National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Alcatel-Lucent VPN Firewall (ALVF) v9.1.329 On Firewall Appliance Models 50, 150, 700 and 1200

Report Number: CCEVS-VR-VID10308-2009
Dated: 22 May 2009
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Jerome Myers (Senior Validator)
Jandria Alexander (TVOR TOP Chair)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Ken Dill
Maria Tadeo

Savvis Federal Systems
Arca Common Criteria Testing Laboratory
45901 Nokes Boulevard
Sterling, Virginia 20166

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Alcatel-Lucent VPN Firewall (ALVF) v9.1.329. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of Alcatel-Lucent VPN Firewall was performed by the Arca Common Criteria Testing Laboratory (CCTL), in Sterling, Virginia, USA and was completed in March 2009.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Alcatel-Lucent. The ETR and test report used in developing this validation report were written by Arca. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, version 3.1, dated September 2007 at Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.1 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, dated September 2007. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Alcatel-Lucent VPN Firewall Security Target. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 4 with ALC_FLR.1. The product is not conformant to any Protection Profile.

1.1 TOE Summary

The evaluated product is a combination of one or more distributed firewall/VPN appliances with centralized management servers. The hardware appliances, marketed by Alcatel-Lucent as the "Brick" family of appliances, are bridging devices with traffic-filter firewall functionality, application filters, and IPSec VPN functionality for both LAN-to-LAN tunnels and termination of remote-client tunnels.

The evaluated product 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 which enables Administrators to manage the security of one or more Firewall Appliances (FA). The SMS software package and the supporting host platform 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) and running on a supporting host platform 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 Remote Navigator is a Graphical User Interface client which enables 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 (the operating systems are outside the TOE boundary) as the supporting host. An Administrator can log into the SMS software package remotely using the SMS Remote Navigator client, which is installed on a Windows host.

1.2 Validation Summary

During this evaluation, the Validators monitored the activities of the Arca evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. In addition to this normal validation activity, an additional validator joined the team as chair of a Technical Oversight Panel (TOP) prior to the lab testing the product. The TOP accomplished a more detailed analysis of the product and test plan proposed by the Lab. The Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validators conclude that the Arca findings are accurate, the conclusions justified, and the conformance claims correct.

It must be noted that the cryptography used in this product has not been FIPS certified, nor has it been analyzed or independently tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested and correct by the vendor.

2 Identification

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

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) products, desiring a security evaluation, enter into a contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant, if any; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Alcatel-Lucent VPN Firewall (ALVF) v9.1.329
Protection Profile	None.
Security Target	*Alcatel-Lucent VPN Firewall Version 9.1 EAL4 Security Target*, Version 1.0 dated April 30, 2009
Dates of evaluation	June 2008 through April 2009

Evaluation Technical Report	• *ASE (Security Target Evaluation): ASE Evaluation Technical Report for Alcatel-Lucent VPN Firewall (ALVF) v9.1 (Firmware Version 9.1.329) with one or more of the Firewall Appliances Models 50, 150, 700 AC, 700 DC, and/or 1200*, document version 1.5, released March 16, 2009. • *ALC (Life Cycle): ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ALC_FLR.1 Evaluation Technical Report for Alcatel-Lucent VPN Firewall (ALVF) v9.1 (Firmware Version 9.1.329) with one or more of the Firewall Appliances Models 50, 150, 700 AC, 700 DC, and/or 1200*, document Version 2.1, released March 16, 2009. • *AGD (Operational and Preparative Guidance): AGD_OPE.1; AGD_PRE.1 Evaluation Technical Report for Alcatel-Lucent VPN Firewall (ALVF) v9.1 (Firmware Version 9.1.329) with one or more of the Firewall Appliances Models 50, 150, 700 AC, 700 DC and/or 1200*, document Version 1.2, released March 16, 2009. • *ADV (Development Evaluation): ADV_FSP.4; ADV_TDS.3; ADV_ARC.1; ADV_IMP.1; Evaluation Technical Report for Alcatel-Lucent VPN Firewall v9.1 (Firmware Version 9.1.329) with one or more of the Firewall Appliances Models 50, 150, 700 AC, 700 DC, and/or 1200*, document Version 1.2 released March 16, 2009. • *ATE (Functional Testing, Testing Coverage, Testing Depth and Independent Testing Evaluation): ATE_COV.2;ATE_DPT.2; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Alcatel-Lucent VPN Firewall (ALVF) v9.1 with one or more of the Firewall Appliance Models 50, 150, 700, and/or 1200*, document Version 1.0, released March 16, 2009 • *AVA (Vulnerability Assessment Evaluation): AVA_VAN.3; Evaluation Technical Report Alcatel-Lucent (ALVF) v9.1 (Firmware Version 9.1.329)*, document version 1.2, released March 16, 2009.
Conformance Result	Part 2 extended and Part 3 conformant, EAL 4 augmented with ALC_FLR.1
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, September 2007 and all applicable NIAP and International Interpretations effective on June 24, 2008
Common Evaluation Methodology (CEM) version	CEM version 3.1R2 dated September 2007and all applicable NIAP and International Interpretations effective on June 24, 2008
Sponsor	Alcatel-Lucent, 26801 Agoura Road, Calabasas, California 91301
Developer	Alcatel-Lucent, 26801 Agoura Road, Calabasas, California 91301
Common Criteria Testing Lab	Savvis Federal Systems, Arca Common Criteria Testing Laboratory, NVLAP Lab Code 200429, 45901 Nokes Boulevard, Sterling, Virginia 20166
Evaluators	Ken Dill and Maria Tadeo of Arca CCTL
Validation Team	Jandria Alexander, Jerome Myers and Mike Allen of The Aerospace Corporation

