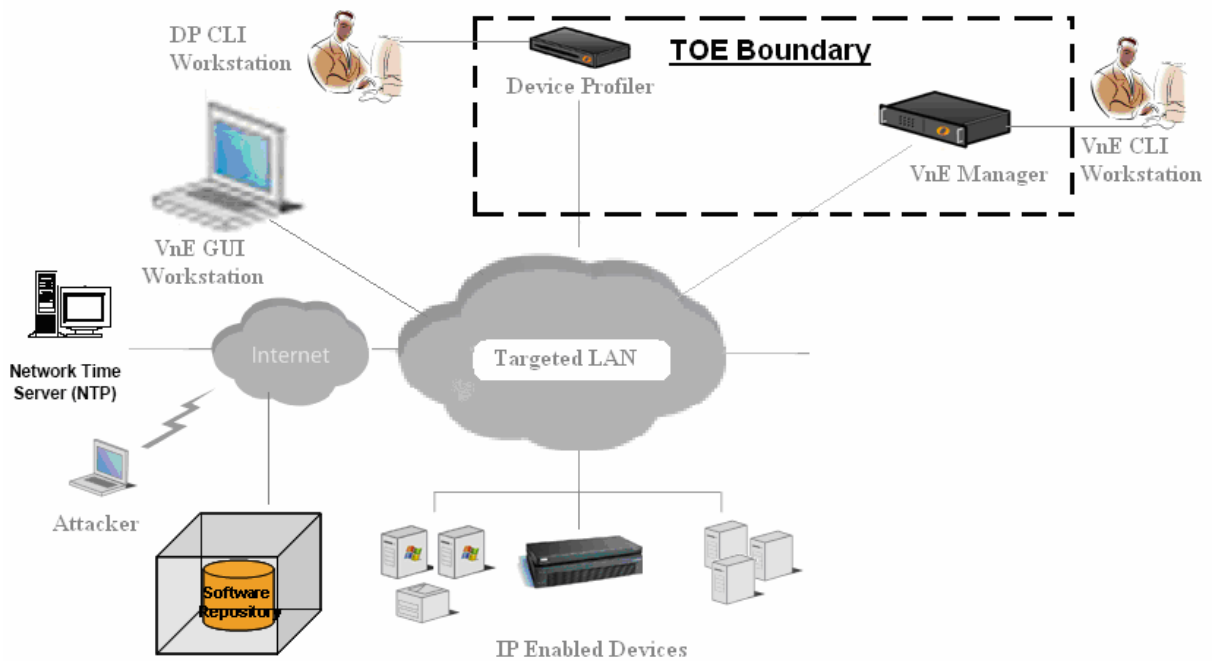


Figure 6 Configuration 2 of Physical Boundary

A list of components and entities that are outside the TOE boundary is included in Table 7. Note that the VnE GUI Workstation is not part of the TOE boundary; however, the VnE GUI itself is part of the TOE boundary and resides in the VnE hardware.

**Table 7 List of Components not Included in the TOE**

<b>Components not Included in the TOE</b>
VnE GUI Workstation
Network Time Server (NTP)
IP Enabled Devices
VnE CLI Workstation
DP CLI Workstation
nTellec™ CLI Workstation
Software Repository
Attacker

## 2.3.2 Logical Boundary

The Logical Boundary of the TOE includes the functions of the TOE listed below:

- Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

### 2.3.2.1 Audit

Audit data of the TOE is stored in a database in the VnE. A critical piece of this product is auditing/logging and maintaining the integrity of the gathered data. The TOE controls access to the audited data whether it is user activity audit records or the data gathered on TOE system functions. The data can be viewed, sorted, ordered and searched by the users of the VnE GUI.

### 2.3.2.2 Identification and Authentication

TOE users must identify themselves and be authenticated in order to gain access to services provided by the TOE. The TOE components provide several entry points for administrators to manage and use the TOE. The VnE provides a Graphical User Interface and a Command Line Interface (CLI) which requires password authentication to access. The Device Profiler and the nTellec™ also each provide a CLI which requires password authentication to configure basic appliance settings. The VnE GUI addresses password guessing attacks by disabling a user's account after three failed attempts to authenticate. The CLI does not address password guessing attacks.

### 2.3.2.3 Security Management

The administrator and restricted user (as determined by the RU\_SFP) are provided with a graphic user interface (GUI) to perform configuration and troubleshooting tasks. Alternatively, the VnE CLI admin and the DP/nTellec™ admin can perform configuration tasks using the CLI Interface.

The TOE maintains four roles, which can be further specified based on very granular privilege controls in the VnE: administrator, restricted user (as determined by the RU\_SFP), VnE CLI admin<sup>1</sup>, and DP/nTellec™<sup>2</sup> CLI admin. These roles of human users that will interact with the TOE will be generally referred to as the IP360™ Users, or just user(s).

<sup>1</sup> The VnE CLI Admin role is performed by the administrator role.

<sup>2</sup> The DP/nTellec™ Admin role is performed by the administrator role.

### 2.3.2.4 Protection of the TSF

The TOE components derive the time used for auditing and logging from the same source, ensuring that records from different devices all reflect the same time source.

The appliance is carefully designed to protect itself from bypass by users. The user does not have access to the operating system and user authentication must occur prior to any actions being performed.

### 2.3.2.5 TOE Access

Session activity is monitored by the TOE. Sessions that have not shown activity in a configurable amount of time are automatically terminated. As such, user activities are disabled and the user needs to log back in for another session.

### 2.3.3 Scope

The TOE environment is composed of the following:

The VnE GUI Workstation

The NTP Server

The IP Enabled Devices

The VnE CLI Workstation

The DP CLI Workstation

The nTellec™ CLI Workstation

The Software Repository

The Attacker

The VnE GUI Workstation:

- Provides an underlying operating system and the monitor, keyboard, and mouse for the TOE user to interact with the web browser interface that is served by the VnE appliance.
- Supports the viewing of the VnE provided interface for administration of the TOE

The VnE can be administered remotely from any machine running a web browser that is included in Table 8:

**Table 8 List of Supported Browsers for The IP360™**

Supported Browsers	Detail
Internet Explorer 5.5® and higher	On Microsoft Windows® operating systems
Netscape Navigator® 7	On Macintosh®, Microsoft Windows®, and Linux operating systems
Mozilla® 1.4, 1.5, 1.6	On Macintosh®, Microsoft Windows®, and Linux operating systems

The VnE GUI Workstation component is evaluated as a required entity in the TOE Environment and as an external interface of the TOE. Accessing the TOE using the VnE GUI workstation over any network other than the targeted LAN is not supported in the evaluated configuration.



The NTP Server:

- Provides reliable and precise time which is regulated by an atomic clock.
- Communicates with the VnE via the NTP protocol
- Supports the accurate time keeping of the TOE devices

The NTP Server component is evaluated as a required entity in the TOE Environment and as an external interface of the TOE. The NTP server is located on a network that is outside of the target network as pictured in Figure 5 and Figure 6.

IP enabled devices on Target Network:

- IP-based devices that are on the target network which could be computer workstations, printers, scanners, servers, etc.

The IP enabled devices on the Target network are evaluated as an entity in the TOE Environment and as an external interface of the TOE. The IP enabled devices are simply included to show the TOE's relationship to the IP enabled devices with which it communicates.

The VnE CLI Workstation:

- Provides an underlying operating system and the monitor, keyboard, and mouse for the TOE user to interact with the Command Line Interface that is served by the VnE appliance.
- Supports the viewing of the VnE Command Line Interface provided for configuration of the VnE
- Connects to the VnE appliance via the physical serial port or keyboard/monitor ports.

The DP CLI Workstation:

- Provides an underlying operating system and the monitor, keyboard, and mouse for the TOE user to interact with the Command Line Interface that is served by the DP appliance.
- Supports the viewing of the DP Command Line Interface provided for configuration of the DP
- Connects to the DP appliance via the physical serial port or keyboard/monitor ports.

