Alcatel-Lucent

Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC

Hardware Versions: 150, 700 AC, and 700 DC; Firmware Version: 9.1.299

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Document Version 3.1

Prepared for:

Alcatel-Lucent
600-700 Mountain Avenue
Murray Hill, NJ 07974
Phone: (908) 582-3000
http://www.alcatel-lucent.com

Prepared by:

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

Revision History

Version	Date	Modified By	Description of Changes
1.0	2007-05-01	Ben Greenberg	Initial Version
1.1	2007-06-15	Xiaoyu Ruan	Revision
1.2	2007-07-19	Xiaoyu Ruan	Added figure of temper-evidence label
1.3	2007-08-06	Xiaoyu Ruan	Addressed Lab's comments
1.4	2007-09-11	Xiaoyu Ruan	Addressed Lab's comments
1.5	2007-09-13	Xiaoyu Ruan	Addressed Lab's comments
1.6	2007-09-14	Xiaoyu Ruan	Addressed Lab's comments
1.7	2007-09-14	Xiaoyu Ruan	Addressed Lab's comments
1.8	2007-10-01	Xiaoyu Ruan	Addressed Lab's comments
1.9	2007-10-17	Darryl Johnson	Added instructions for tamper-evident label placement in Section 2.6.
2.0	2007-10-18	Xiaoyu Ruan	2.5.1
2.1	2007-10-19	Darryl Johnson Xiaoyu Ruan	Added more instructions for tamper-evident label placement in Section 2.6.
2.2	2007-10-22	Xiaoyu Ruan	Addressed Lab's comments
2.3	2007-10-23	Xiaoyu Ruan	Authentication strength
2.4	2007-10-23	Darryl Johnson	Tamper-evident label placement
2.5	2007-11-13	Xiaoyu Ruan	Addressed Lab's comments
2.6	2007-12-20	Xiaoyu Ruan	Addressed Lab's comments
2.7	2008-01-04	Xiaoyu Ruan	Algorithm certificate numbers
2.8	2008-01-18	Xiaoyu Ruan	Version 9.1.299
2.9	2008-03-10	Xiaoyu Ruan	Algorithm certificates
3.0	2008-06-09	Xiaoyu Ruan	Addressed CMVP comments
3.1	2008-07-11	Xiaoyu Ruan	Added Sections 3.6 and 3.7

Table of Contents

1 INTRODUCTION 6
1.1 PURPOSE 6
1.2 REFERENCES 6
1.3 DOCUMENT ORGANIZATION 6

2 ALCATEL-LUCENT VPN FIREWALL BRICKS 150, 700 AC, AND 700 DC 7
2.1 OVERVIEW 7
2.2 LUCENT SECURITY MANAGEMENT SERVER 8
2.3 CRYPTOGRAPHIC MODULES SPECIFICATION 8
2.4 MODULE INTERFACES 9
2.4.1 Brick 150 9
2.4.2 Brick 700 10
2.5 ROLES AND SERVICES 11
2.5.1 Crypto Officer Role 11
2.5.2 User Role 13
2.5.3 Authentication 14
2.5.4 Bypass Mode 15
2.6 PHYSICAL SECURITY 15
2.6.1 Brick 150 16
2.6.2 Brick 700 17
2.7 OPERATIONAL ENVIRONMENT 19
2.8 CRYPTOGRAPHIC KEY MANAGEMENT 19
2.8.1 Cryptographic Algorithms 19
2.8.2 CSPs 20
2.8.3 CSP Zeroization 23
2.9 SELF-TESTS 23
2.10 MITIGATION OF OTHER ATTACKS 23

3 SECURE OPERATION 24
3.1 INITIAL SETUP 24
3.1.1 Installing the Brick 24
3.1.2 Setting up LSMS 24
3.2 MODULE INITIALIZATION AND CONFIGURATION 24
3.2.1 Configuring LSMS-Brick Communication 24
3.2.2 Initializing the Brick 24
3.2.3 Configuring the Brick Serial Port 25
3.3 IPSEC REQUIREMENTS AND CRYPTOGRAPHIC ALGORITHMS 25
3.3.1 IPsec/IKE Requirements 25
3.3.2 External CA Requirements 26
3.3.3 Configuring LAN-LAN Tunnels 26
3.3.4 Configuring Client Tunnels 26
3.4 ZEROIZING KEYS AND CSPS 26
3.5 IDENTIFYING THE ERROR STATE 27
3.6 MAINTAINING PHYSICAL SECURITY 27
3.7 DETERMINING THE FIPS MODE OF OPERATION 27

4 ACRONYMS 28

Table of Figures

FIGURE 1 – ALCATEL-LUCENT VPN FIREWALL BRICK DEPLOYMENT 7
FIGURE 2 – BRICK 150....9
FIGURE 3 – BRICK 700....9
FIGURE 4 – CRYPTO OFFICER LABEL PLACEMENT FOR THE RIGHT AND LEFT SIDES OF THE BRICK 150 16
FIGURE 5 – CRYPTO OFFICER LABEL PLACEMENT FOR THE REAR SIDES OF THE BRICK 150 16
FIGURE 6 – CRYPTO OFFICER LABEL PLACEMENT FOR THE REAR OF THE BRICK 700 17
FIGURE 7 – CRYPTO OFFICER LABEL PLACEMENT FOR THE FRONT OF THE BRICK 700 17
FIGURE 8 – CRYPTO OFFICER LABEL PLACEMENT FOR THE TOP OF THE BRICK 700....18

List of Tables

TABLE 1 – SECURITY LEVEL PER FIPS 140-2 SECTION....8
TABLE 2 – MAPPING OF FIPS 140-2 LOGICAL INTERFACES TO BRICK 150 INTERFACES....10
TABLE 3 – MAPPING OF FIPS 140-2 LOGICAL INTERFACES TO BRICK 700 INTERFACES....11
TABLE 4 – CRYPTO OFFICER SERVICES....12
TABLE 5 – USER SERVICES....13
TABLE 6 – BRICK 150 LABEL PLACEMENT GUIDANCE....16
TABLE 7 – BRICK 700 LABEL PLACEMENT GUIDANCE....18
TABLE 8 – ACRONYMS....28

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC (Hardware versions: 150, 700 AC, and 700 DC; Firmware version: 9.1.299) from Alcatel-Lucent. This Security Policy describes how the Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC meet the security requirements of FIPS 140-2 and how the modules are run in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the modules.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at: http://csrc.nist.gov/groups/STM/index.html.

The Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC are referred to in this document as the Bricks, the cryptographic modules, or the modules.

1.2 References

This document deals only with operations and capabilities of the modules in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the modules from the following sources:

- The Alcatel-Lucent website (http://www.alcatel-lucent.com) contains information on the full line of products from Alcatel-Lucent.
- The CMVP website (http://csrc.nist.gov/groups/STM/index.html) contains contact information for answers to technical or sales-related questions for the modules.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Alcatel-Lucent. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Alcatel-Lucent and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Alcatel-Lucent.

2 Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC

2.1 Overview

The *Alcatel-Lucent Virtual Private Network (VPN) Firewall Brick* product line offers a broad range of enterprise and carrier-class security solutions to protect corporate and service provider networks delivering mission-critical Internet Protocol (IP) applications to headquarter employees, branch offices, trading partners, road warriors and customers. *Alcatel-Lucent VPN Firewall* solutions can help stretch Information Technology (IT) budgets with superb price and performance and a low total cost of ownership. Leading-edge technology can simplify deployment and management of diverse applications including:

- Advanced security services
- VPN services for site-to-site and remote access
- Bandwidth management capabilities
- Secure data center, web and application hosting
- Storage network secure solution
- Mobile data security
- Packet Data Gateway and Packet Data Interworking
- Functions for Dual-Mode Wireless/WiFi VPN and VoIP/Data Security

The Lucent VPN Firewall Bricks deliver the performance needed to provide vital security and VPN services for thousands of enterprise users. High-capacity packet processing capabilities help maximize user efficiency and productivity with up to 1.7 Gbps VPN throughput and a full 4.75 Gbps firewall throughput. A general deployment scenario for the Bricks is depicted in Figure 1 below. All administration of the Bricks is performed by the Lucent Security Management Server (LSMS) software which is described in Lucent Security Management Server 1.2.