3 Security Policy

The TOE enforces the following security policies:

3.1 User Data Protection

All communication between each FA and the SMS application is encrypted and authenticated using an encrypted socket connection.

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 that 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 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, H.323 RAS, DHCP relay, TFTP, Oracle SQL*Net, Microsoft NetBIOS, SUN RPC, DNS, SMTP, and SIP.

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 pre-shared key or certificate.

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

3.2 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 is exhausted, 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.

3.3 Identification and Authentication (I&A)

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[1], and application users[2] 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 lists imported to the TOE from the external CA. To authenticate the user, the SMS

[1] The term VPN user refers to individuals requesting a client tunnel via an approved IPSec client.
[2] The use of application users is not allowed in the evaluated configuration.

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 IT environment to verify the identification and authentication data provided by the user. It is not part of the TOE.

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. 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.

3.4 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).

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.

The TOE provides the following management functions that 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 constitute 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.

3.5 Protection of TOE Security Functions

The security functions which implement the ALVF access control policy are physically separated from the unauthenticated external IT entities that send and receive IP packets through the FA; 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 an operational environment that authenticates 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.

3.6 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) of a TLS-encrypted session.

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

3.7 Redundancy

The TOE provides redundancy features for the SMS. 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.

4 Assumptions and Clarification of Scope

4.1 Usage 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 v9.1.329 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.

4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This section emphasizes what has been evaluated and, more importantly, limitations and clarifications of those elements of the product that were not evaluated.

4.2.1 Evaluated Features

The following features of the ALVF were evaluated to be 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, 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]
- Oracle SQL*Net [dynamic channel opening]
- Microsoft NetBIOS [address translation]
- SUN RPC (Remote Procedure Calls)
- DNS (Domain Name Service)
- SMTP (Simple Message Transfer Protocol).

4.2.2 Unevaluated Features of the Product

This section identifies the features that the ALVF provides, but are not in the scope of the 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 are therefore excluded from the scope of evaluation, 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 has 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.

5 Architectural Information

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.

5.1 TOE Hardware and Software

The physical scope of the TOE includes the components circled in red dashed lines in Figure 1. 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 that figure, 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 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.

