Certification Report

EAL 2+ Evaluation of the

SecureLogix Corporation® TeleWall® System Version 2.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-4
Version: 1.1
Date: November 15, 2000
Pagination: i to v, 1 to 20

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Canadian Certification Scheme using the Common Methodology for Information Technology Security Evaluation, Version 1.0, for conformance to the ISO 15408 Common Criteria for IT Security Evaluation, Version 2.1. This certification report, and associated certificate, applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and associated certificate, is not an endorsement of the IT product by the Communications Security Establishment (CSE) or by any other organization that recognizes or gives effect to this report, and associated certificate, and no warranty of the IT product by the CSE or by any other organization that recognizes or gives effect to this report, and associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (the Canadian CCS) provides a third-party evaluation service for determining the trustworthiness of IT security products. An evaluation is performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Canadian CCS Certification Body (CB), managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has demonstrated the ability to meet the requirements of the Canadian CCS CB for approval to perform Common Criteria evaluations. A significant requirement for such approval by the Canadian CCS CB is accreditation to the requirements of the ISO Guide 25, General requirements for the accreditation of calibration and testing laboratories. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN) administered by the Standards Council of Canada.

The CCEF performing the evaluation of the SecureLogix Corporation® TeleWall® system is EWA-Canada Ltd. located in Ottawa, Ontario, Canada.

By awarding a certificate, a certifying body asserts, to some degree of confidence, that a product complies with the security requirements specified in its Security Target (ST). A ST is a requirement specification-like document that defines and scopes the evaluation activities. The consumer of certified IT products should review the ST, in addition to the Certification Report (CR), in order to gain an overall understanding of the product. This should specifically include any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (Evaluation Assurance Level) to which it is asserted that the product satisfies its security requirements.

The ST associated with this CR is identified by the following nomenclature:

Security Target for the SecureLogix Corporation® TeleWall® System Version 2.0
EWA-Canada Document number: 1362-002-D001
Version 1.4
Dated: 10 November 2000

This CR is associated with the Certificate of Product Evaluation dated 23 October 2000.

CONFIGURATION CHANGE PAGE

Date	Version	Change	Authorization
2000/10/23	**1.0**	**Original version**	**CCS CB**
2000/11/15	**1.1**	**Editorial Changes to 1.0 to improve descriptions of product functionality and correct the trademark references.**	**CCS CB**

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This Certification Report (CR) contains the results of the Common Criteria Evaluation Assurance Level 2+ IT Security Evaluation for the SecureLogix Corporation® TeleWall® system that was performed by EWA-Canada Ltd.

The information in this CR is fully substantiated and supported by the evidence contained in the applicable Evaluation Technical Report (ETR), document number 1362-001-D002.

The evaluation was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (the Canadian CCS). The Canadian CCS has established a Certification Body (CB) that is managed by the Communications Security Establishment (CSE).

The goal of this evaluation was to provide third-party critical analysis and testing of the SecureLogix Corporation® TeleWall® system. SecureLogix Corporation sponsored the evaluation of this system. The Common Criteria Evaluation Facility (CCEF) conducting the evaluation was EWA-Canada Ltd. Evaluation work took place over a 9-month period from February 2000 to October 2000.

The evaluation activities consisted of a comprehensive suite of analysis and testing activities against the requirements of the Common Criteria for Information Technology Security Evaluation (CC) version 2.1, applied using the Common Methodology for Information Technology Security Evaluation (CEM) version 1.0. The CC is an ISO standard (ISO 15408) developed by the multinational Common Criteria Project sponsoring organizations.

The EWA-Canada Information Technology Security Evaluation and Testing (ITSET) facility evaluated different versions of the SecureLogix Corporation® TeleWall® system as it evolved to meet production requirements and those of the CC. The final evaluation version of the SecureLogix Corporation® TeleWall® (v2.0) system included the TeleWall® Management Server version Washington 33 and applicable appliance version 2.0.18 with Digital Signal Processor 2.07.

The TeleWall® system was subjected to a comprehensive suite of documented formal tests during an intensive and fully planned multi-month period. The applicable system documentation was evaluated in accordance with the requirements of the CEM.

A comprehensive suite of security tests were run against the SecureLogix Corporation® TeleWall® system both at the developer's facility and in the EWA-Canada ITSET lab and these are defined and documented in the ETR.

