Alcatel-Lucent VPN Firewall
Version 9.1

EAL4
Security Target

Version: 1.0

April 30th, 2009

Alcatel-Lucent
26801 Agoura Rd
Calabasas, CA 91301

 FINAL

Table of Contents

Figures and Tables

1 Security Target Introduction

This introductory section presents *security target* (ST) identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

An ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., target of evaluation (TOE)). An ST principally defines:

- A set of assumptions about the security aspects of the environment, a list of threats which that product is intended to counter, and any known rules with which the product must comply.
- A set of security objectives and a set of security requirements to address that problem.

The ST for a TOE is a basis for agreement between developers, evaluators, and consumers on the security properties of the TOE and the scope of the evaluation. Because the audience for an ST may include not only evaluators but also developers and, "those responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE" this ST minimizes terms of art from the *Common Criteria for Information Technology Security Evaluations* (CC).

1.1 ST Reference

This section will provide information necessary to identify and control the Security Target and the TOE.

ST Title	Alcatel-Lucent VPN Firewall (ALVF) V9.1 Security Target
Version:	1.0
Publication Date:	April 30th, 2009
ST Author	Arca CCTL
Assurance Level:	Evaluation Assurance Level 4, augmented with ALC_FLR.1 (Basic flaw remediation)

1.2 TOE Reference

The TOE claiming conformance to this ST is identified as:

Alcatel-Lucent VPN Firewall (ALVF) v9.1 (Firmware Version 9.1.329) with one or more of the Firewall Appliance Models 50, 150, 700 AC, 700 DC, and/or 1200 (referred to as ALVF v9.1 throughout the remainder of the ST).

1.3 Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows several operations to be performed on functional requirements; assignment, iteration, refinement, and selection are defined in Section C.4 the CC version 3.1 Part 1.

a) The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].

b) The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

c) The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.

d) The iteration operation is used to repeat or reuse a CC requirement multiple times in the same document with different operations used to complete the requirement for each occurrence. Iterations are denoted by an increasing number inside parenthesis following the requirements short name. Example: FCS_COP.1 (1).

e) Plain *italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

1.4 Terminology

In the Common Criteria, many terms are defined in Section 4 of Part 1. The following terms are a subset of those definitions. In addition to these general definitions, this Security Target also provides the more specialized definitions. They are listed here to aid the user of the Security Target:

Advanced Encryption Standard (AES) – A method for encrypting information using a block cipher. AES is used worldwide and was announced as a federal standard on November 26, 2001as FIPS PUB 197, authorized for use on all unclassified data. Also known as Rijndael.

Authentication data – Information used to verify the claimed identity of a user.

Authorized Administrator – A role human users may be associated with in which to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE. An Authorized administrator also is an authorized operating system administrator.

Authorized external IT entity – Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Brick – See FA.

Data Encryption Standard (DES) – A method for encrypting information. DES was approved as a federal standard in November 1976, and published on 15 January 1977 as FIPS PUB 46, authorized for use on all unclassified data. It was

subsequently reaffirmed as the standard in 1983, 1988 (revised as FIPS-46-1), 1993 (FIPS-46-2), and again in 1998 (FIPS-46-3), the latter prescribing "Triple DES" (see below).

Encrypted Socket Connection – This term is used to refer to the encrypted socket connection between the SMS and other TOE components. If encrypted socket is mentioned without a reference to the TLS protocol then it means that the protocol developed by Alcatel-Lucent which is similar to Secure Socket Layer (SSL) v3.0 is used. It uses Triple DES (Data Encryption Standard) for encryption and keyed SHA-1 (Secure Hash Algorithm) for integrity and authentication. When SMS and FA are communicating, mutual-authentication takes place. All cryptographic operations are FIPS 140-2 compliant.

External IT entity – Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE**.**

FA – The abbreviation used to refer to the Alcatel-Lucent Firewall Appliance which is also known as the Brick.

Human user – Any person who interacts with the TOE.

Identity – A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

IT environment – The environment in which the TOE is operated which is also known as the TOE environment.

Partition – An independent set of VLANs, routing tables, zones, and policy rulesets.

Remote FA – An FA that is not directly connected to an SMS or to a secure management network containing an SMS.

Role – A predefined set of rules establishing the allowed interactions between a user and the TOE.

SCS – The SMS without the database. See SMS.

SCS Host - The machine (hardware and operating system) running the SMS software package with the SMS application installed and configured as SCS.

SHA-1 – This standard specifies a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data file. The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify.

SMS Application – The SMS software package which can be installed as an SMS or SCS.

SMS - Security Management Server is the software which handles the configuration of one or more firewall appliances (FA), management of security policies, and collection and analysis of audit data.

SMS Host - The machine (hardware and operating system) running the SMS software package with the SMS application installed as SMS.

SMS Navigator– The SMS utility that is used by administrators to access and administer the SMS.

SMS Remote Navigator– The SMS utility that is used by administrators to remotely access and administer the SMS.

SMS Remote Navigator Host – The remote machine running the SMS Remote Navigator.

TOE environment – See IT environment.

Transport Layer Security (TLS) – TLS is a cryptographic protocol which provides secure communications on networks. TLS provides endpoint authentication and communications privacy.

Triple DES (3DES) – One solution to overcome the short-key limitation is to run the Data Encryption Standard (DES) algorithm a multiple number of times with different keys.

User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

1.5 Acronyms

The following abbreviations are used in this Security Target:

AES	Advanced Encryption Standard
ALVF	Alcatel-Lucent VPN Firewall
CC	Common Criteria for Information Technology Security Evaluation
CLI	Command Line Interface
DB	Database
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
FA	Firewall Appliance (also known as the brick)
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol

IT	Information Technology
PP	Protection Profile
RAP	Remote Administration Application
RAS	Registration, Administration, and Status
RFC	Request for Comment
RTCP	Real-time transport control protocol
RTP	Real-time transport protocol
SCS	Security Compute Server
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMS	Security Management Server
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol
URI	Universal Resource Indicator
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network

1.6 TOE Overview

The ALVF is a bridging device with a traffic-filter firewall, application filters, VPN software, and management software.

The ALVF architecture consists of three distinct components:

- The Alcatel-Lucent VPN/Firewall Appliance (FA), which controls the flow of Internet Protocol (IP) traffic between network interfaces. The FA is also referred

to as the Brick. This component includes the hardware, operating system, and firewall application code for the Brick.

- The Security Management Server (SMS) software package, enabling administrators to manage the security of one or more Firewall Appliances (FA). The SMS software package, installed as an SMS, running on the host are jointly called the SMS (or SMS host) as a general term for both components together as a workstation. The SMS software package, installed as a compute server (SCS), running on the host are jointly called the SCS host. (An SCS provides most of the same functionality as the SMS but does not have its own DB. Deploying an SCS is optional.)
- The Security Management Server (SMS) Remote Navigator is a Graphical User Interface client, enabling administrators to manage the security of one or more Firewall Appliances by remotely accessing the primary SMS software package.

The Security Management Server software package runs on either Microsoft Windows or Sun Solaris hosts that are in the TOE Environment. An Administrator can log into the SMS software package remotely using the SMS Remote Navigator client, which is installed on a Windows host environment.

The Firewall Appliance (FA) controls the flow of IP packets based on security policy rules. These policy rules are created by the Administrator using the SMS Navigator, SMS CLI or SMS Remote Navigator. The SMS then compiles and pushes the ruleset to the FA when instructed to by the administrator.

The traffic-filter firewall controls the flow of Internet Protocol (IP) packets by matching information contained in IP and upper layer headers against a set of rules specified by the firewall's administrator. This header information includes source and destination host IP addresses, source and destination port numbers, and upper level protocol identifier (e.g., Transmission Control Protocol (TCP) or user datagram protocol (UDP)). Depending upon the rule and the results of the match, the firewall passes, drops, passes & encrypts or decrypts and passes the packet. In addition to protocol header information, traffic-filter firewalls use other information, such as the direction (incoming or outgoing) of the packet on a given firewall interface.

The administrator can choose to apply application filter rules to a traffic filter policy. The application filters screen the flow of network traffic at the application layer by monitoring and intercepting the traffic and then originating the corresponding information flows on behalf of the end points. The application layer traffic monitoring consists of validation, inspection and access control features. The application filters prevent direct application layer connections between two end points through the firewall. The following application filters are available in the evaluated configuration: FTP, HTTP, H.323 VoIP, H.323 RAS, DHCP Relay, TFTP, Oracle SQL*Net, Microsoft NetBIOS, SUN RPC, DNS, SMTP, and SIP services.

The VPN functionality provides the ability to require IPSec VPN tunneling for site-to-site and remote access information flows. VPN tunneling is implemented in the ALVF by configuring the rules to encrypt or decrypt packets. If pass & encrypt or decrypt & pass actions are used, the policy is considered a VPN policy. The VPN policies control the

flow of packets based upon the interface of arrival, interface of egress, source and destination addresses, and action to be taken. IPSec VPN tunneling encrypts and authenticates information flows to and from selected remote trusted IT products, protecting the information flow from disclosure or modification.

The FA passively listens on all its ports in promiscuous mode. The FA can operate in either bridge or router mode, as described below.

The SMS application can be installed as a SMS server or a Security Compute Server (SCS). The DB which contains configuration information, such as user accounts and FA configuration settings, is centrally located on the SMS (that is the SMS Relational database). In the evaluated configuration one to four SMSs and zero to five SCSs for each SMS are allowed. Each SCS is associated with an SMS server and acts as a collection point for Brick log traffic. Each FA can be homed[1] to one of the associated SCSs or to the SMS for logging purposes. An SCS provides the same functionality as an SMS, but does not have an SMS database. Deploying an SCS is optional.

The SMS software package supports the management of the other ALVF security features notably, auditing features (reports, alarms and logs), secure communications and administrator accounts.

The SMS software package includes the SMS Application, the SMS Navigator, the SMS Command Line Interface, Utilities and a database. (Note: Except for the database, these components are present on both an SMS host and an SCS host.) The administrative interface to the SMS software package is provided by the following interfaces:

1. SMS Navigator
2. SMS Command Line Interface
3. SMS Remote Navigator
4. Utilities, including database utilities, Log Viewer and Configuration Assistant

The TOE Environment is required to include the following components, which are not part of the TOE:

- The host machines and the operating systems for the SMS Remote Navigator and SMS software package are in the TOE environment. (A modem is not allowed on the SMS host in the evaluated configuration.)

  If using a Windows host:

  - A standard PC with a 400 MHz Pentium processor or higher. 512MB or more RAM, and 4GB or more hard drive, with the following software:
    - Any of the following operating systems:
      - Windows 2000 Professional and Service Pack 4 or higher
      - Windows 2000 Server and Service Pack 4 or higher

[1] The term “home” means to create an association between a brick and either an SMS or SCS for the purposes of providing management and log collection services.

        - Windows XP Professional and Service Pack 1 or higher
        - Windows Server 2003 Service Pack 2 or higher
      - Adobe Acrobat Reader version 4.05 or higher
      - Netscape Navigator 4.7 or higher or Internet Explorer 5.5 or higher
      - Java Run Time Environment version 1.5.0.10 (Included on TOE installation CD)

    If using a Solaris host:

    - A Sun Ultra Sparc 5 with a 330 MHz processor or higher. 512MB or more RAM, and 500 MB or more free disk space, with the following software:
      - Solaris 8, 9, or 10 with all security patches to date
      - Netscape Navigator 4.7 or higher
      - Adobe 4.05 or higher
      - Java Run Time Environment version 1.5.0.10 (Included in TOE installation CD)

- Monitor and keyboard locally connected to an FA must be available for installation and initial configuration. The monitor and keyboard are optional once the installation and configuration is completed.
- If ALVF is configured to use RADIUS authentication, the TOE is dependent upon a RADIUS authentication server in the TOE environment.
- If ALVF is configured to use VPN certificate authentication for VPN tunnel establishment, the TOE is dependent upon an external CA in the TOE environment.
- If the deployment includes more than one SMS or at least one SCS, a Network Time Protocol (NTP) server in the TOE environment is required to support time synchronization between the SMS and the SCS hosts so that the audit log data can be used to create a traceable history of events.
- If ALVF is configured to use Simple Network Management Protocol (SNMP) Trap actions to notify the administrator when an alarm is generated, the TOE is dependent upon a network management station running an SNMP server in the TOE environment.
- If ALVF is configured to use syslog actions to notify the administrator when an alarm is generated, the TOE is dependent upon a UNIX syslog server in the TOE environment.
- If the system is configured to send e-mail messages when an alarm is triggered, the TOE is dependent upon an SMTP server in the TOE environment.
- Interoperable IPSec Clients and associated host machines
    - Alcatel-Lucent IPSec Client Version 9.0

- Safenet client: High Assurance Remote Version 1.2.1 (Build 10) on Windows XP or Windows 2000 SP 4

1.7 TOE Description

This section provides a general overview of the TOE, in order to provide an understanding of the TOE's security features, the application context and to aid customers in determining whether this product meets their needs. The TOE requires FIPS mode to be enabled to provide secure cryptographic functionality.

1.7.1 Validated Features

The following features of the ALVF are validated in the Common Criteria evaluation (TSF enforcing):

a) Stateful Packet filtering: Every packet is mediated by the FA.

b) Logging: All logging is done in real-time from the FA to its management server (SCS or SMS). The SMS also logs administrative events and user authentication events.

c) Distributed Auditing/Logging: The TOE provides the option of deploying separate compute servers to collect the log data from the FAs.

d) Reporting: The SMS application has the ability to generate HTML-based reports and serve them via its own internal secure web server (HTTPS)

e) Remote administration: An SMS application can manage multiple FAs that are located remotely in a secure manner. An SMS Remote Navigator can manage an SMS application remotely in a secure manner.

f) VPN: The TOE provides confidentiality and integrity of an enterprise's messages by means of Virtual Private Networks (VPNs) between the enterprise's Firewall Appliances (LAN-LAN VPN) as well as Client-to-LAN VPN, using IP Security Protocol (IPSec) encryption and cryptographic checksums.

g) Routing mode: Routing mode enables the ALVF to function as both a router and a traffic-filter firewall. The ALVF is visible to both the internal and external networks in routing mode.

h) Bridge mode: In bridge mode, the ALVF does not have router capabilities. The ALVF functions as a bridge which transparently passes packets through the traffic-filter firewall. The two ALVF (inside and outside) interfaces are connected to one subnet, monitoring all traffic prior to allowing traffic to flow through the FA.

i) Administrator Authentication: The TOE provides the ability to authenticate administrative users using a local password or RADIUS authentication.

j) Client User Authentication: The TOE provides the ability to authenticate client (VPN) users using a local password, RADIUS or VPN certificate authentication.

k) Alarms: The SMS application provides the ability to create alarm triggers and associate them with appropriate actions to facilitate monitoring systems events.

Evaluated alarm actions include sending an e-mail message, syslog message, SNMP trap, and console message (displaying details on the Console Alarm window of the SMS Navigator or SMS Remote Navigator).

l) Denial of Service: The FA offers a variety of denial of service mechanisms tailored to both existing attacks as well as newly-emerging attacks not yet seen. These include SYN flood attack protection and intelligent cache management.

m) Remote Console Connection from Navigator: The brick CLI can be accessed by opening a console window from the SMS navigator.

n) Remote Console Connection from the Command Line: The brick CLI can be accessed from the local SMS host by running a command.

o) Local (Direct) Serial Port Connection: The brick CLI can be accessed by connecting a computer containing a terminal emulation program to a serial port on the back of the FA. This requires physical access to the brick.

p) Local Connection: The brick CLI can be accessed by connecting a monitor and keyboard to the appropriate ports on the back of the FA. This requires physical access to the brick.

q) SMS/SCS Redundancy: The ALVF can be configured with primary and secondary SMS and/or SCS servers that are all active at any given time.

r) The FA has the ability to perform inspection at the application layer of packet-based traffic passing through it using its Application Filter architecture. Support for the following application filter protocols are included in the evaluation:

- HTTP (HyperText Transfer Protocol) [URI pattern match blocking, root directory traversal blocking[2], HTTP command blocking, strict HTTP syntax checking]
- H.323 VoIP [dynamic channel & destination port opening,] H.323 is used to deliver multimedia (voice/video) services over Internet Protocol (IP) networks. It is used to provide Voice Over IP (VoIP) in telephone networks.
- FTP (File Transfer Protocol) [Command filtering, restrict dynamic ports, performs FTP protocol anomaly checking, block specific users, failed user login delays]
- SIP (Session Initiation Protocol): It is used to provide Voice Over IP (VoIP) in telephone networks.
- H.323 RAS (registration, administration, and status between an endpoint and a gatekeeper)
- DHCP Relay (allows DHCP messages to be translated and sent to a preconfigured known DHCP server, on an arbitrary IP network)
- TFTP (Trivial File Transfer Protocol) [dynamic channel opening, address translation]

[2] This prevents a URI from referencing a directory above or adjacent to the root directory provided by the server.

- Oracle SQL*Net [dynamic channel opening]
- Microsoft NetBIOS [address translation]
- SUN RPC (Remote Procedure Calls)
- DNS (Domain Name Service)
- SMTP (Simple Message Transfer Protocol)

1.7.2 Features Not Validated

This section identifies the features that the ALVF provides which are **not** in the scope of current Common Criteria evaluation. These features are not required to meet any of the security claims for the TOE.

The following features do not interfere with the claimed TOE security functionality (non-TSF enforcing) and do not need to be disabled in the evaluated configuration.

a) QoS: The TOE provides Quality of Services features, specifically Bandwidth management functionality.

The following features interfere with the TOE security functionality claims and must be disabled or not configured for use in the evaluated configuration.

a) Proxies: The SMS can be configured to redirect HTTP, SMTP, and FTP sessions to a proxy host running the Lucent Proxy Agent application (LPA). The LPA was discontinued in ALVF v9.1 and replaced with rules-based routing. Functionality supporting the LPA was not been removed from ALVF v9.1 in order to provide backwards compatibility.

b) FA Failover: The ALVF can be configured with a primary (active) FA and standby FA device. The standby FA device is inactive until the active FA device fails. This feature of the FA is not FIPS-certified (it is not permitted by the FIPS security policy) and as such will be excluded from the evaluated configuration.

c) Remote Dial-In Connection: The brick CLI can be accessed by connecting an external modem to the serial port on the FA and dialing into it from a remote computer. The evaluated configuration will not include or allow an external modem.

d) Alarms using the Direct Page Action: Sends a direct page alarm via a PSTN/modem-based connection. The evaluated configuration will not include or allow an external modem.

e) RSA SecurID authentication: The TOE provides the ability to authenticate administrative and client (VPN) users using RSA SecurID authentication. RSA SecurID authentication is not FIPS-certified (it is not permitted by the FIPS security policy) and as such will be excluded from the evaluated configuration.

f) Application User Authentication: The TOE provides the ability to authenticate users attempting to access an application or service through a brick using a local password, RADIUS, or RSA SecurID authentication. This feature is rarely used by customers and in some configurations it can create more security concerns than it solves. The evaluated configuration will not include the creation or use of

application users. Administrative guidance will instruct the administrators against their use.

g) TL1 Alarms: Allows automated telecommunication maintenance systems, like NMA to collect Brick alarm information from the SMS using Transaction Language 1 messages.

h) The FA has the ability to perform inspection at the application layer of packet-based traffic passing through it using its Application Filter architecture. The following application filters are used by communications suppliers and are not used by any government customers. As such, support for the following application filter protocols are not included in the evaluation:

- GTP (General Packet Radio Service (GPRS) Tunneling Protocol)
- ESP (Encapsulating Security Payload)

i) Make A Brick Boot Floppy or USB drive on a Remote Host: The TOE provides the ability to create a brick boot floppy or USB drive on a remote host. This feature can be used to outsource floppy creation. This capability is not allowed in the evaluated configuration because the cryptographic operations used are not FIPS-certified.