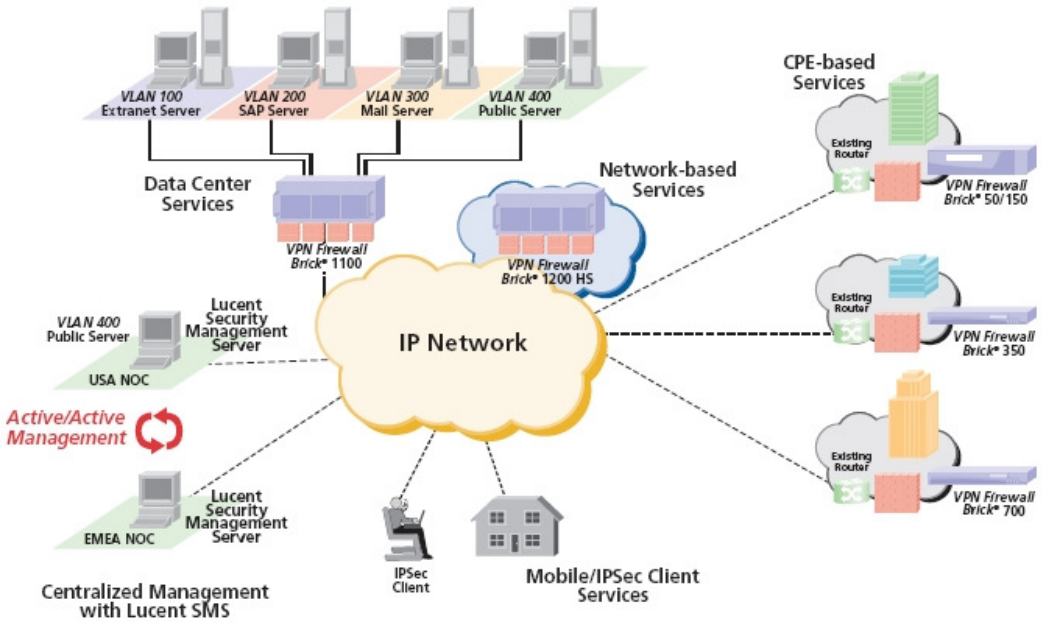

Figure 1 – Alcatel-Lucent VPN Firewall Brick Deployment

2.2 Lucent Security Management Server

The LSMS is a component to any VPN Firewall Brick deployment. All administration of the Bricks is performed via the LSMS. The operators should identify the firmware version of the Brick and use a compatible version of LSMS.

The LSMS software provides advanced carrier-grade IP services management at a low total ownership cost. Teaming with Lucent's award-winning VPN Firewall Brick® portfolio, Lucent Security Management Server lets administrators rapidly provision and manage high-return services for thousands of users in a single console. It integrates firewall, VPN, Quality of Service (QoS), Virtual Local Area Network (VLAN) and virtual firewall policy management; provides industry-leading scalability and availability; delivers robust monitoring, logs and reports; and gives you flexible deployment options — all without the costly additional modules or recurring license fees that competitive products require.

The LSMS provides the following features:

- Fully integrates firewall, VPN, QoS, VLAN, and virtual firewall management
- Comprehensive remote management capabilities with role-based administration
- Flexible management model: controls policies at global, customer, device, interface, VLAN and IP address range levels
- High scalability: supports 20,000 Lucent VPN Firewall Brick units and up to 500,000 simultaneously connected VPN users from one Lucent Security Management Server console.
- Carrier-class reliability: distributable across up to four network operations centers (NOCs) for active/active network redundancy with no single point of failure
- Real time monitoring, robust logging, and customized reporting
- Multiple IP services deployment options: premises-based, network-based, tiered, and data-center architectures

Note that the LSMS software is not included as part of this FIPS 140-2 validation.

2.3 Cryptographic Modules Specification

The Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC are considered to be multi-chip standalone cryptographic modules and are validated at the following levels for each FIPS 140-2 Section:

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	Electromagnetic Interference (EMI) / Electromagnetic Compatibility (EMC)	2
9	Self-tests	2
10	Design Assurance	2

Section	Section Title	Level
11	Mitigation of Other Attacks	N/A

The Bricks come in both a desktop systems form factor and a rack mounted form factor. Each form factor is discussed in detail below.

The Brick 150, shown below in Figure 2, measures 11" (W) x 7.18" (D) x 1.75" (1U) and is intended to be primarily a desktop unit. However, two rack-mounting brackets and two wall-mounting brackets are included for different mounting options.

Figure 2 – Brick 150

A Model 700 Brick device measures 17.4″ (W) x 18.75″ (D) x 1.75″ (H) and is intended to be installed on a standard 19-inch rack. It comes with two optional rack-mounting brackets that can be attached to the sides to secure it to the rack. The Brick is shown in Figure 3 below. The Brick 700 comes in two models. One model is powered by Alternating Current (AC) and the other model is powered by Direct Current (DC).

Figure 3 – Brick 700

2.4 Module Interfaces

The Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC are multi-chip standalone modules that meet overall level 2 FIPS 140-2 requirements. The cryptographic boundary of the Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC is defined by the hard metal chassis of the Bricks.

2.4.1 Brick 150

The following is a list of the physical ports and interfaces of the Brick 150.

- Ethernet ports (x4)
- Serial port (console)
- USB ports (x2)
- Monitor port
- LEDs
- Power connector
- Power switch

The front of the Brick 150 has multiple LEDs to indicate status for power, HD activity, alarm, Ethernet link, and Ethernet activity. The power light stays green as long as the main power supply is providing power to the Brick. When power is lost, the light will go out. The HD activity light flashes green when activity is detected on the hard drive. The alarm light is off during normal operation. If the temperature of the CPU exceeds specified limits then the CPU turns off and the alarm light illuminates red. If the alarm light is red then the Brick is not functional although the LEDs indicating power, HD activity, Ethernet link, and Ethernet activity may still be green. Ethernet link lights are solid green as long as a link is established on the port. If there is no link, the light will be off. The four Ethernet activity lights flash green when activity on the port is detected.

The rear panel has four 10/100baseTX Ethernet interfaces which are labeled Eth3 through Eth0. The panel also has a DB9 serial port, two USB ports, a monitor port, a power jack and a power switch. Note that the USB connectors are covered by tamper-evident labels. The use of USB connectors is not allowed when in FIPS-Approved mode of operation. The Brick has a fan cover on the side of the Brick.

The following table maps the Brick 150 interfaces to the FIPS 140-2 logical interfaces.

Table 2 – Mapping of FIPS 140-2 Logical Interfaces to Brick 150 Interfaces

FIPS 140-2 Logical Interface	Brick 150 Port/Interface
Data Input	Ethernet ports
Data Output	Ethernet ports
Control Input	Ethernet ports, serial port, power switch
Status Output	Ethernet port, serial port, monitor port, LEDs
Power	Power connector

2.4.2 Brick 700

The following is a list of the physical ports and interfaces of the Brick 700.

