Trustwave
Network Access Control (NAC) Software
Version 3.4.0
Security Target

Version 2.4

October 19, 2009

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602
http://www.trustwave.com

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Trustwave Network Access Control (NAC) Software Version 3.4.0 Security Target. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
1.0	April 24, 2009, Initial release
1.1	April 30, 2009, Updates from Trustwave
1.2	June 4, 2009, Addressed DOMUS OR1
1.3	June 23, 2009, Addressed certifiers issues concerning time stamps and intra-TOE communications
2.0	July 14, 2009, Addressed certifier OR v1.1
2.1	August 21, 2009, Addressed DOMUS OR2 and certifier OR v2.0
2.2	August 30, 2009, updated TOE version and changes for FSP consistency
2.3	September 11, 2009, added ALC_FLR.1, updated document list and addressed DOMUS OR4
2.4	October 19, 2009, addressed DOMUS OR8

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

ARP	**Address Resolution Protocol**
CC	**Common Criteria**
CM	**Configuration Management**
EAL	**Evaluation Assurance Level**
HTTP	**HyperText Transfer Protocol**
IP	**Internet Protocol**
IT	**Information Technology**
I&A	**Identification & Authentication**
JRE	**Java Runtime Environment**
LAN	**Local Area Network**
MAC	**Media Access Control**
MOC	**Management Operations Center**
NAC	**Network Access Control**
OS	**Operating System**
RADIUS	**Remote Authentication Dial In User Service**
RFC	**Request For Comments**
SF	**Security Function**
SFR	**Security Functional Requirement**
SMTP	**Simple Mail Transfer Protocol**
SMS	**Systems Management Server**
SNMP	**Simple Network Management Protocol**
SPAN	**Switched Port ANalyzer**
ST	**Security Target**
TCP	**Transmission Control Protocol**
TOE	**Target of Evaluation**
TSF	**TOE Security Function**
URL	**Uniform Resource Locator**
VLAN	**Virtual Local Area Network**
VoIP	**Voice over Internet Protocol**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Trustwave Network Access Control (NAC) Software Version 3.4.0. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1*and all international interpretations through the date the TOE was accepted into evaluation. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Trustwave Network Access Control (NAC) Software Version 3.4.0 Security Target, Version 2.4, dated October 19, 2009.

1.2 TOE Reference

Trustwave Network Access Control (NAC) Software Version 3.4.0-24029

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) augmented by ALC_FLR.1 from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1.

1.4 Keywords

Network Access Control, NAC, Compliance, Threat Detection, Mitigation, Remediation, Security, Risk Management

1.5 TOE Overview

1.5.1 Usage and Major Security Features

Trustwave's NAC solution is an infrastructure-independent NAC that provides the following capabilities:

- Identity-based access control
- Device compliance checks
- Threat detection
- Automated policy enforcement

The Trustwave NAC solution enables network administrators to control which devices gain admission to their network and what network services they may invoke. Sensors are connected to all the network segments that are controlled, and monitor all the network traffic to detect any violations of the network use policy configured by administrators.

As soon as a device attempts to gain access to the network, Trustwave NAC immediately identifies the managed device and may be configured to run a policy check to determine if the device complies with the security policies in the network segment that it is trying to join.

Administrators may optionally configure policies to require the TOE to validate credentials supplied by the user of the managed device to the TOE against an external credential server such as RADIUS and Active Directory. The credentials are exchanged between the managed devices and the TOE via an HTTPS connection. The cryptographic functionality in the TOE used to protect the confidentiality of the credentials has not been FIPS validated. Therefore, this optional functionality is not being evaluated.

When performing policy checks on managed devices, Trustwave NAC may perform monitoring of network traffic to identify attributes of the device and/or a deep scan via a Java applet downloaded to the device via an internet browser session. Network monitoring determines the device type, whether it is known or unknown, network function (e.g. IP telephony device, wireless device), and what services are currently running – such as instant messaging, file transfer protocol services, or peer-to-peer networking. Deep scans obtain more detailed information about the device configuration such as anti-virus version, signature update levels, OS patch levels and the absence or presence of spyware and firewall software. Devices can be re-checked throughout their lifecycle on the network.

All of the information learned about a managed device is then used to evaluate whether to admit each managed device to the network and what services each managed device may access. These decisions are determined by policies configured by administrators. Options that may be configured for network access include:

- Quarantine a device
- Restrict network access to explicitly listed services
- Redirect the device to a configured remediation server

After admission, Trustwave NAC monitors all network traffic, detects exceptions to the configured behavioral policy, and re-evaluates the network access permitted to the managed devices as new information about them is learned.

Administrators control and monitor the operation of Trustwave NAC via an application executing on a Windows PC. A second management interface is provided with restricted ability to view reports generated by the TOE via a web browser. Multiple roles are supported to provide different levels of access to different administrators. Administrators must identify and authenticate themselves before any management access is granted.

Trustwave NAC maintains a log of actions performed by administrators and conclusions reached by the TOE about the managed devices. The log may be reviewed by administrators.

1.5.2 TOE type

Network access control

1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE consists of software executing on multiple platforms. The dependencies for each of the software components are described in subsequent paragraphs.

The Management Operations Center (MOC) must be installed on a PC meeting the minimum requirements in the following table.

Table 1 - MOC Hardware/Software Dependencies

Item	Requirements
Operating System	Windows Vista, Windows 2003 Server, Windows 2000 SP2, Windows XP (Professional, Home)

Item	Requirements
Web Browser	Internet Explorer 7 or above OR Mozilla Firefox 2 or above
Memory	512 MB RAM
Hard Disk Free Space	200 MB

The Management Server software executes on the M-1 or M-10 appliance, which differ only in their disk configuration. These appliances must satisfy the minimum requirements in the following table.

Table 2 - Management Server Software Appliance Dependencies

Item	M-1 Requirements	M-10 Requirements
RAID	RAID 1	RAID 1
Storage	160 GB	1 TB
Network Ports	Redundant 1 Gbps	Redundant 1 Gbps
Processors	Dual Xeon Quad Core 2.0GHz	Dual Xeon Quad Core 2.0GHz
Memory	4 GB	4 GB

The Compliance Server software executes on the A-500 appliance, which must satisfy the minimum requirements in the following table. The network ports on the Compliance Server are used both for the intra-TOE communication and for communication with managed devices.

Table 3 - Compliance Server Software Appliance Dependencies

Item	Requirements
Storage	80 GB
Network Ports	Redundant 100/1000 Ethernet
Processors	Single Pentium Dual Core 2.2GHz
Memory	2 GB

The Sensor software executes on the X-50, X-100, X-500, X-1000 or X-2500 appliance. These appliances must satisfy the minimum requirements in the following table.

Table 4 - Sensor Software Appliance Dependencies

Item	X-50 Requirements	X-100 Requirements	X-500 Requirements	X-1000 Requirements	X-2500 Requirements
Management Ports	One 100/1000 Ethernet	One 100/1000 Ethernet	Two 100/1000 Ethernet	Two 100/1000 Ethernet	Two 100/1000 Ethernet
Network Ports	Two 100/1000	Two 100/1000	Four 100/1000	Four 100/1000	Four or eight

Item	X-50 Requirements	X-100 Requirements	X-500 Requirements	X-1000 Requirements	X-2500 Requirements
	Ethernet	Ethernet	Ethernet	Ethernet	copper or fiber 1 Gbps
Processors	Single Pentium Dual Core 2.2GHz	Single Pentium Dual Core 2.2GHz	Single Pentium Dual Core 2.2GHz	Single Pentium Dual Core 2.2GHz	Dual Xeon Quad Core 2.0GHz
Memory	2 GB	2 GB	2 GB	2 GB	4 GB

The network infrastructure and managed devices that the TOE monitors are not included in the TOE. Network switches, in particular, must be capable of forwarding a copy of all the LAN traffic for a segment to the sensors in order to allow for monitoring of all traffic post-admission. This function is often performed via a SPAN port on the switches.

The Trustwave NAC is able to perform deep scans of managed devices running Windows, Mac OS or Linux. These scans are used to gain additional knowledge about the individual managed devices, such as patch levels and whether or not anti-virus and personal firewall software is being used. This information may be used to determine more fine-grained network access permissions for the systems. In order for deep scans to be performed, the TOE downloads a Java application to the managed device. The managed devices must meet the following requirements to support the Java application.