The nTellec<sup>TM</sup> CLI Workstation:

- Provides an underlying operating system and the monitor, keyboard, and mouse for the TOE user to interact with the Command Line Interface that is served by the nTellec<sup>TM</sup> appliance.
- Supports the viewing of the VnE Command Line Interface provided interface for configuration of the nTellec<sup>TM</sup>
- Connects to the nTellec<sup>TM</sup> appliance via the physical serial port or keyboard/monitor ports.

Software Repository:

- Connects to the TOE via network and provides software upgrades to the TOE

Attacker:

- Potential internet Attacker.

## **2.4 TOE Security Functional Policies (SFP)**

### **2.4.1 Restricted User SFP (RU\_SFP)**

The administrator<sup>3</sup> may grant restricted users read, modify/write, or no access to the following functions:

- Security Audit Event Storage
- Audit Review
- User Attributes
- Security Management

---

<sup>3</sup> The administrator has modify/write access to all functions.

### 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.

#### 3.1 Secure Usage Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

A.ATTACK	Attackers are assumed to have a low level of expertise, resources and motivation.
A.CONNECT	The components of the TOE are assumed to be connected to the target network at all times.
A.ENVRNMT	The TOE is assumed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.
A.INSTALL	The TOE hardware and software are delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
A.INTROP	The TOE is assumed to be interoperable with the IT System it monitors.
A.NOEVIL	Those responsible for the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PHYSICAL	The TOE hardware and software critical to security policy enforcement are assumed to be within controlled access facilities which will prevent unauthorized physical access and modification by potentially hostile outsiders.
A.PRIVILEGE	Users of the TOE are assumed to possess the necessary privileges to access information managed by the TOE.
A.REMOTE	The NTP server and the Software Repository with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints as the TOE
A.TIME	The NTP server shall provide reliable time stamps for the TOE's use.
A.TRUSTED	The users of the internal network from which administration of the TOE is performed are trusted not to attack the TOE, to intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks.

#### 3.2 Threats to Security

The following are threats identified for the TOE The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

##### 3.2.1 Threats Addressed by the TOE

T.ATTACK	An undetected compromise of the TOE may occur as a result of an attacker (whether an insider or an outsider) attempting to perform actions that the individual is not authorized to perform.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by brute force attacking the authentication mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by brute force attacking the authentication mechanism.
T.FACCNT	Unauthorized users attempting to access TOE data or security functions may go undetected by brute force attacking the authentication mechanism.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected by brute force attacking the authentication mechanism.
T.IMPERSON	An attacker (outsider or insider) may gain unauthorized access to information or resources by impersonating an authorized user of the TOE.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by brute force attacking the authentication mechanism.
T.MODIFY	The integrity of information may be compromised due to unauthorized modification or destruction of the TOE data by an attacker

- T.PRIVIL      An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data by brute force attacking the authentication mechanism.
- T.REPEAT      An unauthorized user may repeatedly try to guess authentication data used for performing identification and authentication functionality in order to use this information to launch attacks on the TOE.

## 4 Security Objectives

This section identifies the security objectives for 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 Security Objectives for the TOE

The TOE satisfies the following objectives.

- O.ACCESS The TOE must allow authorized users to access only the TOE functions and data for which they have privileges .
- O.ADMIN The TOE will provide facilities to enable an authorized administrator to effectively manage the TOE and its security function, and will ensure that only authorized administrators are able to access such functionality.
- O.AUDITS The TOE must provide an audit trail of security-related events, with accurate dates and times, and a means to search, sort, or order the audit trail based on relevant attributes.
- O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
- O.PROTECT The TOE must protect itself from unauthorized modifications and access to its functions and data.

### 4.2 Security Objectives for the TOE Environment

The TOE's operating environment must satisfy the following objective. This objective does not levy any IT requirements but are satisfied by procedural or administrative measures.

- O.ATTACK Those responsible for the TOE are proactive in preventing Attacks.
- O.CONNECT Those responsible for the TOE must ensure that all components of the TOE remain connected to the target network at all times.
- O.CREDENT 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.
- O.ENVRNMT Those responsible for the TOE must ensure that the TOE is installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.
- O.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with documented delivery and installation/setup procedures.
- O.INTROP Those responsible for the TOE must ensure that the TOE is interoperable with the IT System it monitors.
- O.NOEVIL Those responsible for the TOE are non-hostile and follow all administrator guidance.
- O.PERSON Those responsible for the TOE shall be carefully selected and trained for proper operation of the TOE.
- O.PHYSICAL Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
- O.PRIVILEGE Those responsible for the TOE possess the necessary privileges to access information managed by the TOE.
- O.REMOTE The NTP server and the Software Repository with which the TOE communicates are under the same management control and operate under the same security policy constraints as the TOE
- O.TIME The time source made available to the TOE via the NTP server is reliable.
- O.TRAIN Those responsible for the TOE must be trained to establish and maintain sound security policies and practices.
- O.TRUSTED Those responsible for the TOE must ensure that the users of the network from which the TOE will be administered are trusted.

## 5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE. These requirements are presented following the conventions identified in Section 1.4.

### 5.1 TOE Security Functional Requirements

The following table provides a summary of the security functional requirements implemented by the TOE.

**Table 9 Functional Requirements for the TOE Mapped to ST Operations**

Functional Component	Description	ST Operation
FAU_GEN.1	Audit Data Generation	Selection and Assignment
FAU_SAR.1	Audit Review	Assignment
FAU_SAR.3	Selectable Audit Review	Selection, Assignment, Refinement, and Iteration
FAU_STG.1	Protected Audit Trail Storage	Selection
FIA_AFL.1	Authentication Failure Handling	Assignment, and Refinement
FIA_ATD.1	User Attribute Definition	Assignment and Refinement
FIA_UAU.2	User Authentication Before Any Action	None
FIA_UID.2	User Identification Before Any Action	None
FMT_MOF.1	Management of Security Functions Behavior	Selection, Assignment, Refinement, and Iteration
FMT_MTD.1	Management of TSF Data	Selection, Assignment, Refinement, and Iteration
FMT_SMF.1	Specification of Management Functions	Assignment
FMT_SMR.1	Security Roles	Assignment
FPT_RVM.1	Non-Bypassability of the TSP	None
FPT_STM.1	Reliable Time Stamps	Iteration
FTA_SSL.3	TSF-Initiated Termination	Assignment

#### 5.1.1 Security Audit

##### 5.1.1.1 FAU\_GEN.1 Audit data generation

###### 5.1.1.1.1 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) [*All audit events detailed in Table 10*].

###### 5.1.1.1.2 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 ST, [*See Table 10*]

**Table 10 Audit Events**

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Start-up and shutdown of audit functions	Successful access to the VnE GUI are audited
FIA_UAU.2	VnE GUI User authentication	Username
FMT_SMF.1	Use of management functions	Any modification made to the VnE GUI functions is audited
FMT_SMR.1	Modifications to the group of users that are part of a role	
FPT_STM.1	Changes to time	All auditable events are time stamped

**5.1.1.2 FAU\_SAR.1 Audit review**

**5.1.1.2.1 FAU\_SAR.1.1**

The TSF shall provide [*the administrator and the restricted user*] (as determined by the RU\_SFP) with the capability to read [*all audit records listed in Table 11 that they have permission to view*] from the audit records.