- Ethernet ports (x8)
- Serial port (console)
- USB ports (x4)
- Monitor port
- PS/2 Keyboard port
- LEDs
- Alarm connector
- Audio Alarm Cut Off switch
- Power connector
- Power switch

The front panel of the AC version of the Model 700 Brick device has three activity lights and a power switch on the left. It also has two USB ports. On the AC model, the Power (PWR) LED turns solid green when the Brick is powered on. When the unit boots up and the Encryption Accelerator Card passes internal diagnostics including Power-Up Self-tests, the Encryption Accelerator LED (EA Act) turns solid green.

In addition to the three lights above, the DC model also has the following activity lights on the front panel:

- A Fault light, which is amber when power is lost to either the A or B power connector.
- An Audio Cut Off Activity (ACO Activity) light, which is amber when a fault exists but the audio alarm has been disabled using the ACO switch on the front panel.

- A -48VA light, which is green when power is applied to the A power connector. The light goes out when power is lost.
- A -48VB light, which is green when power is applied to the B power connector. The light goes out when power is lost.

The rear panel of the Brick 700 device contains eight 10/100/1000baseTX ports. The rear panel also contains a keyboard (PS/2) port, a monitor port, a DB9 serial port, and two USB ports. Note that the USB connectors are covered by tamper-evident labels. The use of USB connectors are not allowed when in FIPS-Approved mode of operation. The DC version also contains visual and audible alarm output connectors. The Visual Alarm Output indicates the Alarm state of the Brick device and remains active until the alarm situation is resolved. The Audible Alarm Output indicates the Alarm state of the Brick device but can be disabled with the ACO (Audible Cut Off) switch and will not reactivate until the existing alarm has been cleared and a new alarm has been generated. The rear panel also contains two power supply fans. Exhaust for the hot air is on the front side of the Brick.

The following table maps the Brick 700 interfaces to the FIPS 140-2 logical interfaces.

Table 3 – Mapping of FIPS 140-2 Logical Interfaces to Brick 700 Interfaces

FIPS 140-2 Logical Interface	Brick 700 Port/Interface
Data Input	Ethernet ports
Data Output	Ethernet ports
Control Input	Ethernet ports, serial port, keyboard port, power switch, Audio Alarm Cut Off switch
Status Output	Ethernet ports, serial port, monitor port, alarm connector, LEDs
Power	Power connector

2.5 Roles and Services

The Bricks support role-based authentication. There are two roles in the modules (as required by FIPS 140-2) that operators may assume: a Crypto Officer role and a User role.

2.5.1 Crypto Officer Role

Whenever a Crypto Officer makes a change to information in the LSMS that affects a configured Brick, that change has to be applied to the affected Brick. Although the changes may be saved in the LSMS database, they will not take effect until they are applied to the device.

As a general rule, a Crypto Officer has to apply any updated information that has been downloaded to a Brick. For example, Brick zone rulesets are assigned to Brick ports; if a Crypto Officer assigns a new ruleset to a port, then that change has to be applied to the Brick.

Similarly, if a Crypto Officer adds a new rule to a ruleset, or changes an existing rule, then that change has to be applied to every Brick to which the ruleset has been assigned.

If a Crypto Officer creates a new Brick zone ruleset, then it is applied automatically when the Crypto Officer applies the ruleset assignment.

Similarly, if a Crypto Officer adds a new user account or create a new user group, the Crypto Officer does not have to perform an apply. However, when the Crypto Officer creates a rule that uses the new user group, then the Crypto Officer has apply the ruleset.

There are a number of ways to perform an apply. See "How to Apply Changes" in the *Administration Guide*. Regardless of which LSMS window is displayed, a Crypto Officer can perform any apply, except a LAN-LAN or client tunnel, from the Utilities menu. In addition, there are other ways to perform each of the apply actions.

See the table below for descriptions of the services available to the Crypto Officer role. "tvpc" is the Brick operating system. It can be either in compressed form, tvpc.zip, or uncompressed form, tvpc.

Table 4 – Crypto Officer Services

Service	Description	Input	Output	Key/ Critical Security Parameter (CSP) Access
Bootstrap (serial port method)	Load configuration information onto Brick flash	configuration information	Status of commands and configuration data	Brick certificate (write); Brick name (write); Brick private key (write); Diffie-Hellman groups (write); LSMS public key (write) access; Serial port password (write)
Bootstrap (non-serial port method)[1]	Load tvpc.zip boot image and initial configuration information onto Brick flash	tvpc.zip boot image and initial configuration information	Status of commands and configuration data	Brick certificate (write); Brick name (write); Brick private key (write); Cyclic Redundancy Check (CRC) checksum for tvpc (write); CRC checksum for tvpc.zip (write); Diffie-Hellman groups (write); LSMS public key (write) access; Serial port password (write)
TLS (using AES)	Provide authenticated and encrypted remote sessions with LSMS to send audit event data.	TLS key establishment parameters, TLS inputs and data	TLS outputs and data	Brick certificate (read access using protocol messages); Diffie-Hellman groups (read access using protocol messages); LSMS public key (read access using protocol messages); TLS session keys (read access using protocol messages); Ruleset (read access using protocol messages)
TLS (using TDES)	Provide authenticated and encrypted remote management sessions while using LSMS management interfaces.	TLS key establishment parameters, TLS inputs and data	TLS outputs and data	Brick certificate (read access using protocol messages); Diffie-Hellman groups (read access using protocol messages); LSMS public key (read access using protocol messages); TLS session keys (read access using protocol messages); Ruleset (read access using protocol messages)
Policy file update[2]	Load Brick ruleset.	Commands and configuration data	Status of file update	Ruleset (write)

[1] Non-serial port bootstrap method services are not authenticated and are not available after the Crypto Officer has installed and configured the Brick according to "Secure Operation" procedures.

[2] LSMS Navigator Window and Menu Bar interfaces to configure Brick zone rulesets that result in policy file updates on the Brick can be found in the Policy Guide. Corresponding LSMS command-line interfaces can be found in the *Tools and Troubleshooting Guide*.

Service	Description	Input	Output	Key/ Critical Security Parameter (CSP) Access
Config file update[3]	Load Brick configuration information.	Commands and configuration data	Status of file update	Diffie-Hellman groups (write); LAN-LAN data authentication key; LAN-LAN data encryption key (write); Preshared key for client tunnels (write); Preshared key for LAN-LAN tunnels (write)
VPN certificate update	Load Brick VPN certificateificate.	Commands and configuration data	Status of file update	Brick VPN certificate (write); Brick VPN private key (write)
VPN Certification Authority (CA) certificate update	Load external CA certificate.	Commands and configuration data	Status of file update	CA certificates (write)
VPN Certificate Revocation List (CRL) update	Load external CA CRL.	Commands and configuration data	Status of file update	CA CRLs (write)
tvpc update (Firmware upgrade)	Load tvpc boot image onto Brick flash.	Commands and configuration data	Status of file update	CRC checksum for tvpc (write); CRC checksum for tvpc.zip (write); LSMS public key (read); Crypto Officer public key (read);
Local (serial) console[4]	Manage Brick	Commands and configuration data	Status of commands and configuration data	Brick name (indirect read access); serial port password (indirect read access)
Key and CSP zeroization	Zeroize keys and CSPs	Commands	Status of commands	All keys and CSPs (delete)
Status monitoring	Monitor Brick status	Commands	Status of Brick	None
Self-test execution	Invoke power-up self-tests	Reboot	Status of self-tests	None

2.5.2 User Role

The User role can access secured and unsecured network traffic services. See the table below for descriptions of the services available to the User role. IPsec/IKE stands for IP Security and Internet Key Exchange protocols.

Table 5 – User Services

Service	Description	Input	Output	Key/CSP Access

[3] LSMS Navigator Window and Menu Bar interfaces to configure Brick ports, host groups, domain name groups, service groups, application filters, network address translation, dependency mask, user authentication, LAN-LAN tunnels, and client tunnels that result in config file updates on the Brick can be found in the *Administration and Policy Guides*. Corresponding LSMS command-line interfaces can be found in the *Tools and Troubleshooting Guide*.