Table 5 - Deep Scan Requirements for Windows Systems

Item	Requirements
Operating System	One of the following: Windows Vista Windows 2000 SP4 Windows Server 2003 SP2 Windows XP SP2
Internet Browser	One of the following: Microsoft Internet Explorer 5.0 or later Firefox 1.5 or later Netscape 8
Java Runtime Environment	One of the following: Sun JRE 1.4.2_13 or later IBM JRE 1.4.2

Table 6 - Deep Scan Requirements for Macintosh Systems

Item	Requirements
Operating System	Mac OS 10.4.5 or later
Internet Browser	One of the following: Safari 2.0.3 Firefox 1.0 or later
Java Runtime Environment	Sun JRE 1.4.2_13 or later

Table 7 - Deep Scan Requirements for Linux Systems

Item	Requirements
Operating System	Fedora 4 or later
Internet Browser	Firefox 1.0.1 or later
Java Runtime Environment	Sun JRE 1.4.2_23, 1.5.0_10, or 1.6

The TOE components communicate with one another via network ports on the appliances. On the system hosting the MOC, the Management Server and Sensors, the network interfaces used are dedicated to the intra-TOE traffic (as well as browser access for reports on the Management Server) and are not used for any traffic exchanges with the managed devices. In the case of the Compliance Server, the network interface is used for both intra-TOE communication as well as communication with managed devices. It is the responsibility of the operational environment to protect the traffic on the management network. Since the Compliance Servers need to communicate directly with managed devices using HTTP, at least one router must interconnect the management network with the Enterprise LAN. Any routers performing this function must be configured so that HTTP traffic between the Compliance Servers and managed devices is permitted to flow between the management network and Enterprise LAN. No other traffic between devices connected to the management network and devices in the Enterprise Network is required by the TOE, and should be prevented unless such communication is required for other purposes.

The Management Server may also be accessed via a web browser. This access mechanism is limited to accessing reports, and is the only access provided to administrators with the Reporting User role. Any systems accessing the Management Server via this mechanism must be connected to the management network in order to protect the information exchanged with the Management Server. The minimum software requirements for systems using a browser to access the Management Server are:

1. Internet Explorer 7 or above, or
2. Mozilla Firefox 2 or above.

1.6 TOE Description

The TOE provides network access control by enforcing administrator-configured policies for network traffic flows to or from managed devices using administrator-configurable rules. The TOE performs both pre-admission and post-admission checking. Pre-admission checks include automatic discovery of devices and policy compliance scanning. To accommodate specialized equipment such as VoIP phones and printers, administrators may exempt specific managed devices from any or all of these steps. Post-admission checks focus on continuous monitoring of the network traffic to enforce the configured behavioral policies.

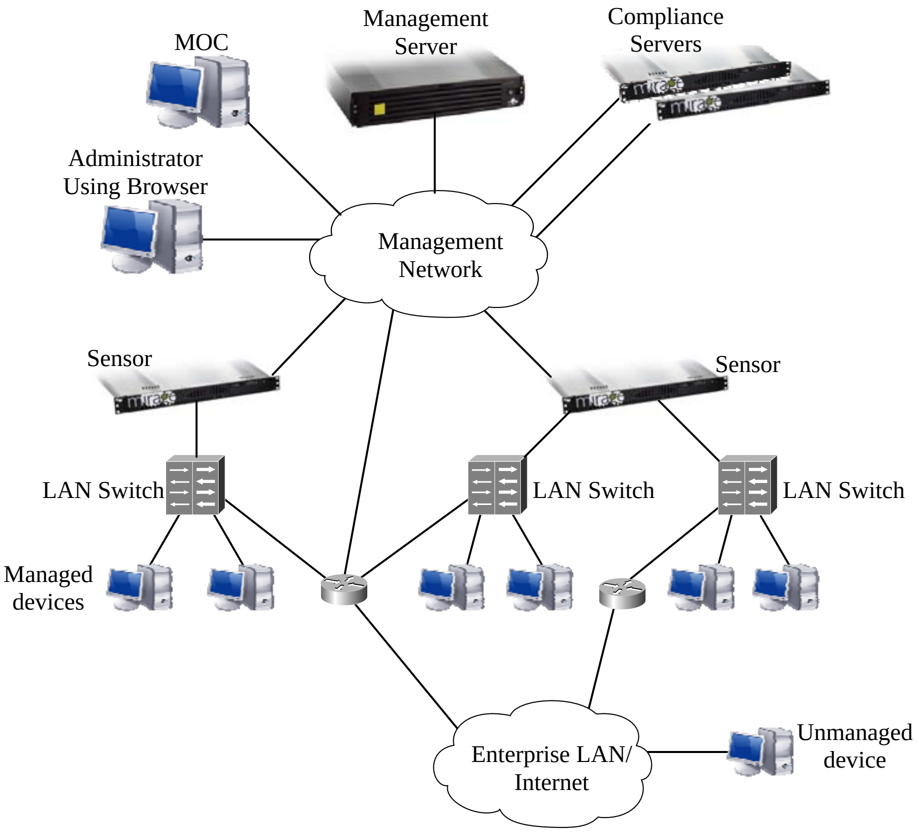
The TOE is the software for the Trustwave Network Access Control product, which consists of multiple components as follows distributed throughout the enterprise network:

1. Management Operations Center (MOC) – Software executing on a Windows PC that provides the user interface for the NAC. MOC communicates with the Management Server. A single MOC is used to control and monitor the NAC infrastructure.

2. Management Server – The Management Server is an appliance that provides the centralized control, monitoring, and data collection functions for the set of Sensors and Compliance Servers in a deployment. A single Management Server is used for the NAC infrastructure.
3. Sensors – The Sensor appliances are connected to one or more LAN segments and control network access for devices connected to the LAN segments. These devices discover managed devices and enforce the network access control policies. A single sensor may service multiple LAN segments. As many sensors are deployed as are required to connect to all the monitored segments.
4. Compliance Servers – The Compliance Server appliances perform the deep scans of managed devices. A Java application is dynamically downloaded to these managed devices when a scan is required. Sufficient compliance servers are installed to handle the number of managed devices in the deployment. These systems may be centralized or distributed.

A typical deployment for these components is shown in the following diagram.

Figure 1 - Typical TOE Deployment



Additional details for the components are provided in the following sections.

1.6.1 MOC

The MOC provides the user interface for control and monitoring of the TOE. The MOC presents a GUI to authorized users; multiple roles are supported to enable different users to have access to varying levels of functionality. The MOC retrieves information from and sends information to the Management Server based upon the actions of the user.

1.6.2 Management Server

The Management Server software acts as the central coordinator for all components of the TOE, in that all other components communicate with it exclusively. The Management Server receives and stores data from Sensors and Compliance Servers, and sends configuration information to those components. The Management Server provides information to the MOC upon request, and processes configuration changes directed by the user of the MOC. The Management Server also provides a web server interface to TOE users who are only authorized for read access to reports (Reporting Users) that were previously generated by authorized users of the MOC.

1.6.3 Sensors

The Sensor software is responsible for monitoring all network traffic on one or more LAN segments. The traffic is analyzed to detect new devices and to scan ongoing traffic from all devices for unauthorized usage. The Sensor software responds to detected conditions by sending ARP messages to quarantine devices that violate configured policies or redirecting browser sessions to a Compliance Server for authentication (via an external credential store) or scanning. This component generates messages that are forwarded to the Management Server for security relevant events involving the managed devices.