**Table 11 Audit Records**

Audit Record	Audit Information Screens
Audit Records of UI Activities	Administer/User Management/Auditing
VnE Logs	Administer/System/VnE Manager/Logs
DP Logs	Discover/Appliances/Logging
nTellect™ Logs	Discover/Appliances/Logging

**5.1.1.2.2 FAU\_SAR.1.2**

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

**5.1.1.3 FAU\_SAR.3 Selectable Audit review**

**5.1.1.3.1 FAU\_SAR.3.1(a)**

The TSF shall provide the ability to perform sorting and ordering of **audit records of UI activities** ~~audit data~~ based on

- [*User*]
- [*Change type*]
- [*Audit Component*]
- [*Date and time*]

**5.1.1.3.2 FAU\_SAR.3.1(b)**

The TSF shall provide the ability to perform searches of **audit records of UI activities** ~~audit data~~ based on

- [*Audit Component(s)*]
- [*User(s)*]
- [*Change Type(s)*]
- [*Date(s)*]

**5.1.1.3.3 FAU\_SAR.3.1(c)**

The TSF shall provide the ability to perform searches of ~~VnE Logs audit data~~ based on

- [Service(s)]
- [Date(s)]

**5.1.1.3.4 FAU\_SAR.3.1(d)**

The TSF shall provide the ability to perform searches of ~~DP Logs audit data~~ based on

- [Date(s)]

**5.1.1.3.5 FAU\_SAR.3.1(e)**

The TSF shall provide the ability to perform searches of ~~nTellec™ Logs audit data~~ based on

- [Date(s)]

**5.1.1.4 FAU\_STG.1****Security audit event storage****5.1.1.4.1 FAU\_STG.1.1**

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

**5.1.1.4.2 FAU\_STG.1.2**

The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail.

**5.1.2 Identification and Authentication****5.1.2.1 FIA\_AFL.1****Authentication Failure****5.1.2.1.1 FIA\_AFL.1.1**

The TSF shall detect when [3] unsuccessful authentication attempts occur related to [user attempting to authenticate to the VnE GUI].

**5.1.2.1.2 FIA\_AFL.1.2**

When the defined number of unsuccessful authentication attempts has been met or surpassed, the ~~VnE GUI~~ ~~TSF~~ shall [disable the user's account for 20 minutes, unless the Administrator enables it manually].

**5.1.2.2 FIA\_ATD.1****User Attribute Definition****5.1.2.2.1 FIA\_ATD.1.1**

The ~~VnE GUI~~ ~~TSF~~ shall maintain the following list of security attributes belonging to individual users: [see Table 12]



**Table 12 User Security Attributes**

User Information	Specification
First name	This field is required for user creation
Last Name	This field is required for user creation
Middle Name	If not specified this field is left blank
Title	If not specified this field is left blank
Email	This field is required for user creation, this is the users' login ID for access to the VnE GUI
Alert Email	If not specified this field is left blank
Manager	If not specified this field is left blank
Red Score	If not specified will use the VnE default or global setting
Phone	If not specified this field is left blank
Password	If not specified user will be prompted to input a new password at first login
Time Zone	If not specified will use the VnE default or global setting
Language	If not specified will use the VnE default or global setting
Group	If not specified this field is left blank

**5.1.2.3 FIA\_UAU.2**

**User Authentication**

**5.1.2.3.1 FIA\_UAU.2.1**

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

**5.1.2.4 FIA\_UID.2**

**User Identification**

**5.1.2.4.1 FIA\_UID.2.1**

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

**5.1.3 Security Management**

**5.1.3.1 FMT\_MOF.1**

**Management of functions in TSF**

**5.1.3.1.1 FMT\_MOF.1.1(a)**

The TSF shall restrict the ability to *modify the behavior of* the functions [listed in Table 13] to [the administrator, and the restricted user (as determined by the RU\_SFP)].

**Table 13 VnE GUI Administrative Interface Functions**

Administrative Interface Functions
create user
assign user rights
manage user passwords
logging user activities

**5.1.3.1.2 FMT\_MOF.1.1(b)**

The TSF shall restrict the ability to *modify the behavior of* the functions [listed in Table 14] to [VnE CLI admin].

**Table 14 VnE CLI Administrative Interface Functions**

Administrative Interface Functions
Manage Software
Daemon Control
Network Diagnostics
Change Password
Halt/reboot

**5.1.3.1.3 FMT\_MOF.1.1(c)**

The TSF shall restrict the ability to modify the behavior of the functions [listed in Table 15] to [DP/nTellec<sup>TM</sup> CLI admin].

**Table 15 DP/nTellec<sup>TM</sup> CLI Administrative interface Functions**

Administrative Interface functions	Detail
Set	configure/change a network interface
Show	view configuration status info
Add	add a static route or ARP entry
Delete	delete a static route or ARP entry
Password	change the appliance password
Write	save configuration changes
Ping	perform ICMP ping check
Upgrade	for upgrades

**5.1.3.2 FMT\_MTD .1**

**Management of TSF Data**

**5.1.3.2.1 FMT\_MTD.1.1(a)**

The VnE GUI ~~TSF~~ shall restrict the ability to modify the [TSF data associated with the VnE GUI functions listed in Table 13] to [the administrator, and the restricted user (as determined by the RU\_SFP)].

**5.1.3.2.2 FMT\_MTD.1.1(b)**

The VnE CLI ~~TSF~~ shall restrict the ability to query or modify the [TSF data associated with the functions listed in Table 14] to [VnE CLI admin].

**5.1.3.2.3 FMT\_MTD.1.1(c)**

The DP/nTellec<sup>TM</sup> CLI ~~TSF~~ shall restrict the ability to query or modify the [TSF data associated with the functions listed in Table 15] to [DP/nTellec<sup>TM</sup> CLI admin].

**5.1.3.3 FMT\_SMF.1**

**Specification of Management Functions**

**5.1.3.3.1 FMT\_SMF.1.1**

The TSF shall be capable of performing the following security management functions: [listed in Table 13, Table 14 and Table 15].

### 5.1.3.4 FMT\_SMR.1 Security Management Role

#### 5.1.3.4.1 FMT\_SMR.1.1

The TSF shall maintain the roles [*administrator, Restricted user, VnE CLI admin*<sup>4</sup>, and *DP/nTellec™ CLI admin*<sup>5</sup>].

#### 5.1.3.4.2 FMT\_SMR.1.2

The TSF shall be able to associate users with roles.

### 5.1.4 Protection of the TSF

#### 5.1.4.1 FPT\_RVM.1 Non-bypassability of the TSP

##### 5.1.4.1.1 FPT\_RVM.1

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

#### 5.1.4.2 FPT\_STM.1 Time Stamps

##### 5.1.4.2.1 FPT\_STM.1.1(a)

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

### 5.1.5 TOE Access

#### 5.1.5.1 FTA\_SSL.3 TSF-Initiated Termination

##### 5.1.5.1.1 FTA\_SSL.3.1

The ~~VnE GUI~~TSF shall terminate an interactive session after a [*configurable time interval of user inactivity with 5 minutes being the minimum and 60 minutes the maximum*].

## 5.2 TOE Environmental Security Functional Requirements

The following table provides a summary of the security functional requirements implemented by the Environment.

**Table 16 Functional Requirements for the TOE Mapped to ST Operations**

Functional Component	Description	ST Operation
FPT_STM.1(b)	Reliable time stamps	Iteration

### 5.2.1 Protection of the TSF

#### 5.2.1.1 FPT\_STM.1 Time Stamps

##### 5.2.1.1.1 FPT\_STM.1.1(b)

The TOE Environment shall be able to provide reliable time stamps for the TOE's own use.

<sup>4</sup> The VnE CLI Admin role is performed by the administrator role.

<sup>5</sup> The DP/nTellec™ Admin role is performed by the administrator role.

### **5.3 TOE Security Assurance Requirements**

This product claims conformance to CC Version 2.2 Part 3 and claims Evaluation Assurance Level 3 (EAL3) including all relevant International Common Criteria interpretations through kick-off meeting date 10/07/2004.

## 6 TOE Summary Specification

This section provides a high-level definition of the IT Security Functions and the Assurance Measures provided by the TOE to meet the SFRs and SARs specified in this ST.

### 6.1 TOE Security Functions

#### 6.1.1 Security Audit (FAU)

The TOE has four types of audit data logs: audit record of UI activities, VnE log, DP log, and nTellec<sup>TM</sup> log. Access control is dictated by the description provided in Protection of the TSF. These logs are accessible to the administrator and restricted user (as determined by the RU\_SFP). No user at any level is able to modify the logs, with only the administrator and restricted user (as determined by the RU\_SFP) being able to archive the audit records.

The TOE audits all information described in Table 10 – Audit Events. No users of the TOE have access to stop the collection of Audit Logs. The start up and shut down of audit functions corresponds to when the VnE, DP, and nTellec<sup>TM</sup> are powered on and off. The start up and shut down of the VnE are logged in the VnE Log.