[4] Interfaces to manage Brick configuration information can be found in the *Tools and Troubleshooting Guide*.

Service	Description	Input	Output	Key/CSP Access
IPsec/IKE (client tunnels)	Access Brick IPsec/IKE services to secure network traffic.	IKE key establishment parameters, IPsec/IKE inputs and data	IPsec/IKE outputs and data	IKE session keys (read access using protocol messages); IPsec data authentication session keys (read access using protocol messages); IPsec data encryption session keys (read access using protocol messages); Ruleset (read access using protocol messages)
IPsec/IKE (LAN-LAN tunnels)	Access Brick IPsec/IKE services to secure network traffic.	IKE key establishment parameters, IPsec/IKE inputs and data	IPsec/IKE outputs and data	IKE session keys (read access using protocol messages); IPsec data authentication session keys (read access using protocol messages); IPsec data encryption session keys (read access using protocol messages); Ruleset (read access using protocol messages)
IPsec (LAN-LAN tunnels)	Access Brick IPsec services to secure network traffic.	IPsec inputs and data	IPsec outputs and data	IPsec data authentication session keys (read access using protocol messages); IPsec data encryption session keys (read access using protocol messages); Ruleset (read access using protocol messages)
Bypass	Access unsecured Brick network traffic services.	Unsecured network traffic	Unsecured network traffic	Ruleset (indirect read access)

2.5.3 Authentication

2.5.3.1 TLS Authentication

Crypto Officers can establish authenticated TLS connections with Bricks using certificates. Crypto Officers log into LSMS using LSMS usernames and passwords. LSMS has a built-in CA which generates certificates for Crypto Officers that have logged into LSMS. LSMS establishes TLS connections with Bricks on behalf of Crypto Officers to perform policy file updates, config file updates, VPN certificate updates, VPN CA certificate updates, VPN CRL updates, and tvpc updates. The authentication in TLS (as well as IKE) relies on 1024-bit DSA, which provides 80 bits of security. The probability of success with a single attempt is 2^{-80}, which is less than 1 in 10^6. To exceed a 1 in 10^5 probability of a successful random attempt, an attacker would have to be capable of $10^{-5}/2^{-80}$ attempts per minute, which far exceeds the operational capabilities that any Brick model can support.

2.5.3.2 Password-Based Authentication

Crypto Officers can log into the Brick serial port console using a password, which implicitly identifies the operator as a Crypto Officer. Crypto Officers can input commands and configuration data using the serial console. Passwords are required to be at least 6 characters long. The Brick enforces the minimum password length. Passwords are obscured with an asterisk * character as they are entered. Numeric, alphabetic (upper and lower case), and punctuation characters (. ? ~ ! @ $ % ^ & - _ + = < > ' * , : / `) can be used, which gives a total of 83 characters to choose from. The number of potential 6-character passwords is 83^6. The probability of success with a single attempt is 83^{-6}, which is less than 1 in 10^6. The Brick imposes a 3-second delay after a failed serial port console password attempt, which means a maximum of 20 attempts per minute. The probability of success with multiple consecutive attempts in one minute is 20×83^{-6}, which is less than 1 in 10^5.

2.5.3.3 IKE Preshared-Key-Based Authentication

Users can establish authenticated IKE/IPsec connections with Bricks using pre-shared keys. IPsec connections that have been established using IKE pre-shared key-based authentication can be used to secure network traffic. Pre-shared keys are required to be at least 8 characters long. The Brick enforces the minimum preshared key length. Valid characters include a-z, A-Z, 0-9, and the 15 following special characters (: ; | + ? " ( ) < > ^ % $ # &) which gives a total of 77 characters to choose from. The number of potential 8-character passwords is 77^8. The probability of success with a single attempt is 77^{-8}, which is less than 1 in 10^6. To exceed a 1 in 10^5 probability of a successful random attempt, an attacker would have to be capable of $10^{-5}/77^{-8}$ pre-shared key attempts per minute, which far exceeds the operational capabilities that any Brick model can support.

2.5.3.4 IKE Certificate-Based Authentication

Users can establish authenticated IKE/IPsec connections with Bricks using certificates. The strength of the IKE certificate-based authentication mechanism is the same as the TLS authentication mechanism. User certificate distinguished name attributes are parsed by the Brick from the certificate and sent to LSMS for checking. Crypto Officers must configure a minimum set of required attributes to check. User certificate distinguished name email (or other configured attribute) is parsed by the Brick from the certificate and sent to LSMS for checking (when passwords are required as a second authentication factor). The Brick then verifies users' certificates by building and verifying certificate paths and checking CRLs, according to configuration.

2.5.4 Bypass Mode

The Brick supports an alternating bypass. The Crypto Officer can configure the Brick to encrypt and decrypt data for certain IP addresses and also configure the module to send plaintext data for certain IP addresses using the Brick Zone Ruleset. The Brick is running in non-bypass mode when its configured Ruleset only contains rules defined with "Action" of "VPN" to determine how the encryption and decryption of IPsec packets will occur. The Brick is running in bypass mode when its Ruleset contains only other rules. The Brick is running in alternating bypass mode when its Ruleset contains one or more rules defined with "Action" of "VPN" and one or more other rules.

2.6 Physical Security

The modules were tested and found conformant to the Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) requirements specified by Title 47 of the Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC are multi-chip standalone cryptographic modules. The entire contents of the modules, including all hardware, firmware and data are enclosed in a metal case. There are different cases for each model. Each case is opaque with ventilation openings that have obstruction with a substantial foam blocking material. Each case is sealed using tamper-evident labels in order to prevent the case cover from being removed without signs of tampering. All circuits in the modules are coated with commercial standard passivation.

All Brick models use tamper-evident labels. Labels are placed in different locations for different Brick models, as described in the following sections. There are tamper-evident labels that Crypto Officers must apply. The tamper-evident labels must be installed during Brick installation and configuration according to "Secure Operation" procedures. Tamper-evident labels that Crypto Officers must apply will be packed with each Brick.

2.6.1 Brick 150

2.6.1.1 Factory-Installed Labels

There is a single factory-installed tamper-evident label on the top side of the appliance chassis that does not need to be removed or replaced. The label spans the top half of the chassis and the bottom half of the chassis (the top half is removable).

2.6.1.2 Crypto Officer-Installed Labels

There are Crypto Officer-installed tamper-evident labels that must be installed as depicted in the figures below:

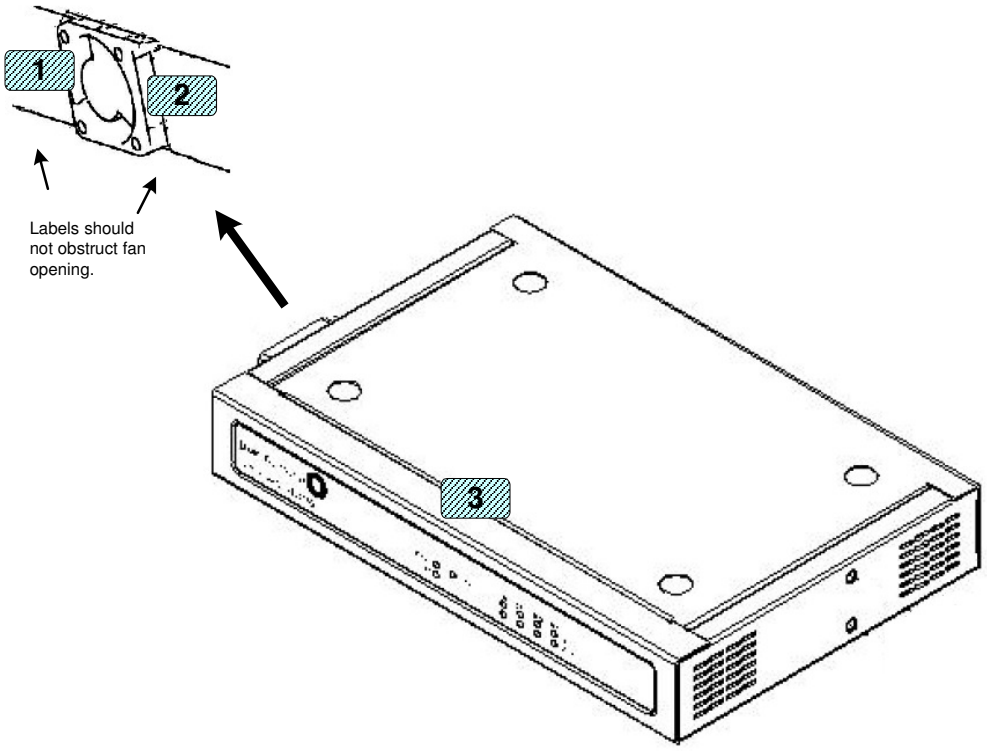

Figure 4 – Crypto Officer Label Placement for the Right and Left Sides of the Brick 150

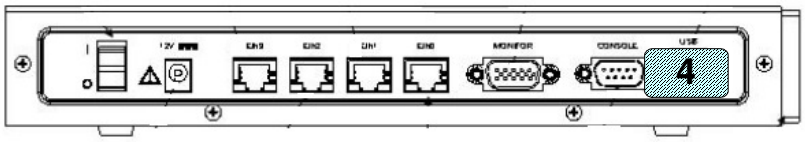

Figure 5 – Crypto Officer Label Placement for the Rear Sides of the Brick 150

The labels must be installed according to the guidance provided in the following table.

Table 6 – Brick 150 Label Placement Guidance

Label #	Description of Label Placement Location

Label #	Description of Label Placement Location
1	Spans one side of the fan and the right-hand side of the chassis
2	Spans the other side of the fan and the right-hand side of the chassis
3	Spans the two sections of the chassis that separate when removing the top cover. Note that if there are existing stickers, they must either be replaced by new stickers or the new stickers must be placed to either immediate side of the existing sticker.
4	Covers USB port on the rear of the chassis entirely

2.6.2 Brick 700

2.6.2.1 Factory-Installed Labels

There is are two factory-installed tamper-evident label on the top side of the appliance chassis that do not need to be removed or replaced. The labels cover screws which must be removed before the top half of the chassis can be removed.

2.6.2.2 Crypto Officer-Installed Labels

There are Crypto Officer-installed tamper-evident labels that must be installed as depicted in the figures below:

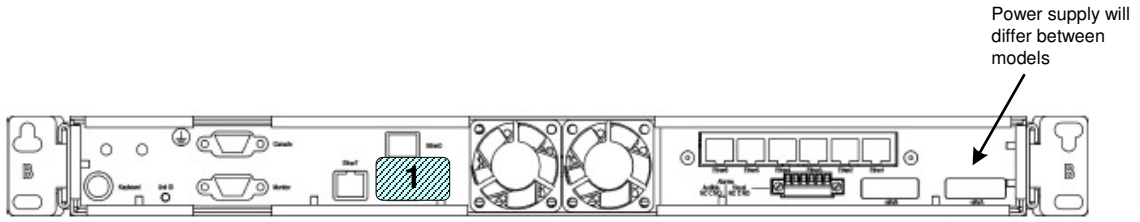

Figure 6 – Crypto Officer Label Placement for the Rear of the Brick 700

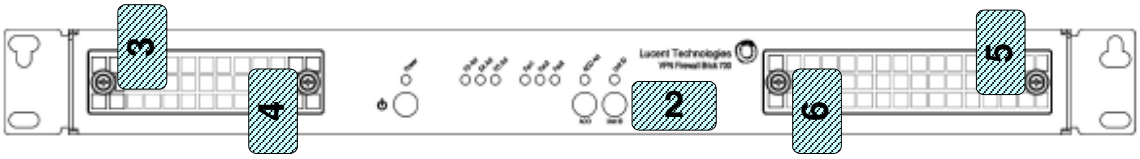

Figure 7 – Crypto Officer Label Placement for the Front of the Brick 700

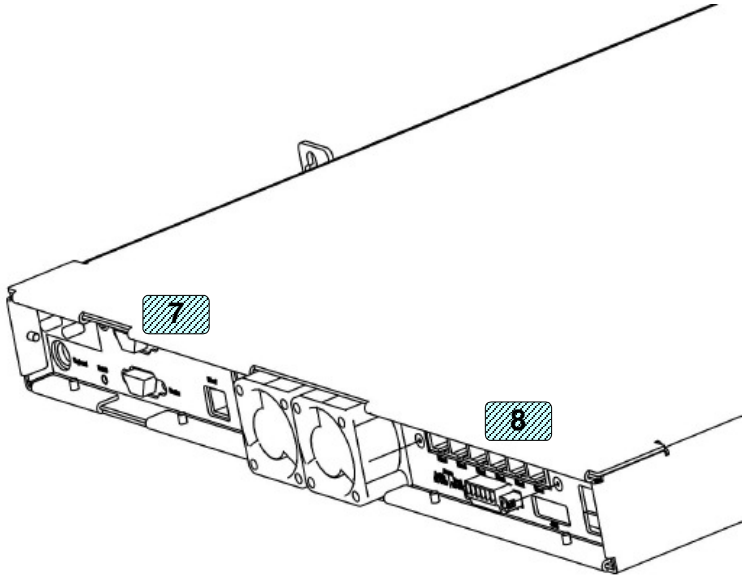

Figure 8 – Crypto Officer Label Placement for the Top of the Brick 700

The labels must be installed as follows:

Table 7 – Brick 700 Label Placement Guidance

Label #	Description of Label Placement Location
1	Covers the USB port on the rear of the chassis entirely
2	Covers USB ports on the front of the chassis entirely
3	Spans the top of the leftmost fan cover and the front of the chassis. The portion of the label that covers the fan cover must cover the flat portion of the fan cover that is towards the center of the fan cover, so that it is not only covering the grate
4	Spans the bottom of the leftmost fan cover and the front of the chassis. The portion of the label that covers the fan cover must cover the flat portion of the fan cover that is towards the center of the fan cover, so that it is not only covering the grate
5	Spans the top of the rightmost fan cover and the front of the chassis. The portion of the label that covers the fan cover must cover the flat portion of the fan cover that is towards the center of the fan cover, so that it is not only covering the grate
6	Spans the bottom of the rightmost fan cover and the front of the chassis. The portion of the label that covers the fan cover must cover the flat portion of the fan cover that is towards the center of the fan cover, so that it is not only covering the grate
7	Covers the screw hole on the top of the chassis entirely. Note that if there are existing stickers, they must either be replaced by new stickers or the new stickers must be placed to either immediate side of the existing sticker.
8	Covers the screw hole on the top of the chassis entirely. Note that if there are existing stickers, they must either be replaced by new stickers or the new stickers must be placed to either immediate side of the existing sticker.

2.7 Operational Environment

The operational environment requirements do not apply to the Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC. The modules do not provide a general purpose Operating System (OS) and only allow the updating of image components after checking a Digital Signature Algorithm (DSA) signature on new software images. Crypto Officers can install a new firmware image on a Brick by downloading the new image to the Brick via USB. This image is signed by a DSA private key (which never enters the modules) and includes the matching public key certificate as part of the download. The Brick verifies the signature on the new firmware image using the public key in the embedded certificate. If the verification passes, the upgrade is allowed. Otherwise the upgrade process fails and the old image is reused.

Notice that the USB ports can only be used during installation. The USB ports are required to be covered with tamper-evident seals after installation.