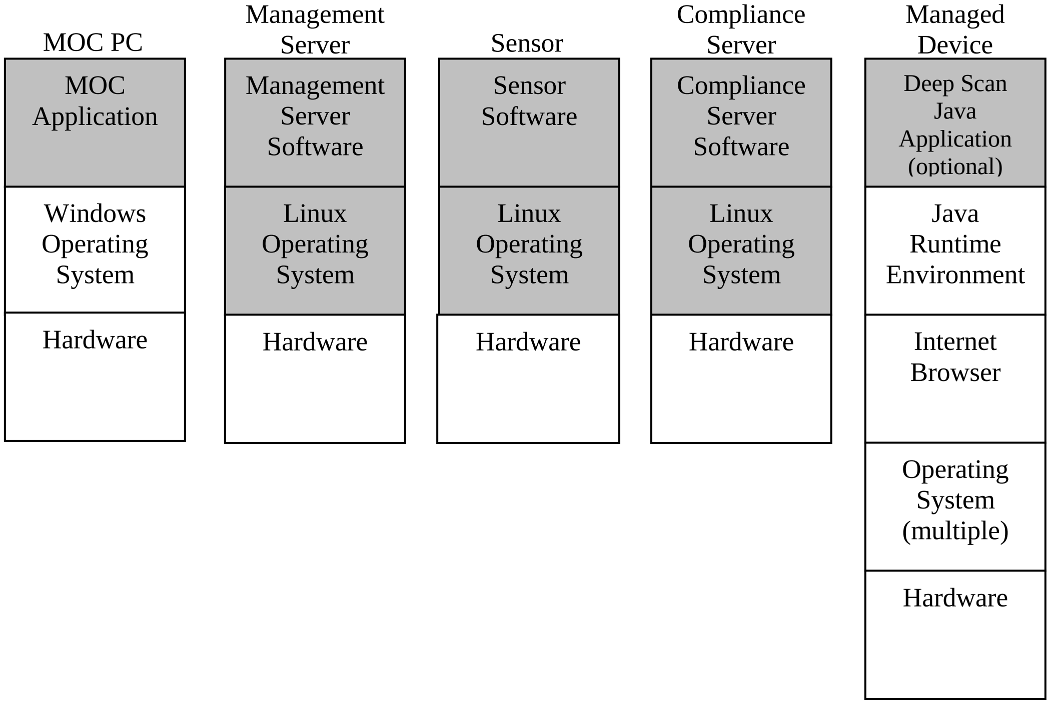
1.6.4 Compliance Servers

The Compliance Server software provides a Java application downloaded to managed devices that are required (by configured policy) to be scanned. The Java application gathers information from a managed device and returns it to the Compliance Server to determine if each managed device is compliant. This component generates messages that are forwarded to the Management Server for security relevant events involving the managed devices.

1.7 Physical Boundary

The physical boundary of the TOE is all the software executing on the appliances, including the operating system, along with the MOC application and the Java application used to perform deep scans on managed devices, as depicted in the following diagram (shaded items are within the TOE boundary).

Figure 2 - Physical Boundary



The physical boundary also includes the following guidance documentation:

1. *Trustwave NAC A-500 Hardware*
2. *Trustwave NAC Advanced Compliance Server Deployment and Branding*
3. *Trustwave NAC M-1/M-10 Hardware Guide*
4. *Management Operations Console User's Guide*
5. *Trustwave NAC X-[50, 100, 500, 1000] Hardware Guide*
6. *Trustwave NAC X-2500 Hardware Guide*
7. *Trustwave NAC Hardware Guide*
8. *Trustwave Network Access Control (NAC) Version 3.4.0 Installation Supplement*

1.8 Logical Boundary

1.8.1 Audit

Audit messages are generated for security relevant events involving managed devices as well as for actions performed by users of the TOE. The audit log is stored on the Management Server and the information is available to authorized users of the MOC.

1.8.2 Identification and Authentication

The TOE performs I&A for all users of the MOC as well as for users accessing reports via the TOE's web server. No access is provided to management functionality until I&A is successfully performed.

1.8.3 Management

The TOE provides management capability to enable the TOE to be controlled and monitored. Four distinct roles are provided so that different users can be granted different levels of access to the management functions.

1.8.4 Network Access Control

The TOE performs network access control on managed segments to enforce the configured policy for devices using the managed segments. The TOE monitors the traffic on managed segments to detect new devices and/or unauthorized behavior. The TOE performs network scans of known devices to determine their open network ports and other characteristics such as the base operating system. The TOE also provides a Java applet that can be downloaded to devices via a web browser to perform deeper scans of the systems to determine finer-grained characteristics.

When policy violations are detected, policies may direct the TOE to send ARP messages to the devices on a managed segment to quarantine an offending device, redirect devices to a configured server (e.g., remediation server), or validate user credentials with existing credential servers.

1.9 Evaluated Configuration

The evaluated configuration consists of the following TOE components, executing on systems complying with the minimum hardware and software requirements specified for each component:

1. One instance of the MOC executing on an IT system dedicated to this purpose
2. One instance of the Management Server
3. One or more instances of the Compliance Server
4. One or more instances of the Sensor

In addition, the following configuration options must be specified to conform to the evaluated configuration:

1. Scanning is enabled at the domain level
2. Restricted access is enabled at the domain level
3. The only External Authorities configured are the Compliance Servers; these are automatically configured during installation
4. All administrative accounts are configured at the top level domain.
5. All management of the TOE after installation is performed using the MOC. The Terminal User Interface (TUI) to the appliances is only used during installation. The configuration functionality available through the Management Server web server functionality is not used.
6. Bypassing the compliance scan is often necessary for network devices such as printers, HVAC controllers, badge readers, security cameras and network infrastructure devices, such as routers and switches. While configuring exclusions for these devices is a normal part of any NAC deployment, basing the exclusions on either the MAC or IP Address of

the device poses risks, since malicious users may attempt to hijack the excluded device's address for the purposes of avoiding the compliance scan. As part of its device visibility functionality, Trustwave provides network-based OS detection of all devices in a managed segment. In order to maintain the integrity of an implemented security policy, Trustwave recommends leveraging this functionality for the purposes of excluding Embedded OS devices from compliance scanning. Setting compliance-scanning exclusions based upon endpoint OS characteristics makes it much more difficult for malicious users to bypass the security policy.

1.10 Glossary

Access Zone - Network devices are grouped into Access Zones based on a series of characteristic condition tests that determine whether they are included or excluded from the zone. Devices can only be members of one zone at a time, although they can move between zones as their characteristics change. Each Access Zone has a set of profiles (Included and Excluded) associated with it that dictates how the devices are allowed to participate on the network.

Device - Computing resource that communicates on a network, i.e. laptop, desktop machine, printer, E-mail server, etc.

Device Session – The period of time a device is on the network, starting from the time a device not in a session is detected until the time activity from that device is no longer detected. The timeout for a device session is restarted every time a packet is monitored from it. If the timer expires, the TOE sends several directed ARP messages to it to see if a reply is received before declaring the session to be over.

Domain - Group of managed resources (appliances, network segments, etc.) organized into hierarchical units such as regions, departments, etc. Domains can be organized into sub-domains to provide an organized view of the network that reflects how the network is managed.

Managed Devices - Devices with IP addresses within a managed segment address range.

Managed Segments - Segments being actively managed and monitored by the TOE, specified by a range of IP addresses.

Policy - A set of conditions that define how devices can enter, and operate within, an organization's network.

Profile - Composition of device properties and behavioral conditions that enables management of classes of devices as a single unit.

Reporting User – An authorized user of the TOE that is only authorized for read access to reports previously generated by users of the MOC. This role is restricted to accessing a web server on the Management Server for access to the reports; no access to the MOC is permitted.

Response - Configurable action taken by the TOE, when a device either on the network or trying to connect to the network matches a profile contained in an Access Zone.

Scanning - Method of collecting device properties for NAC policy evaluation. The TOE collects service port, operating system, routing behavior, and connection type properties for devices scanned. Scanning can be configured to be performed when devices enter or leave an Access Zone.

SPAN Port - Switched Port Analyzer - Mirrors network traffic from a switched segment onto a specified port for traffic monitoring purposes.

Unmanaged Devices – Devices that send or receive network traffic via a managed segment, but that are not themselves connected to (have an IP address assigned to) a managed segment.

1.11 TSF Data

The following table describes the TSF data used in the TOE.

Table 8 - TSF Data Descriptions

TSF Data	Description
Access Zones	A grouping of managed segments (specified by IP address range) and profiles that specify conditions for membership in an access zone. Profiles may be Include or Exclude. None of the configured Exclude profiles may match a device for it to join an access zone, and all of the configured Include profiles must match. Membership is evaluated according to the ordered list of access zones configured for a domain. Each access zone defines actions required upon entry to the access zone as well as authorized actions by managed devices on the network while they are members of the access zone. Access zones are defined by the following security-relevant information: • Include profiles • Exclude profiles • Priority (used in reporting) • Restrict access – members of the access zone have access restricted according to the service access and HTTP response settings • Service access configuration – access may be permitted or denied for an explicitly listed set of {protocol, port, IP address, source port} tuples. • HTTP response – a text message or Redirect URL may be returned to a device attempting HTTP access • Scanning properties – Specifies whether or not scanning is performed on devices that are members of the access zone. Devices may be scanned upon entry to or exit from the access zone, randomly, or at specified frequencies
Access Zone Order	Access zones are organized in an ordered list (top to bottom in the MAC display). Devices are automatically assigned to the first access zone for which the device satisfies all the conditions.
Alert Destinations	Specify the set of SMTP, SNMP, and/or syslog destinations and parameters that may be recipient of alerts within each domain.
Alerts	A set of alerts generated within a domain. Each alert is bound to an access zone, profile, or appliance. Access zone alerts are bound to one of the access zones in the domain and occur upon either entry to or exit from the access zone. Profile alerts are bound to one or more profiles and occur upon either when a device first matches or no longer matches the profile. Appliance profiles are bound to an appliance and occur upon an appliance becoming ready, rebooting, or shutting down. All alerts include an alert destination selected from the list of destinations configured for the domain.

