National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Lucent Technologies

Lucent VPN Firewall (LVF)

Version 7.2 with patch 292

Report Number: CCEVS-VR-06-0005

Dated: 19 January 2006

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

The Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Arca Common Criteria Testing Laboratory
Sterling, VA

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of Lucent Technologies Lucent VPN Firewall V7.2 with patch 292. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by the Arca Common Criteria Testing Laboratory (CCTL), and was completed during January 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by the CCTL. The evaluation determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of **EAL4.** No conformance to any published Protection Profile (PP) is claimed.

The Lucent VPN Firewall is a traffic-filter firewall. The product controls the flow of Internet Protocol (IP) datagrams by matching information contained in IP and higher layer headers against a set of rules specified by the firewall's administrator. This header information includes source and destination host IP addresses, source and destination port numbers, and upper level protocol identifier; e.g., transmission control protocol (TCP), user datagram protocol (UDP). Depending upon the rule and the results of the match, the firewall either passes or drops the packet. In addition to protocol header information, the product uses other information, such as the direction (incoming or outgoing) of the packet on a given firewall interface.

The primary security features for the LVF are:

- **Stateful packet filtering**: Rather than processing each packet individually, every packet processed by the firewall is considered part of a "session", regardless of IP type or higher-layer protocol.
- **Logging**: All logging is done in real-time by the firewall appliance and forwarded to its management server (LSMS). Apart from the logging of events on the VPN Firewall appliance (referred to as the "brick") the LSMS also records administrative events and user authentication events.
- **Policy objects**: LSMS resources are divided into groups wherein each group contains a set of resources. Enterprises can implement a single group that encompasses the entire enterprise, or multiple LSMS Groups.
- **Reporting**: The LSMS has the ability to generate HTML-based reports and provide them via its own internal secure (HTTPS) web server. The internal web server is a Lucent-developed web server that only communicates with the LSMS and provides no external TOE interfaces.
- **Remote administration:** An LSMS can manage multiple firewall appliances that are located remotely (i.e., not directly connected) via a secure connection. Additionally, the TOE supports a remote LSMS Navigator that can be used to manage an LSMS remotely, via a secure connection.

The validation team monitored the activities of the evaluation team, participated in team meetings, 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), witnessed testing, and reviewed successive versions of the evaluation technical report (ETR) and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST) for an EAL4 evaluation. Therefore, the validation team concludes that the CCTL findings are accurate, and the conclusions justified.

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, security evaluations are conducted by 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.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation 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;
- 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	Lucent VPN Firewall Version 7.2 with patch 292
Protection Profile	None
Security Target	*Lucent Technologies Lucent VPN Firewall Version 7.2 (Patch 292) Security Target Version 2.1, December 13, 2005*
Evaluation Technical Report	*Evaluation Technical Report for Lucent VPN Firewall (LVF) Version 7.2 with patch 292*; December 15, 2005
Conformance Result	Part 2 conformant, Part 3 conformant, EAL 4

Sponsor	Lucent Technologies
Developer	Lucent Technologies
Evaluators	Arca Common Criteria Testing Laboratory
Validators	The Aerospace Corporation

3. SECURITY POLICY

3.1. Traffic Filtering

As noted above, the firewall will either allow or block network traffic based upon a set of rules, configurable by the administrator, which use the following characteristics of the traffic:

- presumed address of the source;
- presumed address of the destination;
- transport layer protocol;
- interface on which the traffic is received and departs (i.e., trusted network or untrusted network);
- service;
- time of day.

3.2. I&A

Only authorized administrators may perform the management functions supported by the LSMS, and administrators must be successfully authenticated prior to being able to perform any management functions. Administrators only log onto the LSMS, as no user accounts are supported on the firewall appliance.

4. ASSUMPTIONS

4.1. Usage Assumptions

Although there are several assumptions stated in the Security Target[1], the primary conditions are that

- The TOE executes no arbitrary user processes; the only code that executes on the TOE is the firewall and LSMS code;
- Administrators are authorized, non-malicious, and competent;
- The TOE components are physically protected from unauthorized physical access, and that only authorized administrators have access to the TOE.