2.8 Cryptographic Key Management

2.8.1 Cryptographic Algorithms

The cryptographic modules implement the following FIPS-approved algorithms:

Implemented in Software:

- AES (CBC mode, 128, 192, 256 key sizes) Certificate #672
- TDES (CBC mode 3-key, 2 implementations) Certificates #617 and #620
- Secure Hash Algorithm (SHA)-1 (byte oriented, 2 implementations) Certificates #705 and #708
- Hashed Message Authentication Code (HMAC)- SHA-1 (key size = block size, block size = 20 bytes 2 implementations) Certificates #356 and #359
- DSA (sign/verify 1024, 2 implementations) Certificates #253 and #256
- FIPS 186-2 PRNG (K-Org, SHA-1, seed key = 64 bytes) Certificate #391

Implemented in Hardware (for Hardware version 150, Hifn 7955):

- AES (CBC mode, 128, 192, 256 key sizes) Certificate #747
- TDES (CBC mode, 3-key) Certificate # 664
- SHA-1 (byte-oriented) Certificate # 762
- HMAC-SHA-1 (key size = block size, block size = 20 bytes) Certificate # 405

Implemented in Hardware (for Hardware version 700, Hifn 7956):

- AES (CBC mode, 128, 192, 256 key sizes) Certificate #101
- TDES (CBC mode, 3-key) Certificate #214
- SHA-1 (byte-oriented) Certificate #193
- HMAC-SHA-1 (key size = block size, block size = 20 bytes) Certificate #220

The cryptographic module also contains the following non-Approved algorithms:

- Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 112 bits of encryption strength); allowed in FIPS mode
- Non-Approved Random Number Generator (RNG)
- Symmetric Key Algorithms – DES, ARC4
- Hashing Algorithms –MD5
- ElGamal

- RSA (non-compliant)

2.8.2 CSPs

The module features the following critical security parameters:

2.8.2.1 Brick Certificate and Brick Private Key

The Brick certificate is an X.509 certificate (1024-bit DSA with SHA-1) that is generated by the LSMS built-in CA after LSMS first generates the key pair (the corresponding private key is called the "Brick private key") during Brick installation. The Brick certificate is presented by the Brick to LSMS as authentication data when establishing a TLS connection. The Brick certificate and the Brick private key are both stored in plaintext in configuration files in Brick flash. The Brick certificate and the Brick private key are both loaded during bootstrap. The Brick certificate is output during TLS (either using AES or TDES) key establishment. The Brick private key is not output.

2.8.2.2 LSMS Public Key

The LSMS public key is a copy of the 1024-bit DSA public key of the LSMS built-in CA that is generated during LSMS installation. The LSMS public key is used to build and verify certificate paths involving LSMS CA-issued certificates. LSMS public key is stored in plaintext in configuration files in Brick flash. The LSMS public key is loaded during bootstrap. The LSMS public key is not output.

2.8.2.3 Brick Name

The Brick name is the subject name of the Brick certificate. It can be used to effectively revoke the Brick certificate by changing its value using LSMS, since the LSMS built-in CA does not generate revocation lists. The Brick name is stored separately than the Brick certificate in plaintext in configuration files in Brick flash. The Brick name is loaded during bootstrap. The Brick name is not output.

2.8.2.4 Serial Port Password

The serial port password is the password used to authenticate Crypto Officers to the Brick using the Brick serial port console interfaces. It is used to implicitly identify the operator as a Crypto Officer. The serial port password is stored in plaintext in configuration files in Brick flash. The serial port password is loaded during bootstrap. The serial port password is not output.

2.8.2.5 Brick VPN Certificate and Brick VPN Private Key

The Brick VPN certificate is an X.509 certificate (1024-bit DSA with SHA-1) that is generated by an external CA after LSMS first generates the key pair and corresponding certificate request during Brick installation. The Brick VPN certificate is presented by the Brick to User operators' IPsec client applications or to another Brick as authentication data when IKE has been configured in either or both cases to use certificate-based authentication. The Brick VPN certificate and the Brick VPN private key are both stored in plaintext in configuration files in Brick flash. The Brick VPN certificate and the Brick VPN private key are loaded during VPN certificate update. The Brick VPN certificate is output during IPsec/IKE (either client or LAN-LAN tunnels when configured for certificate authentication). The Brick VPN private key is not output.

2.8.2.6 CA Certificates and CA CRLs

The CA certificates are issuing and intermediate external CA X.509 certificates (1024-bit DSA with SHA-1). External CA certificates and CRLs are used to build and verify certificate paths involving external CA-issued certificates when IKE has been configured for client tunnels to use certificate-based authentication. The external CA

certificates and CRLs are stored in plaintext in configuration files in Brick flash. The external CA certificates are loaded during VPN CA certificate update. The CRLs are loaded during VPN CRL update.

2.8.2.7 Preshared Key for Client Tunnels

The preshared key for client tunnels is presented by User operators' IPsec client applications as authentication data when IKE has been configured to use preshared key-based authentication. The preshared key for client tunnels is stored in plaintext in configuration files in Brick flash. The preshared key for client tunnels is loaded during config file update. The preshared key for client tunnels is not output.

2.8.2.8 Preshared Key for LAN-LAN Tunnels

The preshared key for LAN-LAN tunnels is presented by one Brick to another LAN as authentication data when IKE has been configured to use preshared key-based authentication. There is one preshared key for LAN-LAN tunnel for each LAN-LAN tunnel. IPsec/IKE is configured separately for client and for LAN-LAN tunnels. The preshared key for LAN-LAN tunnels is stored in plaintext in configuration files in Brick flash. The preshared key for LAN-LAN tunnels is loaded during config file update. The preshared key for LAN-LAN tunnels is not output.

2.8.2.9 LAN-LAN Data Encryption Key

The LAN-LAN data encryption key is a 128/192/256-bit AES or 168-bit TDES key. If Encapsulating Security Protocol (ESP) data encryption has been configured, it is used to encrypt data in a LAN-LAN configuration when IKE has not been configured for use with IPsec. Crypto Officers enter this key into the LSMS Graphical User Interface (GUI), and LSMS in turn sends the key to the Brick after a TLS connection has been established. The LAN-LAN data encryption key is stored in plaintext in configuration files in Brick flash. The LAN-LAN data encryption key is loaded during config file update. The LAN-LAN data encryption key is not output.

2.8.2.10 LAN-LAN Data Authentication Key

The LAN-LAN data authentication key is a 160-bit HMAC-SHA-1 key. If either Authentication Header (AH) or ESP data authentication has been configured, it is used to authenticate data in a LAN-LAN configuration when IKE has not been configured for use with IPsec. Crypto Officers enter this key into the LSMS GUI, and LSMS in turn sends the key to the Brick after a TLS connection has been established. The LAN-LAN data authentication key is stored in plaintext in configuration files in Brick flash. The LAN-LAN data authentication key is loaded during config file update. The LAN-LAN data authentication key is not output.

2.8.2.11 Crypto Officer Public Key

The Crypto Officer Public key is a 1024-bit DSA public key used to verify the integrity of the tvpc file during tvpc upgrade. After the validity of the Crypto Officer Public key certificate is verified (using the LSMS public key), the module will use the Crypto Officer Public key to verify the signature of the tvpc file. The Crypto Officer Public key is loaded each time during tvpc upgrade and not stored within the module.

2.8.2.12 CRC Checksums

The CRC checksums are 32-bit checksums that are used by the Brick to compare against the calculated checksum of the tvpc or the tvpc.zip when the Brick boots. It is generated at the factory and provided as part of the tvpc file included with the LSMS distribution. The CRC checksum is appended to the tvpc file (either the uncompressed tvpc or the compressed tvpc.zip or both depending on configuration) in Brick flash. The CRC checksum is loaded during boostrap and during tvpc update. The CRC checksum is not output.