TSF Data	Description
Appliances	Each appliance (server, sensor, or compliance server) is defined by an IP address and port for intra-TOE communication.
Domains	A grouping of managed resources organized into a hierarchical structure. A domain consists of the following security-relevant information: • Access zones • Active access zones • User accounts • Appliances • Alert destinations • Alerts • Managed segments • Available profiles • Service access restrictions enabled • Scanning enabled • IP locking list – a list of MAC/IP address pair bindings that must be enforced. Devices that attempt to access the network that violate a binding are quarantined. • Never scan – a single profile may be specified; any matching devices are exempt from scanning • Never restrict - a single profile may be specified; any matching devices are exempt from service access restrictions • Never monitor - a single profile may be specified; any matching devices are exempt from monitoring for behavioral violations Domain configuration settings apply to all subordinate domains.
Forced Access Zone Bindings	Managed devices are normally bound to access zones automatically based upon matched profiles and the profiles in access zone include and exclude lists. Alternatively, managed devices may be forced into an access zone by administrators. Devices stay in that access zone until the forced binding is removed.
Managed Device Attributes	A set of attributes discovered about a managed device based upon traffic analysis, authentication of user-supplied credentials, and compliance scans. These attributes are compared to the conditions specified in profiles to determine access zone membership. Attributes may include • Access zone membership - A managed device may only belong to one zone at a time. Membership is automatically determined by the TOE based upon the configured profiles and device attributes. • Matched profiles – A list of profiles that each device matches. • Deep scan completed • MAC address • IP address • Operating system name, version, missing patch severity, SMS configuration, SMS last scanned • Operating system missing patch level • Anti-Spyware software installed, enabled, version, last scanned, last updated • Anti-Virus software installed, enabled, version, last

TSF Data	Description
	scanned, last updated • Firewall software installed, enabled • Router • Gateway • IP Telephony • Registered • MAC/IP address binding locked • Managed • Wireless • Open network ports/services
Managed Segments	The monitoring interfaces within a Sensor are defined by segments, which are paired interfaces – one for receiving all the traffic via a switch mirror or SPAN port, and one used for sending network traffic from the Sensor. The attributes for each segment are the IP address/subnet mask and (optionally) a VLAN.
Profiles	Profiles define matching criteria for device properties and conditions. They are used to enforce NAC policy across the network of managed segments, and drive alert notifications when violated. Profiles also serve as Access Zone membership criteria, defining the conditions under which a device is included in or excluded from the Access Zone. A profile consists of the following information: • Include conditions – All include conditions must match. • Exclude conditions – No exclude conditions can match. • Categories – Associates a profile with report types.
User Accounts	Defined accounts for authorized users of the MOC and/or the reporting interface of the Management Server. Each account includes a username (common name), userid, password, and role. Accounts created in the root domain have access to all sub-domains, while accounts created within sub-domains can only manage resources of their own sub-domain and any domains under that sub-domain.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 2

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

The TOE is conformant with EAL2 augmented by ALC_FLR.1.

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

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

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following table are assumed to exist in the TOE environment.

Table 9 - Assumptions

A.Type	Description
A.ARP	Managed devices will process received Address Resolution Protocol messages as specified in RFC826.
A.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
A.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
A.NETWORK	There will be a network that supports communication between distributed components of the TOE. This network functions properly.
A.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

3.3 Threats

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

Table 10 - Threats

T.Type	TOE Threats
T.AUDIT_ COMPROMISE	A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTH_ACCESS	Authorized devices may attempt unauthorized access to other IT systems via the network.

T.Type	TOE Threats
T.UNAUTH_CONFIG	Devices with unauthorized configurations may access protected information via the network, and because of the unauthorized configuration fail to protect that information from unauthorized disclosure.
T.UNAUTH_DEVICES	Unauthorized devices may attempt to access systems or data on the network.
T.UNIDENT_ACTIONS	The administrator may not have the ability to notice potential security violations such as attempts by users to gain unauthorized access to the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach.

3.4 Organisational Security Policies

The organizational security policies identified in the following table are addressed by the TOE and the Operational Environment.

Table 11 - OSPs

T.Type	OSPs
P.MANAGE	The authorized administrators of the TOE must have the necessary functions and facilities to effectively manage the TOE.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 12 - Security Objectives for the TOE

O.Type	Security Objective
O.AUDIT_GEN	The TOE will provide the capability to detect and create records of security-relevant events.
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit and system data information from unauthorized access.
O.AUDIT_REVIEW	The TOE will provide the capability to view audit and system data information in a human readable form.
O.DETECT_DEVICES	The TOE will provide the capability to detect new devices on managed segments.
O.I&A	The TOE will provide the capability to identify and authenticate administrators.
O.IDANLZ	The TOE must apply analytical processes and information to information learned about managed devices to derive and store conclusions about unauthorized network usage or noncompliant device security configurations (past, present, or future).
O.IDSCAN	The TOE must collect static configuration information that might be indicative of the potential for future unauthorized network usage or noncompliant device security configurations or the occurrence of past unauthorized network usage or noncompliant device security configurations of a managed device.
O.IDSENS	The TOE must collect information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of managed devices.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE.
O.RESTRICT_DEVICES	The TOE will provide the capability to restrict network access to and from devices based upon the derived conclusions about unauthorized network usage or noncompliant device security configurations.
O.TIME_STAMP	The TOE will provide reliable time stamps for accountability purposes.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.

4.2 Security Objectives for the Operational Environment

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

Table 13 - Security Objectives of the Operational Environment

OE.Type	Operational Environment Security Objective
OE.ARP	IT systems on managed segments shall process Address Resolution Protocol messages according to the relevant RFCs.
OE.COMM	The Operational Environment will protect communication between distributed components of the TOE from disclosure.
OE.ENVIRON	The Administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
OE.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
OE.MIRROR	The operational environment will provide the capability to provide a copy of all network traffic on managed segments to the TOE.
OE.NETWORK	The Administrator will install and configure a network that supports communication between the distributed TOE components. The administrator will ensure that this network functions properly.
OE.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.
OE.RESTRICT	The operational environment will restrict traffic exchanged between the management network and the remainder of the Enterprise network to authorized traffic between managed devices and Compliance Servers.
OE.TIME	The Operational Environment will provide support to the TOE to provide time stamps.

5. Extended Components Definition

5.1 Extended Security Functional Components

All of the components in this section are based on the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

This class of requirements is taken from the IDS System PP to specifically address the data collected and analysed by an IDS scanner and analyzer. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of system data and provide for requirements about collecting, reviewing and managing the data.

5.1.1 IDS_SDC.1 System Data Collection

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) [selection: *Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, detected known vulnerabilities*]; and

b) [assignment: *other specifically defined events*].

IDS_SDC.1.2 At a minimum, the System shall collect and record 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) The additional information specified in the *Details* column of **the table below**.

Table 14 - System Data Collection Events and Details

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	none
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDs, requested access, source address, destination address
IDS_SDC.1	Service Requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDs, location of object, source address, destination address
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings

Component	Event	Details
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked passwords, account policy parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Application Note: The rows in this table must be retained that correspond to the selections in IDS_SDC.1.1 when that operation is completed. If additional events are defined in the assignment in IDS_SDC.1.1, then corresponding rows should be added to the table for this element.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the events to be collected.

Audit:

There are no auditable events foreseen.

5.1.2 IDS_ANL.1 Analyser Analysis

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all system data received: [assignment: *analytical functions*].

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:

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

b) [assignment: *other security relevant information about the result*].

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

5.1.3 IDS_RCT.1 Analyser React

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

IDS_RCT.1.1 The System shall send an alarm to [assignment: alarm destination] and take [assignment: appropriate actions] when unauthorized network usage or noncompliant device security configuration is detected.

Application Note: There must be an alarm, though the ST should refine the nature of the alarm and define its target (e.g., administrator console, audit log). The Analyser may optionally perform other actions when unauthorized network usage or noncompliant device security configurations are detected; these actions should be defined in the ST. Unauthorized network usage or noncompliant device security configurations in this requirement apply to any conclusions reached by the analyser related to past, present, and future unauthorized network usage or noncompliant device security configurations (actual or potential).