The audit record of UI activities contains audit logs of the modifications made to the VnE GUI functions listed in Table 13. The VnE GUI is the primary tool that administrator and other VnE GUI users use to access and manage the VnE and the overall TOE. Audit records of UI activities are stored in the database. The audit records of UI activities can be viewed by the administrator and restricted user (as determined by the RU\_SFP) by logging into the GUI of the IP360<sup>TM</sup>, clicking respectively on the following tabs: Administer/User Management/Auditing, and further refining the search criteria.

The VnE log contains audit records of the activity of and modifications made to the VnE from the VnE GUI. The VnE log is stored in the hard drive as a flat file and can be accessed by logging into the VnE GUI, clicking respectively on the following tabs: Administer/System/VnE Manager/Logs. The Log screen provides the authorized users with the ability to further refine the search criteria, if any, before pulling the stored logs.

The DP log contains audit records of the activity and modifications made to the DP from the VnE GUI. The DP log is stored in the database and can be accessed by logging into the VnE GUI and clicking respectively on the following tabs Discover/Appliance/Logging.

The nTellec<sup>TM</sup> log contains audit records of the activity and modifications made to the nTellec<sup>TM</sup> from the VnE GUI. The nTellec<sup>TM</sup> log is stored in the database and can be accessed by logging into the VnE GUI and clicking respectively on the following tabs Discover/Appliance/Logging.

While the VnE, DP, and nTellec<sup>TM</sup> logs indicate state changes, the User Activities Audit Log indicates user access changes (e.g., updates to the system via VnE GUI). All attempts to authenticate to the TOE via VnE GUI are logged to the User Activities. The audit records generated by the TOE also include a timestamp, the event being logged, the subsystem triggering the log, and the outcome of the event. By default all audit records result from successful operations and unsuccessful operations are ceased and not audited with the exception of login failures.

The provided explanation meets the following functional requirement: FAU\_GEN.1.

##### 6.1.1.1 Audit Review

The logs of the different services housed in the VnE can be viewed by the administrator and restricted user (as determined by the RU\_SFP) by logging into the VnE GUI, clicking respectively on the following tabs: Administer/System/VnE Manager/Logs. The Log screen provides the authorized users with the ability to further refine the search criteria, if any, before pulling the stored logs. There is an option to search the audit records by specifying which service(s) audit record to view and the date of occurrence.

Both the DP and nTellec<sup>TM</sup> logs can be viewed by the user by logging into the VnE GUI, and clicking respectively on the following tabs Discover/Appliance/Logging. The Log screen provides the authorized users with the ability to further refine the search criteria, if any, before pulling the stored logs. There is an option to search the audit records by specifying the date of occurrence.

The audit records of UI activities can be viewed by the administrator and restricted user (as determined by the RU\_SFP) by logging into the GUI of the IP360<sup>TM</sup>, clicking respectively on the following tabs: Administer/User Management/Auditing and further refining the search criteria. There is an option to search the audit records by specifying the audit component the User(s), the change type(s) and the date(s). After submitting a search, the audit records are displayed in a sorted format and can be reordered and resorted based on the criteria listed below

- *[User]*
- *[Change type]*
- *[Audit Component]*
- *[Date and time]*

The VnE, DP, and nTellec<sup>TM</sup> logs are presented in a plain text file. The log data are sorted and ordered; there is no direct mechanism that allows the VnE GUI administrator and restricted user (as determined by the RU\_SFP) to change the sorting or ordering of the data, thus the VnE, DP, and nTellec<sup>TM</sup> logs can only be searched. On the other hand, the audit records of UI activities are presented sorted and the authorized user is provided with the means to change the ordering or sorting by clicking one of the criteria listed above, thus either searching and ordering or searching and sorting can be applied to the audit records of UI activities.

In essence, the searching, sorting and ordering features, allow the audit logs to be presented in a manner suitable for the user to interpret the information.

There are three roles within the VnE GUI and each role has different privileges to access audit and logged data. The administrator has access rights to all audit records whereas the restricted user (as determined by the RU\_SFP) has access rights to the audit records specified by the administrator. The radio button or tab of audit records that a user has no access right to is not displayed on the user interface. The VnE CLI admin and the DP/nTellec<sup>TM</sup> CLI admin have no access to the audit logs.

The CLI interfaces are used for initial configuration of the VnE, DP, and nTellec<sup>TM</sup>; therefore the operation related to the CLI need not to be audited.

The provided explanation meets the following functional requirements: FAU\_SAR.1 and FAU\_SAR.3.

### **6.1.1.2 Security Audit Event Storage**

nCircle<sup>TM</sup> does not provide a mechanism for any TOE User to delete the audit logs directly. Audit logs can not be modified by any level of user of the TOE. The audit logs are read-only for all users and are backed up in the hard drive as text files a day after they are generated for a configurable amount of time which is by default 3 days. Audit logs can then be archived. nCircle<sup>TM</sup> defines archiving as copying records to an external system (outside the TOE) and then deleting the records after they are archived. The administrator and the restricted user (as determined by the RU\_SFP), can specify how long the audit records should stay in the hard drive before being archived.

The provided explanation meets the following functional requirement: FAU\_STG.1.

### **6.1.2 Identification and Authentication (FIA)**


Access control is dictated by the description provided in Protection of the TSF. A typical attacker in the intended environment for the TOE is assumed to have a low level of sophistication, but may have knowledge of vulnerabilities and access to attack methods that are in the public domain. The purpose of the attacks could be to gain access to the resources of the TOE; therefore, the attack potential which is applicable for AVA\_SOF.1 calculations is LOW. Any residual vulnerabilities may only be exploited by an attacker of moderate or high attack potential. The strength of function claim is therefore SOF-BASIC.

### 6.1.2.1 Authentication Failure

An authorized user of the system can authenticate to the TOE in four ways – VnE GUI with a username and password, VnE CLI with a username and password, DP or the nTellecT™ using a password.

All the passwords are stored using a hashing algorithm. After being hashed, the VnE GUI passwords are stored into the database table, the VnE CLI password is stored in a text file into the hard drive, and the DP and the nTellecT™ passwords are stored in a text file into the flash memory.

When a password is entered, it is checked against all valid passwords. In essence, all passwords entered are hashed and compared to the previously hashed passwords. The User is authenticated if the hash password entered matches the stored hash. Otherwise, s/he may retry to login. As a means to mitigate brute force attacks on passwords, users are allowed by default up to two unsuccessful authentication attempts (note that this only applies to the VnE GUI). After three unsuccessful attempts, regardless of the time between attempts, the account becomes temporarily disabled for 20 minutes. The system records the time of the third unsuccessful attempt and sets a flag in the database to indicate that the account is temporarily locked. An account disabled in this way is automatically re-enabled after 20 minutes. At the time of lock out, the time the lockout occurred is recorded in the database and until the 20 minutes — have passed, the concerned user account remains disabled. Alternatively, accounts can also be manually enabled and disabled by the administrator

To enable or disable a user account, an Administrator with the permission to do so, will click respectively on the following tabs: Admin ister/User Management/Users and click  to change the account status.

The Appliance CLI does not provide the unsuccessful login tracking and instead rely on physical security to control password attacks.

The provided explanation meets the following functional requirement: FIA\_AFL.1.

### 6.1.2.2 User Attribute Definition

As a good security practice, detail information about each user of the TOE can be collected when a new account is set up. The database maintains a list of security attributes in the form of individual records that belong to a particular user. These attributes are the user identity, authentication data, authorizations (roles), password expiration information and lockout parameters (see Table 12). These attributes can be modified by the administrator or restricted user(as determined by the RU\_SFP) from the GUI.

First Name, Last Name, Email and Password are the only attributes belonging to the user that are required. The Middle Name, Alert Email, Phone, Group and Manager, attributes are optional and left blank if not specified. The VnE default or global setting is used for The Red Score, Time Zone, and Language attributes if not specified.

The provided explanation meets the following functional requirement: FIA\_ATD.1.