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

- VPN Firewall Brick Model 700
- VPN Firewall Brick Model 1200

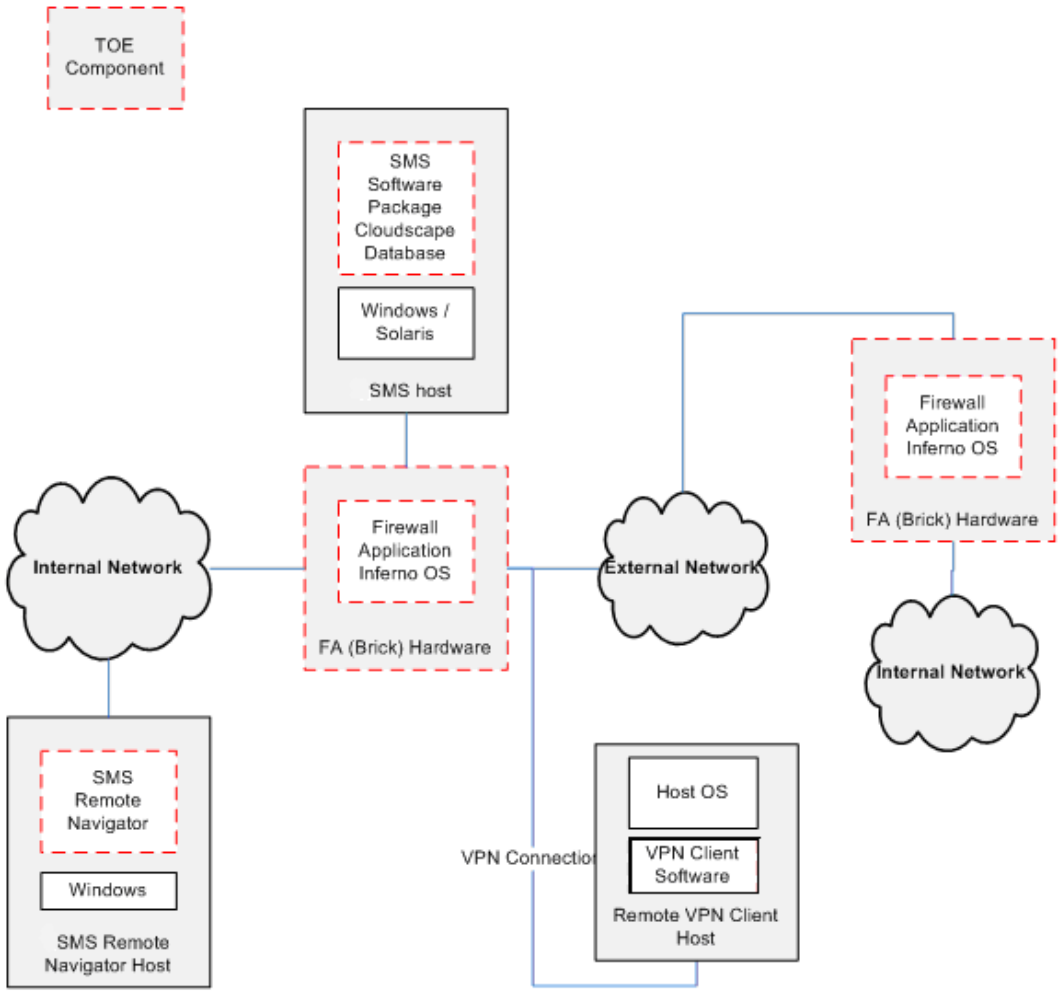

Figure 1: Physical TOE Boundary and Environment

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.

Table 2: Firewall Appliance Hardware

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

The FAs vary in hardware configurations as shown in the above table (e.g., 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 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 runs on all FA models, 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 serves as the same identical executable applicable to all FA models.

The administrative interface to the SMS software package is provided by the following interfaces:

1. SMS Navigator, a Graphical User Interface (GUI)
2. SMS Command Line Interface (CLI)
3. SMS Remote Navigator, the remote version of SMS Navigator
4. Utilities, including command line database utilities, and Graphical User Interface Log Viewer and Configuration Assistant

5.2 Environmental Components

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

- The operating systems and underlying hardware for the SMS Remote Navigator and SMS software package are in the TOE environment. (Use of a modem is not permitted on the SMS host in the evaluated configuration.)

  Using a Windows host for SMS requires:

  - 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
      - 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)

Using a Solaris host for SMS requires:

- 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 initial configuration. The monitor and keyboard are optional once the initial configuration is completed such that the FA has been "homed" to an SMS.

- 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 an SMS 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 an SMS 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 an SMS 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 include:
  - 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

6 Documentation

The hardware and software for the TOE are purchased as a single item. The customer is delivered a CD that contains installation software and documentation. The following product documentation is included on the CD in the \Documentation directory, and available for download from the user support site at https://www.lucent-ipsec.com:

Table 3: TOE Documentation

Title/Description	Date	Evaluated
Alcatel-Lucent VPN Firewall Version 9.1.329 Supplemental CC Guidance	March 2009	YES
Release Notes for ALSMS Patch v9.1.329 (alsms9.1-329-readme.pdf)	February 2009	YES
LSMS v9.1 What's New Manual (whats_new9.1.pdf)	August 2006	YES
Updated - Install Guide, (install_guide-v9.1.299.pdf)	December 2007	YES
Updated - Administration Guide (admin_guide-v9.1.299.pdf)	December 2007	YES
Updated - Policy Guide (policy_guide-v9.1.299.pdf)	January 2008	YES
Updated - Reports, Alarms & Logs Guide (reports_logs_v9.1.308.pdf)	May 2008	YES
Updated -Tools & Troubleshooting Guide – CLI (tools_trouble_v9.1.308.pdf)	May 2008	YES
LSMS v9.1 Technical Overview (tech_ov9.1.pdf)	August 2006	YES

7 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

Note: The cryptography used in this product 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 and correct by the vendor.