1.7.3 Application Context

The ALVF is a bridging device used to connect networks where information flows to and from the networks must be controlled. The type and degree of control is based on security policies created by the Administrator.

The ALVF which consists of one to four SMS hosts, one or more ALVF FAs, up to 5 optional SCS hosts for each SMS host, and, optionally, SMS Remote Navigator applications can be deployed in various ways as shown in the figure below.

One SMS host can support up to 5 SCS hosts and each SCS can collect log data from up to 1,000 FAs.

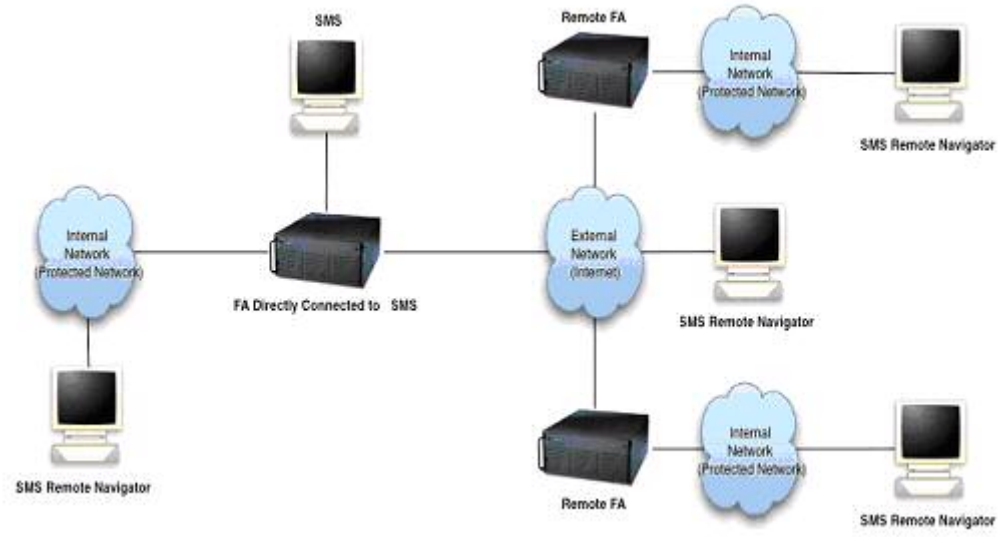

Figure 1: Possible Deployment Configuration

1.7.4 Physical Scope and Boundary

The Alcatel-Lucent VPN Firewall architecture consists of three physically distinct components:

- The Firewall Appliance, which controls the flow of IP packets between network interfaces; and
- The SMS software package, which enables administrators to manage the security of one or more FA's. This software package can be installed as an SMS or an SCS.
- The Security Management Server (SMS) Remote Navigator software, enabling administrators to manage the security of one or more FA's by remotely accessing SMS application.

The following conditions must be met for the TOE to be deployed in the evaluated configuration:

1. At least one Firewall Appliance (There can be more than one FA deployed in the evaluated configuration.)
2. At least one SMS whose host machine is directly connected to a FA (brick) or is connected via a secure management network. There can be at most four SMSs.
3. An SMS Remote Navigator host can be present on any Internal Network (a network protected by an FA) or on an External Network, such as the Internet. The use of SMS Remote Navigator hosts is optional in the evaluated configuration. All of the evaluated security functionality defined in this ST is met whether or not the Remote Navigator is deployed.

4. The deployment can optionally include up to 5 SCSs to collect audit data from an FA. The SCS can collect audit data from one or more Firewall Appliances (FA). In the evaluated configuration, the host machine is connected to the FA (brick) over a secure management network. All of the evaluated security functionality defined in this ST is met whether or not the deployment includes an SCS.
5. To utilize all of the evaluated security functionality of the TOE, the TOE environment would include commercially available RADIUS authentication servers, Certificate Authorities, and IPSec clients. (The approved list of IPSec clients is provided at the end of this section.)

Figure 2: TOE Configuration #1 represents the minimal set of the TOE components required to provide the full set of functionality described in this ST, plus a SMS Remote Navigator. Figure 3: TOE Configuration #2 is a superset of TOE Configuration #1 and shows how additional FA's and SMS Remote Navigators can be added to the deployment. Figure 4: TOE Configuration #3 is a superset of TOE Configuration #2 and shows how SCSs can be added to the deployment.

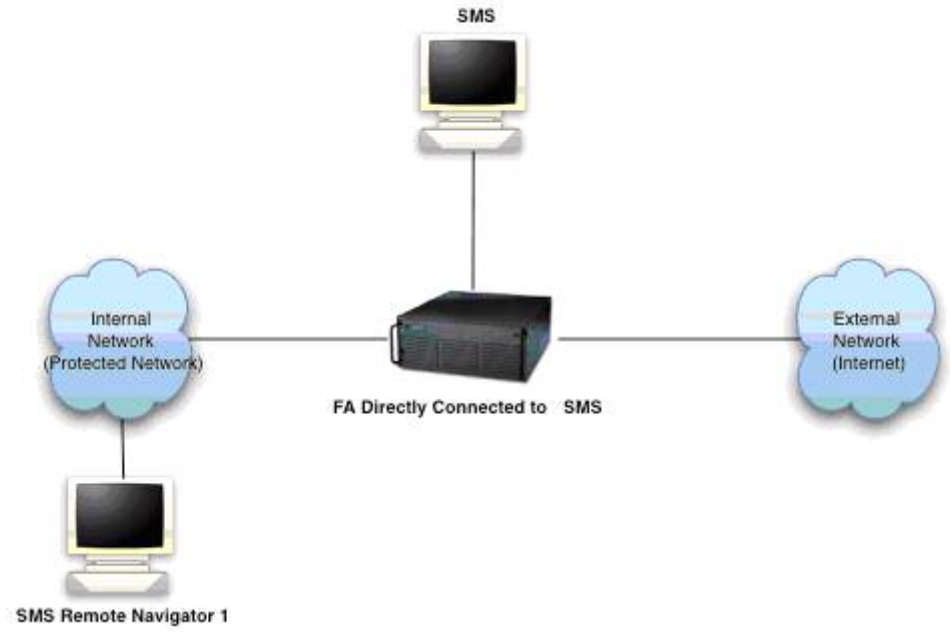

Figure 2: TOE Configuration[3] #1

There are two secure communication paths that are established through the connections depicted in Figure 2.

- The SMS application negotiates and establishes an encrypted socket connection from the SMS application to the FA.

[3] It is recommended to secure the host running LSMS Remote Navigator. Further guidance on how to secure the LSMS Remote Navigator is provided in the Supplemental CC Guidance, Appendix A

- The SMS application negotiates and establishes an encrypted socket connection from the SMS application to the SMS Remote Navigator. The initial request to establish an encrypted socket connection is made by the SMS Remote Navigator.

Figure 3: TOE Configuration #2 depicts an evaluated configuration containing two Firewall Appliances, two SMS Remote Navigators, and one SMS software package.

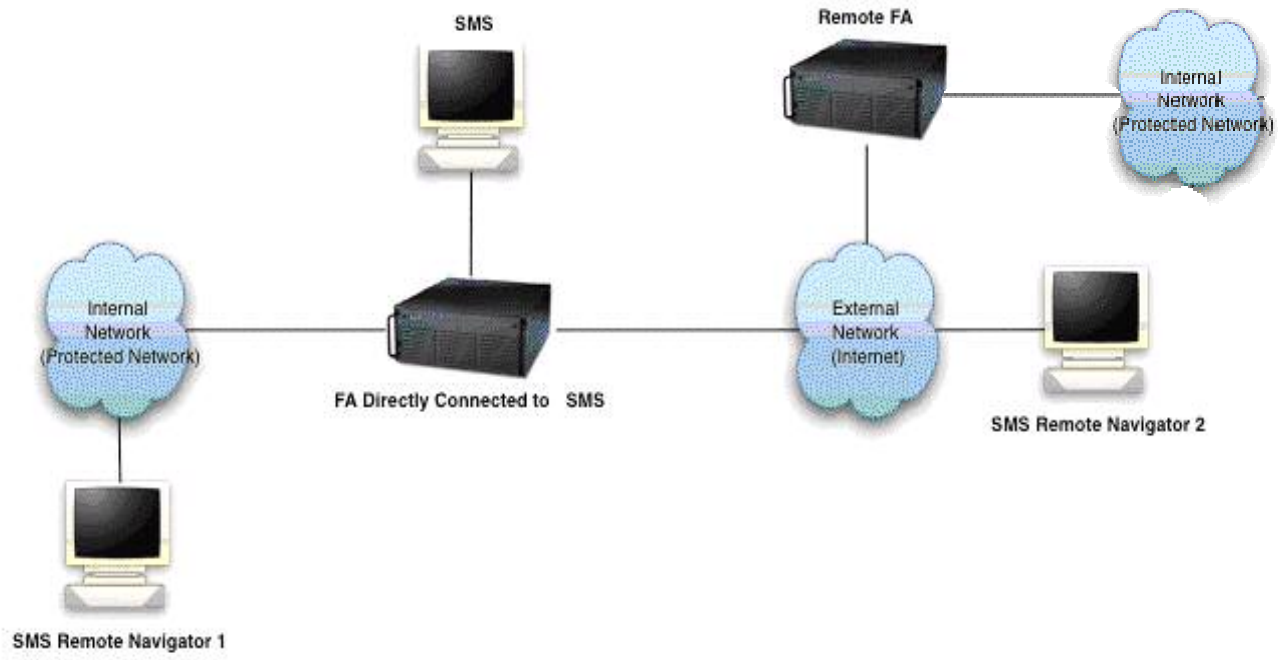

Figure 3: TOE Configuration #2

There are two secure communication paths that are established through the connections depicted in Figure 3.

- The SMS application negotiates and establishes an encrypted socket connection from the SMS application to any FA whether it is locally connected or remotely located.
- The SMS application negotiates and establishes a secure communication from the SMS to any SMS Remote Navigator, whether is it on an internal or external network. The initial request to establish an encrypted socket connection is made by the SMS Remote Navigator.

Figure 4: TOE Configuration #3 depicts an evaluated configuration containing five FAs, four SMS Remote Navigators, one SMS host and one SCS host connected to an FA via a secure management network. The three FAs connected to the Secure Management Network depicted in Figure 4 are not configured for FA failover.

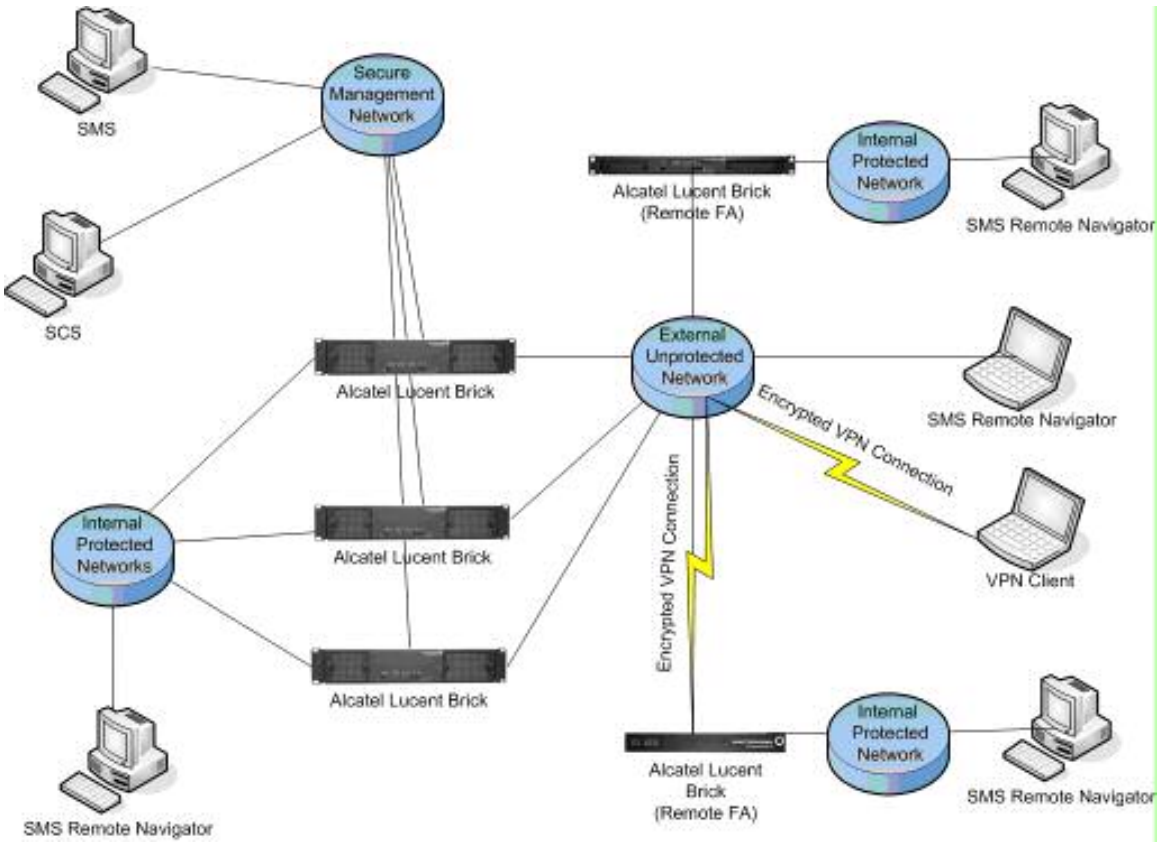

Figure 4: TOE Configuration #3

There are five secure communication paths that are established through the connections depicted in Figure 4.

- The SMS negotiates and establishes an encrypted socket connection from the SMS to any FA whether it is locally connected or remotely located.
- The SMS negotiates and establishes a secure communication from the SMS to any SMS Remote Navigator, whether is it on an internal or external network. The initial request to establish an encrypted socket connection is made by the SMS Remote Navigator.
- The SCS negotiates and establishes an encrypted socket connection from the SCS to any FA whether it is locally connected or remotely located.
- The SCS negotiates and establishes an encrypted socket connection from the SCS to the SMS.
- The Encrypted VPN connections are initiated by the IPSec endpoints and allowed by the security policy rules enforced by the FA.

Each model of the firewall appliance has multiple network interfaces as described in Section 2.3: Physical Scope and Boundary, Table 1: Firewall Appliance Hardware. When VLANs are not used, three network interfaces are used in the evaluated configurations; one for connecting to the External Network, one for connecting to the Internal Network,

and one for connecting directly to the SMS host or to a secure management network. The FA is used to control information flow between the internal and external networks. For the TOE configuration at least one FA must be directly connected to the SMS host or to a secure management network. Additional FAs can be installed anywhere geographically but must be on an interconnected network with an SMS.

The SMS Remote Navigator host could be located on either an internal network (protected network) or an external interconnected network (i.e. the internet).

The scope of the evaluated configuration allows an administrator to administer multiple FAs from a single SMS application. Additionally an administrator can connect to the SMS application to perform FA administration from an SMS Remote Navigator.

The communications between the SMS application and the FA, and the communications between the SMS Remote Navigator and SMS application are all through an encrypted socket connection, which provides confidentiality and integrity. When deployed in a redundant configuration, communication between redundant SMSs and between redundant SCSs are conducted through an encrypted socket connection. The cryptographic software modules on the SMS Remote Navigator, SMS application and the FA that provide secure communications for the TOE are all FIPS 140-2 compliant cryptographic modules).

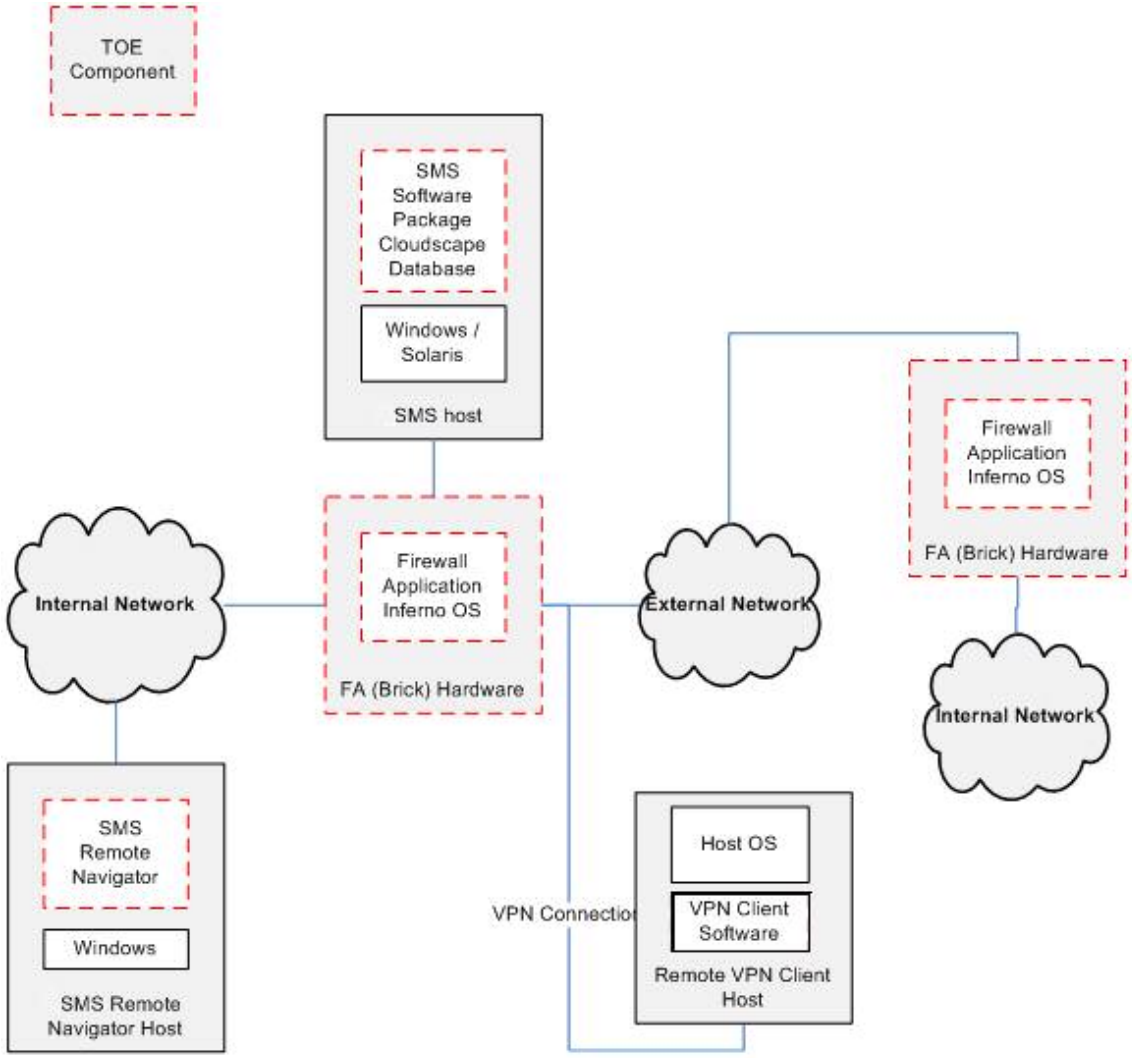

Figure 5: Physical TOE Boundary and Environment

The physical scope of the TOE includes the components circled in red dashed lines in Figure 5. Note that since the SMS and SCS share the same SMS software package, an SCS host would be represented the same as the SMS host is represented in Figure 5, except the SCS does not include the Cloudscape DB.