Management:

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

Audit:

There are no auditable events foreseen.

Application Note: Consideration should be given to generation of a System Data record that includes the action taken as part of the reaction..

5.1.4 IDS_RDR.1 Restricted Data Review

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection
IDS_ANL.1 Analyser Analysis

IDS_RDR.1.1 The System shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

Management:

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the system data records.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Attempts to read system data that are denied.

b) Detailed: Reading of information from the system data records.

Application Note: The audit event definition is consistent with CCEVS Policy Letter #15, which states that only access failures are auditable at the Basic level of audit.

5.1.5 IDS_STG.1 Guarantee of System Data Availability

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection
IDS_ANL.1 Analyser Analysis

IDS_STG.1.1 The System shall protect the stored System data from unauthorised deletion.

IDS_ STG.1.2 The System shall protect the stored System data from modification.

Application Note: Authorised deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

IDS_ STG.1.3 The System shall ensure that [assignment: metric for saving System data] System data will be maintained when the following conditions occur: [selection: System data storage exhaustion, failure, attack].

Management:

The following actions could be considered for the management functions in FMT:

a) maintenance of the parameters that control the system data storage capability.

Audit:

There are no auditable events foreseen.

5.2 Extended Security Assurance Components

No extended security assurance components are defined.

6. Security Requirements

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

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

> *Assignment: indicated in italics*
>
> <u>Selection: indicated in underlined text</u>
>
> <u>*Assignments within selections: indicated in italics and underlined text*</u>
>
> **Refinement: indicated with bold text**

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

6.1 TOE Security Functional Requirements

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

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

b) All auditable events for the <u>not specified</u> level of audit; and

c) *the events specified in the table below*.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the additional details specified in the table below*.

Table 15 - FAU_GEN.1 Detail

SFR	Event	Description	Additional Details
FAU_GEN.1	Appliance Started (System)	The appliance is starting up	Appliance name
	Appliance is being shutdown (System)	The appliance is being shut down	Appliance name
	Appliance is being rebooted (System)	The appliance is being rebooted	Appliance name

SFR	Event	Description	Additional Details
	Shutdown (Security)	An administrator directed an appliance to shut down	Username
	Reboot (Security)	An administrator directed an appliance to shut down	Username
FIA_UAU.2	Login (Security)	Successful login	Username and userid
	Logout (Security)	User logout from the system	Username and userid
	Login Failure (Security)	I&A failed during a login attempt	Userid
FIA_UID.2	Login (Security)	Successful login	Username and userid
	Logout (Security)	User logout from the system	Username and userid
	Login Failure (Security)	I&A failed during a login attempt	Userid
FMT_MOF.1	Update Config (Security)	TSF data has been modified	Username
	Create Config – save (Security)	TSF data has been created	Username
FMT_MTD.1	Update Config (Security)	TSF data has been modified	Username
	Create Config – save (Security)	TSF data has been created	Username
	Delete Config (Security)	TSF data has been deleted	Username
	Create Config – reevaluate Device (Security)	TSF data is being modified because the administrator directed a device to be re-evaluated	Username

Application Note: The TOE places audit event records into one of the following categories: Security, and System. The table above specifies which of the categories each audit event type belongs to.

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *users with administrator, operator or observer roles* with the capability to read *audit information applicable to the domain or sub-domain to which they are bound as well as all subordinate sub-domains* from the audit records.

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

6.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply *searching and sorting* of audit data based on *the audit data type and parameters specified in the following table*.

Table 16 - FAU_SAR.3 Details

Audit Data Type	Method	Parameters
Security Audit	Search	Time range and User Account(s)
	Sort	Timestamp, Operation, User Account, Description, or Policy Domain
System Events	Search	Appliance and Time range
	Sort	Timestamp, Description, or Appliance

6.1.1.6 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorised modifications to the audit records in the audit trail.

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the *Access Zone Service Restriction SFP* on

1. *Subjects: Managed devices*
2. *Information: IP datagrams with destination MAC addresses in the range of values used for service restrictions (00:9c:xx:xx:xx:xx) received on managed segments*
3. *Operations: Forward, discard, HTTP redirect, HTTP response.*

6.1.2.2 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the *Access Zone Service Restriction SFP* based on the following types of subject and information security attributes:

1. *Managed devices: Access Zone membership*
2. *IP datagram: Source MAC address, destination MAC address, source IP address, destination IP address, IP protocol field, source TCP/UDP port, destination TCP/UDP port, TCP flags, ICMP type*

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

1. *For IP datagrams sent from a managed device with membership in an Access Zone with service restrictions:*
    a. *If any of the service restriction rules for permitted flows match the attributes of the IP datagram, processing continues with step 2.*
    b. *If the service restriction rules specify HTTP redirection and the incoming packet is HTTP (based on the destination TCP port), an HTTP Redirect with the*

configured URL is sent to the source of the IP datagram and the incoming IP datagram is discarded.

   c. *If the service restriction rules specify HTTP response and the incoming packet is HTTP (based on the destination TCP port), an HTTP response with the configured message is sent to the source of the IP datagram and the incoming IP datagram is discarded.*

   d. *The incoming IP datagram is discarded and processing stops.*

2. *For IP datagrams sent to a managed device with membership in an Access Zone with service restrictions:*

   a. *If any of the service restriction rules for permitted flows match the attributes of the IP datagram, processing continues with step 3.*

   b. *The incoming IP datagram is discarded and processing stops.*

3. *The IP datagram is forwarded to the managed device after substituting the destination MAC address of the true destination and the source MAC address used for service restrictions of the originator of the IP datagram.*

FDP_IFF.1.3 The TSF shall enforce the *no additional information flow control SFP rules*.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules:

1. *If the domain-level Never Restrict parameter is on, IP datagrams are always forwarded.*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *none*.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

1. *Userid*
2. *Password*
3. *Username*
4. *Role*
5. *Associated domain (or sub-domain)*

6.1.3.2 FIA_SOS.1 Verification of Secrets

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

1. *Passwords must be at least 8 characters long.*
2. *Passwords must start with an upper or lower case character A-Z or a-z.*
3. *Passwords must contain a lower case character a-z.*
4. *Passwords must contain an upper case character A-Z.*

5. *Passwords must contain a number 0-9.*
6. *Passwords must contain a symbol ! @ # % _ + - = : , . /*
7. *Passwords must not contain an illegal symbol $ ‘ \ ~ * | ; < > ‘ “ ? ^ & ( ) [ ] { }.*
8. *Passwords must not contain spaces.*

6.1.3.3 FIA_UAU.2 User Authentication Before any Action

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

6.1.3.4 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *asterisks echoed back to the user as characters are typed for passwords* to the user while the authentication is in progress.

6.1.3.5 FIA_UID.2 User Identification Before any Action

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

6.1.3.6 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: *username, userid, role and associated domain (or sub-domain)*.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *the username, userid, role and domain are associated with an administrative session when I&A is successful*.

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

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behaviour of, disable, enable, modify the behaviour of the functions *specified in the following table* to *the authorised identified roles in the following table*.

Table 17 - FMT_MOF.1 Details

Function	Determine	Disable/ Enable	Modify
Potential security violation definitions	Administrator, Operator, Observer	Administrator	Administrator
Responses to potential security violations	Administrator, Operator, Observer	Administrator	Administrator

Application Note: The authorized roles may determine (view), disable/enable and modify information for their associated domain and subordinate sub-domains.

6.1.4.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete the *items listed in the following table* to *Administrator, Operator, Observer, and Reporting User roles as specified in the following table*.

Table 18 - TSF Data Management Details

TSF Data	Administrator	Operator	Observer	Reporting User
Access Zones	Query, modify and delete in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	None
Access Zone Order	Query and modify in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	None
Alert Destinations	Query, modify and delete in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	None
Alerts	Query, modify and delete in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	None
Appliances	Query in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	None
Domains	Query, modify and delete in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	None
Forced Access Zone Bindings	Query, modify and delete in the associated domain and subordinate sub-domains.	Query, modify and delete in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	None
Managed Device Attributes	Query and modify (re-evaluate) in the associated domain and subordinate sub-domains.	Query and modify (re-evaluate) in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains, via reports only.
Managed	Query, modify and	Query in the	Query in the	None

TSF Data	Administrator	Operator	Observer	Reporting User
Segments	delete in the associated domain and subordinate sub-domains.	associated domain and subordinate sub-domains.	associated domain and subordinate sub-domains.	
Profiles	Query, modify and delete in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	Query in the associated domain and subordinate sub-domains.	None
User Accounts	Query, modify and delete in the associated domain and subordinate sub-domains. Passwords are never displayed.	Query the user's own account only. Users may modify their own password. Passwords are never displayed.	Query the user's own account only. Users may modify their own password. Passwords are never displayed.	None

6.1.4.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. *Manage User Accounts*
2. *Manage potential security violation definitions*
3. *Manage responses to potential security violations*
4. *Manage system parameters*
5. *Monitor device and system status.*

6.1.4.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *administrator, operator, observer, and reporting user*.