[1] See section 3.1 of the ST

4.2. Environmental Assumptions

The IT environment for the TOE consists of:

- The hardware platform and O/S (i.e., Windows or Solaris) for the administrator workstation;
- The hardware platform and O/S (i.e., Windows) for the LSMS Remote Navigator

The essential assumptions for the IT environment are that no non-TOE applications are hosted, and that the elements of the IT environment are physically protected.

5. ARCHITECTURAL INFORMATION

The TOE consists of three components:[2]

- The Lucent VPN Firewall Appliance (FA), which controls the flow of IP traffic between network interfaces. The FA (also referred to as "the brick") runs on *Inferno*, a Bell Labs-developed operating system. Both the *Inferno* O/S and the hardware platform for the FA are defined as being within the TOE boundary.

- The Lucent Security Management Server (LSMS) software package, which provides the capability for administrators to manage one or more firewall appliances. The LSMS executes on either a Windows or Solaris O/S and although the LSMS software and the host platform are jointly referred to as "the LSMS," both the hardware and the hosting O/S are defined as being in the IT environment (i.e., are not included in the TOE boundary).

- The Lucent Security Management Server Remote Navigator, a GUI client that enables administrators to manage one or more firewall appliances by remotely accessing the primary LSMS. The LSMS Remote Navigator client executes on a Windows platform, with both the O/S and the hardware that host the Remote Navigator being in the IT environment.

The firewall appliance is physically distinct from the management server. The LSMS is always directly connected to a firewall appliance, although not each firewall appliance need have a directly connected LSMS, as an LSMS may manage several firewall appliances. As noted earlier, the LSMS software runs on a separate Windows NT/Windows 2000 platform, which is defined as being in the IT environment.

The LSMS Remote Navigator, as the name implies, is intended to be remotely located—possibly on an external network—and can be used to manage firewall appliances by communicating with one of the LSMS'.

Communications between an LSMS and the firewall appliances, and between the LSMS Remote Navigator and the LSMS with which it is communicating are encrypted.[3]

---

[2] The reader is referred to the Security Target, Sections 2.2 and 2.3, for some illustrative configurations of these components

[3] Note: The encryption mechanisms were not evaluated as part of the evaluated configuration.

6. DOCUMENTATION

The TOE is delivered on a CD ROM, and includes the following administrator documentation:

- Lucent Technologies, Lucent VPN Firewall Version 7.2 (Patch 292) TOE ReadMe File (Version 2.5, December 13, 2005);
- Lucent Security Management Server v7.2 Installation Guide (Version 7.2-1, March 2004);
- Lucent Security Management Server v7.2 Administration Guide (Version 7.2-1, March 2004);
- Lucent Security Management Server v7.2 Reports, Alarms and Logs (Version 7.2-1, March 2004);
- Lucent Security Management Server v7.2 Tools and Troubleshooting Guide (Version 7.2-1, March 2004);
- Lucent Security Management Server v7.2 Technical Overview (Version 7.2-1, March 2004);
- Lucent Security Management Server v7.2 Brick Hardware Guide (Version 7.2-1, March 2004);
- Lucent Security Management Server v7.2 Policy Guide (Version 7.2-1, March 2004)

7. IT PRODUCT TESTING

7.1. Developer Testing

The developer's approach to security testing is essentially focused on the testing of the interfaces. For each TFSI, security checks and effects are identified, and tests devised for each. Test documentation includes a high-level test plan that describes the philosophy of testing, and provides a mapping between the system components, security functions (i.e., SFRs), and specific test cases.

Developer testing included tests for:

- LSMS logon
- Administrator interface
- Brick zone rulesets
- Log Viewer
- Restart LSMS Services
- Service groups
- Network interface
- LSMS Command Line Interface (CLI) lsmslogon
- LSMS Command line list brickruleset
- LSMS Command line save brickruleset

- Windows Command Line
- LSMS command line logout
- Windows 2000 Event Viewer
- Windows 2000 Date and Time
- Configuration Assistant

The developer's test documentation mapped test cases to each of the SFRs defined in the Security Target, also identifying both the externally-visible and the internal interfaces exercised by the test cases. Also described in the developer's documentation is the purpose of each of the various test cases and a description of how each exercises the TOE to demonstrate how compliance with the SFRs is achieved. Other mappings identify how each of the TOE subsystems are tested, and which externally-visible interfaces are exercised for each of the subsystems that comprise the TOE.