The physical TOE components include:

- The SMS software packages installed as an SMS on one to four SMS hosts.
- SMS Relational Database: Cloudscape version 3.6 (this DB is included on the installation CD)
- One to multiple Firewall Appliances along with the FA operating system and the firewall application software that runs on the FA hardware. The internal (protected) network must be logically (using VLANs) and/or physically (using separate NICs) separated from the external network. If the FA is attached directly to the SMS or to a secure management network an additional separate physical NIC is required for this connection.

- Zero to multiple SMS Remote Navigators.
- The SMS software package installed as an SCS on none to five SCS hosts.

The simplest TOE configuration consists of one SMS directly connected to an FA. The SMS can manage one to many FAs and can support remote management from one to many SMS Remote Navigators. Management of a single FA is the same as managing multiple FAs. All the same security features, including secure communication, exist for each additional FA installed in the configuration. Further, the SMS handles one SMS Remote Navigator connection in the same fashion as multiple SMS Remote Navigators connecting to perform management. All of the same security features, including secure communication, exist for each additional SMS Remote Navigator installed in the configuration. Therefore, installing one SMS and any number of Bricks and SMS Remote Navigators will still allow the deployment to remain EAL 4 compliant because the TOE components will continue to operate in the same fashion and will provide the same set of security functionality. The additional SMS Remote Navigators will operate with the SMS Software Package in the same fashion as the single SMS Remote Navigator and they will provide the same security functionality and services as the single SMS Remote Navigator. Likewise, the additional Bricks will operate with the SMS Software Package and provide the same security functionality as the single Brick in TOE Configuration #1.

Deploying the TOE with compute servers provides a more scalable solution. The SCSs act as collection points for Brick log traffic, freeing resources on the SMS and extending the number of bricks and amount of log traffic that can be processed. An SCS provides the same functionality as an SMS except it does not have its own database. The database is located on the SMS. The SMS and SCS communicate using a protected communication channel. The SMS and SCS together provide all the same security features as provided by a TOE configuration without any SCSs. Therefore, installing one SMS, at least one brick and any number of SCSs will still allow the deployment to remain EAL 4 compliant because the TOE components continue to operate in the same fashion.

The TOE provides redundancy features for the SMS and SCS. For SMS redundancy, one SMS is installed and designated the Primary SMS and up to three SMSs are installed and designated as Secondary SMSs. All SMSs are active simultaneously. Each SMS has its own DB and the data is replicated between the databases so that they have the same data. One to five SCSs can be linked to each SMS server to act as a log collection point for the FA log data in order to free SMS computing resources for other activities. The order in which the SMSs and/or SCSs take over management and log collection of each FA is defined by the Home SMS/SCS Priority Table for the FA.

The firewall application and the Inferno Operating System can be run on several hardware models, which are called Firewall Appliances (FA) or Bricks or VPN Firewall Brick Models. The different Brick models provide different scalable solutions. They are all FIPS compliant and are all included in this evaluation:

- VPN Firewall Brick Model 50
- VPN Firewall Brick Model 150
- VPN Firewall Brick Model 700

- VPN Firewall Brick Model 1200

The VPN Firewall Brick models listed above differ only in throughput and network interface capacity rather than functionality. They all run the same version of the firewall application and the Inferno operating system as pushed down by the SMS application.

The following table provides the detailed specifications of the VPN Firewall Brick Models or FA or Brick hardware models.

VPN Firewall Brick Model Number	Processor	Memory	Ethernet ports	Copper/Fiber Gigabit interfaces	Capacity Clear text	Encryption Accelerator
50 (FIPS Compliant)	466MHz Geode	64 MB RAM	3 10/100 Base TX Ethernet RJ45	N/A	195 Mbps	1 built-in supporting 3DES and AES
150 (FIPS Compliant)	600 MHz Celeron	128 MB RAM	4 10/100 Base TX Ethernet RJ45	N/A	334 Mbps	1 built-in supporting 3DES and AES
700 Basic, VPN, and DC versions (FIPS Compliant)	2.8 GHz Pentium 4	512 MB RAM	8 10/100/1000 Base TX Ethernet RJ45	N/A	1.7 Gbps	Basic: software supporting 3DES and AES VPN and DC: 1 supporting 3DES and AES
1200 Basic (AC version only) (FIPS Compliant)	3.2 Ghz Pentium 4	1GB RAM	8 10/100/1000 Base TX Ethernet RJ45	2	3.0 Gbps	1 supporting 3DES and AES
1200 HS Brick (AC and DC version only) (FIPS Compliant)	3.6 Ghz Pentium 4	2GB RAM	14 10/100/1000 Base TX Ethernet RJ45	6 SFP ports	4.75 Gbps	1 supporting 3DES and AES

Table 1: Firewall Appliance Hardware

The FAs vary in hardware configurations as shown in the above table (i.e. memory size, number of Ethernet ports). The software image that implements the security enforcing functionality is the same on all FAs. Hence all the FA models are considered identical from a security functionality viewpoint. They are identical because one can take any software binary image (tvpc or tvpc.zip file) from any FA and run it on any other FA. This can be verified simply by doing a “make/package floppy” operation for each FA and then comparing the image files on the floppy or USB for each FA.

The same software binary image ("tvpc.zip") runs on all modules, so all features are available on all module platforms. The binary images are identical across all platforms, regardless of the FA’s model number or configuration setup.

However, since the OS image provides a superset of all drivers that can interface with the module, each module only needs to use a subset of the drivers installed. The encryption accelerator driver is selected by the FA. For the Model 700 and 1200, the FA selects drivers and uses the SMS to determine the number of ports. When the administrator creates the bootable OS image from the Security Management Server for the FA Model 50 and 150, one of the selectable options (via a drop down box) in the SMS application is to reference the specific driver configurations of the FA model. This selection of the FA model (50 or 150) specifies which subset of drivers (except for the encryption accelerator) is needed and places this configuration data within a separate configuration file ("inferno.ini"), which is created alongside the OS image. The purpose of the configuration file is to distinguish which drivers are applicable to the module it is installed on, while the binary image file ("tvpc.zip") serves as the same identical executable applicable to all FA models.

1.7.4.1 Guidance

There are no non-administrative users for the TOE, only different levels of administrators. Therefore, there is no non-administrative user guidance provided with the product.

The TOE includes the following administrative guidance:

- *Alcatel-Lucent Security Management Server (SMS), Release 9.1, Installation Guide, Issue 3, December 2007*
- *Alcatel-Lucent Security Management Server (SMS), Release 9.1, Administration Guide, Issue 3, December 2007*
- *Alcatel-Lucent VPN Firewall Release 9.1,Supplemental CC Guidance, version 0.7, March 12, 2009*
- *Alcatel-Lucent Security Management Server (SMS), Release 9.1, Reports, Alarms, and Logs Guide, Issue 6, May 2008*
- *Alcatel-Lucent Security Management Server (SMS), Release 9.1, Tools and Troubleshooting Guide Issue 6, May 2008*
- *Alcatel-Lucent Security Management Server (SMS), Release 9.1, Policy Guide Issue 8, January 2008*

1.7.5 Logical Scope and Boundary

The security functional requirements implemented by the ALVF are grouped under the following classes or families:

The TSF data consists of the following:

- Information flow policy rules
- Audit trail
- User account attributes as defined in FIA_ATD.1
- Configuration settings, including SMS/SCS definitions
- Report templates
- Cryptographic keys

The user data is the network datagrams (network traffic) that is attempting to flow through the TOE.

The security attributes consist of the following:

- Information flow policy rules
- User account attributes as defined in FIA_ATD.1
- Cryptographic keys
- The security attributes listed in FDP_IFF.1

1.7.5.1 User Data Protection

The firewall software that runs on the FA is based on the Inferno™ operating system, a Bell Labs-developed operating system. The firewall code is imbedded within the Inferno™ operating system kernel. The operating system itself has no user accounts. The entire firewall software resident on the FA fits on a single 3.5-inch floppy diskette. The FA can boot from a floppy or USB drive. The FA communicates with its Security Management Server using IP.

The FA must be assigned a logical IP address. To preserve network invisibility, the FA protecting the SMS host must be configured to communicate only with the SMS's over a private network address, where the administrative policies only allow administrative traffic while dropping all other communication attempts.

All communications between each FA and the SMS application are encrypted and authenticated using an encrypted socket connection.

The FA (local or remote) must be visible to the Security Management Server's IP address on at least one physical interface, but must be invisible at the network layer to network elements on the other physical interface ports. The firewall software in the FA consists of modules and applications. The FA boot diskette contains the FA operating system, firewall application (the operating system and firewall application are a single executable), FA assigned IP address and subnet address for each FA interface, Certificate

Authority key, and the IP address of the SMS host responsible for managing the FA. The default deny firewall rules are hard-coded in the firewall application.

The FA initially boots from a floppy diskette or USB device that is created by the SMS. Boot images after the initial boot are loaded from FLASH disk. The FA operating system can be pushed to each FA from the SMS when the FA is capable of communicating with the SMS, without physically interacting with the device. However, if the FA is being setup and installed for the first time in a remote location from the SMS, a boot floppy/USB drive will need to be delivered to that location and the FA will needed to be administered accordingly.

The FA controls the flow of incoming and outgoing IP packets. The security policy rulesets are created by authorized administrators using the SMS Navigator or SMS Remote Navigator. The SMS Navigator is the GUI component of the SMS software package. The Security Management Server (SMS) is the means by which administrators manage the security of one or more FAs. The policy rulesets are then pushed from the SMS application to the operating system (Inferno) on the FA. The security policy which controls the information flow through the FA is embedded within the Inferno™ operating system kernel. The FA extracts information from the IP packet header and applies rules from a security policy. The information within an IP packet that is used to make access control decisions includes source and destination address, TCP or UDP port number, and packet type. Unless an authorized administrator explicitly configured the FA to accept requests based on specific security attributes, the ALVF will successfully reject any and all requests.

The FA provides application filters that screen the flow of network traffic at the application layer by monitoring and intercepting the traffic and then originating the corresponding information flows on behalf of the end points. The application layer traffic monitoring consists of validation, inspection and access control features. The application filters prevent direct application layer connections between two end points through the firewall. The TOE provides application filters for the following services: FTP, HTTP, H.323 VoIP, H323 RAS, DHCP relay, TFTP, Oracle SQL*Net, Microsoft NetBIOS, SUN RPC, DNS, SMTP, and SIP.

FTP is a protocol for exchanging files over a network between an FTP server and an FTP client. HTTP defines a method for transmitting messages between a web server and client browser. The H.323 protocol suite consists of several session and application layer protocols for exchanging multimedia traffic across an IP network, typically using a combination of TCP and UDP. The H.323 Registration, Administration, and Status (RAS) channel generally uses a fixed port and is processed by the H.323 RAS filter. The H.323 RAS filter monitors RAS messages and bandwidth changes between two H.323 entities. The H.323 VoIP filter processes the H.245 messages sent over TCP and the RTP, and RTCP messages sent over UDP. The DHCP relay filter allows DHCP client requests to be forwarded by the FA to a DHCP server on another network. DHCP is a set of rules to allow devices to request and obtain an IP address from a server which has a list of addresses available for assignment. The TFTP filter allows TFTP traffic resulting from READ and WRITE commands. The Oracle SQL*Net filter processes SQL*NET messages containing the REDIRECT command. The Microsoft NetBIOS filter is always enabled for UDP and performs network address translation. The SUN RPC filter inspects

RPC streams for message format violations, allowed program, procedure, and version triplets, and port mapper responses needing a separate dynamic port. The DNS filter is designed to avoid a DNS spoof attack by ensuring that an outside DNS server will not provide information on an inside host. The SMTP filter prevents mail relay attacks, MIME attacks, buffer overflow attacks, address spoofing attacks, and covert channel attacks. SIP is a signaling protocol used in applications such as VoIP and instant messaging services. The TFTP, Oracle SQL*Net, and Microsoft NetBIOS application filters do not have any configuration options.

The VPN software provides for secure channel establishment with remote external trusted IT entities (i.e., IPSec clients). The security rules define which packets will be encrypted/decrypted. The TOE is capable of establishing IPSec VPN tunnels (encrypted network paths) for both LAN-LAN and client tunnels. The devices or hosts at either end of the VPN are called tunnel endpoints. For both types of VPN tunnels, one of the tunnel endpoints is a port on the FA. In a LAN-LAN tunnel, the other tunnel endpoints are network devices or a non-Alcatel-Lucent IPSec client application. In a client tunnel, the other tunnel endpoint is represented by the IP address of the host running the approved IPSec client. Client tunnels perform user authentication whereas LAN-LAN tunnels authenticate using only the preshared key or certificate.

The FA has a rule-based SYN flood protection feature that allows the administrator to define the number of half open sessions that will be allowed and determine how long sessions can remain half open after the threshold has been reached. The FA can also be configured to automatically purge sessions to clear cache memory if cache usage approaches a pre-defined threshold. The FA performs fragment reassembly, controlling the number of outstanding fragments.

For use in service provider environments, the FA can be configured with "partitions," which are independent sets of VLANs, routing tables, zones, and policy rulesets. Partitions ensure isolation between different logical FA devices within a single FA appliance such that packets traversing the FA within one partition cannot cross boundaries into another partition even when those two partitions on one FA use overlapping or conflicting IP addresses.

The primary component of the ALVF that implement the user data protection is the Firewall Appliance.

1.7.5.2 Security Audit

The FA detects the occurrence of selected events, gathers information concerning them, and sends that information to the SMS or SCS host. The SMS software package collects this information; time stamps it and stores it in log files on the SMS/SCS host operating system in the TOE Environment. The SMS application also detects the occurrence of selected events (e.g., security administrator actions performed on the SMS/SCS), gathers information concerning them, and records them.

Audit review is accomplished by SMS/SCS reports generated by a web server and log viewer which are components of the SMS software package. The primary components of the ALVF that implement the Security Audit are the SMS software package (SMS and SCS) and the FA.

If the TOE is deployed using SCSs, a Network Time Protocol (NTP) server is required to support time synchronization between the SMS and the SCS hosts so that the audit log data can be used to create a traceable history of events. The NTP server is in the TOE environment. The NTP clients on the SMS and SCS hosts must use a synchronized time source, which could be implemented using the same NTP server or two different NTP servers slaved to the same master NTP source.

The TOE provides the authorized administrator with the ability to configure the log file maximum size and the amount of disk space to allocate for all logs together in a directory.

The audit storage management architecture ensures that if audit data storage exhaustion takes place, the brick stops passing traffic. An authorized administrator configures the SMS in such a way not to lose any audit data and halt the FA if any of the log directories reach the maximum allocated size.

The SMS provides the ability to create alarm triggers and associate them with appropriate actions to facilitate monitoring systems events. Evaluated alarm actions include sending an e-mail message, syslog message, SNMP trap, and console message. Alarms are configured on a per-Administrator basis and are not shared among Administrators.

1.7.5.3 Identification and Authentication (I&A)

The SMS software and the Brick CLI perform identification and authentication in the TOE.

The SMS software provides the tools to manage the security policies of the Groups that are applied to the FA. The software runs at the application layer using Java™ on the resident operating system. The SMS application implements and enforces an administrator privilege model.

The TOE allows only a small number of services to be accessed by an unauthenticated entity before the entity is identified and authenticated as an SMS administrative user. These services include the DB Utilities, Start Services, Stop Services, Restart Services, SMS Status, Configuration Assistant, Schedule Editor, New Feature Setup, and unauthenticated information flows. (Note: Users must successfully be identified and authenticated to the underlying SMS host OS in order to use these services, except for unauthenticated information flows.)

When used from the SCS, the processing of requests is performed on the SCS using remote database operations to post/retrieve data to/from the database. The administrator on the SMS/SCS is required to authenticate to modify the data in the database.

When deployed in an SMS redundant configuration, the secondary SMSs use the same user account information as configured on the primary SMS. The user account information is stored in the DB and the primary database built on the Primary SMS is replicated onto the Secondary SMSs. Refer to Section 1.7.5.7 for more information on redundancy.

Two categories of administrators can be created on the SMS/SCS: SMS administrators and Group administrators. There can be multiple SMS Administrators and Group

Administrators. A group is a collection of objects, FA's, Users, and /or policies that are managed as a whole.

An SMS Administrator can edit anything in any Group. The Group administrator can only edit those items for which they have been granted the right by an SMS Administrator.

Every SMS or Group administrator must have a valid user account stored in the SMS database. This account information includes the User ID, Password and real name of the SMS or Group administrator

Administrators have to successfully log into the operating system before an SMS/SCS login. The SMS application requires administrators to identify and authenticate themselves before they can perform any other SMS/SCS actions. The primary components of the ALVF that implement I&A are the SMS software package, the SMS Remote Navigator, and the brick CLI.

The SMS application supports authentication of administrators, VPN users[4], and application users[5] by means of local user id and password, and RADIUS authentication. VPN users can also be authenticated via VPN certificates (IKE v2).

Use of VPN certificates requires an external CA in the environment to generate and manage the VPN certificates. The TOE performs certification revocation checks using the certificate revocation list imported to the TOE from the external CA. To authenticate the user, the SMS application verifies the validity of the certificate provided by the user. The external CA is in the TOE environment.

Use of RADIUS authentication requires a RADIUS authentication server in the environment to verify the identification and authentication data provided by the user. The RADIUS authentication server is in the TOE environment.

The SMS must be configured to require a strong password that is designed to comply with the Sarbanes-Oxley (SOX) requirements. The strong password option is enabled by default. When enabled, the strong password requirements apply to new or changed local passwords for:

- Local passwords for user accounts
- Local passwords for administrator accounts, including the master user created during installation
- User login passwords for the Brick device console

The SMS also monitors the unsuccessful authentication attempts and locks out the administrator after an administrator-defined number of consecutive unsuccessful authentication attempts.

The Brick CLI requires users to authenticate themselves using the brick CLI password when the brick CLI is accessed via the Local Connection or Local Serial Port connection.

[4] The term VPN users refers to individuals requesting a client tunnel via an approved IPSec client.

[5] The use of application users is not allowed in the evaluated configuration.

The brick CLI does not require users to identify themselves when using these access methods, however physical access to the device is required. The brick CLI password is stored on the brick. When the brick CLI is accessed from either of the Remote Console Connections, the user is required to login to the SMS.

The Brick CLI administrator is the role required to use the brick CLI from one of the local Connection methods. Any user with the Brick CLI password and physical access to the TOE is a Brick CLI administrator.

1.7.5.4 Security Management

The SMS and Brick CLI provide all ALVF security management capabilities. Administrators manage the security policy rules enforced by the FA and configuration parameters and administrator accounts using the SMS. All edits to the policy and user account information of the SMS are stored in the SMS relational database (DB). Since the SMS is on a private network protected by the FA and installation guidance requires security policy rulesets preventing access to the DB from the public network, the DB can only be accessed by the TOE. In addition, the OS hosting the SMS protects the DB files from unauthorized access.

The primary components of the TOE that implement the Security Management are the DB, SMS software package, the SMS Remote Navigator. A brick can also be accessed or configured from a compute server or brick console. The Brick CLI provides commands for query and troubleshooting purposes.

When the management functions provided in the SMS software package are used from the SCS, the processing of requests is performed on the SCS using remote database operations to post/retrieve data to/from the database. The DB which contains configuration information, such as user accounts and FA configuration settings, is centrally located on the SMS (that is the SMS Relational database). All SMS management functions, except the database management functions, are available on SCS. Note: These commands/utilities may still have a name with SMS even though it is on an SCS.