### 6.1.2.3 User Authentication and Identification

After being hashed, the VnE GUI passwords are stored into the database table, the VnE CLI password is stored in a text file into the hard drive, and the DP and the nTellecT™ passwords are stored in a text file into the flash memory.

Authorized users must provide a valid username along with a valid password associated with it for successful authentication. Usernames and passwords entered by users in the VnE are captured by the TOE, and the user's information and privileges are retrieved from the database record in the case of the VnE GUI. The TOE hashes the user provided password and compares the new hash with the stored hash of the password. When the two are equal the user is granted the privileges that have been stored in association with that user role. The VnE GUI refers to the user's attributes stored in the database table to grant privileges. The TOE does not provide any services to an unauthenticated user of the VnE GUI, except to request authentication.

The CLI grants administrator access to the user who has provided the CLI administrator password. The VnE CLI admin is the only user of the VnE CLI; therefore has access to all the VnE CLI functions. Similarly, the DP/nTellec™ CLI Admin is the only user of the both the DP and the nTellec™ CLI; therefore has access to all the DP and the nTellec™ CLI functions.

In order to start a session with the VnE GUI, the user must open a web browser and initiate a secure session by typing ‘https://’ followed by the IP address of the VnE. The user will not be redirected to ‘https://’ if ‘http://’ is typed. A list of the supported browsers is shown in Table 8. After initiating a secure session, the login page comes up. The user is then prompted to enter a valid username and password before being granted access. User authentication is performed in the database session by making sure that the username and associated password entered figure on the database list of valid usernames and associated passwords. If the user is successfully authenticated; therefore successfully identifies itself, the user is logged into the VnE GUI. Only then are additional functions and types of access made available.

After opening the VnE CLI, the VnE CLI Admin must enter a valid username and password before any action is permitted. The VnE CLI Admin is prompted to use a valid username along with a valid password associated with it. If the user is successfully authenticated, the user is logged into the VnE CLI. Only one username and password can be set on the VnE Manager CLI, i.e., username and password of the VnE CLI Admin. Any user of the TOE that need to access the VnE CLI requires the username and password of the VnE CLI Admin.

Likewise, In order to authenticate into the DP or nTellec™ CLI, the DP/nTellec™ CLI admin needs to enter a valid password before any action is permitted. The DP/nTellec™ CLI admin is prompted to use a valid password. If the user is successfully authenticated; therefore successfully identifies itself, the user is logged into the VnE CLI. Only one password can be set on each; therefore, any user of the TOE that needs to access either the DP or nTellec™ CLI shall use the password of the DP/nTellec™ admin.

The Appliance CLI does not provide the unsuccessful login tracking and instead relies on physical security to control password attacks.

This implies that the TOE does not allow any action to be performed on behalf of the user prior to being successfully authenticated and identified itself. Whether using the VnE GUI or the CLI interface, the user is logged into the desired interface only after successfully identifying and authenticating themselves. The TOE ensures that a user can only access the TOE login page before identification. No other functions or types of access are permitted prior to identification and authentication.

The provided explanation meets the following functional requirements: FIA\_UAU.2 and FIA\_UID.2.

### **6.1.3 Security Management (FMT)**

The TOE allows very granular access permission controls for each user. Access control is dictated by the description provided in Protection of the TSF. The administrator specifies Read/Write, Read or No Access rights for each function a TOE user could potentially access. If a user does not have access to a VnE GUI function, the function does not appear in the user’s session. Users can be granted read/write or read permissions for the VnE GUI functions listed in Table 13. The permission-enforcement database of the VnE GUI compares the user access for all incoming requests to the access privileges of the user provided and maintained by the authorization database. For instance, if the user does not have write permission to a function that s/he is trying to modify, the current user’s access request is denied. As such, the administrator is allowed to define the vulnerability management rules. This applies to the ability to modify the behavior of the functions of analysis and reaction; only the administrator role and the restricted user (as determined by the RU\_SFP) are able to perform these modifications. The VnE CLI admin, and the DP/nTellec™ admin are restricted from changing of modifying the behavior of the VnE GUI functions listed in Table 13. As such, the administrator and the restricted user (as determined by the RU\_SFP) are the only users of the TOE that are able to modify the TSF data associated with the VnE GUI functions.

The VnE CLI admin is the only user of the VnE CLI and has read write access to all the functions listed in Table 14. Therefore, any user of the TOE that needs to access the VnE CLI would have to use the username and password of the VnE CLI admin. Needless to say, all the users of the TOE but the VnE CLI admin are restricted from changing



or modifying the behavior of the functions listed in Table 14. This applies to the restriction to query or modify the TSF associated with the functions listed in Table 14 to the VnE CLI admin.

Similarly, the DP/nTellec™ Admin is the only user of both the DP and the nTellec™ and has read write access to all the functions listed in Table 15. Therefore, any user of the TOE that needs to access either the DP or nTellec™ CLI would have to use the password of the DP/nTellec™ admin. Needless to say, all the users of the TOE but the DP/nTellec™ CLI admin are restricted from changing or modifying the behavior of the functions listed in Table 15. This applies to the restriction to query or modify the TSF associated with the functions listed in Table 15 to the DP/nTellec™ CLI admin.

The provided explanation meets the following functional requirements: FMT\_MOF.1 and FMT\_MTD.1

The TOE provides a series of functions that allow the authorized users of the TOE to configure the TOE to perform its services. A list of functions is provided in Table 13, Table 14, and Table 15, respectively. Access to the TOE and TOE data is controlled by the authentication and access control mechanisms that the TOE provides and implements.

The provided explanation meets the following functional requirement: **FMT\_SMF.1**.

The TOE maintains a list of security attributes in the form of individual records that belong to a particular user; one of these attributes is the user's role. Each user or group of users is associated with one of the three defined roles.

The following roles are defined on the TOE:

- **Administrator** – Full access to the VnE GUI. This role is able to manage the users of the VnE GUI and to view/modify the configuration of the TOE and the logs.
- **Restricted user** – Access is determined according to the RU\_SFP.
- **VnE CLI admin**– Full access to the VnE CLI. This is the only role for the VnE CLI and naturally has read and write access to all the functions listed in Table 14.
- **DP/nTellec™ CLI Admin** – Full access to the DP or nTellec™ CLI. This is the only role for the DP and nTellec™ CLI and has read and write access to all the functions listed in Table 15.

The provided explanation meets the following functional requirement: FMT\_SMR.1.

#### 6.1.4 Protection of the TSF (FPT)

The TOE ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The TOE is a hardware device that executes all of its processes internally. It is accessible only via the defined interfaces and only authorized administrators are able to modify the functionality of the TOE.

The TOE only provides two types of interfaces: management interfaces and network interfaces. Each TOE component (Device Profiler, nTellec™, and VnE appliance) provides these two types of interfaces. The Device Profiler and the nTellec™ have no open ports and as such all communication across a network interface is outbound communication. The Device Profiler and the nTellec™ do offer a management interface in the form of the CLI; however, this is only available via a direct connection to the serial port. This CLI require a user to authenticate before any services are provided and even then the CLI monitors and controls the services that are made available to the user.

The VnE provides two management interfaces: a GUI, and a CLI via the serial port. Both management interface require the user to authenticate before receiving any services. Once the user has authenticated through one of the management interfaces, the management interface component will determine what functionality (depending on the user's group) is presented to the user. The VnE does have an open network interface (Port 2708 which is configurable), which listens for communication from the Device Profiler and the nTellec™. The only connections that are allowed on that port are forced to authenticate using x.509 certificates and encrypted within a TLS session using a shared key.

Unauthorized users cannot bypass the identification and authentication mechanisms, and network traffic cannot bypass the networked interfaces to enter the TOE.

The provided explanation meets the following functional requirement: FPT\_RVM.1.

A system time maintained by the VnE is used by the TOE. The Device Profiler maintains its time by periodically comparing its stored value to the real-time clock on the VnE. Both the DP and the nTelect<sup>TM</sup> synchronize their time with the VnE time.