7.1 Developer Testing

The developer maintains a set of function-specific test plans for confirming the ALVF product line meets its advertised functional requirement. As required for EAL4, the developer provided actual results of testing for each TSFI and each SFR. At least one test case was mapped to every external interface. Many of the interfaces were exercised by multiple tests. An evaluation team review of all of the security functions and the mapping between security functions and tests confirmed that security functions were appropriately tested by the developer tests. Actual results were generated at the developer's development and testing facility in New Jersey. The actual test results provided from the developer for this evaluation were generated on a deployment of ALVF components consistent with the Security Target, and installed in accordance with the Alcatel-Lucent VPN Firewall Version 9.1.329 Supplemental CC Guidance.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team also ensured that all TSFI interfaces were tested by the developer by creating a mapping of test cases to module and SFR's.

The evaluation team performed a subset of the developer's test suite and devised an independent set of team tests and penetration tests. The test cases (sample of vendor tests) and independent test that were run by the evaluation team with vendor engineers, covered 13 of 45 (29%) SFRs, included 4 out of 7 (57%) TSFs and used 30 out of 227 (13%) TSFIs across 15 of 39 (38%) modules for the TOE.

The evaluation team also performed flaw hypothesis analysis of the product to prepare for a penetration testing effort. The analysis examined each SFR to determine whether it was possible that the evaluated configuration could be susceptible to vulnerability. The specific penetration tests executed include the following:

- Used a port scanner to enumerate listening services on each of the distributed TOE components.
- Attempted privilege escalation by testing the limitations imposed on user group levels, and restricted access to privileged commands and operations.

- Checked for known vulnerabilities on each of the distributed TOE components network vulnerability scanners.

The evaluation team constructed and ran each of the identified tests. The results of the penetration test execution verified that none of the hypothesized flaws was exploitable.

The network configuration used for the execution of the CCTL testing is documented in the figure below.