The TOE provides the following management functions which can be performed prior to authentication to SMS: DB Utilities, Start Services, Stop Services, Restart Services, LSMS Status, Configuration Assistant, Schedule Editor, and New Feature Setup. DB utilities provide an interface to request services from the DB, such as backup, restore, and configuration changes. Start Services starts all services that support the SMS application. Stop Services stops all services that support the SMS application. Restart Services stops all the services that support the SMS application and starts them again. LSMS Status is used only to view the status of different FA services and running SMS services that constitutes the TOE. Configuration Assistant sets values to the following security relevant parameters that are included in the TOE: alarms, log files, limit on concurrent reports generation, Web Server ports and detailed policy auditing. Schedule Editor modifies the actions of the Task Scheduler by stopping and restarting services. New Feature Setup expands the number of FAs or IPSec users that can be managed via the SMS.

1.7.5.5 Protection of TOE Security Functions

The security functions which implement the ALVF access control policy are physically separated from the unauthenticated external IT entities which send and receive IP packets through the FA; and the design of these functions is such that they cannot be bypassed by those external IT entities.

The TOE protects most of its management functions by isolating them through identification and authentication of administrative users. The utilities that do not require the TOE to perform I&A must be executed locally on the SMS/SCS. These utilities are protected by operational environment which authenticate the authorized administrators and ensures that the servers are located in a controlled access facility.

The SMSs/SCSs and SMS Remote Navigators rely upon their underlying operating system to operate correctly and benignly to protect them from manipulation by unauthorized external entities. In addition, the underlying operating system for these servers requires that all users identify and authenticate themselves.

Secure communications between the distributed portions of the TOE provides additional protection for the secure operation of the TOE. The SMS Remote Navigator host can be located on any interconnected network and must be granted access to the SMS/SCS via the FA protecting the SMS/SCS. The only communications that the SMS/SCS receives are from remote trusted IT entities, such as the FA that it monitors, the SMS Remote Navigator hosts, the RADIUS server, CA, SMTP server, and the NTP server.

The FA, SMS and SCS hosts run only processes that are needed for their proper execution and do not run any other user processes.

The primary components of the ALVF that implement Protection of TOE Security Functions are the SMS software package and the FA.

1.7.5.6 Secure Communications

The communications between the SMS application and the FA, between the SMS and SCS, between primary and secondary SMSs, and between SMS Remote Navigator and SMS are all through an encrypted socket connection which provides confidentiality and integrity. Communications between the SMS and SCS hosts consist of database requests and status information. Policy and configuration information is sent from the SMS/SCS to the FA.

The SMS application also has a simple Web server (part of the Remote Administration Application (RAP) subsystem) which is used to deliver reports and help files. This Web server is configured for HTTPS for the purposes of this TOE. Once an administrator is logged in and connected to the RAP, the web server is used to display reports and online documentation (including help files). FIPS 140-2 approved TLS mode is required since reports may contain sensitive information.

The primary components of the TOE that implement this are the SMS Remote Navigator, the SMS software package, and the FA.

1.7.5.7 Redundancy

The TOE provides redundancy features for the SMS and SCS. Note: An SCS is dependent upon its associated SMS for database access.

For SMS redundancy, one SMS is installed and designated the Primary SMS and up to three SMSs are installed and designated as Secondary SMSs. All SMSs are active simultaneously. The primary database is built on the Primary SMS and replicated onto the Secondary SMS. When connectivity is interrupted between redundant SMSs, each SMS keeps track of interim changes made in its own version of the database. Then when connectivity is restored, these interim changes are reconciled in the common dataset.

One to five SCSs can be linked to an SMS server to act as a log collection point for the FA log data in order to free SMS computing resources for other activities. An FA can be homed to an SCS to serve as the log collection point for that FA.

The order in which the SMSs and/or SCSs take over management of each FA is defined by the Home SMS/SCS Priority Table for the FA. An FA always attempts to home to its Priority 1 entry after rebooting or after SMS/SCS services have been restarted. Up to five SMSs or SCSs can be entered in the priority list for each FA. If the FA cannot connect to the Priority 1 entry, it attempts to connect to the Priority 2 entry, and so on.

2 Conformance Claims

2.1 CC Conformance Claims

This ST was developed to Common Criteria (CC) for Information Technology Security Evaluation Part 1 – September 2006 Version 3.1, Revision 1 and CC for Information Technology Security Evaluation Parts 2 & 3 – September 2007 Version 3.1 Revision 2.

The ST claims to be:

CC Version 3.1 Release 2 Part 2 extended

CC Version 3.1 Release 2 Part 3 conformant

2.2 PP and Package Claims

The ST claims to be Evaluation Assurance Level 4 augmented with ALC_FLR.1.

The ST is not conformant to any Protection Profiles.

2.3 Conformance Rationale

The ST is not conformant to any Protection Profiles, so the conformance rationale is not provided.

This ST does not claim conformance to the U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.1 (TFFPP) due to the following:

- The TOE provides remote administration, but does not provide a single-use authentication mechanism. The TOE is capable of requiring SecurID, but use of SecurID is not included in the FIPS certification and the SecurID server performing the authentication is part of the IT environment.
- The TOE does not audit the failure of cryptographic operations and the SMS does not audit changes to the time (the SMS time is recorded in the audit records).
- The TOE does not perform sorting based on subject address or ranges of addresses.
- The TOE only protects the audit records at the interfaces provided by the TOE; it relies upon the IT environment to protect the audit records from network or OS interfaces.

This ST does not claim conformance to the U.S. Government Virtual Private Network (VPN) Boundary Gateway Protection Profile for Medium Robustness Environments, Version 1.1 (VPNPP) due to the following:

- The TOE does not implement security alarm acknowledgement.
- The TOE does not audit all of the events required by the VPNPP, including failure of cryptographic operations and the SMS does not audit changes to the time (the SMS time is recorded in the audit records).

- The TOE does not perform sorting based on subject address or ranges of addresses.
- The TOE only protects the audit records at the interfaces provided by the TOE; it relies upon the IT environment to protect the audit records from network or OS interfaces.
- The TOE does not provide a maintenance mode.
- The TOE does not provide the extended TSF testing capabilities.

3 Security Problem Definition

This section aims to clarify the nature of the security problem that the ALVF v9.1 is intended to solve. It does so by describing:

- Any known or assumed threats to the assets against which specific protection within the ALVF v9.1 or its environment is required.
- Any organizational security statements or rules with which the ALVF v9.1 must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the ALVF v9.1 is intended to be used.

The TOE is intended to be used in environments in which, at most, sensitive but unclassified information is processed.

3.1 Threats

This section helps define the nature and scope of the security problem by identifying assets which require protection as well as threats to those assets.

Threats may be addressed either by the ALVF v9.1, by its intended environment (for example, using personnel, physical, or administrative safeguards) or by a combination of the ALVF v9.1 and the intended environment.

The threat agents are divided into two categories:

- Attackers who are not administrative TOE users: They have public knowledge of how the TOE operates and are assumed to possess average expertise, limited resources to alter TOE configuration settings/parameters and no physical access to the SMS host or the Firewall Appliance.
- Administrative TOE users: They have knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE users are however assumed not to be willfully hostile to the TOE)

The threats identified assume that the threat agent has a low attack potential that possesses an average expertise, few resources, and low to moderate motivation. The IT assets requiring protection are the audit data, user data saved on or transitioning through the TOE, and the hosts on the protected network.

T.NOAUTH An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.ASPOOF An unauthorized entity may use a spoofed source IP address to transmit information through the TOE into a connected network.

T.MEDIAT A user on a network may attempt to access unauthorized services or connect to unauthorized hosts on another network.

T.OLDINF Persons may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows for the TOE.

T.AUDACC Persons may not be accountable for the actions that they conduct in the TOE Environment, thus allowing an attacker to escape detection due to lack of reliable timestamps or by tampering the TSF data stored in the TOE Environment.

T.SELPRO An unauthorized user may read, modify, or destroy security critical TOE configuration data stored on the TOE.

T.AUDFUL An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust storage capacity, thus masking an attackers actions.

T.REPEAT An unauthorized person may repeatedly try to guess authentication data used for performing I & A functionality in order to use this information to launch attacks on the TOE.

T.PROCOM An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between remotely located parts of the TOE.

T.TRANS An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete data transmitted between the TOE and an authenticated external IT entity.

T.TUSAGE The TOE may be used and administered in an insecure manner by either authorized persons.

3.2 Organizational Security Policies

There are no organizational Security Policies specified.

3.3 Assumptions

This section helps define the scope of the security problem by identifying assumptions about the security aspects of the environment and/or of the manner in which the ALVF v9.1 is intended to be used.

A.PUBLIC The FA and SMS/SCS do not host public data.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance.

A.SINGEN Information can not flow among the internal and external networks unless it passes through the Firewall Appliance.

A.GENPUR The SMS and SCS hosts only store and execute security-relevant applications and only store data required for its secure operation.

A.DIRECT The SMS and SCSs are available to authorized administrators only.

A.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

A.PHYSEC The FA, SMS, and SCSs will be located within controlled access facilities that mitigate unauthorized physical access.

A.REMACC The authorized administrators will install and properly configure all the necessary security features on all SMS Remote Navigator hosts.

A.MGNET If deployed using a secure management network, the network connecting the SMS and/or SCS hosts to an FA is a private, separate physical network that is not globally routable and that is protected from attacks and from unauthorized physical access.

4 Security Objectives

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives of the TOE, and
- Security objectives for the Operating Environment.

4.1 Security Objectives for the TOE

O.IDANDA The TOE must ensure that the claimed identity of all SMS users is uniquely identified and authenticated before granting a user access to protected TOE functions or, for certain specified services, to a connected network. The TOE must also ensure that all users of the Brick CLI are authenticated prior to allowing access to the CLI functions.

O.INSPEC The FA must mediate the flow of all information between users on an internal network connected to the FA and users on an external network connected to the FA, and must ensure that residual information from previous information flow is not transmitted in any way.

O.DEFALT Upon initial start-up of the TOE service, the TOE must not compromise its resources or those of any connected network.

O.DOMSEP The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

O.ACCOUN The TOE must provide user accountability for information flows through the FA and for authorized administrator use of TOE security functions.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.CRYPTO The TOE must provide cryptographic operations (i.e., encryption/decryption, digital signature operations, etc.) to maintain the confidentiality and integrity of the communications between different components of the TOE separated physically by a network.

O.VPN The TOE must provide the ability to authenticate endpoints transmitting data and to protect data transmitted to and from an authenticated external IT entity from modification and disclosure.

4.2 Security Objectives for the Operating Environment

This section defines the non-IT security objectives for the environment and the IT security objectives for the environment.

4.2.1 Non-IT Security Objectives For The Operating Environment

The non-IT security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures and will not require the implementation of functions in the TOE hardware and/or software.

OE.PHYSEC	The FA, SMS, and SCSs will be located within controlled access facilities that mitigate unauthorized, physical access.
OE.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
OE.GENPUR	The operating environment that hosts the SMS and SCSs only stores and executes security-relevant applications and only stores data required for its secure operation.
OE.PUBLIC	The FA and SMS/SCS do not host public data.
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance.
OE.SINGEN	Information can not flow among the internal and external networks unless it passes through the Firewall Appliance.
OE.DIRECT	The SMS and SCS hosts are available to authorized administrators only.
OE.REMACC	The TOE operating environment shall provide all the necessary security features installed and properly configured by authorized administrators on the SMS Remote Navigator host to protect the SMS Remote Navigator and host operating system from attacks aimed at compromising the SMS Remote Navigator.
OE.MGNET	If deployed using a management network, the network connecting the SMS and/or SCS hosts to an FA is a private, separate physical network that is not globally routable and that is protected from attacks and from unauthorized physical access.
OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of sound security policies and practices for both the TOE and required TOE Environment components. They do not tamper with the TOE Environment image, configuration files and log files from the file system of the operating system on which the TOE resides. Administrators review the environment audit logs to ensure security.
OE.GUIDAN	Those responsible for the TOE must ensure that the TOE is delivered, installed, administered, operated in a manner that maintains security and the TOE Environment is setup in a secure way such that it supports the TSF.

4.2.2 IT Security Objectives For The Operating Environment

The following IT security objectives for the environment are to be addressed by the operating environment by technical means.

OE.DOMSEP The SMS/SCS and SMS Remote Navigator hosts, which are in the TOE operating environment, shall protect the TOE against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

OE.IDAUTH If the TOE is configured to use external authentication, the TOE operating environment shall provide the ability to uniquely identify and authenticate users.

OE.TMSTMP The TOE operating environment shall be able to generate reliable timestamps for the TOE's use.

4.3 Security Objectives Rationale

4.3.1 Tracings between Security Objectives and the Security Problem Definition

	T.NOAUTH	T.ASPOOF	T.MEDIAT	T.OLDINF	T.AUDACC	T.SELPRO	T.AUDFUL	T.REPEAT	T.PROCOM	T.TRANS
O.IDANDA	X									
O.INSPEC		X	X	X						
O.DEFALT	X					X				
O.DOMSEP	X					X		X		
O.AUDREC					X					
O.ACCOUN					X					
O.SECFUN	X						X			
O.CRYPTO									X	
O.VPN										X

Table 2: Tracings between Threats and TOE Security Objectives

	T.NOAUTH	T.AUDACC	T.SELPRO	T.TUSAGE	A.PUBLIC	A.NOEVIL	A.SINGEN	A.PHYSEC	A.GENPUR	A.MODEXP	A.REMACC	A.DIRECT	A.MGNET

OE.GUIDAN				X									
OE.ADMTRA		X		X									
OE.PUBLIC					X								
OE.NOEVIL						X							
OE.SINGEN							X						
OE.PHYSEC								X					
OE.MODEXP										X			
OE.REMACC											X		
OE.GENPUR									X				
OE.DIRECT												X	
OE.MGNET													X
OE.DOMSEP	X		X										
OE.TMSTMP		X											
OE.IDAUTH	X												

Table 3: Tracings between Threats/Assumptions and Security Objectives for the Environment

4.3.2 Rationale for Assumptions to Security Objectives mapping

Assumptions	Security Objectives for TOE and Environment
A.PUBLIC The FA and SMS/SCS do not host public data.	OE.PUBLIC covers this assumption by the objective that the FA and SMS/SCS do not host public data.
A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance.	OE.NOEVIL covers this assumption by ensuring that the Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN Information can not flow among the internal and external networks unless it passes through the Firewall Appliance.	OE.SINGEN covers this assumption by ensuring that Information can not flow among the internal and external networks unless it passes through the Firewall Appliance.
A.GENPUR The SMS and SCS hosts only store and execute security-relevant applications and only store data required for its secure operation.	OE.GENPUR covers this assumption by ensuring that the SMS and SCS hosts only store and execute security-relevant applications and only store data required for its secure operation.
A.DIRECT The SMS and SCSs are available to authorized administrators only.	OE.DIRECT covers this assumption by ensuring that SMS and SCS hosts are available to authorized administrators only.

Assumptions	Security Objectives for TOE and Environment
A.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.	OE.MODEXP covers this assumption by ensuring that the threat of malicious attacks aimed at discovering exploitable vulnerabilities is moderate.
A.PHYSEC The FA, SMS, and SCSs will be located within controlled access facilities that mitigate unauthorized physical access.	OE.PHYSEC covers this assumption by ensuring that the TOE Environment will be set up to provide controlled access facilities that mitigate unauthorized, physical access to the FA, SMS, and SCSs.
A.REMACC The authorized administrators will install and properly configure all the necessary security features on all SMS Remote Navigator hosts.	OE.REMACC covers this assumption by ensuring the TOE operating environment shall provide all the necessary security features installed and properly configured by authorized administrators on the SMS Remote Navigator host to protect the SMS Remote Navigator and host operating system from attacks aimed at compromising the SMS Remote Navigator.
A.MGNET If deployed using a secure management network, the network connecting the SMS and/or SCS hosts to an FA is a private, separate physical network that is not globally routable and that is protected from attacks and from unauthorized physical access.	OE.MGNET covers this assumption by ensuring that if the TOE is deployed with a management network, the management network in the TOE environment will be set up as a private, separate physical network that is not globally routable and that is protected from attacks and unauthorized physical access.

Table 4: Assumptions to Security Objectives Rationale

4.3.3 Rationale for Threats to Security Objectives mapping

Threats	Security Objectives for TOE and Environment
T.NOAUTH An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.	O.IDANDA covers this threat by making sure that before any access is granted to the SMS TSF functions or any services inside the protected network successful identification and authentication is performed. O.IDANDA also makes sure that before access is granted to the CLI successful authentication is performed. O.DEFALT covers this threat by ensuring that the TOE up-on startup or recovery from an interruption in the TOE service doesn't compromise any of its resources or doesn't allow any free flow of information through it to the connected network. O.SECFUN covers this functionality by ensuring that only authorized users can access the TOE security functions. O.DOMSEP covers this threat by ensuring that the TOE has the capability to protect itself against attempts by unauthorized users to bypass, deactivate or tamper with TOE security functions. OE.DOMSEP assists in covering this threat by ensuring that the TSF on the SMS/SCS and SMS Remote Navigator hosts are protected from users through mechanisms in the TOE environment. OE.IDAUTH assists in covering this threat when the TOE is configured to use external authentication, by providing the ability to uniquely identify and authenticate users.
T.ASPOOF An unauthorized entity may use a spoofed source IP address to transmit information through the TOE into a connected network.	O.INSPEC covers this threat by ensuring that the Firewall Appliance mediates the flow of all information between users on an internal network connected to the FA and users on an external network connected to the FA. The traffic flows includes traffic within a tunnel and inter TOE component secure communications.
T.MEDIAT A user on a network may attempt to access unauthorized services or connect to unauthorized hosts on another network.	O.INSPEC covers this threat by ensuring that Firewall Appliance mediates the flow of all information from users on a connected network to users on another connected network. The traffic flows include traffic within a tunnel and inter TOE component secure communications.

Threats	Security Objectives for TOE and Environment
T.OLDINF Persons may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows for the TOE.	O.INSPEC covers this threat by ensuring that the Firewall Appliance will never allow residual information of a previous information flow to be transmitted in subsequent information flows through the Firewall Appliance. The traffic flows include traffic within a tunnel and inter TOE component secure communications.
T.AUDACC Persons may not be accountable for the actions that they conduct in the TOE Environment, thus allowing an attacker to escape detection due to lack of reliable timestamps or by tampering the TSF data stored in the TOE Environment.	O.AUDREC covers this threat by ensuring that the TOE provide a means to record events with accurate dates and times and also provide capabilities to do search and sort of the audit trail based on relevant attributes. O.ACCOUN covers this threat by ensuring that only authorized administrators have control over the audit trail and no unauthorized tampering of the audit trail. OE.TMSTMP covers this threat by ensuring that the TOE is provided with a reliable timestamp for its use. OE.ADMTRA covers this threat by ensuring that the operating system administrators do not tamper with the audit logs that are stored on the file system of the underlying operating system and they review the environment audit logs to ensure security.
T.SELPRO An unauthorized user may read, modify, or destroy security critical TOE configuration data stored on the TOE.	O.DEFALT covers this threat by ensuring that upon initial start-up of the TOE service, the TOE must not compromise its resources or those of any connected network. O.DOMSEP covers this threat by ensuring that the TOE has the capability to protect itself against attempts by unauthorized users to bypass, deactivate or tamper with TOE security functions. OE.DOMSEP assists in covering this threat by ensuring that the TSF on the SMS/SCS and SMS Remote Navigator hosts are protected from users through mechanisms in the TOE environment.
T.AUDFUL An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust storage capacity, thus masking an attackers actions.	O.SECFUN covers this threat by ensuring authorized users posses the functionality to use the TOE security functions and further by ensuring that such functionality is available to only authorized administrators.