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

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time-stamps.

6.1.6 IDS Component Requirements (IDS)

6.1.6.1 IDS_SDC.1 System Data Collection

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) <u>service configuration</u>; and

b) *Anti-Spyware status, Anti-Virus status, Firewall status, network function, Operating System, Operating System patch status, and suspicious network behaviour.*

IDS_SDC.1.2 At a minimum, the System shall collect and record 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) The additional information specified in the *Details* column of **the table below**.

Table 19 - System Data Collection Details

Component	Item	Details
IDS_SDC.1	Anti-Spyware status	Anti-spyware installed, enabled, scan last completed time, software last updated time
IDS_SDC.1	Anti-Virus status	Anti-virus installed, enabled, scan last completed time, software last updated time
IDS_SDC.1	Firewall status	Firewall installed, enabled
IDS_SDC.1	Network function	Gateway, web server, wireless device, IP telephony device
IDS_SDC.1	Operating System	Operating system identification
IDS_SDC.1	Operating System patch status	Auto update configuration, missing patches, missing patch severity level
IDS_SDC.1	Suspicious network behavior	Profile condition specifying the behaviour (specific packet contents, excessive unique device contacts, excessive port accesses, or MAC/IP address locking violation) detected
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols

6.1.6.2 IDS_ANL.1 Analyser Analysis

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all system data received: *comparison of the device attributes to profiles in active access zones to determine the managed device's access zone membership*.

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:

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

b) *Managed device, and the property type (Access Zone or Profile).*

Application Note: ***System data analytical result events are saved in the TOE as Device events and may be viewed using the same mechanism used for audit records. Audit records are saved as*** *Security or System events.*

6.1.6.3 IDS_RCT.1 Analyser React

IDS_RCT.1.1 The System shall send an alarm to *the alert destination configured for the access zone the managed device is assigned to or for the matching profiles determined for the managed device* and take *the service restriction actions configured for the access zone the managed device is assigned to* when unauthorized network usage or noncompliant device security configuration is detected.

6.1.6.4 IDS_RDR.1 Restricted Data Review

IDS_RDR.1.1 The System shall provide *users with administrator, operator or observer roles* with the capability to read *System data analytical results applicable to the domain or sub-domain to which they are bound as well as all subordinate sub-domains* from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

6.1.6.5 IDS_STG.1 Guarantee of System Data Availability

IDS_STG.1.1 The System shall protect the stored System data from unauthorised deletion.

IDS_ STG.1.2 The System shall protect the stored System data from modification.

Application Note: Authorised deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

IDS_ STG.1.3 The System shall ensure that *the oldest* System data will be maintained when the following conditions occur: System data storage exhaustion.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.1. These requirements are summarised in the following table.

Table 20 - EAL2+ Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.1	Basic flaw remediation
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

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

Table 21 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_GEN.2	No other components.	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by FIA_UID.2
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FAU_SAR.3	No other components.	FAU_SAR.1	Satisfied
FAU_STG.1	No other components.	FAU_GEN.1	Satisfied
FDP_IFC.1	No other components.	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components.	FDP_IFC.1, FMT_MSA.3	Satisfied Not satisfied. This SFR is not required since the attributes are dynamically determined by the TOE
FIA_ATD.1	No other components.	None	na
FIA_SOS.1	No other components.	None	na
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UAU.7	No other components.	FIA_UAU.1	Satisfied by FIA_UAU.2
FIA_UID.2	FIA_UID.1	None	na
FIA_USB.1	No other components.	FIA_ATD.1	Satisfied
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	na
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2
FPT_STM.1	No other components.	None	na
IDS_SDC.1	No other components.	None	na
IDS_ANL.1	No other components.	IDS_SDC.1	Satisfied
IDS_RCT.1	No other components.	IDS_ANL.1	Satisfied
IDS_RDR.1	No other components.	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied
IDS_STG.1	No other components.	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied

7. TOE Summary Specification

7.1 Audit

The TOE generates and stores audit records for security-relevant events. Audit records are saved for 30 days then deleted. No mechanism is provided for administrators to modify or delete audit records.

The audit records that are generated are specified in the table following FAU_GEN.1. The TOE categorizes each audit record type as a security event or system event. All audit records contain a time stamp of when the record was generated and the audit event type. The table following FAU_GEN.1 specifies the additional contents of the audit records. When appropriate, the audit record includes the identity of the administrator that initiated the action causing the audit record to be generated.

The administrator, operator, and observer roles may retrieve audit records for events within their domain as well as all subordinate sub-domains. The reporting user role does not have access to any audit records.

The TOE provides a search capability when retrieving records, as well as sort capability by clicking on a table heading to sort in ascending or descending order. The table following FAU_SAR.3 specifies the parameters available for searching and sorting for each of the categories.

If storage space for audit records is exhausted, new information is ignored.

7.2 Identification and Authentication

The TOE performs I&A for all administrative access to the TOE before granting any other access. I&A is performed for MOC access to a management server as well as for HTTP access to reports.

When I&A is required, the user must enter a userid and password. As the password is entered, asterisks are echoed back. When the credentials are submitted, the TOE verifies them against its store of defined accounts. If the credentials are not valid, the user is notified via a text message and is again prompted for credentials. When valid credentials are entered, the user attributes are bound to the session so that appropriate privileges may be enforced. The TOE supports multiple simultaneous management sessions and tracks the attributes for each session individually.

During a session the attributes do not change. If an administrator modifies the attributes for a session while the corresponding user has an active session, those changes do not take effect until that user logs out and logs back in.

7.3 Management

The TOE provides management capability to enables the TOE to be controlled and monitored. The administrator, operator, observer and reporting user roles provide different privileges to accommodate different user roles in an operational environment. The specific privileges for management functions associated with each role are defined in the tables following FMT_MOF.1 and FMT_MTD.1.

When an administrator configures a password for an account, password construction rules as defined in FIA_SOS.1 are enforced. When an existing account is viewed, only asterisks are displayed.

7.4 Network Access Control

The TOE monitors all network traffic on each managed segment. The monitoring is performed in order to:

1. Detect new managed devices communicating on a managed segment.
2. Detect suspicious network behavior by devices as defined by administrators via the profiles that are associated with active Access Zones. Suspicious behaviors may be specified to detect MAC/IP address locking violations (IP spoofing), an excessive number of devices being contacted by a managed device, an excessive number of ports being contacted by a managed device, or managed devices sending IP datagrams matching templates defined by an administrator.

If configured by an administrator, the TOE performs scanning of the devices to determine characteristics about them. Scanning may consist of one or both of:

1. Examination of the network packets returned from a device in response to probe packets sent by the TOE. The probe packets are specially constructed to elicit responses indicative of specific operating systems or network functions (e.g. wireless devices).
2. Determination of detailed device configuration information via a Java applet downloaded to a device via a browser session. This form of scanning is initiated by a Sensor redirecting an HTTP session initiated from a managed device to the Compliance Server.

The information learned about each device is analyzed to determine which of the configured profiles match that device’s characteristics. Changes to profile matches cause analytical result events to be generated and saved as device events. Alerts to SMTP servers, SNMP managers, or syslog servers upon entry to or exit from the matching profiles. Each device is then assigned to an access zone based upon analysis of the matching profiles and the profiles defined for the Access Zones. Only Access Zones that are active are considered during this process. Changes to Access Zone membership cause analytical result events to be generated and saved as device events. Access Zones may be configured to generate alerts to SMTP servers, SNMP managers, or syslog servers upon entry to or exit from the Access Zone.

If network traffic is restricted for a managed device (as specified by the Access Zone membership), the TOE sends ARP messages to cause that managed device to send all its network traffic to the attached sensor rather than directly to the intended recipient. Any device on the managed segment that communicates with that managed device is directed to send network traffic for the managed device to the attached sensor rather than sending it directly to the managed device. The TOE uses a special range of MAC addresses (00:9c:xx:xx:xx:xx) to identify traffic to or from managed devices with restrictions. The sensor then enforces the network traffic restrictions.

