# National Information Assurance Partnership


TM

# Common Criteria Evaluation and Validation Scheme Validation Report

## Lucent Technologies

## Lucent VPN Firewall version 7.0 (Patch 531)

**Report Number: CCEVS-VR-03-0048**

**Dated: 29 October 2003**

**Version: 2.0**

**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

Donald Phillips, Lead Validator, Mitretek Systems

Mario Tinto, Validator, Aerospace Corporation

### Common Criteria Testing Laboratory

Cable and Wireless Common Criteria Testing Laboratory

Sterling, Virginia

## Table of Contents

# 1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of Lucent Technologies Lucent VPN Firewall V7.0 (Patch 531). 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 Cable and Wireless Common Criteria Testing Laboratory, and was completed during October 2003. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by Cable and Wireless. The evaluation determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of **EAL2.** Additionally, the product was found to be conformant with the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Final, Version 1.1 April 1999 (referred to as TFFPP).

The Lucent VPN Firewall V7.0 (Patch 531) is a traffic-filter firewall (referred to as LVF)[1] The product controls the flow of the 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 (for transmission control protocol (TCP) or user datagram protocol (UDP), e.g.). 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 LVF provides the following features.

The primary security features for the LVF are:

- **Stateful Packet filtering**: Every packet process by the VPN Firewall brick[2] is considered part of a "session", regardless of IP type or higher-layer protocol instead of processing each and every packet individually.
- **Logging**: All logging is done in real-time from the VPN Firewall brick to its management server (LSMS). Apart from the logging events on the VPN Firewall brick the LSMS also logs administrative events and user authentication events.
- **Policy objects**: LSMS resources are divided into groups where each group contains a set of resources. Enterprises can use a single group or multiple LSMS Groups.

[1] Although the vendor's designation for this product is *Lucent VPN Firewall*, neither the definition of the TOE nor the evaluation included VPN features. Thus, this report should not be understood to imply any judgment relative to the VPN capability provided by the vendor's product.

[2] The Lucent VPN Firewall Appliance is also commonly referred to as the Lucent VPN "Brick"

- **Reporting**: The LSMS has the ability to generate HTLM-based reports and serve them via its own internal secure (HTTP or HTTPS). The internal web server is a Lucent-developed web server that only communicates with the LSMS and provides no external TOE interfaces.

The Target of Evaluation (TOE) does not make any claims or references to any cryptographic functions, nor does the TOE defined for this evaluation support the remote administration feature that is packaged with the product.

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), and reviewed successive versions of the 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 EAL2 evaluation, and is conformant with the requirements of the Traffic Filter Firewall Protection Profile. Therefore, the validation team concludes that the Cable and Wireless CCTL findings are accurate, the conclusions justified, and the conformance claims to the TFFPP are correct.

# 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 7.0 (Patch 531) |
| Protection Profile | U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Final, Version 1.1 April 1999 |
| Security Target | *Lucent Technologies Lucent VPN Firewall Version 7.0 (Patch 531) Security Target Version 1.3, October X. 2003* |
| Evaluation Technical Report | *Evaluation Technical Report for Lucent VPN Firewall;* Version xx, October x 2003 |
| Conformance Result | CC Part 2 conformant, CC Part 3 conformant |
| Sponsor | Lucent Technologies |
| Developer | Corsec Security, Inc. for Lucent Technologies |
| Evaluators | Cable and Wireless |
| Validators | Donald Phillips, Lead, Mitretek Systems<br>Mario Tinto, Aerospace Corp |

# 3. SECURITY POLICY

The TOE implements a traffic filtering policy; it either passes or blocks traffic on a per-packet basis in accordance with a rule-set that is configurable by an authorized administrator. Datagram parameters that are taken into account in the policy are:

- interface at which incoming datagram arrives;
- interface from which datagram outgoing datagram is being sent;
- source address;
- destination address;
- higher level protocols;
- ports.

# 4. ASSUMPTIONS

## 4.1 Usage Assumptions

The primary assumptions regarding the use and operation of the TOE are:

- Only administrators may gain physical access to the TOE, and in particular, the LSMS;
- Administrators are non-malicious;

## 4.2 Environmental Assumptions

All of the assumptions stated in section 3.1 of the Security target are considered to be security objectives for the environment. The assumptions were taken from the U.S. Government Traffic Filter Firewall Protection Profile for Low-Risk Environments Version 1.1, April 1999. The intent of the specified assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

# 5. ARCHITECTURAL INFORMATION

The Lucent VPN Firewall is a security system consisting of one or more Firewall Appliances to mediate information transfer between domains and a Lucent Security Management Server (LSMS) to administer the firewall appliance.