Each of the developer's functional test suites includes a high-level design document that describes the intent of the test suite, the APIs addressed, the testing approach (including expected test results), any special considerations, and instructions for using the test suite.

The evaluation team concluded that for the vast majority of interfaces test procedures had been defined to directly invoke the interface and test the security functions and/or effects. In cases for which interfaces could not be tested directly, procedures were devised to test the interface indirectly; for example, by testing the low-level function upon which the interface is built.

7.2. Evaluator Testing

Prior to testing, the evaluation team verified that the TOE was as identified in the ST, and then proceeded to install and configure the TOE as described developer's documentation, specifically:

- Installation guide;
- Administrative guide;
- Tools and troubleshooting guide;
- Policy guide;
- Installation readme file (V2.5).

A representative test configuration was implemented that was consistent with the Security Target, and which would allow testing of all claims for the various components of the TOE.

The test configuration allowed the evaluators to exercise management, via the LSMS, of a directly-connected brick; a remote brick (i.e., with no local LSMS); and management of the LSMS via a remote navigator, which then enables Remote Navigator to manage any and all bricks associated with the LSMS.[4]

[4] See the configuration shown in the Security Target in Figure 3: TOE Configuration #2.

The evaluation team executed a subset of the developer tests, chosen after an analysis of the developer's test coverage and depth mappings, determining areas where additional or negative testing would be beneficial. During the execution of the developer tests, the evaluation team confirmed that the test results were consistent with the expected test outcomes.

The evaluation team also devised a set of independent tests, in part covering areas that were felt to be missing from, or insufficiently covered by the developer's test suites. The evaluation team's conclusion is that between team and vendor testing, the entire TSF is addressed.

8. EVALUATED CONFIGURATION

The evaluated and tested configuration consists of:

- The VPN Firewall brick (both the 1100 and 350 models), running the Lucent Firewall (Inferno) operating system patched to level 292;
- The LSMS Console (LSMS software package 7.2 patched to level 292) hosted on Compaq DL 380 hardware running Windows 2000 Professional with Service Pack 4;
- LSMS Remote Navigator hosted on Compaq DL 380 hardware running Windows 2000 Professional with Service Pack 4.

9. RESULTS OF THE EVALUATION[5]

The evaluation team determined the product to be **CC Part 2 conformant, CC Part 3 conformant,** and to meet the requirements of **EAL 4**. No conformance to any Protection Profile (PP) is claimed. In short, the product satisfies the security technical requirements specified in *Lucent Technologies Lucent VPN Firewall Version 7.2 (Patch 292) Security Target Version 2.1, December 13, 2005*

10. EVALUATOR COMMENTS

There are no Evaluator Comments.

11. SECURITY TARGET

The ST, *Lucent Technologies Lucent VPN Firewall Version 7.2 (Patch 292) Security Target Version 2.1, December 13, 2005* is included here by reference.

[5] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

12. LIST OF ACRYONYMS

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
LSMS	Lucent Security Management Server
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Lucent Technologies Lucent VPN Firewall Version 7.2 (Patch 292) Security Target Version: 2.1, dated 13 December 2005.

[8] Evaluation Technical Report, for the Lucent VPN Firewall Version 7.2 (Patch 292), Version 5.0, December 15 2005.

[9] Lucent VPN Firewall Version 7.2 (Patch 292) Tests: Coverage, Depth, and Functional Tests (Proprietary); Version 1.0, October 10 2005.

[10] Lucent Technologies, Inc; Lucent VPN Firewall (LVF 7.2 with Patch 292; Team Test Plan Version 5.0, Version 5.0, December 15 2005 (Savvis Proprietary).