The SecureLogix Corporation® TeleWall® system is a telecommunications firewall that provides the same type of visibility and control over the use of the telephone network that traditional firewalls provide for Transmission Control Protocol/Internet Protocol (TCP/IP) networks. The SecureLogix Corporation® TeleWall® system provides an enterprise with the ability to counter the threat of unauthorized access to the data network through

user-connected modems. It physically interfaces with each telephone voice or data line in the enterprise and enforces a user-defined security policy based on calling number, called number, time of day/day of week, call direction (inbound, outbound), and call type (voice, modem, STU III or fax). Through the security policy, users can define which calls will be allowed, which will be terminated and what other actions will take place such as logging events, alerting security personnel (alerts, pages, email, etc.), or forwarding simple network management protocol (SNMP) messages to network management systems. The SecureLogix Corporation® TeleWall® system can force users to access the data network through controlled remote access services and prevent access through user-configured access points. The SecureLogix Corporation® TeleWall® system can prevent the misuse of telephone lines for other than their designated functions such as restricting the use of fax lines for voice or modem traffic. The TeleWall® appliances can be installed on either the trunk side or station side of the private branch exchange (PBX). It is able to provide enterprise-wide visibility into activity and is compatible with multi-vendor and multi-generational PBXs. This enterprise-wide visibility into the complete telephone network provides user insight into resource utilization on an enterprise level providing empirical data to support telecommunications acquisition and reallocation tasks. The SecureLogix Corporation® TeleWall® system has a distributed architecture that allows the user to remotely manage all aspects of an enterprise-wide deployment of the SecureLogix Corporation® TeleWall® systems including the remote installation of security policies as well as the remote updating of system software simultaneously across the enterprise.

A SecureLogix Corporation® TeleWall® system consists of a management server (or many servers for a large organization) and associated appliances that are matched to an organization's telephone systems. The appliances are installed on the telephone circuits and a single management server can manage multiple appliances or arrays of appliances. The appliances are available in three different types: analog, for traditional plain old telephone systems (POTS), T1 and ISDN/PRI for digital types of telephone lines. The basic processing for security policy enforcement and management for all appliance types is similar, with the main differences being related to telephony signal conditioning and processing within the appliances.

The evaluation of the SecureLogix Corporation® TeleWall® system demonstrated that this security product conforms to the security functionality requirements specified in the Security Target, and that it is conformant to the assurance requirements for Evaluation Assurance Level 2 with the following augmentations:

- ACM_CAP.3 – Authorisation controls
- ACM_SCP.1 – Configuration management coverage
- ALC_DVS.1 – Identification of security measures

CSE, as the Canadian CCS Certification Body, declares that the SecureLogix Corporation® TeleWall® system version 2.0 evaluation meets all the conditions of the Common Criteria Recognition Arrangement (CCRA) and will be placed on the Certified Products List.

1 Identification

This report pertains to the SecureLogix Corporation® TeleWall® system, version 2.0, comprising the TeleWall® Management Server, version Washington 33, and the TeleWall® Appliance, version 2.0.18 with Digital Signal Processor 2.07. The TeleWall® software is available for Windows 98, Windows NT and Solaris, however only Windows NT version 4.0 was used for this evaluation. An example SecureLogix Corporation® TeleWall® system configuration is shown in Figure 1.