Threats	Security Objectives for TOE and Environment
T.REPEAT An unauthorized person may repeatedly try to guess authentication data used for performing I & A functionality in order to use this information to launch attacks on the TOE.	This threat has been mapped to the objective O.DOMSEP which states that the TOE must have the ability to protect itself against attempts by unauthorized users to bypass, deactivate or tamer with TOE security functions.
T.PROCOM An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between remotely located parts of the TOE.	This threat has been mapped to the objective O.CRYPTO which states the TOE should ensure the confidentiality and integrity of the communications between different components of the TOE separated physically by a network. The cryptography implemented for O.CRYPTO will make it infeasible for an attacker to view, modify or delete security-relevant information in transit from physically separated parts of the TOE.
T.TRANS An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete data transmitted between the TOE and an authenticated external IT entity.	O.VPN covers this threat by ensuring the confidentiality and integrity of the communications between the TOE and an external IT entity.
T.TUSAGE The TOE may be used and administered in an insecure manner by either authorized persons.	OE.ADMTRA covers this threat by ensuring that the operating system administrators are trained as to establishment and maintenance of sound security policies and practices for both the TOE and required TOE Environment components. This would include the setup, secure physical access practices, and access control configuration practices for the TOE environment items like the host operating systems and the Alcatel-Lucent IPSec Client personal firewall. Administrators are trained to follow secure practices and OE.GUIDAN covers this threat by ensuring that the TOE is delivered, installed, administered, operated in a manner that maintains security and the TOE Environment is setup so that it supports the TSF.

Table 5: Threats to Security Objectives Rationale

5 Extended Components Definition

This section defines the new components (also known as extended components) used to define the security requirements for this ST. The extended components defined in this section are to be members of existing CC Part 2 families and are based on the existing CC Part 2 SFRs.

5.1.1 FIA Identification and Authentication

The FIA class is extended to include four additional components.

The FIA class addresses the requirements to verify a claimed user identity. The extended components defined in this section require the TOE to ensure that claimed user identities are verified by either the IT environment or the TOE and require that the TOE can be configured to use an authentication server for verifying a claimed user identity.

5.1.1.1 FIA_UAU_TRD.1 Timing of authentication with a third party

FIA_UAU_TRD.1 is a member of the FIA_UAU family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the authentication to be required by the TOE, but performed by either the TOE or IT environment. This extended SFR is based on CC Part 2 FIA_UAU.1.

Management: FIA_UAU_TRD.1

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

- If authentication is by the TOE, management of the authentication data by an administrator
- If authentication is by the TOE, management of the authentication data by the associated user
- Managing the list of actions that can be taken before the user is authenticated.

Audit: FIA_UAU_TRD.1

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

- Minimal: Unsuccessful use of the authentication mechanism;
- Basic: All use of the authentication mechanism;
- Detailed: All TSF mediated actions performed before authentication of the user.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification or
FIA_UID_TRD.1 Time of identification with a third party.

FIA_UAU_SRV.1 Authentication via authentication server

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

by the [selection: *IT environment, TOE or the IT environment as configured by the administrator*].

FIA_UAU_TRD.1.2 The TSF shall require each user to be successfully authenticated by [selection: *IT environment, TOE or the IT environment as configured by the administrator*] before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.2 FIA_UID_TRD.1 Timing of identification with a third party

FIA_UID_TRD.1 is a member of the FIA_UID family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the identification to be required by the TOE, but performed by either the TOE or IT environment. This extended SFR is based on CC Part 2 FIA_UID.1.

Management: FIA_UID_TRD.1

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

- If identification is by the TOE, management of the user identities;
- If an authorized administrator can change the actions allowed before identification, the managing of the action lists.

Audit: FIA_UID_TRD.1

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

- Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided;
- Basic: All use of the user identification mechanism, including the user identity provided.

Hierarchical to: No other components.

Dependencies: FIA_UID_SRV.1 Identification via authentication server

FIA_UID_TRD.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is identified by the [selection: *IT environment, TOE or the IT environment as configured by the administrator*].

FIA_UID_TRD.1.2 The TSF shall require each user to be successfully identified by the [selection: *IT environment, TOE or the IT environment as configured by the administrator*] before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.3 FIA_UAU_SRV.1 Authentication via authentication server

FIA_UAU_SRV.1 is a member of the FIA_UAU family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the authentication to be performed by an authentication server which is in either the TOE or IT environment. This extended SFR is based on CC Part 2 FIA_UAU.1.

Management: FIA_UAU_SRV.1

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

- If authentication is by the TOE, management of the authentication data by an administrator
- If authentication is by the TOE, management of the authentication data by the associated user
- Configuration of the authentication server(s) used to authenticate users.

Audit: FIA_UAU_SRV.1

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

- Minimal: Unsuccessful use of the authentication mechanism, including the user identity provided if applicable;
- Basic: All use of the authentication mechanism, including the user identity provided if applicable;

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification or

FIA_UID_TRD.1 Time of identification with a third party or

FIA_UID_SRV.1 Identification via authentication server

FIA_UAU_SRV.1.1 When invoked by the TSF, the [assignment: list of authentication server(s)] in the [selection: *TOE*, *IT environment*] shall determine if the user has provided valid authentication data and pass the results of that determination back to the TOE.

5.1.1.4 FIA_UID_SRV.1 Identification via authentication server

FIA_UID_SRV.1 is a member of the FIA_UID family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the identification to be performed by an authentication server which is in either the TOE or IT environment. This extended SFR is based on CC Part 2 FIA_UID.1.

Management: FIA_UID_SRV.1

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

- If authentication server is in the TOE, management of the user identities;
- Configuration of the authentication server(s) used to identify users.

Audit: FIA_UID_SRV.1

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

- Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided if applicable;

- Basic: All use of the user identification mechanism, including the user identity provided if applicable.

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID_SRV.1.1 When invoked by the TSF, the [assignment: list of authentication server(s)] in the [selection: *TOE*, *IT environment*] shall determine if the user has provided valid identification data and pass the results of that determination back to the TOE.

6 Security Requirements

This section defines the security requirements for the TOE and the operational environment (that is, for hardware, software, or firmware external to the TOE and upon which satisfaction of the TOE's security objectives depends).

The CC divides security requirements into two categories:

- Security functional requirements (SFRs), that is, requirements for security functions such as information flow control, audit, I&A.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment).

6.1 TOE Security Functional Requirements

This section defines the TOE SFRs that are directly taken from the CC Version 3.1 or from the extended components defined in Section 5. The TOE shall satisfy the SFRs stated in the table below which lists the names of the SFR components. Following the table, the individual functional requirements are restated with any necessary operations completed.

Functional Component ID	Functional Component Name
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.3(1)	Selectable audit review – Searches
FAU_SAR.3(2)	Selectable audit review – Sorting
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Distribution
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1 (1)	Cryptographic Operation – encryption services
FCS_COP.1 (2)	Cryptographic Operation – hashing
FCS_COP.1 (3)	Cryptographic Operation – IKE
FCS_COP.1 (4)	Cryptographic Operation – digital signatures
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple security attributes

FDP_RIP.1	Subset residual information protection
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU_TRD.1	Timing of Authentication with a third party
FIA_UID_TRD.1	Timing of Identification with a third party
FMT_MOF.1 (1)	Management of security functions behavior (SMS)
FMT_MOF.1 (2)	Management of security functions behavior (Brick)
FMT_MOF.1 (3)	Management of security functions behavior (SMS Admin)
FMT_MOF.1 (4)	Management of security functions behavior (Reboot)
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1 (1)	Management of TSF data (manage policy rules)
FMT_MTD.1 (2)	Management of TSF data (audit trail)
FMT_MTD.1 (3)	Management of TSF data (user attributes)
FMT_MTD.1 (4)	Management of TSF data (user accounts and user groups)
FMT_MTD.1 (5)	Management of TSF data (SCS)
FMT_MTD.1 (6)	Management of TSF data (query policy rules)
FMT_MTD.1 (7)	Management of TSF data (alarms)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with Preservation of Secure State
FPT_ITT.1	Basic internal TSF data transfer protection
FRU_FLT.1	Degraded fault tolerance
FRU_RSA.1(1)	Maximum quotas (transport layer quotas)
FRU_RSA.1(2)	Maximum quotas (intelligent cache management)
FTP_ITC.1	Inter-TSF trusted channel

Table 6: TOE Security Functional Requirements

6.1.1 FAU Security Audit

6.1.1.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take [the action of sending an e-mail message, syslog message, SNMP trap, or console message] upon detection of a potential security violation.

6.1.1.2 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 **relevant** auditable events for *not specified* level of audit **specified in Table 7: Auditable Events**; and

c) [None]**.**

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 identit**y**, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [information specified in column three of the Table below]

Functional Component	**Auditable Events**	**Additional Audit Record Contents**
FAU_ARP.1	Action taken due to the potential security violation.	None.
FAU_STG.4	Actions taken due to audit storage failure.	None.
FMT_SMR.1	Modifications to the group of users that are part of a role.	The identity of the administrative user performing the modification and the user identity being associated with the role.
FIA_UAU_TRD.1	Any use of the authentication mechanism.	The user identities provided to the TOE
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.

Functional Component	Auditable Events	Additional Audit Record Contents
FMT_MOF.1 (1), (4)	Use of the functions listed in these requirements, except for the following: ▪ Make a FA boot floppy or USB drive ▪ View tunnels ▪ View SMS/SCS & Brick status information.	The identity of the administrative user performing the operation
FMT_MSA.1	Modifications of the values of security attributes.	The identity of the administrative user performing the operation
FMT_MTD.1 (1), (3), (4)	Modifications, deletions, and additions of TSF data.	The identity of the administrative user performing the operation
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration.	The identity of the administrator making the authentication attempts and the administrative user who unlocks the user account.
FIA_UAU.5	The final authentication decision.	The user identities provided to the TOE.
FRU_RSA.1 (2)	Rejection of fragment allocation operation due to resource limits	None
FTP_ITC.1	All attempts to establish a VPN tunnel.	Identification of initiator and target of all failed trusted channels.

Table 7: Auditable Events

6.1.1.3 FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation of combination of [auditable events in Table 8] known to indicate a potential security violation;

b) [other detection criteria for each event as defined in Table 8].

Functional Component	Auditable Events	Additional Detection Criteria
FDP_IFF.1	Decisions on requests for information flow which match the Alarm Code in the rule	Threshold period – time period in which the number of events must occur before an alarm is generated Sleep period – after initial alarm is generated, the amount of time that must elapse before another alarm is generated
FRU_RSA.1 (2)	Activation of Intelligent Cache Management	Actual percentage of cache full & absolute number of sessions before pruning Actual percentage of cache full & absolute number of sessions after pruning Sleep period
FIA_UAU.5	Failed user authentication attempts (via SMS administrator, Group administrator, VPN user)	Threshold period – time period in which the number of events must occur before an alarm is generated Sleep period
FPT_ITC.1	IKE initiated or failed	Sleep period

Table 8: Alarm Triggers

6.1.1.4 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [SMS administrator and Group Administrator with View and Full privilege] with the capability to read [for the SMS administrator, all audit trail data including real time audit data and for the Group administrator, all audit trail data for the corresponding group] 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.

6.1.1.5 FAU_SAR.3 (1) Selectable audit review - Searches

FAU_SAR.3.1 (1) The TSF shall provide the ability to perform *searches* of audit data based on

a) [user identity;

b) presumed subject address;

c) ranges of dates;

d) ranges of times;

e) ranges of addresses.]

6.1.1.6 FAU_SAR.3 (2) Selectable audit review - Sorting

FAU_SAR.3.1 (2) The TSF shall provide the ability to perform *sorting* of audit data based on

a) [the chronological order of audit event occurrence.]

6.1.1.7 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall *prevent auditable events, except those taken by the authorized user with special rights* and [shall limit the number of bytes lost to 65535 and lost audit records related to a new session for the duration the SMS server is unavailable to the brick] if the audit trail is full.

6.1.2 FCS Cryptographic Support

6.1.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [pseudo-random number generation] and specified cryptographic key sizes [128-4096 bits] that meet the following: [PRNG portion of FIPS 140-2].

6.1.2.2 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [IKEv1, IKEv2, manual] that meets the following: [RFC 2409 for IKEv1, RFC 4306 for IKEv2, and FIPS140-2].

6.1.2.3 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization of all cryptographic keys within the FA, SCS, SMS and SMS Remote Navigator] that meets the following: [FIPS 140-2].

6.1.2.4 FCS_COP.1 (1) Cryptographic Operation – encryption services

FCS_COP.1.1 (1) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [3DES CBC or AES CBC] and cryptographic key sizes [168 bits for 3DES and 128, 192, 256 for AES] that meet the following [FIPS 46-3 for 3DES and FIPS PUB 197 for AES] **using a FIPS 140-2 compliant module**.

6.1.2.5 FCS_COP.1 (2) Cryptographic Operation - hashing

FCS_COP.1.1 (2) The TSF shall perform [message hashing] in accordance with a specified cryptographic algorithm [HMAC-SHA-1 and SHA-1] and cryptographic key sizes [160 bits] that meet the following [FIPS 180-1] **using a FIPS 140-2 compliant module**.

6.1.2.6 FCS_COP.1 (3) Cryptographic Operation - IKE

FCS_COP.1.1 (3) The TSF shall perform [IKE (Internet key exchange)] in accordance with a specified cryptographic algorithm [Diffie-Hellman] and cryptographic key sizes [768, 1024, 1536, and 2048 bits] that meet the following [RFC 2409 (IKEv1), RFC 4306 (IKEv2)] **using a FIPS 140-2 compliant module**.

6.1.2.7 FCS_COP.1 (4) Cryptographic Operation – digital signatures

FCS_COP.1.1 (4) The TSF shall perform [digital signature generation and verification] in accordance with a specified cryptographic algorithm [RSA and DSA] and cryptographic key sizes [1024, 1536, 2048, 3072, 4096 bits for RSA and 1024 bits for DSA] that meet the following [PKCS #1 for RSA and FIPS PUB 186-1 for RSA and DSA] **using a FIPS 140-2 compliant module**.

6.1.3 FDP User Data Protection

6.1.3.1 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [TRAFFIC FILTER SFP] on:

a) [subjects: external IT entities that send and receive information through the TOE to one another.

b) information: traffic sent through the TOE from one subject to another (including FTP, HTTP, H.323, SIP, SUN RPC, SMTP, DHCP, DNS);

c) operation: drop information, pass information without modification, encrypt and pass information, decrypt and pass information.]

6.1.3.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [TRAFFIC FILTER SFP] based on **at least** the following types of subject and information security attributes:

a) [subject security attributes:

1) presumed address;

2) user name for FTP;

3) user group name for FTP

b) information security attributes:

1) presumed address of source subject;

2) presumed address of destination subject;

3) network protocols;

4) TOE interface on which traffic arrives and departs;

5) service;

6) time of day.

7) FTP attributes (FTP commands, data ports, user ids);

8) HTTP attributes (URI, HTTP requests);

9) H.323 VoIP attributes (dynamic channels and destination ports);

10) SIP attributes (endpoint name/address, port number, SIP methods)

11) H323 RAS attributes (ports)

12) SUN Remote Procedure Call (RPC) attributes (dynamic port, program/version/protocol triplet)

13) SMTP attributes (SMTP commands, MIME types, attachments, From address)

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

a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all

possible combinations of the values of the information flow security attributes, created by the authorized administrator;

- the presumed address of the source subject, in the information translates to an external network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.].

FDP_IFF.1.3 The TSF shall enforce the [following additional information flow control SFP rules:

a) encryption and decryption of IPSec packets when an action of VPN is selected for the matching information flow security policy rule based on the specific VPN action setting contained in the rule

b) subjects negotiating a VPN tunnel are authenticated].

FDP_IFF.1.4 The TSF shall provide the following [additional SFP capabilities:

a) delay response to an invalid user name to establish an FTP session

b) drop reconnect attempts after a strict HTTP syntax checking violation or violation of the SIP filter

c) DHCP relay

d) discard additional resource record sections in DNS responses

e) block queries of the root node of the DNS database].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow **of administrative traffic** based on the following rules: [Network Address Translation (NAT)].

Application Note: *The evaluated configuration requires that administrative traffic flowing to the SMS host must be Network Address Translation (NAT) enabled.*

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:

a) [The TOE shall reject requests if there is no rule in the policy ruleset which explicitly allows the information flow ;

b) The TOE shall reject requests if any of the attributes identified in FDP_IFF.1.1 do not match;

c) The TOE shall reject requests for access or services where the presumed source address is not included in the set of addresses for the source subject[6];

d) The TOE shall reject requests for access or services where the presumed source address specifies a broadcast network[7];

e) The TOE shall reject requests for access or services where the presumed source address of the information received by the TOE specifies the loopback network;

f) The TOE shall reject requests in which the information received by the TOE contains the route (set of host network addresses) by which information shall flow from the source subject to the destination subject;

g) The TOE shall reject malformed service requests, including FTP and SMTP protocol anomalies, HTTP syntax conformance and SUN RPC message format violations.]

6.1.3.3 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following objects: [resources that are used by the subjects of the TOE to communicate through the TOE to other subjects].

6.1.4 FIA Identification and Authentication

6.1.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within [the range 0 – 25]*[8] unsuccessful authentication attempts occur related to [SMS authentication attempts by an administrator].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [lock the administrator account].

6.1.4.2 FIA_ATD.1 User attribute definition

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

---

[6] The intent of this requirement is to ensure that a user cannot send packets originating on one TOE interface claiming to originate on another TOE interface.

[7] A broadcast network specifies more than one host address on that network. The TOE can only know the sub-netting configuration of networks directly connected to the TOE's interfaces and therefore can only be aware of broadcast addresses on those networks.

[8] A value of 0 means that the TSF will never disable the administrator account due to failed login attempts.

a) [identity of SMS administrative users and VPN users;

b) authentication data, if configured for authentication by the TOE;

c) association of a human user with a role and assigned privilege;]

6.1.4.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following composition rules if the strong password option is enabled and the user is authenticated via the local password:

a) The password must be a minimum of 8 characters or the minimum password length set for the local password authentication service, whichever is greater

b) The password must contain at least one alphabetic character and one non-alphabetic character;

c) The password cannot contain 3 or more repeated alphanumeric characters in a row

d) The password cannot contain 3 or more consecutive, ascending or descending, alphanumeric characters in a row

e) The password cannot contain the User account name or its mirror (reverse character format)

f) The password cannot be one of the previous 3 most recently used passwords.

g) The password (except for Brick passwords) expires in an administrator configurable value of 30-120 days.

h) The TSF can be configured to require that the password contain at least one non-alphabetic character that is not in the first or last position].

6.1.4.4 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [a password mechanism and certificate verification mechanism] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [following multiple authentication mechanism rules:

- Reusable password mechanism can be configured for administrators accessing the TOE
- Reusable password mechanisms can be configured on a user-basis for VPN users
- VPN certification authentication (signature verification) can be configured on a user-basis for VPN users].

6.1.4.5 FIA_UAU_TRD.1 Timing of Authentication with a third party

FIA_UAU_TRD.1.1 The TSF shall allow [identification as stated in FIA_UID_TRD.1, information flows authenticated with support from the IT environment] on behalf of the user to be performed before the user is authenticated by the *TOE or the IT environment as configured by the administrator*.

FIA_UAU_TRD.1.2 The TSF shall require each user to be successfully authenticated by the *TOE or the IT environment as configured by the administrator*, before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.6 FIA_UID_TRD.1 Timing of Identification with a third party

FIA_UID_TRD.1.1 The TSF shall allow [DB Utilities, Start Services, Stop Services, Restart Services, SMS Status, Configuration Assistant, Schedule Editor, New Feature Setup and unauthenticated information flows] on behalf of the user to be performed before the user is identified by the *TOE or the IT environment as configured by the administrator*.