2.8.2.13 Diffie-Hellman Group and Parameters

The Diffie-Hellman Oakley groups are used by Brick TLS and IKE Diffie-Hellman implementations to establish TLS protocol and IKE 128-bit AES or 168-bit TDES ephemeral session keys. The Brick supports 1024-bit, 1536-bit, and 2048-bit Diffie-Hellman using the exponent defined for IKE Group 2, Group 5, and Group 14, respectively. The configured Diffie-Hellman group and its parameters are stored in plaintext in configuration files in Brick flash. The configured Diffie-Hellman group and its parameters are is loaded during config file update. The configured Diffie-Hellman group and its parameters are not output.

2.8.2.14 TLS Session Keys

The TLS session key is a 128-bit AES or 168-bit TDES ephemeral session key where AES is used only for audit channels. It is established using Diffie-Hellman. It is used to encrypt LSMS-Brick communication. The TLS session key is stored in plaintext in Brick Random Access Memory (RAM).

2.8.2.15 IKE Session Keys

The IKE session key is a 128/192/256-bit AES or 168-bit TDES ephemeral session key. It is established using Diffie-Hellman. It is used to encrypt AH and ESP Security Association (SA) negotiation messages when establishing client tunnels (and/or LAN-LAN tunnels if IKE has been configured for use with IPsec for LAN-LAN tunnels). It is generated while negotiating the ISAKMP SA. The IKE session key is stored in plaintext in Brick RAM.

2.8.2.16 IPsec Data Encryption Session Keys

The IPsec data encryption session key is a 128/192/256-bit AES or 168-bit TDES ephemeral session key. It is established as a result of ESP SA negotiation messages. It is used to encrypt client tunnels (and/or LAN-LAN tunnels if IKE has been configured for use with IPsec for LAN-LAN tunnels). It is generated while negotiating the ISAKMP SA. The IPsec data encryption session key is stored in plaintext in Brick RAM.

2.8.2.17 IPsec Data Authentication Session Keys

The IPsec data authentication session key is a 160-bit HMAC-SHA-1 ephemeral session key. It is established as a result of AH (or ESP, if data authentication has been configured) SA negotiation messages. It is used to authenticate (data, not operators) client tunnels (and/or LAN-LAN tunnels if IKE has been configured for use with IPsec for LAN-LAN tunnels). It is generated while negotiating the ISAKMP SA. The IPsec data encryption session key is stored in plaintext in Brick RAM.

2.8.2.18 Ruleset

The ruleset can be input or upgraded by Crypto Officers via LSMS GUI. The ruleset is stored in the policy file in plaintext. The policy file is stored in plaintext in Brick flash. The ruleset is loaded during policy file update. The ruleset is not output.[5]

2.8.2.19 PRNG Seed-Key

The PRNG seed-key is a value that is generated by Brick hardware used as input to the FIPS 186-2 Appendix 3.2 PRNG. The PRNG seed-key is stored in plaintext in Brick RAM. The PRNG seed-key is not output.

---

[5] LSMS maintains a copy of the ruleset each time it sends it to the Brick.

2.8.3 CSP Zeroization

2.8.3.1 Persistent CSPs

After the Brick has been zeroized, CSPs will have been overwritten, the "tvpc" boot image (if there was one as the result of an upgrade) will have been deleted, and the original "tvpc.zip" that had been installed on the Brick at the factory will have been restored, overwriting any tvpc.zip that had been installed on the Brick previously. The Brick VPN secret key is not zeroized. However, it is not considered a key/CSP.

2.8.3.2 Ephemeral CSPs

All ephemeral CSPs such as session keys are zeroized when the sessions are over. They can also be zeroized on demand by rebooting the Brick.

2.9 Self-Tests

The Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC perform the following self-tests at power-up:

- Firmware integrity test
- Known Answer Test (KAT) on AES (encrypt/decrypt)
- KAT on TDES (encrypt/decrypt)
- KAT on SHA-1
- KAT on HMAC-SHA-1
- DSA pairwise consistency test (sign/verify)
- Diffie-Hellman pairwise consistency test
- KAT on the FIPS 186-2 Appendix 3.2 PRNG

The Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC perform the following conditional self-tests:

- Continuous random number generator test for the FIPS 186-2 Appendix 3.2 PRNG
- Continuous random number generator test for the non-Approved RNG
- Firmware load test
- Bypass test

2.10 Mitigation of Other Attacks

The modules do not claim to mitigate other attacks in a FIPS mode of operation.

3 Secure Operation

The Alcatel-Lucent VPN Firewall Bricks 150, 700 AC, and 700 DC meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the modules in a FIPS-approved mode of operation.

3.1 Initial Setup

3.1.1 Installing the Brick

First, the Crypto Officer must unpack and inspect the Brick according to the User's Guide. Installation and configuration instructions for the Bricks can also be found in the User's Guide. Each model of Brick has its own User's Guide which contains installation instructions, maintenance information, safety tips, and more.

Next, the Crypto Officer must load a Brick boot image using a non-serial port bootstrap method, which consists of copying files generated by LSMS to either a floppy or a flash disk and then loading them onto the Brick.

> Warning: There is a bootstrap method option to use the serial port, but this method must not be used, it does not copy FIPS validated executable files onto the Brick, only configuration files.

Finally, the Crypto Officer must apply the supplied tamper-evident labels as described in Section 2.6 of this document. Note that labels require 12 hours to cure.

3.1.2 Setting up LSMS

The Crypto Officer is responsible for the proper initial setup of the LSMS software and the VPN Firewall Bricks. Setup of the LSMS software is done by installing the software on an appropriate Windows or Solaris server. Specific instructions for initial setup can be found in Section 1 of *Lucent Security Management Server Administrative Guide*.

3.2 Module Initialization and Configuration

3.2.1 Configuring LSMS-Brick Communication

The Crypto Officer is responsible for configuring the Bricks to work in the FIPS mode of operation. FIPS mode can only be enabled or disabled using the LSMS software.

To enable FIPS mode, in LSMS, go to the Configuration Assistant window and edit the "FIPS" parameter. Check the "Enable FIPS 140-2 Mode" box.

3.2.2 Initializing the Brick

The Crypto Officer must perform the initial configuration. The version indicated on the cover page is the only allowable image; no other images may be loaded. Specific instructions for Brick initialization and configuration can be found in Section 2 of *Lucent Security Management Server Administrative Guide*.

Only non-serial port boostrap methods are allowed in the FIPS mode of operation. The Crypto Officer must not use serial port to boostrap the Brick. The Crypto Officer needs to protect disk/flash regardless of whether or not password is used to encrypt the flash image. To create a new bootstrap image, the Crypto Officer can use either serial or non-serial port methods. For detailed instructions on the initialization and configuration process, please see Section 3 of the *Lucent Security Management Server Administration Guide.*

The Crypto Officer must not perform the "upgrade" operation after installation and configuration, unless the Crypto Officer is upgrading the Brick to a newer FIPS 140-2 validated version.

3.2.3 Configuring the Brick Serial Port

If you intend to use the Brick serial port to access the command line interface, go to the *Options* tab and click the *Enable Serial Port* checkbox, and enter a password twice, once in the Remote Password field and again in the Verify Password field. The password can be from 6 to 72 characters (letters and numbers). The password is case sensitive, so capitalization must be consistent. To access the command line interface, you can connect a terminal or a modem to the Brick serial port. Serial port parameters are 115,200 baud, no parity, 8 data bits and 1 stop bit.

3.3 IPsec Requirements and Cryptographic Algorithms

3.3.1 IPsec/IKE Requirements

The Crypto Officer must select from the following settings during Brick configuration to configure it to operate in FIPS mode.