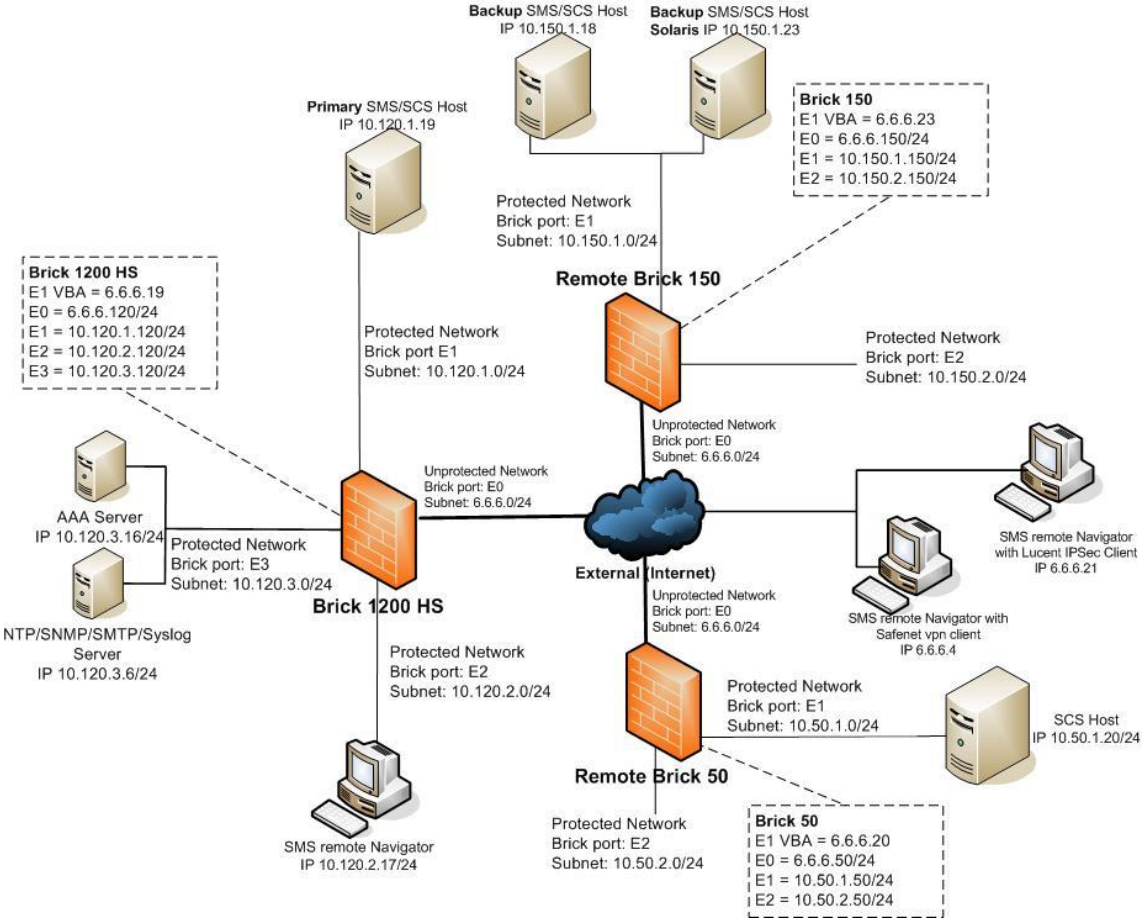

Figure 2: CCTL testing environment

8 Evaluated Configuration

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 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.

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.)

TOE configurations depicted in the diagrams below:

- 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.
- 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.
- TOE Configuration #3 is a superset of TOE Configuration #2 and shows how SCSs can be added to the deployment.

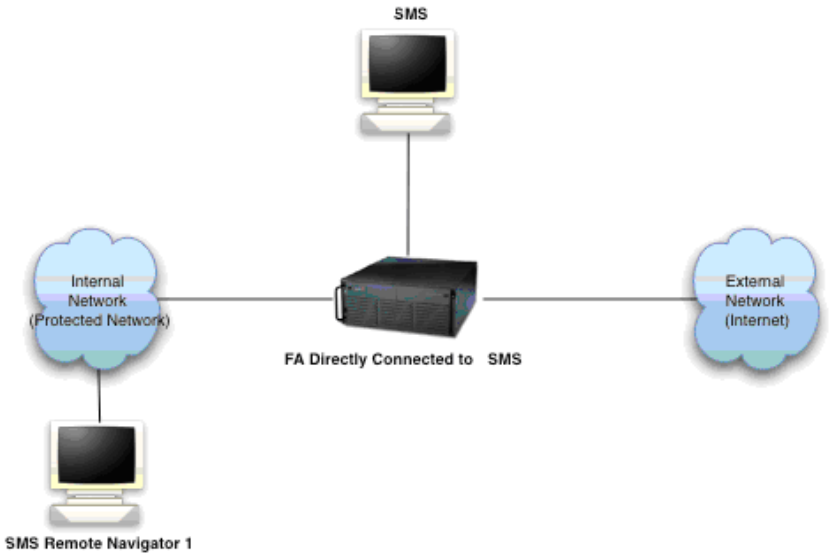

Figure 3: TOE Configuration[3] #1

[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

There are two secure communication paths that are established through the connections depicted in Figure 3: TOE Configuration #1.

- The SMS application negotiates and establishes an encrypted socket connection from the SMS application to the FA.
- 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 4: TOE Configuration #2 depicts an evaluated configuration containing two Firewall Appliances, two SMS Remote Navigators, and one SMS software package.

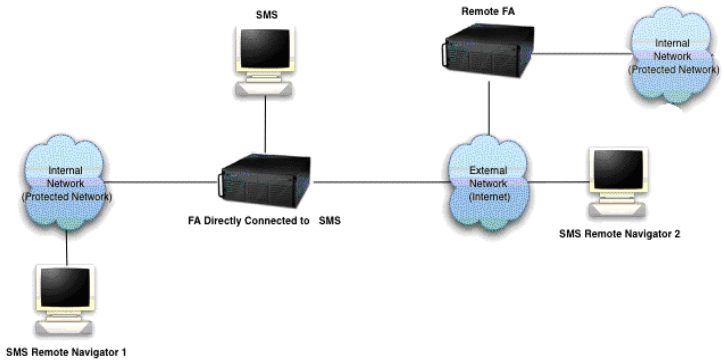

Figure 4: TOE Configuration #2

There are two secure communication paths that are established through the connections depicted in Figure 4: TOE Configuration #2.