FIA_UID_TRD.1.2 The TSF shall require each user to be successfully identified by the *TOE or the IT environment as configured by the administrator* before allowing any other TSF-mediated actions on behalf of that user.

6.1.5 FMT Security Management

6.1.5.1 FMT_MOF.1 (1) Management of security functions behavior (SMS)

FMT_MOF.1.1 (1) The TSF shall restrict the ability to ***perform*** the functions

a) [startup and shutdown the audit functions

b) unlock locked administrators

c) Add, Remove, Update FAs

d) Make a FA boot floppy or USB drive

e) Create, delete an authentication service

f) View, enable, disable, permanently delete tunnels and terminate client tunnel sessions

g) View SMS/SCS and Brick status information]

to [an SMS administrator or a corresponding Group administrator].

6.1.5.2 FMT_MOF.1 (2) Management of security functions behavior (Brick)

FMT_MOF.1.1 (2) The TSF shall restrict the ability to ***perform*** the functions [delete session] to [a Brick CLI administrator].

6.1.5.3 FMT_MOF.1 (3) Management of security functions behavior (SMS Admin)

FMT_MOF.1.1 (3) The TSF shall restrict the ability to ***perform*** the functions [

a) force a logout of an administrator

b) obtain and import digital certificates

c) configure the system to run commands at scheduled times

d) view, enable, disable, configure Concurrency Control[9]

e) rehome a brick]

to [an SMS administrator].

6.1.5.4 FMT_MOF.1 (4) Management of security functions behavior (Reboot)

FMT_MOF.1.1 (4) The TSF shall restrict the ability to ***perform*** the functions [reboot FA] to [an SMS administrator, a corresponding Group administrator, or a Brick CLI administrator].

6.1.5.5 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [TRAFFIC FILTER SFP] to restrict the ability to [*manipulate*[10]] the security attributes [referenced in the indicated policies] to [SMS administrator or Group administrator]**.**

6.1.5.6 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

6.1.5.7 FMT_MSA.3 Static attributes initialization

FMT_MSA.3.1 The TSF shall enforce the [TRAFFIC FILTER SFP] to provide *restrictive* default values for **information flow** security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow an [SMS administrator and Group Administrator] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.8 FMT_MTD.1 (1) Management of TSF data (manage policy rules)

FMT_MTD.1.1 (1) The TSF shall restrict the ability to *modify, delete, [create]* the [information flow security policy rules] to [an SMS administrator

[9] Concurrency control provides the ability to prevent changes to objects by multiple administrators at a time.

[10] The term "manipulate" indicates that the security attributes in FDP_IFF.1.1 may be used to create additional "attributes" that can be used in specifying information flow security policy rules (for example, a set of network addresses that can be used as a "group"); this requirement restricts who can perform such operations. It is important to note that the attributes associated with stateful packet inspection are not expected to be managed by any administrator.

or a corresponding Group administrator].

6.1.5.9 FMT_MTD.1 (2) Management of TSF data (audit trail)

FMT_MTD.1.1 (2) The TSF shall restrict the ability to *query* the [audit trail] to [an SMS administrator or a corresponding Group administrator].

6.1.5.10 FMT_MTD.1 (3) Management of TSF data (user attributes)

FMT_MTD.1.1 (3) The TSF shall restrict the ability to *query, modify, delete, [create]* the [user attribute values defined in FIA_ATD.1 and authentication options] to [an SMS administrator or a corresponding Group administrator].

6.1.5.11 FMT_MTD.1 (4) Management of TSF data (user accounts and user groups)

FMT_MTD.1.1 (4) The TSF shall restrict the ability to *[create]* the [user accounts and user groups] to [an SMS administrator or a corresponding Group administrator].

6.1.5.12 FMT_MTD.1 (5) Management of TSF data (SMS/SCS)

FMT_MTD.1.1 (5) The TSF shall restrict the ability to *query, modify, delete, [add]* the [Secondary SMSs and SCSs] to [an SMS administrator].

6.1.5.13 FMT_MTD.1 (6) Management of TSF data (query policy rules)

FMT_MTD.1.1 (6) The TSF shall restrict the ability to *query* the [information flow security policy rules] to [an SMS administrator, a corresponding Group administrator, or a Brick CLI administrator].

6.1.5.14 FMT_MTD.1 (7) Management of TSF data (alarms)

FMT_MTD.1.1 (7) The TSF shall restrict the ability to *query, [configure]* the [alarm actions and alarm triggers] to [an SMS administrator or a Group administrator].

6.1.5.15 FMT_SMF.1 Specification of management functions

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

a) Startup and shutdown the application

b) Unlock locked administrators

c) Add, remove, update, reboot FAs

d) Make a FA boot floppy or USB drive

e) Create, delete an authentication service

f) View, enable, disable, permanently delete tunnels and terminate client tunnel sessions

g) Delete session

h) Force a logout of an administrator

i) Obtain and import digital certificates

j) Configure the system to run commands at scheduled times

k) View, enable, disable, or configure Concurrency Control

l) Query, modify, create, delete, backup and restore information flow security policy rules & manipulate security attributes

m) Query/view the audit trail

n) Query, modify, create, delete, backup and restore user accounts and user groups

o) Query/view, modify, delete, add secondary SMSs and SCSs

p) View/set SMS system parameters (including Log file parameters, parameters defining the SMTP and/or syslog server used for alarms, enable/disable alarm codes, FIPS-mode, and strong passwords)

q) Copy, backup, reinstall, setup, and restore the database

r) Verify the integrity of the configuration change files

s) View SMS/SCS and Brick status information.

t) Configure the alarm actions and alarm triggers

u) Rehome a brick].

6.1.5.16 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [Brick CLI administrator, SMS administrator and Group Administrator].

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

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [

a) secondary SMSs are installed and configured and connectivity is interrupted between the primary and secondary SMSs, provided connectivity is restored within 7 days

b) redundancy is configured and connectivity is interrupted between the FA and its homed SMS/SCS.]

6.1.6.2 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data transmitted from *disclosure*,

modification when it is transmitted between separate parts of the TOE.

6.1.7 FRU Resource utilisation

6.1.7.1 FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of [all the management and log collection capabilities, except possible loss of audit records and changes made to the security configuration that occur within the 5 seconds of the connection being lost] when the following failures occur: [

a) secondary SMSs are installed and configured and connectivity is interrupted between the primary and secondary SMSs, provided connectivity is restored within 7 days

b) redundancy is configured and connectivity is interrupted between the FA and its homed SMS/SCS.]

6.1.7.2 FRU_RSA.1 (1) Maximum quotas (transport layer quotas)

FRU_RSA.1.1 (1) The TSF shall enforce maximum quotas of the following resources: [transport layer representation[11]] that ***a source subject identifier*** can use *over a specified period of time*.

6.1.7.3 FRU_RSA.1 (2) Maximum quotas (intelligent cache management)

FRU_RSA.1.1 (2) The TSF shall enforce maximum quotas of the following resources: [session cache[12]] that ***the FA*** can **have active** *simultaneously*.

6.1.8 FTP Trusted path/channels

6.1.8.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the TSF* **or** *the remote trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [negotiation and establishment of a VPN tunnel].

[11] Transport layer representation refers specifically to the TCP SYN flood attack, where half-open TCP/IP connections are established thus exhausting the connection table resource.

[12] A session is a TCP connection, UDP packets or ICMP packets.

6.2 TOE Security Assurance Requirements

The Security assurance requirements (SARs) provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment). The table below identifies the security assurance requirements for the TOE drawn from CC Part 3: Security Assurance Requirements,

Assurance Class	Assurance Component ID	Assurance Component Name
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Basic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: security enforcing modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability	AVA_VAN.3	Focused vulnerability analysis

assessment		

Table 9: Security Assurance Requirements

6.3 Security Functional Requirements for the Operational Environment

This section presents the SFRs for the operational environment that are taken from the CC Version 3.1 or from the extended components defined in Section 5. The operational environment shall satisfy the SFRs stated in the table below which lists the names of the SFR components. These requirements do not levy any additional requirements on the TOE itself, but rather on the operational environment. Following the table, the individual functional requirements are restated with any necessary operations completed.

Functional Component ID	Functional Component Name
FIA_UAU_SRV.1	Authentication via authentication server
FIA_UID_SRV.1	Identification via authentication server
FMT_MTD.1 (8)	Management of TSF Data (Environment)
FPT_STM.1	Reliable Time Stamps
FAU_STG.1	Protected Audit Trail Storage

Table 10: Security Functional Requirements for Operational Environment

6.3.1 FMT_MTD.1 (8) Management of TSF data (Environment)

FMT_MTD.1.1 (8) The **IT Environment hosting the SMS/SCS** shall restrict the ability to *delete, clear, view and modify* the [All TSF data on the residing operating system] to [an authorized OS administrator].

6.3.2 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The **IT Environment hosting the SMS/SCS** shall provide reliable time stamps for **the TOE's** use.

6.3.3 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The **IT Environment hosting the SMS/SCS** shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The **IT Environment hosting the SMS/SCS** shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

6.3.4 FIA_UAU_SRV.1 Authentication via authentication server

FIA_UAU_SRV.1.1 When invoked by the TSF, the [RADIUS server] in the *IT Environment* shall determine if the user has provided valid

authentication data and pass the results of that determination back to the TOE.

6.3.5 FIA_UID_SRV.1 Identification via authentication server

FIA_UID_SRV.1.1 When invoked by the TSF, the [RADIUS server] in the *IT Environment* shall determine if the user has provided valid identification data and pass the results of that determination back to the TOE.

6.4 Security Requirements Rationale

6.4.1 Rationale For Not Satisfying All Dependencies

This section includes a table of all the TOE security functional requirements and their associated dependencies with a rationale for any dependencies that are not satisfied.

SFR	Dependencies	Met by the TOE?
FAU_ARP.1	FAU_SAA.1	YES
FAU_GEN.1	FPT_STM.1	NO, but addressed by OE.TMSTMP. FPT_STM.1 is an SFR on the operational environment
FAU_SAA.1	FAU_GEN.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FAU_SAR.3(1), (2)	FAU_SAR.1	YES
FAU_STG.4	FAU_STG.1	NO, but addressed by OE.ADMTRA. FAU_STG.1 is an SFR on the operational environment
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4 FMT_MSA.2	YES
FCS_CKM.2	FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	YES
FCS_CKM.4	FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1 FMT_MSA.2	YES

SFR	Dependencies	Met by the TOE?
FCS_COP.1(1) - (4)	FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	YES
FDP_IFC.1	FDP_IFF.1	YES
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	YES
FDP_RIP.1	None	N/A
FIA_AFL.1	FIA_UAU.1	YES, via FIA_UAU_TRD.1
FIA_ATD.1	None	N/A
FIA_SOS.1	None	N/A
FIA_UAU_TRD.1	FIA_UID.1 or FIA_UID_TRD.1 FIA_UAU_SRV.1	YES
FIA_UAU.5	None	N/A
FIA_UID_TRD.1	FIA_UID_SRV.1	NO, but addressed by OE.IDAUTH. FIA_UID_SRV.1 is an SFR on the operational environment
FMT_MOF.1 (1), (2), (3), (4)	FMT_SMF.1 FMT_SMR.1	YES
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	YES
FMT_MSA.2	ADV_SPM.1 FDP_ACC.1 or FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	YES
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	YES

SFR	Dependencies	Met by the TOE?
FMT_MTD.1 (1) – (7)	FMT_SMR.1 FMT_SMF.1	YES
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	YES, via FIA_UID_TRD.1.
FPT_FLS.1	ADV_SPM.1	YES
FPT_ITT.1	None	N/A
FRU_FLT.1	FPT_FLS.1	YES
FRU_RSA.1 (1), (2)	None	N/A
FTP_ITC.1	None	N/A

Table 11: SFR Dependencies

Functional Component FIA_AFL.1 depends on FIA_UAU.1 Timing of Authentication which requires users to be authenticated by the TOE prior to performing certain actions. This dependency is satisfied by FIA_UAU_TRD.1 Timing of Authentication which requires users to be authenticated by either the TOE or the IT environment prior to performing certain actions.

Functional Component FMT_SMR.1 depends on FIA_UID.1 Timing of Identification which requires users to be identified by the TOE prior to performing certain actions. This dependency is satisfied by FIA_UID_TRD.1 Timing of Identification which requires users to be identified by either the TOE or the IT environment prior to performing certain actions.

NOTE: Dependencies on SFRs for the IT Environment do not need to be met.

6.4.2 TOE SFR to TOE Security Objective Tracings

	O.IDANDA	O.INSPEC	O.DEFALT	O.DOMSEP	O.AUDREC	O.ACCOUN	O.SECFUN	O.CRYPTO	O.VPN
FMT_SMR.1							X		
FIA_ATD.1	X			X					
FIA_AFL.1	X			X		X			
FIA_SOS.1	X								
FIA_UID_TRD.1	X					X			

	O.IDANDA	O.INSPEC	O.DEFALT	O.DOMSEP	O.AUDREC	O.ACCOUN	O.SECFUN	O.CRYPTO	O.VPN
FIA_UAU_TRD.1	X			X					
FIA_UAU.5	X								
FTP_ITC.1	X								X
FDP_IFC.1		X							X
FDP_IFF.1		X							X
FRU_RSA.1 (1), (2)		X		X					
FMT_MSA.1			X				X		
FMT_MSA.2								X	X
FMT_MSA.3		X	X				X		
FDP_RIP.1		X							
FAU_ARP.1						X			
FAU_GEN.1					X	X			
FAU_SAA.1						X			
FAU_SAR.1					X				
FAU_SAR.3 (1), (2)					X	X			
FAU_STG.4						X	X		
FMT_MOF.1 (1) - (4)			X				X		
FMT_MTD.1 (1) – (7)			X				X		
FMT_SMF.1			X				X		
FPT_ITT.1								X	
FCS_COP.1 (1), (3), (4)								X	X
FCS_COP.1 (2)								X	
FCS_CKM.1								X	X
FCS_CKM.2								X	X
FCS_CKM.4								X	X
FPT_FLS.1				X					
FRU_FLT.1				X					

Table 12: Tracings between TOE SFRs and Security Objectives

6.4.3 TOE SFR to TOE Security Objective Rationale

O.IDANDA

FIA_ATD.1 exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user.

FIA_AFL.1 exists to minimize guessing the authentication information of authentic users by brute force method. A user account is locked until further actions are taken by an authorized administrator when a predefined number of consecutive unsuccessful login attempts are reached.

FIA_SOS.1 exists to reduce the possibility that attempting to guess the authentication information of authentic users by brute force method will succeed by requiring complex passwords.

FIA_UID_TRD.1 ensures that before any operations other than those mentioned in the requirement occurs on behalf of a user, the user's identity is verified by the TOE or IT environment.

FIA_UAU_TRD.1 ensures that users are authenticated at the TOE by either the TOE or the TOE environment before any operations other than those mentioned in the requirement occurs on behalf of the user. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator.

FIA_UAU.5 requires the TOE to provide two different authentication methods: password and certificate.

FTP_ITC.1 ensures that a trusted channel is established for VPN sessions and that the trusted channel provides assured identification of tunnel endpoints.

O.INSPEC

FDP_IFC.1 identifies the entities involved in the TRAFFIC FILTER information flow control SFP (i.e., users sending information to other users and vice versa).

FDP_IFF.1 identifies the attributes of the users sending and receiving the information in the TRAFFIC FILTER SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow and whether or not that flow is encrypted/decrypted.

FRU_RSA.1 (1) and (2) were chosen to ensure that the TSF is capable of protecting itself against denial of service attacks.

FDP_RIP.1 ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows.

FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules.

O.DEFALT

FMT_MOF.1 (1) and (3) define the behavior of the SMS management security functions.

FMT_MOF.1 (2) defines the behavior of the security function to delete sessions using the Brick CLI.

FMT_MOF.1 (4) defines the behavior of the security function to reboot bricks using SMS management interfaces or the Brick CLI.

FMT_MSA.1 ensures that the TSF provides the SMS administrator or Group administrator with the ability to manipulate the security attributes to define a ruleset.

FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules.

FMT_MTD.1 (1) – (5) and (7) ensure that the TSF provides the SMS administrator or Group administrator with the ability to manage the TSF data (e.g., query the audit trail, create user accounts, configure alarms, etc.).

FMT_MTD.1 (6) ensures that the TSF provides the Brick CLI administrator, SMS administrator or Group administrator with the ability to query the information flow security policy rules.

FMT_SMF.1 defines the management functions provided by the TOE, which includes SMS, Brick CLI, database, and other utilities.

O.DOMSEP

FIA_ATD.1 exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user.

FIA_AFL.1 exists to minimize guessing the authentication information of authentic users by brute force method. A user account is locked until further actions are taken by an authorized administrator when a predefined number of consecutive unsuccessful login attempts are reached.

FIA_UAU_TRD.1 ensures that users are authenticated at the TOE by either the TOE or the TOE environment before any operations other than those mentioned in the requirement occurs on behalf of the user. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator.

FRU_RSA.1 (1) and (2) were chosen to ensure that the TSF is capable of protecting itself against denial of service attacks.

FRU_FLT.1 ensures that when redundancy is configured, management and log collection services continue after connectivity is interrupted between the FA and its homed SMS/SCS. It also ensures that when secondary SMSs are installed and configured, management and log collection services continue after connectivity is interrupted between the primary and secondary SMSs, provided connectivity is

restored within 7 days.

FPT_FLS.1 ensures that when redundancy is configured, the TOE preserves a secure state after connectivity is interrupted between the FA and its homed SMS/SCS and when secondary SMSs are installed and configured, the TOE preserves a secure state after connectivity is interrupted between the primary and secondary SMSs, provided connectivity is restored within 7 days.

O.AUDREC

FAU_GEN.1 outlines what data must be included in audit records and what events must be audited.

FAU_SAR.1 ensures that the audit trail is understandable.

FAU_SAR.3 (1) ensures that a variety of searches can be performed on the audit trail. FAU_SAR.3 (2) ensures that sorting of the audit data can be performed based on the chronological order of audit event occurrence. The TOE provides a Log Viewer tool where filters can be created based on the presumed subject address and range of addresses. When the filter is applied against the log data the relevant data matching against the filter is fetched and displayed. Before the filter is applied the range of dates for which the filtered audit data is requested can be mentioned in one of the screens of the Tool. The data is displayed in manner suitable for sorting by clicking on the heading section tab of each column.

O.ACCOUN

FIA_AFL.1 exists to minimize guessing the authentication information of authentic users by brute force method. A user account is locked until further actions are taken by an authorized administrator when a predefined number of consecutive unsuccessful login attempts are reached.

FIA_UID_TRD.1 ensures that before anything other than those mentioned in the requirement occurs on behalf of a user, the user's identity is verified by the TOE or IT environment.

FAU_ARP.1 ensures that the TSF can detect potential security violations and take the appropriate action.

FAU_GEN.1 outlines what data must be included in audit records and what events must be audited.

FAU_SAA.1 ensures that the TSF can detect when a basic threshold of security violations have been reached.

FAU_SAR.3 (1) ensures that a variety of searches can be performed on the audit trail. FAU_SAR.3 (2) ensures that sorting of the audit data can be performed based on the chronological order of audit event occurrence. The TOE provides a Log Viewer tool where filters can be created based on the presumed subject address and range of addresses. When the filter is applied against the log data the relevant data matching against the filter is fetched and displayed. Before the filter is applied the range of dates for which the filtered audit data is requested can be mentioned in one of the screens of the Tool. The data is displayed in manner suitable for sorting by clicking on the heading section tab of each column.