Client tunnels allow the use of following approved and allowed cryptographic functions:

- IKE
  - User authentication methods allowed: either preshared keys or certificates (DSA with SHA-1)
  - Phase 1 Main Mode and Aggressive Mode key establishment: Diffie-Hellman Group 2, Group 5, or Group 14
  - Phase 2 Quick Mode MAC: HMAC-SHA-1
  - Phase 2 Quick Mode symmetric key generation: AES CBC 128/192/256-bit or TDES CBC 168-bit
- IPsec - AH
  - MAC: HMAC-SHA-1
- IPsec - ESP
  - MAC, if configured: HMAC-SHA-1
  - Symmetric key encryption: AES CBC 128/192/256-bit or TDES CBC 168-bit

LAN-LAN tunnels allow the use of following approved and allowed cryptographic functions:

- IKE
  - User authentication methods allowed: either preshared keys or certificates
  - Phase 1 Main Mode and Aggressive Mode key establishment: Diffie-Hellman Group 2, Group 5, or Group 14
  - Phase 2 Quick Mode MAC: HMAC-SHA-1
  - Phase 2 Quick Mode symmetric key generation: AES CBC 128/192/256-bit or TDES CBC 168-bit
- IPsec - AH
  - MAC: HMAC-SHA-1
- IPsec - ESP
  - MAC, if configured: HMAC-SHA-1
  - Symmetric key encryption: AES CBC 128/192/256-bit or TDES CBC 168-bit

LAN-LAN tunnels also allow the use of following approved and allowed cryptographic functions using manual key entry (ESP symmetric keys are entered into the LSMS then loaded onto each Brick by LSMS):

- IPsec - AH
  - MAC: HMAC-SHA-1
- IPsec - ESP
  - MAC, if configured: HMAC-SHA-1
  - Symmetric key encryption: AES CBC 128/192/256-bit or TDES CBC 168-bit

3.3.2 External CA Requirements

The Brick relies on an external CA to provide certificates for use with IPsec tunnels operating in the approved encrypting modes when certificate-based IKE authentication is used. These certificates are called VPN certificates. Each Brick can be configured with its own VPN certificate. Only Brick VPN certificates that use DSA with SHA-1 are supported for IKE certificate-based authentication when the Brick is operating in FIPS mode. The Brick provides built-in support for Entrust and VeriSign CAs. For more information about supported CAs see Section 10 of *Lucent Security Management Server Policy Guide*[6]. LSMS generates new Brick VPN key pairs and corresponding certificate requests and send to external CAs. Instructions to generate a new Brick VPN key pair and certificate request can be found in Section 10 of *Lucent Security Management Server Policy Guide*. Notice that the sizes for DSA scheme used must be at least 1024 bits. Instructions to import a VPN certificate (and issuing CA certificate, and CRLs) into LSMS and assign the imported VPN certificate to the Brick and then load it on the Brick can be found in Section 10 of *Lucent Security Management Server Policy Guide*.

3.3.3 Configuring LAN-LAN Tunnels

Instructions to configure two Bricks such that they are operating in a LAN-LAN configuration can be found in Section 11 of *Lucent Security Management Server Policy Guide*. The *Policy Guide* document explains how to set up a LAN-LAN tunnel between two devices so that hosts behind both devices will be able to communicate securely with one another over a public network such as the Internet. Step-by-step instructions to setup a LAN-LAN tunnel in LSMS can be found in "How to Set Up a LAN-LAN Tunnel" in Section 10 of *Lucent Security Management Server Policy Guide*.

3.3.4 Configuring Client Tunnels

The Brick supports IKE v1 and v2 and IPsec v1 and v2 client tunnels (IPsec connections between client users and the Brick) that operate in approved encrypting modes. The Brick supports preshared key and certificate-based user authentication in approved encrypting modes, according to configuration. The Brick supports username and password, RADIUS, and SecurID second factor authentication mechanisms as well, according to configuration. Instructions to configure a Brick such that it can be used to establish client tunnels can be found in Section 12 of *Lucent Security Management Server Policy Guide*. The *Policy Guide* document explains how to set up a client tunnel endpoint so that users of the Lucent IPsec Client application (or a compatible IPsec client application) can establish a tunnel between their hosts and a Brick. If certificates are used for authentication for client tunnels, they must be obtained before the Brick can be configured to support client tunnels that use certificate-based authentication. Creating client tunnels using LSMS includes creating a certificate-based authentication service, creating a client tunnel (which includes configuring IPsec services such that they operate in an approved encrypting mode), and then creating client tunnel users. Note that when a non-Entrust CA is used as the external CA, client tunnel users must be configured to use the LSMS local password service.

3.4 Zeroizing Keys and CSPs

CSPs stored in the flash can be zeroized by initializing the flash. CSPs in all Brick models are zeroized using the same procedures. Zeroization consists of connecting to the Brick using a serial terminal and issuing an "initialize flash" command. Use the following instructions to zeroize CSPs:

1. Power up the Brick.

[6] Minimally CA certificates in addition to basic constraints indicating the certificate is for a CA, and subject and authority key identifiers, must include digital signature, non-repudiation, key encipherment, data encipherment, certificate sign, and CRL sign extensions

2. Connect to the Brick's serial port. Log in using the Brick general command "login" as described in section 13 of the *Tools and Troubleshooting Guide*.
3. Disconnect all Ethernet cables from the Brick.
4. Wait until the console displays the error message "EUA Connection to *Brick IP address here* lost".
5. Enter the following Brick command: "initialize flash" and then the press the <return> key.
6. Enter "y" then press the <return> key when prompted "This will cause the Brick to return to factory state. Proceed (y/n)".
7. Enter "y" then press the <return> key when prompted "Brick will initialize flash and reboot immediately. Are you sure? (y/n)".
8. Verify that the console displays the message "Initializing flash, Please wait…".
9. After the "initialize flash" command completes, the Brick will automatically reboot. After the Brick reboots, verify that the console displays the message "*date/time stamp* – This Brick is in factory-ship state. Bootstrap the Brick".

3.5 Identifying the Error State

The error messages are sent to the console interface. The console interface in Bricks 150 and 700 is the serial port and monitor port. Other status output interfaces in general are not used to indicate FIPS-related status information.

3.6 Maintaining Physical Security

See Section 2.6 of this document for locations of tamper-evident labels. The operator shall examine the enclosure regularly and see if there are signs of tamper attempts. If damage to tamper-evident labels is found, then the device is not considered operating in the FIPS mode of operation. The device must be returned to factory for service before it can operate in the FIPS mode of operation again.

3.7 Determining the FIPS Mode of Operation

If and only if the device has been configured according to the instructions in Sections 3.1, 3.2, and 3.3 of this document, it is operating in the FIPS mode of operation.

4 Acronyms

Table 8 – Acronyms

Acronym	Definition
AC	Alternating Current
AES	Advanced Encryption Standard
AH	Authentication Header
ARP	Address Resolution Protocol
CA	Certification Authority
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSP	Critical Security Parameter
CPU	Central Processing Unit
DC	Direct Current
DSA	Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Protocol
DES	Digital Encryption Standard
FIPS	Federal Information Processing Standard
GBIC	Gigabit Interface Converter
GUI	Graphical User Interface
HD	Hard Drive
HMAC	Hashed Message Authentication Code
HS	High Speed
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security
IT	Information Technology
KAT	Known Answer Tests
LED	Light Emitting Diodes
LSMS	Lucent Security Management Server
MAC	Media Access Control

Acronym	Definition
NIST	National Institute of Standards and Technology
OS	Operating System
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SA	Security Association
SFP	Small Form-factor Pluggable
SHA	Secure Hash Algorithm
TDES	Triple Digital Encryption Standard
TLS	Transport Layer Security
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network