The TOE requires a NTP server to be in the TOE Environment to provide reliable time. The NTP sever is not included in the TOE.

The provided explanation meets the following functional requirement: FPT\_STM.1.

### **6.1.5 TOE Access (FTA)**

By default, a user is automatically logged out of VnE after 60 minutes of inactivity. Administrators can change that value (minimum value = 5, maximum value = 60). When the user is logged out, the last display viewed by the user is cleared making the current contents unreadable. All permissions and accesses that had been granted during the session are removed until the user re-authenticates by logging back into the TOE. When the user is logged out, the GUI clears and overwrites the current display by making the contents unreadable. That is simply achieved by displaying a generic screen and closing the session. As such, any user activity, data access/display device is disabled and the user needs to log back in for another session. In order to re-authenticate, the user must first click on the login tab and enter a valid username and password. Session termination only applies to the VnE GUI.

The provided explanation meets the following functional requirement: FTA\_SSL.3.

## 6.2 TOE Security Assurance Measures

This section of the ST maps the assurance requirements for a CC EAL3 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 assurance requirements.

**Table 17 Assurance Measures Mapping to Security Assurance Requirements (SARs)**

<b>Assurance Component</b>	<b>Assurance Measure</b>
ACM_CAP.3, ACM_SCP.1	nCircle™ Configuration Management Plan
ADO_DEL.1	nCircle™ Secure Delivery Procedure
ADO_IGS.1	IP360™ Installation and Setup Procedure
ADV_FSP.1	IP360™ Functional Specification
ADV_HLD.2	IP360™ High Level Design
ADV_RCR.1	IP360™ Representation Correspondence Analysis
AGD_ADM.1, AGD_USR.1	IP360™ Guidance Documents
ALC_DVS.1	nCircle™ Development Environment and Development Tools Description
ATE_COV.2, ATE_DPT.1, ATE_FUN.1	IP360™ Testing Depth & Coverage Analysis
ATE_IND.2	Evaluator Independent testing of the IP360™
AVA_MSU.1, AVA_SOF.1, AVA_VLA.1	IP360™ Vulnerability Analysis

## **7 Protection Profile Claims**

This Security Target does not claim conformance with a Protection Profile.

## 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 and threat that compose the Security Target. Table 9 Security Environment vs. Objectives demonstrates the mapping between the assumptions, threats, and policies to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

**Table 18 Security Environment vs. Objectives**

	Security Objective for the TOE					Security Objective for the TOE Environment														
	O.ACCESS	O.ADMIN	O.AUDITS	O.IDAUTH	O.PROTECT	O.ATTACK	O.CONNECT	O.CREDENT	O.ENVRNMT	O.INSTALL	O.INTROP	O.NOEVIL	O.PERSON	O.PHYSICAL	O.PRIVILEGE	O.REMOTE	O.TIME	O.TRAIN	O.TRUSTED	
A.ATTACK						X														
A.CONNECT							X													
A.ENVRNMT									X											
A.INSTALL										X										
A.INTROP											X									
A.NOEVIL								X				X							X	
A.PHYSICAL														X						
A.PRIVILEGE															X					
A.REMOTE																X				
A.TIME																	X			
A.TRUSTED												X	X						X	X
T.ATTACK	X		X		X															
T.COMDIS				X	X															
T.COMINT				X	X															
T.FACCNT			X	X																
T.IMPCON		X		X	X															
T.IMPERSON	X			X	X															
T.LOSSOF				X	X															
T.MODIFY			X	X																
T.PRIVIL				X	X															
T.REPEAT				X																

**A.ATTACK** Attackers are assumed to have a low level of expertise, resources and motivation. The O.ATTACK objective ensures that proactive measures in preventing attacks are taken.

**A.CONNECT** The components of the TOE are assumed to be connected to the target network at all times. The O.CONNECT objective ensures that all components of the TOE remain connected to the target network at all times.

**A.ENVRNMT** The TOE is assumed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product. The O.ENVRNMT objective ensures that the TOE is installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.

- A.INSTALL** The TOE hardware and software are delivered, installed, and setup in accordance with documented delivery and installation/setup procedures. The O.INSTALL objective ensures that the TOE is delivered, installed managed, and operated in a manner which is consistent with documented delivery and installation/setup procedures.
- A.INTROP** The TOE is assumed to be interoperable with the IT System it monitors. The O.INTROP ensures that the TOE is interoperable with the IT System it monitors.
- A.NOEVIL** Those responsible for the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The O.CREDDENT objective ensures that all access credentials are protected by the users in a manner which is consistent with IT security. The O.NOEVIL objective ensures that the users of the TOE are non-hostile and follow all administrator guidance. The O.TRAIN objective ensures that the users of the TOE must be trained to establish and maintain sound security policies and practices.
- A.PHYSICAL** The TOE hardware and software critical to security policy enforcement are assumed to be within controlled access facilities which will prevent unauthorized physical access and modification by potentially hostile outsiders. The O. PHYSICAL objective ensures that the TOE is protected from any physical attack.
- A.PRIVILEGE** Users of the TOE are assumed to possess the necessary privileges to access information managed by the TOE. The O. PRIVILEGE objective ensures that the users of the TOE posse the necessary privileges to access information managed by the TOE.
- A.REMOTE** The NTP server and the Software Repository with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints as the TOE. The O.REMOTE objective ensures that the NTP server and the Software Repository with which the TOE communicates are under the same management control and operate under the same security policy constraints as the TOE.
- A.TIME** The NTP server shall provide reliable time stamps for TOE's use. The O.TIME objective ensures that the time source made available to the TOE via the NTP server is reliable.
- A.TRUSTED** The users of the internal network from which administration of the TOE is performed are trusted not to attack the TOE, to intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks. The O.NOEVIL objective ensures that the users of the TOE are non-hostile and follow all administrator guidance. The O.PERSON objective ensures that the users of the TOE are carefully selected and trained for proper operation of the TOE. The O.TRAIN objective ensures that the users of the TOE must be trained to establish and maintain sound security policies and practices. The O.TRUSTED objective ensures that the users of the network from which the TOE will be administered are trusted.
- T.ATTACK** An undetected compromise of the TOE may occur as a result of an attacker (whether an insider or an outsider) attempting to perform actions that the individual is not authorized to perform. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.AUDITS objective addresses this threat by ensuring that the TOE provide an audit trail of security-related events, with accurate dates and times, and a means to search, sort, or order the audit trail based on relevant attributes. The O.PROTECT objective addresses this threat by providing TOE self-protection.
- T.COMDIS** An unauthorized user may attempt to disclose the data collected and produced by brute force attacking the authentication mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.PROTECT objective addresses this threat by providing TOE self-protection.

- T.COMINT** An unauthorized user may attempt to compromise the integrity of the data collected and produced by brute force attacking the authentication mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.PROTECT objective addresses this threat by providing TOE self-protection.
- T.FACCNT** Unauthorized users attempting to access TOE data or security functions may go undetected by brute force attacking the authentication mechanism. The O.AUDITS objective addresses this threat by ensuring that the TOE provide an audit trail of security-related events, with accurate dates and times, and a means to search, sort, or order the audit trail based on relevant attributes. The O.IDAUTH objective provides for authentication of users prior to any TOE data access.
- T.IMPCON** An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected by brute force attacking the authentication mechanism. The O.ADMIN objective counters this threat by providing facilities to enable an authorized administrator to effectively manage the TOE and its security function, and will ensure that only authorized administrators are able to access such functionality. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.PROTECT objective addresses this threat by providing TOE self-protection.
- T.IMPERSON** An attacker (outsider or insider) may gain unauthorized access to information or resources by impersonating an authorized user of the TOE. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE Data. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.PROTECT objective addresses this threat by providing TOE self-protection.
- T.LOSSOF** An unauthorized user may attempt to remove or destroy data collected and produced by brute force attacking the authentication mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.PROTECT objective addresses this threat by providing TOE self-protection.
- T.MODIFY** The integrity of information may be compromised due to unauthorized modification or destruction of the TOE data by an attacker. The O.AUDITS objective addresses this threat by ensuring that the TOE provide an audit trail of security-related events, with accurate dates and times, and a means to search, sort, or order the audit trail based on relevant attributes. The O.IDAUTH objective provides for authentication of users prior to any TOE data access.
- T.PRIVIL** An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data by brute force attacking the authentication mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.PROTECT objective addresses this threat by providing TOE self-protection.
- T.REPEAT** An unauthorized user may repeatedly try to guess authentication data used for performing Identification and authentication functionality in order to use this information to launch attacks on the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE data access.