Each access zone defines the policies for managed devices that belong to it based upon the associated profiles and device attributes. The Access Zone then specifies the allowed types of network traffic for the devices in that Access Zone. Administrators may configure an Access Zone to restrict network traffic via the following methods:

1. Specified contents of IP datagrams may be explicitly allowed or denied
2. For HTTP sessions, redirect the session to a configured server (e.g., a remediation server in the operational environment to resolve an issue with operating system patches or

device configuration). This functionality can be used to redirect HTTP sessions to a Compliance Server for download of the Java applet to perform scanning of the managed device, or to collect credentials for validation against a credential store in the operational environment.

3. For HTTP sessions, a text message may be returned to the device. The text message may include an embedded URL, which can be clicked on by users of a managed device to initiate an HTTP session to a Compliance Server for download of the Java applet to perform scanning of the device, or to collect credentials for validation against a credential store in the operational environment.

All of these methods apply to IP datagrams sent from a managed device with network traffic restrictions. Only the first method (IP datagram content matching) applies to IP datagrams sent to a managed device with network traffic restrictions.

Upon command by an administrator or operator, the matching profiles for a managed device are re-analyzed and the access zone membership may change. Managed devices may be forced into a specific access zone by administrators or operators. Once forced into a zone, the managed device remains in that access zone until the forced condition is removed.

The TOE generates and stores system data analytical result records. System data analytical result records are saved for 30 days then deleted. No mechanism is provided for administrators to modify or delete the records.

Records are generated when changes to profile matches or Access Zone membership occur. The TOE categorizes each record as a device event. All system data analytical result records contain a time stamp of when the record was generated and the system data analytical result event type.

The administrator, operator, and observer roles may retrieve system data analytical results for events within their domain as well as all subordinate sub-domains. The reporting user role does not have access to any system data analytical results. All records for system data analytical results are stored as device events.

If storage space for system data analytical result records is exhausted, new information is ignored.

8. Protection Profile Claims

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

8.1 Protection Profile Reference

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

8.2 Protection Profile Refinements

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

8.3 Protection Profile Additions

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

8.4 Protection Profile Rationale

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

9. Rationale

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

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 22 - Threats and Assumptions to Security Objectives Mapping

	O.AUDIT_GEN	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.DETECT_DEVICES	O.I&A	O.IDANLZ	O.IDSCAN	O.IDSENS	O.MANAGE	O.RESTRICT_DEVICES	O.TIME_STAMP	O.TOE_ACCESS	OE.ARP	OE.COMM	OE.ENVIRON	OE.INSTALL	OE.MIRROR	OE.NETWORK	OE.NOEVILADMIN	OE.RESTRICT	OE.TIME
T.AUDIT_COMPROMISE		X																			
T.MASQUERADE					X							X		X						X	
T.UNAUTH_ACCESS						X	X	X		X			X				X				
T.UNAUTH_CONFIG						X	X			X			X								
T.UNAUTH_DEVICES				X		X	X	X		X			X				X				
T.UNIDENT_ACTIONS	X		X								X										X
A.ARP													X								
A.ENVIRON															X						
A.INSTALL																X					
A.NETWORK																		X			
A.NOEVILADMIN																			X		
P.MANAGE									X												

9.1.1 Rationale Showing Threats to Security Objectives

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

Table 23 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.AUDIT_COMPROMISE	**O.AUDIT_PROTECTION** mitigates this threat by requiring the TOE to control access to the audit trail.
T.MASQUERADE	**O.TOE_ACCESS** mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how authorized users can access the TOE, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. **O.I&A** is necessary so that each administrator is properly identified and appropriate privileges may be enforced for each. **OE.COMM** is necessary to protect the intra-TOE communication. **OE.RESTRICT** is necessary to limit TOE access from any managed devices to Compliance Servers only. All other traffic between systems on the Enterprise LAN or Internet and other systems connected to the management network or TOE components via their management interfaces is prevented.
T.UNAUTH_ACCESS	**O.RESTRICT_DEVICES** mitigates this threat by requiring the TOE to be able to restrict network access for devices that attempt unauthorized access. **O.IDSENS** supports the first objective by requiring the TOE to be able to detect devices as they become active on the network and monitor their access. **O.IDSCAN** supports the first objective by requiring the TOE to be able to learn attributes about devices so that appropriate access permissions may be determined. **O.IDANLZ** supports the first objective by requiring the TOE to analyze the information learned about devices to determine the access permissions appropriate for the device. **OE.ARP** supports the first objective by requiring all devices to properly process ARP messages. The TOE uses ARP messages to implement the network access restrictions. **OE.MIRROR** supports the first objective by requiring the network equipment in the operational environment to be able to provide a copy of the network traffic to the TOE so that the TOE is able to monitor the traffic.
T.UNAUTH_CONFIG	**O.RESTRICT_DEVICES** mitigates this threat by requiring the TOE to be able to restrict network access for devices that violate configuration policies. **O.IDSCAN** supports the first objective by requiring the TOE to be able to learn attributes about devices so that appropriate access permissions may be determined. **O.IDANLZ** supports the first objective by requiring the TOE to analyze the information learned about devices to determine the access permissions appropriate for the device. **OE.ARP** supports the first objective by requiring all devices to properly process ARP messages. The TOE uses ARP messages to implement the network access restrictions.

T.TYPE	Security Objectives Rationale
T.UNAUTH_DEVICES	**O.RESTRICT_DEVICES** mitigates this threat by requiring the TOE to be able to restrict network access for unauthorized devices. **O.IDSENS** supports the first objective by requiring the TOE to be able to detect devices as they become active on the network and monitor their access. **O.IDSCAN** supports the first objective by requiring the TOE to be able to learn attributes about devices so that appropriate access permissions may be determined. **O.IDANLZ** supports the first objective by requiring the TOE to analyze the information learned about devices to determine the access permissions appropriate for the device. **OE.ARP** supports the first objective by requiring all devices to properly process ARP messages. The TOE uses ARP messages to implement the network access restrictions. **OE.MIRROR** supports the first objective by requiring the network equipment in the operational environment to be able to provide a copy of the network traffic to the TOE so that the TOE is able to monitor the traffic.
T.UNIDENT_ACTIONS	**O.AUDIT_REVIEW** helps to mitigate this threat by providing the Administrator with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the TOE monitors the occurrences of these events. **O.AUDIT_GEN** helps to mitigate this threat by recording actions for later review. **O.TIME_STAMP** helps to mitigate this threat by ensuring that correct timestamps are available for audit records. **OE.TIME** helps to mitigate this threat by providing support to the TOE to keep track of time, such as tracking time in a Real Time Clock chip in hardware or via a Network Time Protocol server.

9.1.2 Rationale Showing Assumptions to Environment Security Objectives

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

Table 24 - Assumptions to Security Objectives Rationale

A.TYPE	Environment Security Objective Rationale
A.ARP	**OE.ARP** addresses this assumption by requiring managed devices to properly process ARP messages.
A.ENVIRON	**OE.ENVIRON** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.INSTALL	**OE.INSTALL** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.NETWORK	**OE.NETWORK** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.NOEVILADMIN	**OE.NOEVILADMIN** addresses this assumption by restating it as an objective for the Administrator to satisfy.

9.1.3 Rationale Showing OSPs to Security Objectives

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

Table 25 - OSPs to Security Objectives Rationale

P.TYPE	Security Objectives Rationale
P.MANAGE	**O.MANAGE** addresses this OSP by requiring the TOE to provide administrators with functions and facilities to effectively manage the TOE.