The firewall function is physically separated from its management server, with the firewall code running on Inferno, a small Bell Labs-developed operating system. In the evaluated configuration, the LSMS communicates with the firewall appliance via a dedicated, local connection (i.e., no remote communications). The LSMS software runs on a separate Windows NT/Windows 2000 platform.

The Firewall Appliance (FA) executes LVF FA, Version 7.0 software on hardware referenced in the document Lucent VPN Firewall V7.0 (Patch 531). The LSMS Software is designed to be platform independent by implementing a Java Execution environment for the LSMS GUI. This GUI is the same whether running on Windows 2000 or Windows NT. The various VPN Firewall Brick models listed in the table above differ only in throughput and network interface capacity rather than functionality. All the Brick models run on the same version of the Lucent Inferno operation operating system as pushed down by the LSMS console. The LSMS GUI is the same whichever model is used.

The LVF FA executes LVF Version 7.0 FA software. This software consists of the Inferno operating system and simple firewall code that is imbedded within the operating system kernel. The operating system provides no user accounts or file systems. to be of a security concern.

All communications between each FA and the LSMS is encrypted and authenticated using native Inferno encryption and authentication mechanisms (Diffie-Hellman for key exchange, DSS for digital signatures and signature verification, and Triple-DES for session encryption**). Note: These encryption mechanisms listed above were not evaluated as part of the evaluated configuration.**

The FA software supports stateful packet filtering, logging, creation of policy objects, and reporting.

# 6. DOCUMENTATION

During the course of the evaluation, the CCTL had access to an extensive amount of documentation and evidence, covering:

- Design details and system internals;
- Configuration management and lifecycle documentation;
- Delivery procedures and operation guidance;
- Vendor test plans and configurations, test suites, and test results;
- Vulnerability assessment documentation and strength of function analyses;
- Security Target

# 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 and specific test suites.

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 in the installation readme file. The

following evaluation test configurations were installed to comply with the developers test procedures:

- Lucent Brick 1000 VPN Firewall Brick
- LSMS Console – Windows 2000 Professional & Service Pack 3/ Lucent Security Management Server 7.0 and patch 531.
- Internal Client – Windows 2000 Pro with Service Pack 3
- External Client – Windows 2000 Pro with Service Pack 3
- CCTLNESSUS Server – Red Hat Linux 8.0

The entire manual test suite was executed on each of these configurations

## 7.2 Evaluator Testing

The evaluation team also devised a set of independent tests, in part covering areas that the evaluation team felt to be missing from, or inadequately covered by the developer's test suit. The evaluators used the same test configuration that was specified to complete the developers tests.

The evaluation team tested the TOE Security Functional Interfaces (TFSI), which are listed below.

- 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 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.

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

# 8. EVALUATED CONFIGURATION

The evaluated configuration consists of the Lucent VPN Firewall 7.0 and the components are identified as the Lucent Security Management Server v7.0 (patched to build 531 as identified through the Help/About function 7.0.531) installed on Windows 2000 professional (patched to service pack 3 and installed according to the administrative guidance and TOE Readme document version 0.9). This is combined with the Lucent VPN Firewall Brick model 1000.

# 9. RESULTS OF THE EVALUATION[3]

The evaluation team determined the product to be **CC Part 2 conformant, CC Part 3 conformant,** and to meet the requirements of **EAL 2**. Additionally, the product is conformant to the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Final, Version 1.1 April 1999. This implies that the product satisfies the security technical requirements specified in *The Lucent Technologies Lucent VPN Firewall Version 7.0 (Patch 531) Security Target Version 1.3 Release Date: October 27, 2003.*

# 10. EVALUATOR COMMENTS

There are no Evaluator Comments.

# 11. SECURITY TARGET

The ST, *Lucent Technologies Lucent VPN Firewall Version 7.0 (Patch 531) Security Target Version 1.3, October27, 2003* is included here by reference.

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

# 12. GLOSSARY

| | |
|---|---|
| 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 |
| 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 7.0 (Patch 531) Security Target Version: 1.3, dated 27 October 2003

[8] U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments Version 1.1, April 1999

[9] Evaluation Technical Report, for the Lucent VPN Firewall Version 7.0 (Patch 531), Version 0.4 Final, 4 October 2003.

[10] Evaluation Team Test Plan for Lucent VPN Firewall 7 – EAL2 (Proprietary), Version 1.3, 3 October 2003.