## 8.2 Security Functional Requirements Rationale

Table 19 Mapping of Functional Requirements to Objectives

	O.ACCESS	O.ADMIN	O.AUDITS	O.IDAUTH	O.PROTECT	O.TIME
FAU_GEN.1			X			
FAU_SAR.1	X	X	X			
FAU_SAR.3.1(a)		X	X			
FAU_SAR.3.1(b)		X	X			
FAU_SAR.3.1(c)		X	X			
FAU_SAR.3.1(d)		X	X			
FAU_SAR.3.1(e)		X	X			
FAU_STG.1	X			X	X	
FIA_AFL.1				X		
FIA_ATD.1				X		
FIA_UAU.2	X			X		
FIA_UID.1	X			X		
FMT_MOF.1.1(a)	X	X		X	X	
FMT_MOF.1.1(b)	X	X		X	X	
FMT_MOF.1.1(c)	X	X		X	X	
FMT_MTD.1.1(a)	X	X		X	X	
FMT_MTD.1.1(b)	X	X		X	X	
FMT_MTD.1.1(c)	X	X		X	X	
FMT_SMF.1	X	X		X		
FMT_SMR.1				X		
FPT_RVM.1					X	
FPT_STM.1.1(a)			X			X
FPT_STM.1.1(b)			X			X
FTA_SSL.3					X	

Note the only environmental objective that maps to an SFR is O.Time; as such, O.Time is the only environmental objective that is included in Table 19.

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



- O.ACCESS** The TOE must allow authorized users to access only the TOE functions and data for which they have privileges. The TOE meets this objective by enforcing the following rules
- The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU\_SAR.1].
  - TOE is required to protect the audit data from deletion [FAU\_STG.1].
  - Users authorized to access the TOE are defined using an identification and authentication process [FIA\_UID.2, FIA\_UAU.2].
  - 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.1.1(a), FMT\_MOF.1.1(b), FMT\_MOF.1.1(c)].
  - 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(a), FMT\_MTD.1.1(b), FMT\_MTD.1.1(c)].
  - The TOE is required to be capable of performing the defined security management functions of the TOE [FMT\_SMF.1].
- O.ADMIN** The TOE will provide facilities to enable an authorized administrator to effectively manage the TOE and its security function, and will ensure that only authorized administrators are able to access such functionality. The TOE meets this objective by enforcing the following rule :
- The TOE must provide the ability to review and manage the audit trail of the System [FAU\_SAR.1, FAU\_SAR.3.1(a), FAU\_SAR.3.1(b), FAU\_SAR.3.1(c), FAU\_SAR.3.1(d), FAU\_SAR.3.1(e)].
  - 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.1.1(a), FMT\_MOF.1.1(b), FMT\_MOF.1.1(c)].
  - 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(a), FMT\_MTD.1.1(b), FMT\_MTD.1.1(c)].
  - The TOE is required to be capable of performing the defined security management functions of the TOE [FMT\_SMF.1].
- O.AUDITS** The TOE must provide an audit trail of security-related events, with accurate dates and times, and a means to search, sort, or order the audit trail based on relevant attributes. The TOE meets this objective by enforcing the following rule :
- Security relevant events must be defined and auditable for the TOE [FAU\_GEN.1].
  - The TOE must provide the ability to review and manage the audit trail of the System [FAU\_SAR.1, FAU\_SAR.3.1(a), FAU\_SAR.3.1(b), FAU\_SAR.3.1(c), FAU\_SAR.3.1(d), FAU\_SAR.3.1(e)].
  - The TOE is required to use the reliable time provided by the NTP server, to provide reliable time for its own use [FPT\_STM.1].
- O.IDAUTH** The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The TOE meets this objective by enforcing the following rule:
- The TOE is required to protect the stored audit records from unauthorized deletion [FAU\_STG.1].
  - The TOE is required to disable a user account subsequent to three consecutive failed login attempts [FIA\_AFL].
  - 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.2, FIA\_UAU.2].
  - 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.1.1(a), FMT\_MOF.1.1(b), FMT\_MOF.1.1(c)].

- 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(a), FMT\_MTD.1.1(b), FMT\_MTD.1.1(c)].
- The TOE is required to be capable of performing the defined security management functions of the TOE [FMT\_SMF.1].
- The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT\_SMR.1].

**O.PROTECT** The TOE must protect itself from unauthorized modifications and access to its functions and data. The TOE meets this objective by enforcing the following rule:

- The TOE is required to protect the audit data from deletion [FAU\_STG.1].
- The TOE is required to provide the ability to restrict managing the behavior of modules and functions of the TOE to authorized users of the TOE [FMT\_MOF.1.1(a), FMT\_MOF.1.1(b), FMT\_MOF.1.1(c)].
- 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(a), FMT\_MTD.1.1(b), FMT\_MTD.1.1(c)].
- The TSP enforcement functions must be invoked and succeed before each function within the TSC is allowed to proceed [FPT\_RVM.1].
- The TOE is required to logout interactive sessions after remaining inactive for a configurable amount of time which is by default 60 minutes [FTA\_SSL.3].

**O.TIME** The time source made available to the TOE via the NTP server is reliable. The TOE meets this objective by enforcing the following rule:

- The TOE is required to use the reliable time provided by the NTP server, to provide reliable time for its own use [FPT\_STM.1.1(a), FPT\_STM.1.1(b)].

### 8.3 Rational For Refinements of Security Functional Requirements

The following Security Functional Requirements have been refined from the CC to more closely match the functionality of this specific TOE.

- FAU\_SAR.3      In iterations a, b, c, d, and e of the functional requirement FAU\_SAR.3, ~~audit data~~ was replaced by **audit records of UI, audit records of UI, VnE Log , DP Log, and nTellec<sup>TM</sup> Log** respectively. The motivation behind the substitutions is to better specify the differences in the audit review functionality that is provided for each log type.
- FIA\_AFL          ~~TSF~~ was replaced with **VnE GUI** in order to better specify the component of the TOE that detects the occurrence of 3 unsuccessful authentication attempts related to user Attempting to authenticate to the VnE GUI.
- FIA\_ATD          ~~TSF~~ was replaced with **VnE GUI** in order to better specify the component of the TOE that maintains the list of attribute (see Table 12) belonging to individual users. In addition, there are several different user types of the TOE and different attributes are captured for different user types.
- FMT\_MTD          In iterations a, b, and c of the FMT\_MTD.1 functional requirement, TSF was replaced with **VnE GUI, VnE CLI, and DP/nTellec<sup>TM</sup> CLI** respectively. The purpose of the substitutions is to better specify the components of the TOE that actually perform the restriction of users access to specific operations that are listed in the requirement.
- FTA\_SSL.3        ~~TSF~~ was replaced with **VnE GUI** in order to better specify the component of the TOE that provides this functionality

## 8.4 Security Assurance Requirements Rationale

EAL3 was chosen to provide a moderate to high level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

While the TOE 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. The chosen assurance level was also selected for conformance with the client's needs.

Configuration Management – The Configuration Management documentation provides a description of tools used to control the configuration items and how they are used at the nCircle™. The documentation provides a complete configuration item list and a unique reference for each 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.