FAU_STG.4 ensures that the authorized administrator will be able to take care of the audit trail if it should become full. Further it ensures that if the space allocated for all audit records exceeds, the FA will halt all traffic through itself with the exception of Administrator traffic. This component ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. Once the audit trail is restored to a non full status the FA will no longer halt traffic and resume its regular operation. The maximum number of audit records that could be lost is 656 (assuming that the average message size is 100 bytes and the queue is 65,536 bytes (64K)).

O.SECFUN

Each of the CC class FMT components in this Security Target depend on FMT_SMR.1 which defines the role(s) provided by the TOE.

FAU_STG.4 ensures that the authorized administrator will be able to take care of the audit trail if it should become full. Further it ensures that if the space allocated for all audit records exceeds, the FA will halt all traffic through itself with the exception of Administrator traffic. The authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status.

FMT_MOF.1 (1) and (3) define the SMS management/administration/security functions.

FMT_MOF.1 (2) defines the security function to delete sessions using the Brick CLI.

FMT_MOF.1 (4) defines the behavior of the security function to reboot bricks using SMS management interfaces or the Brick CLI.

FMT_MSA.1 ensures that the TSF provides the SMS administrator or Group administrator with the ability to manipulate the security attributes to define a ruleset.

FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules.

FMT_MTD.1 (1) – (5) and (7) ensure that the TSF provides the SMS administrator or Group administrator with the ability to manage the TSF data (e.g., query the audit trail, create user accounts, configure alarms, etc.).

FMT_MTD.1 (6) ensures that the TSF provides the Brick CLI administrator, SMS administrator or Group administrator with the ability to query the information flow security policy rules.

FMT_SMF.1 defines the management functions provided by the TOE, which includes SMS, Brick CLI, database, and other utilities.

O.CRYPTO

FPT_ITT.1 requires that the communications between separate parts of the TOE protect the TSF data being transmitted from unauthorized modification and disclosure.

FMT_MSA.2 ensures that the security attributes (keys) used for the cryptographic operations performed by the TOE are secure and non-trivial.

FCS_CKM.1 provides secure communications between the TOE components. This component ensures that the keys used for the cryptographic operations are generated using a FIPS 140-2 approved method.

FCS_CKM.2 requires the use of IKEv1 or IKEv2 for cryptographic key distribution in VPNs.

FCS_CKM.4 provides secure communications between the TOE components. This component ensures that the keys used for the cryptographic operations are destroyed using a FIPS 140-2 approved method.

FCS_COP.1 (1) provides encryption services between the TOE components and between the TOE and approved IPSec clients.

FCS_COP.1 (2) provides message hashing for secure communications between the TOE components).

FCS_COP.1 (3) and (4) perform IKE and digital signature generation and verification between the TOE and approved IPSec clients.

O.VPN

FDP_IFC.1 identifies the entities involved in the TRAFFIC FILTER information flow control SFP (i.e., users sending information to other users and vice versa).

FDP_IFF.1 identifies the attributes of the users sending and receiving the information in the TRAFFIC FILTER SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow and whether or not that flow is encrypted/decrypted.

FTP_ITC.1 ensures that a trusted channel is established for VPN sessions and that the trusted channel provides assured identification of tunnel endpoints.

FMT_MSA.2 ensures that the security attributes (keys) used for the cryptographic operations performed by the TOE are secure and non-trivial.

FCS_CKM.1 provides secure communications between the IPSec client and the FAs or between the two FAs. This component ensures that the keys used for the cryptographic operations are generated using a FIPS 140-2 approved method.

FCS_CKM.2 requires the use of IKEv1 or IKEv2 for cryptographic key distribution in VPNs.

FCS_CKM.4 provides secure communications between the IPSec client and the FAs or between the two FAs. This component ensures that the keys used for the cryptographic operations are destroyed using a FIPS 140-2 approved method.

FCS_COP.1 (1) provides encryption services between the TOE components and between the TOE and approved IPSec clients.

FCS_COP.1 (3) and (4) perform IKE and digital signature generation and verification between the FA and approved IPSec clients or between the two FAs.

6.4.4 SAR Rationale

The TOE and this ST are EAL4 conformant, augmented with ALC_FLR.1.

EAL4 was chosen to provide a moderate to high level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment. EAL4 was chosen to provide a moderate to high level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. Additionally, the product vendor has specific customer requests for the evaluation of the TOE at this assurance level. These potential customers of the product vendor have determined for their own networks that an EAL4 evaluation of the product will provide satisfactory assurance.

EAL4 is augmented with ALC_FLR.1 to assist in ensuring that discovered security flaws are tracked and are corrected by the developer and that TOE users are aware of how to report a security flaw and receive corrective fixes.

7 TOE Summary Specification

This section presents a description of how the TOE SFRs are satisfied.

TOE SFR	Description of how the TOE meets the SFR
FAU_ARP.1 FAU_SAA.1	The TOE can be configured to detect potential security violations (alarm events) and take an appropriate action. The TOE can detect when a basic threshold of security violations have been reached (alarm trigger). The SMS/SCS provides the Administrator with an automated alarms tool that reviews audit logs for configurable alarming events, and when found, notifies the administrator. The SMS provides the ability to create alarm triggers and actions to notify Administrators of events occurring in the system. Alarm triggers are the conditions required to generate an alarm. There are many types of alarm triggers. The security-relevant alarm triggers are defined in Table 8: Alarm Triggers An alarm action defines how the administrator is notified that an alarm was generated. Alarm actions included in the evaluated configuration are: e-mail, syslog message, SNMP trap, and console message. Administrators configure alarm triggers and assign actions to the trigger. Alarm triggers can be associated with information security flow rules using an alarm code. When an alarm code is embedded in a rule and the rule is invoked a specified number of time within a specific time frame, an alarm is generated. The SMS and SCS handle alarms identically, except that the console message action on the SCS forwards the action contents to the associated SMS. Other alarm actions are directly performed by the SCS.
FAU_GEN.1	The FA detects the occurrence of selected events, gathers information concerning them, and sends that information to the SMS or SCS. The SMS/SCS also detects the occurrence of selected events (e.g., security administrator actions performed on the SMS/SCS), gathers information concerning them, and records it. Audit reporting and alarm features are also provided by the SMS/SCS. The reporting feature of the ALVF allows Administrators to view and analyze internal and system information of the ALVF. Using Report Wizards, audit event items can be extracted and presented in a legible and coherent format. Selected administrative actions performed on the Brick CLI are audited. The audit records are sent to the SMS and placed in the Administrative Events Log for storage.

	The audit events are recorded in the Administrative Events Log, the Session Log, the VPN log, the User Authentication log, and the Proactive Monitoring log. The types of events recorded in each log is defined in *Alcatel-Lucent Security Management Server (SMS), Release 9.1, Reports, Alarms, and Logs Guide*. The security-relevant types of audit events are defined in the FAU_GEN.1 SFR. The ability to audit the startup and shutdown of the audit functions is provided by the ability to startup and shutdown the application which automatically starts up and shuts down auditing. The FA records the start and end of a session. It extracts information from the session cache to uniquely identify each session, and it records: a) Start and stop times b) Action taken c) Statistics, such as number of bytes and packets passed The FA bundles this information into an audit message and sends it to an awaiting audit server, located on the SMS/SCS. The SMS/SCS logs session info sent to it by FA, and logs operational information from all SMS/SCS Subsystems (including FA Subsystems). The SMS/SCS reformats the log events it receives, applies a time stamp from the native SMS/SCS operating system clock, and writes the event to the appropriate log file on the associated SMS/SCS. The SMS/SCS uses the clock setting on the resident operating system (TOE Environment) to generate timestamps for audit records. When SCSs are used to collect data, an NTP server is required in the TOE environment to ensure that the time is synchronized between the SCSs and the SMS. Synchronizing the time allows administrators to correlate the audit events stored on the separate servers. The auditable events mentioned in Table 7: Auditable Events are audited in the above mentioned logs (Session, Administrative Events, User Authentication,VPN log, and Proactive Monitoring). All log records are required to include the following information: o Type o Source Type (e.g., SMS process, Brick, Proxy Server) o Source (e.g., subsystem name, brick name, or proxy name) o Timestamp (time that the logger received and processed the record) o Outcome of the event
FAU_SAR.1	The SMS/SCS enables an Administrator to view critical user and

	system information (e.g., FA up/down status and logged on users, etc). This ability is also provided by the SMS Status utility. The SMS/SCS also enables Administrators to monitor the configuration of and access to the FA deployed throughout the network. The SMS/SCS provides a Log Viewer which provides the administrator the capability to read the audit trail from User Authentication logs, Session logs, Administrative Events logs, Proactive Monitoring (promon) logs, and VPN logs. These logs can be viewed real-time or historically. The log viewer enables creation of filters to filter the audit data based on log filter parameters and the type of log that has to be processed. Reports are generated using logged administrative events and FA session log data. SMS/SCS Administrators can run reports for any group. Group Administrators can only run reports for groups for which they have at least View privileges. Reports cannot display real time information, as logs can, they do allow access to the same information as contained in the historical logs from any location, except for promon information. Only the log viewer provides access to promon information. The report "wizards" are displayed to enable Administrators to filter and sort data. Through this interface, the administrator has the capability to generate "Memorized Reports" (i.e., report templates) and to generate Closed Session, Session, and Administrative Events reports. While logged into the SMS or SCS, administrators can view all audit trail data.
FAU_SAR.3(1), (2)	The SMS/SCS provides a Log Viewer which provides authorized administrators with the ability to perform searches on the audit data based on user identity, presumed subject address, range of dates, times, and addresses and perform sorting based on the chronological order of audit event occurrence The information contained in the audit logs can be retrieved through filtering and sorting options provided in the Reporting subsystem. Reports are based on records from an audit log. Each line in an audit log is a record. A record consists of fields and each field contains a value. Some fields can be filtered to look for specific user-defined values. Logical "AND" and "OR" functions can be performed across filterable fields. A report 'wizard' enables the user to specify values for filterable fields to hone in on field criteria values. The 'wizard' permits selection of fields on which to sort and allows selection of sorting direction (ascending or descending). When generating an Administrative Events or Session Log report, the ability to search the raw log file by entering a text string is also provided. Reports are generated using logged administrative events and FA

	session log data. Reports cannot display real time information, as logs can, they do allow access to the same information as contained in the historical logs from any location, except for promon information. Only the log viewer provides access to promon information. The report "wizards" are displayed to enable Administrators to filter and sort data. Through this interface, the administrator has the capability to generate "Memorized Reports" (i.e., report templates) and to generate Closed Session, Session; and Administrative Events reports.
FAU_STG.4	The SMS/SCS provides the authorized administrator with the capability to configure the log file maximum size and the amount of disk space to allocate for all logs together in a directory. When an audit file reaches the configured log file size or a new day is started, the SMS/SCS closes the current log file and starts a new audit file. This goes on until the log file directory is full. The SMS/SCS must be configured to not lose audit data and halt the traffic through the FA if any of the log directories reach the maximum allotted size. When the contents of the log directory reach the configured maximum size, disk space has to be reclaimed by an administrator of the residing operating system by clearing the log files to create space to allow traffic through the FA. This capability can be separately configured for each of the logs (Administrative Events, Session, User Authentication, Proactive Monitoring, and VPN). The audit storage management architecture ensures that if audit data storage exhaustion takes place, the brick stops passing traffic. An authorized administrator configures the SMS in such a way not to lose any audit data and halt the FA if any of the log directories reach the maximum allocated size. When disk space of the log directories reaches the configured limit, disk space needs to be reclaimed by an administrator of the resident operating system, by clearing the log directories to create space and allow traffic through the FA. This mechanism ensures that audit records are not lost if audit trail is full. The Configuration Assistant utility also provides the ability to manage audit disk space allocation.
FCS_CKM.1	The TOE generates cryptographic keys that are used for protected communications between the separate TOE components. The keys that are used for encryption and hashing during the ALVF protected channel are based on parts of the key negotiated during Diffie-Hellman key agreement. A FIPS 140-2 approved Pseudo Random Number Generator (PRNG) is used to generate keys that are used during the cryptographic communication process. The usage of the PRNG ensures that non-trivial keys are generated.

	The TOE also generates cryptographic keys (compliant with FIPS 140-2 approved) that are used for IKE. See Section 7.1 for more information on the FIPS 140-2 cryptographic support provided by the TOE.
FCS_CKM.2 FCS_COP.1 (3)	The TOE distributes cryptographic keys used during IKE authentication in a FIPS 140-2 approved way. IPSec key management can be manual or Internet Key Exchange (IKE). IKE establishes shared tunnel security parameters and authenticated keys between IPSec peers. IKE is performed on the FA. This protocol provides the assured identification and authentication of the tunnel endpoints. The IKE protocol relies upon the following cryptographic services: key distribution, key exchange, message hashing, and digital signature generation and verification. If the manual key exchange is used, an administrator must create the SAs. The IPSec and IKE implementation in the TOE is FIPS-140-2 compliant. See Section FIPS 140-2 Compliance for more details on the cryptographic services provided by the TOE. The Certificate Manager utility is used to obtain and import digital certificates. See Section 7.1 for more information on the FIPS 140-2 cryptographic support provided by the TOE.
FCS_CKM.4	All keys stored by the TOE are destroyed by overwriting the old keys with new keys. All ephemeral keys are destroyed when cryptographic modules of the TOE reboot. All key destruction mechanisms used are FIPS 140-2 compliant. The TOE destroys cryptographic keys that are used for communications between the SMS Remote Navigator, SMS application and the FA in a FIPS 140-2 approved way. See Section 7.1 for more information on the FIPS 140-2 cryptographic support provided by the TOE.
FCS_COP.1 (1)	The TOE provides encryption services between the TOE components and between the TOE and approved IPSec clients. The encryption services are used as a means for its distributed components (SMS application, FA, Web server, CLI and GUI (SMS Navigator, SMS Remote Navigator)) to communicate through an encrypted socket connection which provides confidentiality and integrity of the data transmitted. See Section 7.1 for more information on the FIPS 140-2 cryptographic support provided by the TOE.

FCS_COP.1 (2)	The TOE provides message hashing for secure communications between the SMS application, FAs, Web server, CLI and the GUI (SMS Navigator, SMS Remote Navigator) to communicate through an encrypted socket connection which provides confidentiality and integrity of the data transmitted. See Section 7.1 for more information on the FIPS 140-2 cryptographic support provided by the TOE.
FCS_COP.1 (4)	The FA provides digital signature services used in the implementation of the IPSec and IKE protocols. See Section 7.1 for more information on the FIPS 140-2 cryptographic support provided by the TOE.
FDP_IFC.1 FDP_IFF.1	The FA controls the incoming and outgoing IP packets and imposes security policy to filter them. The policy rulesets are then pushed from the SMS to the operating system (Inferno) on the FA. The FA extracts information from the IP packet header and applies rules from a security policy. The default is DROP, which means the FA will discard the packet and not allow it through. Unless an authorized administrator explicitly configured the FA to accept requests based on specific security attributes; the ALVF will successfully reject any and all requests. Security rules in the security policy perform this traffic filtering function based on pieces of information (security attributes) in each packet to determine if they match the same information in the rule. These security attributes include the direction of the packet, source address, destination address, direction of flow and service, and transport protocol. Attributes of an IP packet are compared to the rule properties as defined in FDP_IFF.1. Application filters provide the application layer validation, inspection, and access control. The application filters included in the evaluated configuration are provided for FTP, HTTP, H.323 VoIP, H.323 RAS, DHCP Relay, TFTP, Oracle SQL*Net, Microsoft NetBIOS, SUN RPC, DNS, SMTP, and SIP services. Many of the application filters check for protocol anomalies. The application filters provide additional capabilities, such as delaying responses to invalid FTP user names, dropping reconnect attempts, DHCP relaying, discarding additional resource record sections in DNS responses, and blocking queries of the root node in the DNS DB. In addition to the above mentioned security attributes there exists a field in the policy rule that defines the action that the FA will take when it encounters a packet that matches all the information in the above four fields. The default is “DROP”, which means the FA will discard the packet and not allow it through. To allow a

	matching packet through the FA unmodified, the field must be set to “PASS”. To encrypt or decrypt a matching packet prior to allowing it through the FA, the action field must be set to “VPN”. The Virtual Private Network field defines when packets are encrypted or decrypted. Packets are allowed to pass through the TOE only if the defined rules are met. The ALVF implements VPNs using the IPSec protocol. IPSec is a framework of open standards used to provide private, secure network communications. The cryptographic operations used are determined by the IPSec Security Association (SA) which is defined by the packet’s destination IP address, a security protocol (e.g., encryption/authentication types and keys), and a unique identification value, called a Security Parameter Index (SPI). The SA associates the security services and a key with the network packets being protected. The IPSec protocol relies upon the following cryptographic services: encryption and decryption of VPN traffic, message hashing, and digital signature generation and verification. The TOE provides the ability to create both LAN-LAN and client tunnels. Both LAN-LAN and client tunnels authenticate the devices/hosts via a preshared key or certificate. Client tunnels perform also user authentication.
FDP_RIP.1	The TOE ensures that the residual information is unavailable to other resources. When packets arrive on a FA interface they are written into memory for processing. The packet overwrites information previously stored in that memory location. Pointers are used by the operating system to identify the beginning and ending of each packet in memory. The correct operation of these pointers ensures that data from a prior packet stored in memory is not inadvertently included in a later packet.
FIA_AFL.1	If the administrator makes a configurable number of consecutive unsuccessful authentication attempts then the user account is locked until it is unlocked by another authorized administrator. If the administrator configures the system to disable the administrator after 0 failed login attempts, the user will never be disabled due to failed attempts. Even the last SMS Administrator is locked after the configured number of unsuccessful consecutive attempts is reached, so the administrator guidance instructs the Administrators to ensure that there are at least 2 SMS administrators at any given time.