- 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 5: 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 this figure are not configured for FA failover.

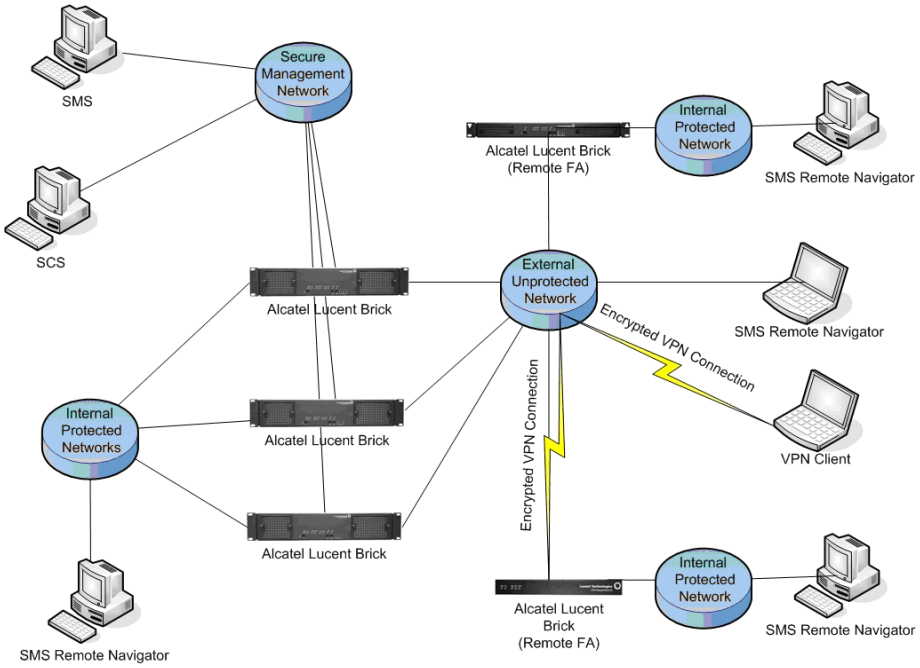

Figure 5: TOE Configuration #3

There are five secure communication paths that are established through the connections depicted in Figure 5: TOE Configuration #3.

- 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. 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 is conducted through an encrypted socket connection.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R2.

The Validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validators therefore conclude that the evaluation team's results are correct and complete.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Alcatel-Lucent VPN Firewall (ALVF) v9.1.329 on Firewall Appliance Models 50, 150, 700 and 1200 meet the claims stated in the Security Target. The validation team also wishes to add the following notations about the use of the product.

- The VPN Certificate Authority is in the Environment and not evaluated as part of this evaluation.
- The "Application Users" feature of the product is not permitted in the Evaluated Configuration.
- A Configuration which uses Security Compute Servers (SCSs) must use a Network Time Protocol (NTP) server in the environment which was not evaluated as part of this evaluation.
- The cryptography used in this product 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 to function correctly by the vendor.

11 Security Target

The Security Target is identified as theAlcatel-Lucent VPN Firewall Version 9.1 EAL4 Security Target, Version: 1.0, April 30, 2009. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4 augmented with ALC_FLR.1.

12 Glossary

The following abbreviations and terms are used throughout this document:

ACL	Access Control List
ALVF	Alcatel-Lucent VPN Firewall
API	Application Programming Interface
Brick	An ALVF appliance
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCIMB	Common Criteria Implementation Board
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CMS	Certificate Management System
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FA	Firewall Appliance
Gbps	Gigabits per second
GUI	Graphical User Interface
ID	Identifier
Mbps	Megabits per second
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
RAM	Random Access Memory
RFC	Request for Comment
SAR	Security Assurance Requirement
SCS	Security Compute Server
SFR	Security Functional Requirement
SMS	Security Management Server
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target Of Evaluation
TSF	TOE Security Function
URL	Uniform Resource Locator
VPN	Virtual Private Network

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1.) Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2006, version 3.1, revision 1.

2.) Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2007, version 3.1, revision 2.

3.) Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2007, version 3.1, revision 2.

4.) Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2007, version 3.1, revision 2.

5.) Alcatel-Lucent VPN Firewall v9.1 EAL4 Security Target, Version 1.0, dated April 30, 2009.