Corresponding CC Assurance Components:

- Configuration Items

Delivery and Operation – The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by nCircle™ to protect against TOE modification during product delivery. The Installation Documentation provided by nCircle™ 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 administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

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

Development – The nCircle™ design documentation consist 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 Correspondence Demonstration

Guidance Documentation – The nCircle™ Guidance documentation provides administrator and user 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 on how to administer the TOE in a

secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's Security. nCircle™ provides a single version document which addresses 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
- User Guidance

Tests – There are a number of components that 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. nCircle™ 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.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing

Vulnerability and TOE Strength of Function Analyses – A Vulnerability Analysis 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 evaluation
- Developer Vulnerability Analysis
- nCircle™ Vulnerability Analysis
- nCircle™ Strength of Function Analysis
- nCircle™ Guidance Misuse Analysis

## 8.5 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 20 lists each requirement from the four Protection Profiles to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

**Table 20 Functional Requirements Dependencies**

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FIA_AFL.1	FIA_UAU.1	Yes**
FIA_UAU.2	FIA_UID.1	Yes***
FMT_MOF.1	FMT_SMF.1 and FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1 and FMT_SMR.1	Yes
FMT_SMR.1	FIA_UID.1	Yes***
FTA_SSL.3	FIA_UAU.1	Yes**

\*\* By including FIA\_UAU.2 which is hierarchical to FIA\_UAU.1, the dependency of FIA\_UAU.1 is satisfied.

\*\*\* By including FIA\_UID.2 which is hierarchical to FIA\_UID.1, the dependency of FIA\_UID.1 is satisfied.

### 8.6 TOE Summary Specification Rationale

The following table represents a mapping between the security functions in this ST to their related TOE security functional requirements and provides a rationale for how each security function meets the corresponding security functional requirement.

**Table 21 Mapping of Security Functional Requirements to TOE Security Functions**

Functional Requirement:	TOE Security Functions:	Rationale:	
FAU_GEN.1	Audit Data Generation	Security Audit (FAU)	The Audit Data Generation function satisfies this requirement by providing audit data generation for the IP360™ components.
FAU_SAR.1	Audit Review		The Audit Review function satisfies this requirement by providing the capability for VnE GUI administrator and restricted user (as determined by the RU_SFP) to view the TOE's audit data.
FAU_SAR.3	Selectable Audit Review		The Selectable Audit Review function satisfies this requirement by providing the administrator and restricted user (as determined by the RU_SFP) with the ability to perform sorting of audit data based on various parameters.
FAU_STG.1	Protected audit trail storage	Identification and Authentication (FIA)	The protection of Audit Data satisfies this requirement by protecting audit records from unauthorized deletion.
FIA_UAU.2	User authentication before any action		The User authentication before any action function satisfies this requirement by not allowing any other actions to be performed prior to successful authentication.
FIA_AFL.1	Authentication Failure Handling		The Authentication Failure Handling function satisfies this requirement by tracking the number of unsuccessful authentication attempts a user has tallied and, if this number reaches a pre-set limit which is 3, locking out this account for 20 minutes. the other option is to have the administrator or restricted user (as determined by the RU_SFP) to manually unlock the account by following the instructions given in the TSS section of this functional requirement.
FIA_ATD.1	User Attribute Definition		The User Attribute Definition function satisfies this requirement by maintaining a list of security attributes for each user of the VnE GUI.
FIA_UID.2	User identification before any action		The User identification before any action function satisfies this requirement by requiring each user to be successfully identified before allowing the user to perform any other action.
FMT_MOF.1	Management of Security Functions Behavior	Security Management (FMT)	The Management of Security Functions Behavior function satisfies this requirement by restricting access to modify the behavior of or change the configurations of the security functions for authorized TOE administrators.
FMT_MTD.1	Management of TSF Data		The Management of TSF Data function satisfies this requirement by restricting access to query and add VnE, DP, nTelect™ and new user.
FMT_SMF.1	Specification of Management Functions		The Specification of Management Functions function satisfies this requirement by requiring the ST author to identify the security management functions that the TSF is capable of performing.
FMT_SMR.1	Security Roles		The Security Roles function satisfies this requirement by providing roles and associating each user to a role.

Functional Requirement:	TOE Security Functions:		Rationale:
FPT_RVM.1	Non-Bypassability of the TSP	Protection of the TSF (FPT)	The Non-Bypassability of the TSP function satisfies this requirement by ensuring that TSP enforcement functions (e.g. identification & authentication procedures) are invoked and succeed before each function is allowed to proceed.
FPT_STM.1	Reliable Time Stamps		The Reliable Time Stamps function satisfies this requirement by ensuring that the TOE has access to a reliable time stamp that is maintained by the VnE and can only be updated from an NTP server to the VnE, Note that the NTP server is not part of the TOE boundary but is part of the TOE Environment.
FTA_SSL.3	TSF-initiated Termination	TOE Access (FTA)	The TSF-initiated session locking function satisfies this requirement by make use of a standard security practice; the VnE GUI logs out a user session after being inactive for a configurable amount of time which is by default 60 min.



## 8.7 Strength of Function Rationale

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL 3 assurance requirements. The evaluated TOE is intended to operate in commercial and DoD. This security function is in turn consistent with the security objectives described in Section 4.

The rationale for the chosen level is based on the low attack potential of the threat agents identified in this ST. The list of relevant security functions and security functional requirements which have probabilistic or permutational functions are:

FIA_UAU.2	User Authentication before any action
FIA_AFL.1	Authentication Failure Handling

The passwords used to log into the VnE GUI are the only probabilistic or permutational functions on which the strength of the VnE GUI authentication mechanism depends. The corresponding TSFs are listed in Section 6.1.2 Identification and Authentication (FIA).

The password used by The VnE Manager CLI admin is the only probabilistic or permutational function on which the strength of the VnE CLI authentication mechanism depends.

The VnE Manager CLI admin chooses a password when initially authorized to use the system; the system places the following restrictions on the passwords selected by the user:

The password must be at least six characters long

The password used by The DP/nTellec™ CLI admin is the only probabilistic or permutational function on which the strength of the DP or nTellec™ CLI authentication mechanism depends.

The DP/nTellec™ CLI admin chooses a password when initially authorized to use the system; the system places no restriction on the password selected.

The Appliances' CLI do not provide the unsuccessful login tracking and instead rely on physical schedule to control password attacks.

A proof that the TOE meets its SOF-Claims can be found in the "nCircle™ IP360™ V6.3.4 Vulnerability Assessment" document.

## 9 Acronyms and Terms

<b>AES</b>	Advanced Encryption Standard
<b>CC</b>	Common Criteria
<b>CLI</b>	Command Line Interface
<b>CM</b>	Configuration Management
<b>CPU</b>	Central Processor unit
<b>DES</b>	Data Encryption Standard
<b>3DES</b>	Triple Data Encryption Standard
<b>DP</b>	Device Profiler
<b>EAL</b>	Evaluation Assurance Level
<b>FreeBSD</b>	Free Berkeley Software Distribution
<b>GB</b>	Gigabyte
<b>GHZ</b>	Gigahertz
<b>GUI</b>	Graphical User Interface
<b>IP</b>	Internet Protocol
<b>ISO</b>	International Organization for Standardization
<b>IT</b>	Information Technology
<b>LAN</b>	Local area Network
<b>MB</b>	Megabyte
<b>MHZ</b>	Megahertz
<b>NSA</b>	National Security Agency
<b>OpenSSL</b>	Open Source Implementation of the Secure Sockets Layer
<b>OS</b>	Operating System
<b>RAM</b>	Random Access Memory
<b>SAR</b>	Security Assurance Requirement
<b>SDRAM</b>	Synchronous Dynamic Random Access Memory
<b>SFR</b>	Security Functional Requirement

<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SNMP</b>	Simple Network Management Protocol
<b>SOF</b>	Strength of Function
<b>SSH</b>	Secure Shell
<b>SSL</b>	Secure Sockets Layer
<b>ST</b>	Security Target
<b>TCP</b>	Transmission Control Protocol
<b>TOE</b>	Target of Evaluation
<b>TBA</b>	To Be Announced
<b>TBD</b>	To Be Determined
<b>TLS</b>	Transport Layer Security
<b>TSF</b>	Target of Evaluation (TOE) Security Function
<b>TSP</b>	Target of Evaluation (TOE) Security Policy
<b>VnE</b>	Vulnerability and Exposures Manager