FIA_ATD.1	A brick can also be accessed from the brick console. The Brick CLI password is stored on the brick. The SMS provides the ability for the System Administrator accounts to create other accounts. The user attributes for user accounts are stored in the SMS relational database. The user attributes include: • identity of the SMS administrative users and VPN users • user's password if configured for local password authentication • user's certificate is if configured for certificate authentication • role and assigned privileges.
FIA_SOS.1	The TOE requires users who are authenticated via the local password mechanism to use a complex password. Using the Configuration Assistant, the SMS must be configured to require a strong password that is designed to comply with the Sarbanes-Oxley (SOX) requirements. The strong password option is enabled by default. When enabled, the strong password requirements apply to new or changed passwords for: • Local passwords for user accounts, including the master user created during installation • Local passwords for administrator accounts • Brick CLI passwords For local password authentication, the password complexity rules when the strong password option is enabled are: • The password must be a minimum of 8 characters or the minimum password length set for the local password authentication service, whichever is greater • The password must contain at least one alphabetic character and one non-alphabetic character; • The password cannot contain 3 or more repeated alphanumeric characters in a row • The password cannot contain 3 or more consecutive, ascending or descending, alphanumeric characters in a row • The password cannot contain the User account name or its mirror (reverse character format) • The password cannot be one of the previous 3 most recently used passwords. Except for Brick CLI passwords, the password expires in an

	administrator configurable value of 30-120 days. In addition, the TSF can be configured to require that the password contain at least one non-alphabetic character that is not in the first or last position (this is disabled by default).
FIA_UAU_TRD.1 FIA_UID_TRD.1	The TOE requires that SMS administrative users and VPN users be identified and authenticated prior to accessing most security-related functions. Brick CLI administrative users must be authenticated prior to accessing the Brick CLI. Non-VPN users sending information through the TOE are not authenticated (unauthenticated information flows). If the administrator is logged in to the SMS host, the DB utilities, Start Services, Stop Services, Restart Services, SMS Status, Configuration Assistant, Schedule Editor, and New Feature Setup are available prior to the administrator identifying and authenticating to the SMS. The SMS can be configured to require that users be authenticated by either the TOE or the IT environment. All administrative users logging into the administrative interfaces of the SMS/SCS are authenticated by the SMS's local password authentication mechanism or RADIUS server. The administrator provides his user identifier and authentication data within the SMS Navigator or SMS Remote Navigator login window. A Java based GUI is installed on the System Administrator's desktop to provide the Primary User Interface and to secure the communications between the Java GUI and the SMS. The GUI manages the administrator's interface. This includes interacting with the administrator management screens presented within the GUI JVE (Java Virtual Environment) to provide the appropriate Java GUI in response to administrator's input. Such interactions include – based on type of administrator (SMS or Group) administrator input, presenting the System Administrator interface the appropriate Java GUI for management of System Administrator accounts, logging, and group management. The SMS enforces the role/privilege required to perform management functions. If configured for external authentication, the SMS transmits the userID and authentication information provided to it to the configured external authentication server (RADIUS) for verification. The external authentication server sends the results of the authentication check to inform the SMS whether or not the user is successfully authenticated. The Brick CLI requires users to authenticate themselves when the Brick CLI is accessed via the Local Connection or Local Serial

	Port connection. The Brick CLI does not require users to identify themselves when using these access methods, however physical access to the device is required. The Brick CLI password is stored on the brick. When the Brick CLI is accessed from either of the Remote Console Connections, the user is required to login to the SMS. For client tunnels in the evaluated configuration, VPN users are identified and authenticated using one of four different mechanisms. The mechanism used to identify and authenticate users is configured by the administrator on a user-by-user basis. The only action that VPN users can perform before identification and authentication is unauthenticated information flows. For client tunnels in the evaluated configuration, VPN users are identified and authenticated by the SMS's local password authentication mechanism, local certificate authentication or RADIUS server. For local password authentication, the user provides their user identifier and password. For RADIUS authentication, the user provides the information requested by the RADIUS server, which is located in the TOE environment. For certificate authentication, the user must provide a password to unlock or access their certificate, which was generated by an external CA located in the TOE environment. For local password authentication, the TOE verifies the validity of the provided userID and password. For VPN certification authentication, the TOE verifies the validity of the certificate. For RADIUS authentication, the RADIUS server checks the validity of the identification and authentication data and sends the results to the TOE. For LAN-LAN tunnels, the endpoints are authenticated using only either a preshared key or a certificate. There is no VPN user authentication for LAN-LAN tunnels.
FIA_UAU.5	The TOE has the ability to authenticate VPN users using RADIUS authentication, local password or certificate authentication. The TOE has the ability to authenticate administrators using RADIUS authentication and local password authentication. The SMS uses user associated account information to make authentication decisions that are based upon the userID and password provided to it.

FMT_MOF.1 (1)	The SMS provides ability to start-up and shutdown, unlock locked administrator accounts, make a FA boot floppy or USB drive, create an authentication service, terminate client sessions, view status information for SMS/SCS and bricks, and add, remove and update FAs. The SMS Navigator and SMS Remote Navigator provide the interface to the SMS to perform these functions. Utilities also provide the ability to start, stop, and restart SMS services. The SMS is used to configure alarm actions, triggers, and codes and associate them with rules. Prior to configuring an e-mail or syslog action, SMTP or syslog servers must have been configured using the Configuration Assistant.
FMT_MOF.1 (2)	A brick can also be accessed from the brick console. The Brick CLI provides commands for query and troubleshooting purposes by the Brick CLI administrator. Sessions can be deleted from the Brick CLI. Deleting a session removes it from the session cache, resulting in the network session being disconnected.
FMT_MOF.1 (3)	Management of security functions behavior (SMS Admin) The SMS Navigator and SMS Remote Navigator provide the ability to force a logout of an administrator and the ability to view, enable, disable, configure Concurrency Control by an SMS administrator.
FMT_MOF.1 (4)	Management of security functions behavior (Reboot) The SMS Navigator, SMS Remote Navigator, SMS CLI, and Brick CLI provide the ability to reboot FAs.
FMT_MSA.1	The SMS Navigator, SMS Remote Navigator, and SMS CLI provide ability for SMS administrators and Group administrators to create additional security attributes that can be used in specifying information flow policy rules (for example, a set of network addresses that can be used as a “group”). The Firewall Appliance permits the security policies to be loaded into the FA from the SMS. The administration applications of the SMS also provide system status information.
FMT_MSA.2	The TOE uses secure and non-trivial security attributes (cryptographic keys) while performing the various cryptographic operations i.e. the TSF shall ensure that only secure values are accepted for these cryptographic keys. The cryptographic modules used in secure communications have strict requirements on the values of the attributes used in satisfying the cryptographic modules. The modules are FIPS 140-2 compliant.

FMT_MSA.3	The TSF provide restrictive default values for the information flow security attributes which can be overridden and managed by users in certain roles. By default, the policy rules drop packets. The TOE does not allow default values to be specified for general policy-based filtering. Default values are allowed for LAN-LAN and Client-LAN tunnels. The SMS and Group administrators can then alter these values to allow creation of Zone policy rulesets for appropriate information flow. These rulesets include the ability to require encryption/decryption of the information flow The SMS Navigator, SMS Remote Navigator, and SMS CLI provide ability for SMS administrators and Group administrators to create modify the information flow security policy rules. All modifications to the policy information of the SMS are stored in the SMS relational database (DB), which provides storage for the TSF configuration data. Since the SMS is on a private network protected by the FA and installation guidance requires security policy rulesets preventing access to the DB from the public network, the DB can only be accessed by the components of the TOE.
FMT_MTD.1 (1)	The SMS Navigator, SMS Remote Navigator, and SMS CLI provide the ability to modify, delete and create information flow security polices. These policies include the rules for information flows, encryption/decryption, and alarm configuration. Group security policies can be created in accordance with a corporate security policy on behalf of the Administrators. The SMS/SCS is responsible for the Administrator zone security policy specified rules, host groups, domain name groups, service groups, dependency masks, and VPN information and encoding it (policy compilation) into a file format suitable for local storage and/or downloading to a FA Subsystem. The dependency mask is a tool that allows an Administrator to set up a dependency between a particular rule in a brick zone ruleset and a specific session in the session cache. This means that even if a packet matches the rule, and the rule is a pass rule, that packet will still not be permitted to pass through the brick until the brick verifies that a certain session, identified in the dependency mask, already exists in the session cache. SMS administrators and corresponding group administrators can manage the information flow security policy rulesets.
FMT_MTD.1 (2)	The SMS Navigator, SMS Remote Navigator, and SMS CLI provide the ability to view the audit trail. This capability is also provided by the LogViewer. SMS administrators and corresponding group administrators can view the audit trail.

FMT_MTD.1 (3)	The SMS Navigator and SMS Remote Navigator provide the ability to modify, delete and create user attributes for both administrator accounts and VPN user accounts. SMS administrators and corresponding group administrators can perform these functions for VPN user. Only SMS administrators can edit other administrative accounts.
FMT_MTD.1 (4)	The SMS Navigator and SMS Remote Navigator provide the ability to create user accounts and user groups. SMS administrators and corresponding group administrators can perform these functions. The first SMS Administrator login is created automatically during the software installation process. This administrator can then create other administrator accounts (SMS and Group).
FMT_MTD.1 (5)	The SMS Navigator and SMS Remote Navigator provide the ability to view, add, modify, and delete secondary SMSs or SCSs. Only an SMS administrator can perform these functions.
FMT_MTD.1 (6)	The SMS Navigator, SMS Remote Navigator, and SMS CLI provide the ability to view the information flow security policy rulesets. These interfaces can be used by an SMS administrator or a corresponding Group administrator. The Brick CLI provides commands for query and troubleshooting purposes by the Brick CLI administrator. No configuration changes can be made from the Brick CLI. The information flow security policy rules can be queried.
FMT_MTD.1 (7)	The SMS Navigator and SMS Remote Navigator provide the ability for an SMS administrator or a Group administrator to view and configure alarm actions and alarm triggers. These alarm triggers and actions are configured on a per-Administrator basis and are not shared among Administrators.
FMT_SMF.1	The TOE's management functions are provided by the SMS Navigator, SMS Remote Navigator, SMS CLI, Brick CLI, Utilities (including DB utilities). The administrative guidance is provided for securely administering the TOE using these interfaces. The SMS Navigator and SMS Remote Navigator provide the capability to: • Startup and shutdown the application which automatically starts and stops the audit functions • Unlock locked administrators • Add, remove, reboot FAs • Make a FA boot floppy or USB drive

	• Create, delete an authentication service • View, enable, disable, permanently delete tunnels • Terminate client tunnel sessions • Delete session • Force a logout of an administrator • Configure the system to run commands at scheduled times • Enable/disable alarms • View, enable, disable, or configure Concurrency Control • Query, modify, create, delete, backup and restore information flow security policy rules (including the ability to keep or clear the FA session cache when applying changes and to configure tunnel rules) and manipulate security attributes • Query/view the audit trail • Query, modify, create, delete, backup and restore user accounts and user groups • Query/view, add, modify, delete secondary SMSs and SCSs • View SMS/SCS and Brick status information • View / configure alarm actions and alarm triggers • Rehome a brick The SMS CLI provides the capability to: • Add, remove, reboot FAs • Query, modify, create and delete information flow security policy rules • View, enable, disable, permanently delete tunnels • Rehome a brick The database utilities provide the ability to: • Copy, backup, reinstall, setup, and restore the database, which includes information flow security policy rules and user attribute values • Verify the integrity of the configuration change files The Brick CLI provides the capability to: • Make a FA boot floppy or USB drive • Reboot FAs

	• Delete session • Query information flow security policy rules The Configuration Assistant utility provides the ability to view/set SMS system parameters, including: • configure the SMTP and/or syslog servers used when an alarm is triggered • enable/disable alarm codes • require a strong password that is designed to comply with the Sarbanes-Oxley (SOX) requirements • view/set Log file parameters, including file size and allocated disk space • disable or enable and configure FIPS 140-2 mode. The SMS Navigator, SMS Remote Navigator and utilities (SMS Status and Log Viewer) provide the ability to query/view the audit trail.
FMT_SMR.1	There are two types of roles in the TOE: SMS roles and the Brick CLI role. There are two SMS roles: Group administrators and SMS administrators. SMS Administrators have full privileges over all groups, which means they can access all functional areas in all groups and make any additions, modifications, or deletions they deem necessary. The functional areas are devices (bricks), policies & VPN (rulesets, tunnels, authentication services), and users and user groups. Group Administrators can only access the specific groups to which they are assigned. In addition, Group Administrators can be given three levels of privilege over the functional areas in their groups: None, View and Full. The Brick CLI administrator is the role required to use the Brick CLI from one of the local Connection methods. Any user with the Brick CLI password and physical access to the TOE is a Brick CLI administrator.
FRU_RSA.1(1)	The ALVF implements SYN flood protection and robust fragment reassembly to protect against denial-of-service attacks. The brick provides rule-based SYN flood protection that can be activated from the SMS. This feature allows the administrator to allow certain sessions through, to set a threshold for the number of half open sessions allowed, and to set a countdown timer controlling how long half open sessions remain open after the threshold is reached. The robust fragment reassembly feature frees single reassembly queues when the threshold is reached.

FRU_RSA.1(2)	The ALVF implements intelligent cache management to protect against denial-of-service attacks. When the intelligent cache management feature is activated, the brick will periodically scan its session cache and remote established sessions to free session cache memory as needed.
FPT_ITT.1	The SMS and the FA(s) communicate through a protected communication channel. The SMS and SCS communicate using the same protected communication channel technology. All communications between the SMS CLI, SMS Navigator, SMS Remote Navigator and the SMS are sent through a communication channel that is secure and confidential. The SMS communications with the FA involve security-relevant information such as configurations settings and policy settings as well user's authentication information. Communications between the SMS and SCS hosts consist of database requests and status information. All policy and configuration information from the SMS to the FA are sent through a communication channel that provides confidentially and integrity. Similarly, an administrator sitting on a remote machine can make security-relevant policy changes to a remote FA via an SMS using the SMS Remote Navigator. All protected communications are encrypted using an Alcatel-Lucent developed protocol that is similar to Secure Socket Layer (SSL) v3.0. When the SMS is first installed, a root certificate is created which includes a public/private DSA key pair. A certificate is also created for the SMS itself which is signed using the root public/private key pair. When an FA is created, yet another certificate is created, also signed with the root public/private key pair. All of these certificates include a common set of Diffie-Hellman parameters (alpha, p, etc). When the SMS and FA want to talk to each other (securely), they exchange the public parts of their certificates and verify that the owner of the certificate is what they expect and that the certificate is signed using the same private key (i.e., they were both created on the same SMS). There is also a Diffie-Hellman key exchange performed at this time. The shared secret resulting from that process is used as the triple-DES key as well as the input to the SHA digest algorithm. Each new session from the SMS to the FA uses Diffie-Hellman for key agreement between the SMS and FA. The SMS and FA use a 3DES or AES-128 implementation, which are both FIPS 46-3 validated, for the encryption of the messages between each other. The 3DES implementation uses SHA-1 hashing, which is FIPS 180-1 validated, for a message integrity check. The AES-128

	implementation uses the characteristics of CBC algorithms to implement the message hash by including a sequence number in the message stream after the message text itself. A message digest is generated for each message. For the 3DES connections, the digest of the clear text is sent in the clear. Initially the SMS Remote Navigator and the SMS will exchange keys to set up a 3DES tunnel. Once the tunnel is in place, the SMS will authenticate the administrator ID and password. If the ID and password are indeed valid, another 3 DES tunnel is enabled to maintain maximum security throughout the session. A simple Web server is used to deliver reports and help files. This Web server when configured for HTTPS uses a TLS connection between the SMS Navigator/SMS Remote Navigator and the Web server. Once an administrator is logged in and connected to the RAP subsystem, the Web server is used to display reports and online documentation (including help files). Web server is required to use FIPS 140-2 approved TLS mode of operation since reports may contain sensitive information. When HTTPS is used, Reports and Help files are retrieved via an established TLS connection. A web browser (Netscape or IE) is used to display reports.
FTP_ITC.1	The TOE requires assured identification of VPN tunnel endpoints when VPN tunnels are established. The ALVF implements VPNs using the IPSec protocol. IPSec is a framework of open standards used to provide private, secure network communications. The cryptographic operations used are determined by the IPSec Security Association (SA) which is defined by the packet's destination IP address, a security protocol (e.g., encryption/authentication types and keys), and a unique identification value, called a Security Parameter Index (SPI). The SA associates the security services and a key with the network packets being protected. The IPSec protocol relies upon the following cryptographic services: encryption and decryption of VPN traffic, message hashing, and digital signature generation and verification. The TOE provides the ability to create both LAN-LAN and client tunnels. Both LAN-LAN and client tunnels authenticate the devices/hosts via a preshared key or certificate. Client tunnels perform also user authentication.
FPT_FLS.1	The redundancy security function preserves a security state when redundancy is configured and connectivity is lost. The connection is considered lost when five consecutive heartbeats are not acknowledged within a specified timeframe. When SMS redundancy is configured, the primary database is built

	on the Primary SMS and replicated on the Secondary SMSs. The redundant SMSs synchronize their data at the time the data is modified. When connectivity is interrupted between redundant SMSs, each SMS keeps track of interim changes made in its own version of the database. When connectivity is restored within 7 days, any interim changes made during the interruption are reconciled in the common dataset (after that, all changes made on the secondary will be discarded when they are reconnected). If an SMS is not able to synchronize a database change with the other SMSs, an alarm is triggered. The secure state information is stored on the SMSs, not on the SCSs. So when the FA is homed to an SCS and the connection between the FA and SCS is lost, the secure state is preserved on the SMS associated with the SCS.
FRU_FLT.1	The redundancy security function ensures the operation of all management and log collection services, except possible loss of audit records and changes made to the security configuration that occur within 5 seconds of the connection being lost. When SMS redundancy is configured and connectivity is interrupted between the Primary and a Secondary SMS, each SMS keeps track if interim changes made in its own version of the database. When connectivity is restored within 7 days, any interim changes made during the interruption are reconciled in the common dataset (after that, all changes made on the secondary will be discarded when they are reconnected). If an SMS is not able to synchronize a database change with the other SMSs, an alarm is triggered. The Home SMS/SCS Priority Table for each FA determines the management device to which the FA is homed. The Home SMS/SCS Priority Table can define up to five SMSs or SCSs. After booting or restarting its services, an FA attempts to home to its Priority 1 entry. If the FA loses connectivity with the Priority 1 entry, the FA attempts to re-home with the Priority 2 entry and so on.

Table 13: TOE Summary Specification

7.1 FIPS 140-2 Compliance

All the cryptographic operations within the TOE are performed by one of two FIPS 140-2 compliant cryptographic modules.

7.1.1 VPN Firewall Brick

The cryptography used in the VPN Firewall Brick has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The VPN Firewall Brick Models vary in hardware configurations as shown in the Table 1: Firewall Appliance Hardware (i.e. memory size, number of Ethernet ports). The software image that implements the security enforcing functionality is the same on all VPN Firewall Brick Models. All the VPN Firewall Brick models are considered identical with respect to implementing security features. They are identical because one can take any software binary image (tvpc or tvpc.zip file) from any VPN Firewall Brick and run it on any other VPN Firewall Brick. This can be verified simply by doing a “make/package floppy” operation for each VPN Firewall Brick and then comparing the image files on the floppy/USB drive for each VPN Firewall Brick.

The same software binary image ("tvpc.zip") runs on all modules, so all features are available on all module platforms. The binary images are identical across all platforms, regardless of the VPN Firewall Brick’s model number or configuration setup.

However, since the OS image provides a superset of all drivers that can interface with the module, each module only needs to use a subset of the drivers installed. When the administrator creates the bootable OS image from the Security Management Server, one of the selectable options (via a drop down box) in the SMS application is to reference the specific driver configurations of the VPN Firewall Brick model. This selection of the VPN Firewall Brick model specifies which subset of drivers is needed and places this configuration data within a separate configuration file ("inferno.ini"), which is created alongside the OS image. The purpose of the configuration file is to distinguish which drivers are applicable to the module it is installed on, while the binary image file ("tvpc.zip") serves as the same identical executable applicable to all VPN Firewall Brick models.

The VPN Firewall Brick Models uses the FIPS compliant cryptographic module to establish an encrypted socket connection between the SMS application and itself during transmission of audit data and during reception of policies from the SMS application. The encrypted socket uses SHA-1 for message (or packet) integrity checking and 3DES or AES to encrypt the message/package/packet for confidentiality. When connections are established all the key material is generated by the FIPS 140-2 compliant module. Likewise, when the connection is terminated the key material is destroyed by the FIPS 140-2 compliant module.

7.1.2 SMS

The SMS software package and the SMS Remote Navigator both use the following FIPS 140-2 validated cryptographic module**:**

- Phaos Crypto Software Versions 3.0 and 3.0.1 (FIPS Certificate # 337).

The SMS software package and the SMS Remote Navigator use this module for all cryptographic functionality required to negotiate and maintain the encrypted socket connections between:

- The SMS Navigator/SMS Remote Navigator/SMS CLI/SMS Log Viewer and the SMS/SCS host.
- The FIPS enabled TLS connection between the SMS/SCS Web server and a web browser (located in the TOE environment)
- The SMS/SCS host and the FA during policy push to an FA and during reception of log data from a FA.
- The SMS host and the SCS host.
- The primary SMS host and secondary SMS hosts.
- One FA and another FA via VPN.
- FA to an IPSec client

FIPS 140 certificates and Non-Proprietary Security Policies are available on the Cryptographic module Validation Program website:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.