9.2 Security Requirements Rationale

9.2.1 Rationale for Security Functional Requirements of the TOE Objectives

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

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 26 - SFRs to Security Objectives Mapping

	O.AUDIT_GEN	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.DETECT_DEVICES	O.I&A	O.IDANLZ	O.IDSCAN	O.IDSENS	O.MANAGE	O.RESTRICT_DEVICES	O.TIME_STAMP	O.TOE_ACCESS
FAU_GEN.1	X											
FAU_GEN.2	X											
FAU_SAR.1			X									
FAU_SAR.2			X									
FAU_SAR.3			X									
FAU_STG.1		X										
FDP_IFC.1										X		
FDP_IFF.1										X		
FIA_ATD.1					X							
FIA_SOS.1									X			
FIA_UAU.2					X							
FIA_UAU.7					X							
FIA_UID.2					X							
FIA_USB.1					X							X
FMT_MOF.1									X			X
FMT_MTD.1									X			X
FMT_SMF.1									X			
FMT_SMR.1									X			X
FPT_STM.1											X	
IDS_SDC.1				X			X	X				
IDS_ANL.1						X						
IDS_RCT.1										X		
IDS_RDR.1			X									

	O.AUDIT_GEN	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.DETECT_DEVICES	O.I&A	O.IDANLZ	O.IDSCAN	O.IDSENS	O.MANAGE	O.RESTRICT_DEVICES	O.TIME_STAMP	O.TOE_ACCESS
IDS_STG.1		X										

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

Table 27 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.AUDIT_GEN	**FAU_GEN.1** addresses the objective by requiring the TOE to generate audit records for specified security-relevant events. **FAU_GEN.2** addresses the objective by requiring the audit records to include information about the administrator causing the event (when appropriate).
O.AUDIT_PROTECTION	**FAU_STG.1** addresses the objective by requiring the TOE to prevent unauthorized modification or deletion of audit records. **IDS_STG.1** addresses the objective by requiring the TOE to prevent unauthorized modification or deletion of system data analytical result records, and defining the behavior of the TOE when storage space is exhausted.
O.AUDIT_REVIEW	**FAU_SAR.1** addresses the objective by requiring the TOE to provide authorized users with the ability to read the audit records. **FAU_SAR.2** addresses the objective by requiring the TOE to prevent any access to the audit records by unauthorized users. **FAU_SAR.3** addresses the objective by requiring the TOE to provide facilities to assist authorized users in reviewing the audit records. **IDS_RDR.1** addresses the objective by requiring the TOE to provide authorized users with the ability to read the system data analytical result records.
O.DETECT_DEVICES	**IDS_SDC.1** addresses the objective by requiring the TOE to detect devices using the network.
O.I&A	**FIA_UID.2** and **FIA_UAU.2** address the objective by requiring the TOE to successfully identify and authenticate administrators before granting them access to any management functionality. **FIA_ATD.1** supports the objective by defining the attributes that are associated with each authorized account. **FIA_UAU.7** supports the objective by requiring password entry to be protected from disclosure. **FIA_USB.1** supports the objective by defining the attributes that are associated with a user session when I&A is successful and requiring that those attributes do not change during the session.
O.IDANLZ	**IDS_ANL.1** addresses the objective by requiring the TOE to analyze

Security Objective	SFR and Rationale
	the information learned about manage devices to determine the Access Zone membership and save result records.
O.IDSCAN	**IDS_SDC.1** addresses the objective by requiring the TOE to learn information about the configuration of managed devices to use in the analysis function.
O.IDSENS	**IDS_SDC.1** addresses the objective by requiring the TOE to monitor network traffic for managed devices to learn information about them and detect suspicious behavior.
O.MANAGE	**FMT_MOF.1** addresses the objective by defining the security functions and operations that are available to and authorized for each of the defined roles. **FMT_MTD.1** addresses the objective by defining the available and authorized TSF data access for each of the defined roles. **FMT_SMF.1** supports the objective by defining the security functions available to authorized administrators. **FMT_SMR.1** supports the objective by defining the set of roles supported by the TOE. **FIA_SOS.1** supports the objective by defining the rules for passwords specified for accounts by authorized administrators.
O.RESTRICT_DEVICES	**FDP_IFC.1** and **FDP_IFF.1** address the objective by requiring the TOE to be able to restrict the network access of managed devices per the service restrictions configured in Access Zones. **IDS_RCT.1** supports the objective by requiring the TOE to • generate alarms per the Access Zone configurations so that administrators are informed about managed devices that violate configured policies • enforce the service restrictions configured in Access Zones
O.TIME_STAMP	**FPT_STM.1** addresses the objective by requiring the TOE to provide reliable time stamps for audit records.
O.TOE_ACCESS	**FMT_MOF.1** addresses the objective by defining the security functions and operations that are authorized for each of the defined roles. **FMT_MTD.1** addresses the objective by defining the authorized TSF data access for each of the defined roles. **FMT_SMF.1** supports the objective by defining the security functions available to authorized administrators. **FMT_SMR.1** supports the objective by defining the set of roles supported by the TOE. **FIA_SOS.1** supports the objective by defining the rules for passwords specified for accounts by authorized administrators. **FIA_USB.1** supports the objective by defining the attributes that are associated with a user session when I&A is successful so that appropriate privileges may be enforced.

9.2.2 Security Assurance Requirements Rationale

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

The general level of assurance for the TOE is:

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

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented by ALC_FLR.1 from part 3 of the Common Criteria.

9.3 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

Table 28 - SFRs to TOE Security Functions Mapping

	Audit	I&A	Management	Network Access Control
FAU_GEN.1	X			
FAU_GEN.2	X			
FAU_SAR.1	X			
FAU_SAR.2	X			
FAU_SAR.3	X			
FAU_STG.1	X			
FDP_IFC.1				X
FDP_IFF.1				X
FIA_ATD.1		X		
FIA_SOS.1			X	
FIA_UAU.2		X		
FIA_UAU.7		X		
FIA_UID.2		X		
FIA_USB.1		X		
FMT_MOF.1			X	
FMT_MTD.1			X	
FMT_SMF.1			X	
FMT_SMR.1			X	
FPT_STM.1	X			
IDS_SDC.1				X
IDS_ANL.1				X
IDS_RCT.1				X
IDS_RDR.1				X
IDS_STG.1				X

Table 29 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1	**Audit** – The TOE generates audits of the events specified in FAU_GEN.1. The audit records are separated into one of three categories.
FAU_GEN.2	**Audit** – When appropriate, the audit records include the identity of the user that caused the record to be generated.
FAU_SAR.1	**Audit** – Audit and system data analytical result records may be reviewed by administrators, operators or observers for events within their domain or subordinate sub-domains.
FAU_SAR.2	**Audit** – Reporting users are not authorized to review any audit or system data analytical result records.
FAU_SAR.3	**Audit** – Authorized users may perform searches and sorts of the audit and system data analytical result information according to the event categories.
FAU_STG.1	**Audit** – The TOE does not provide any mechanism for users to modify or delete audit information.
FDP_IFC.1	**Network Access Control** – As configured by an administrator for specific access zones, the TOE may forward network traffic, discard network traffic, redirect HTTP sessions, or return a text message for HTTP sessions.
FDP_IFF.1	**Network Access Control** – As configured by an administrator for specific access zones, the TOE may forward network traffic, discard network traffic, redirect HTTP sessions, or return a text message for HTTP sessions.
FIA_ATD.1	**I&A** – The TOE a set of attributes for each defined account.
FIA_SOS.1	**Management** – When a password is configured for an account, the TOE enforces password policies.
FIA_UAU.2	**I&A** – The TOE requires each user to successfully authenticate before access is granted to any management functions.
FIA_UAU.7	**I&A** – When a password is entered, only asterisks are echoed back to the user.
FIA_UID.2	**I&A** - The TOE requires each user to successfully identify him/herself before access is granted to any management functions.
FIA_USB.1	**I&A** – Upon successful I&A, attributes are bound to the session for the duration of the session.
FMT_MOF.1	**Management** – The privileges for management functions for each role are clearly defined and enforced by the TOE.
FMT_MTD.1	**Management** - The access privileges to TSF data for each role are clearly defined and enforced by the TOE.
FMT_SMF.1	**Management** – The set of management functions are provided by the MOC interface and the web server.
FMT_SMR.1	**Management** – The set of roles for management access is clearly defined and enforced by the TOE.
FPT_STM.1	**Audit –** The TOE inserts a time stamp into each audit record generated.
IDS_SDC.1	**Network Access Control** – The TOE monitors network traffic to detect new devices, detect network behaviour that violates configured usage policies, and determine information about devices. The TOE also scans managed devices to learn more detailed information about them.
IDS_ANL.1	**Network Access Control** – The TOE analyzes information learned about devices to determine matching profiles, which are in turn used to determine Access Zone membership.
IDS_RCT.1	**Network Access Control** – As configured by an administrator for specific access zones or profiles, the TOE may generate an alarm and/or restrict network traffic.

SFR	SF and Rationale
IDS_RDR.1	**Network Access Control** – System data analytical result records may be reviewed by administrators, operators or observers for events within their domain or subordinate sub-domains.
IDS_STG.1	**Network Access Control** – The TOE does not provide any mechanism for users to modify or delete System data analytical result records.

9.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 8.