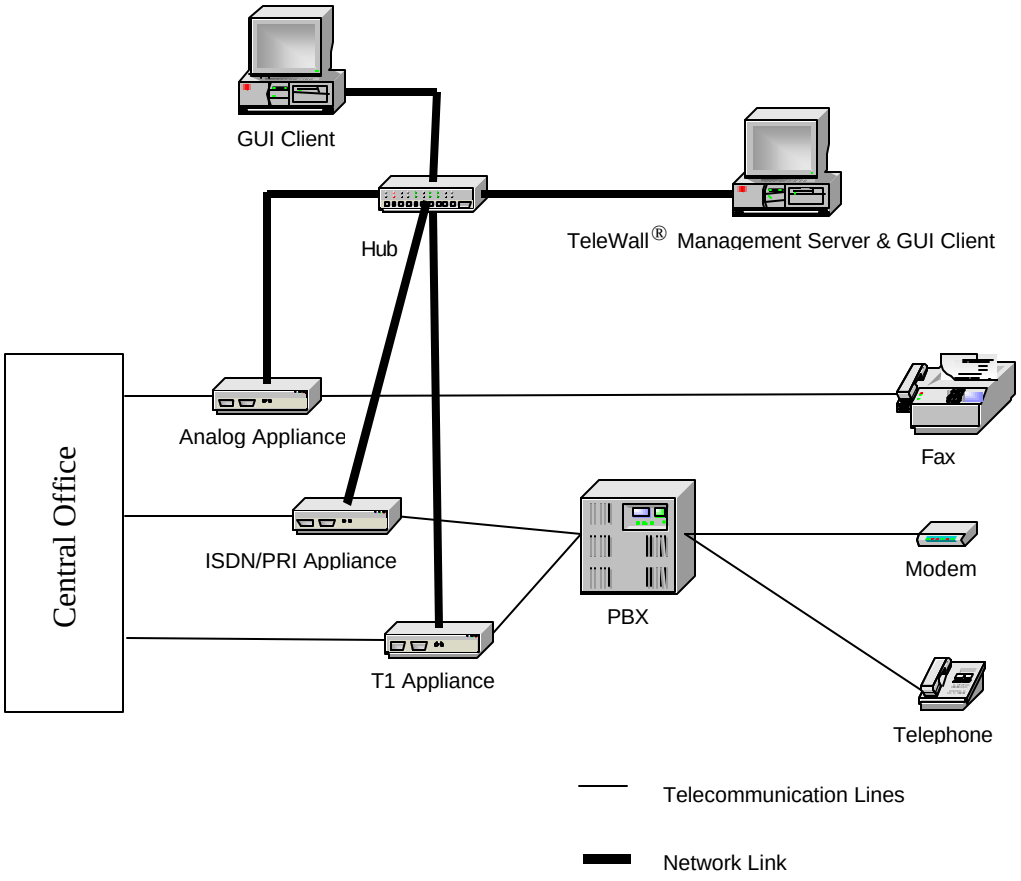

Figure 1: Example SecureLogix Corporation® TeleWall® System Configuration

2 Security Target

The Security Target (ST) associated with this Certification Report (CR) is identified by the following nomenclature:

Security Target for the SecureLogix Corporation® TeleWall® System Version 2.0
EWA-Canada Document number: 1362-002-D001
Version: 1.4
Dated: 10 November 2000

3 Security Policy

The SecureLogix Corporation® TeleWall® system is a telecommunications firewall that provides the same type of visibility and control over the use of the telephone network that traditional firewalls provide for Transmission Control Protocol/Internet Protocol (TCP/IP) networks. The SecureLogix Corporation® TeleWall® system is a product that provides an enterprise with the ability to counter the threat of unauthorized access to the data network through user-connected modems. It physically interfaces with each telephone voice or data line in the enterprise and enforces user-defined security policy based on source number, destination number, time of day/day of week, call direction (inbound, outbound), and call type (voice, modem, STU III, or fax).

Through the security policy, users can define which calls will be allowed, which will be terminated and what other actions will take place such as logging events, alerting security personnel (alerts, pages, email, etc.), or forwarding SNMP messages to network management systems. The SecureLogix Corporation® TeleWall® system can force users to access the data network through controlled remote access services and prevent access through user-configured access points. The SecureLogix Corporation® TeleWall® system can prevent the misuse of telephone lines for other than their designated functions such as restricting the use of fax lines for voice or modem traffic.

The TeleWall® appliances can be installed on either the trunk side or station side of the private branch exchange (PBX). It is able to provide enterprise-wide visibility into activity and is compatible with multi-vendor and multi-generational PBXs. This enterprise-wide visibility into the complete telephone network provides user insight into resource utilization on an enterprise level providing empirical data to support telecommunications acquisition and reallocation tasks. The distributed architecture of the SecureLogix Corporation® TeleWall® system allows the user to remotely manage all aspects of an enterprise-wide deployment, including the remote installation of security policies as well as the remote updating of system software simultaneously across the enterprise.

A hardware setting exists to determine the default failure-mode behaviour should a TeleWall® appliance fail (due to a power outage, for example). The TeleWall® appliances can be configured to fail-safe (allow all calls), or fail-secure (deny all calls).

3.1 SecureLogix Corporation® TeleWall® System Security Functions

The SecureLogix Corporation® TeleWall® system provides a large and comprehensive set of security functions to enforce an organization's telephony security policy. These security functions can be grouped into three categories: access control, audit and human-machine interface. Table 1 summarizes the Security Functional Requirements specified in the Security Target.

Functional Components	
Identifier	**Name**
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication

Functional Components	
Identifier	**Name**
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps

Table 1: Summary of Security Functional Requirements

A brief summary of the security functions claimed by SecureLogix Corporation is provided in the following sections.

3.1.1 Access Control

The SecureLogix Corporation® TeleWall® system allows administrators to create rules which allow/block user calls based on calling number, called number, call type (voice, fax, modem, STU III), direction (inbound, outbound), and time of day/day of week. Administrator access to the appliances is via the GUI, ASCII window, telnet, and serial port. Administrators must authenticate using a username and password. The SecureLogix Corporation® TeleWall® system performs quality checks on the password to ensure only strong (to prevent brute force password guessing attempts) values are accepted.

3.1.2 Audit

The SecureLogix Corporation® TeleWall® system provides a comprehensive audit capability for the configuration and operation of the appliances. The SecureLogix Corporation® TeleWall® system has extensive auditing and reporting capabilities. The levels of events to be audited can be set by the administrator. Each audit record contains a unique identification number, date and time stamps, and the appliance or appliance array that originated the record. All call details (numbers, times, telecommunication line specifics, etc.) are recorded and can be viewed in a generated report or plotted as a graph through the client GUI.

Audit records concerning telecommunication information flow and appliance status are generated at the appliances. The audit data is then uploaded to the TeleWall® Management Server. Each appliance contains a memory card that can store the audit records temporarily if the TeleWall® Management Server is unavailable. The memory cards can hold the audit data in a circular buffer where they will eventually be overwritten with newer records, however there is sufficient memory to hold multiple days of audit logs even under heavy telecommunications traffic.

Note that similar extensive audit functionality for the TeleWall® Management Server is neither provided nor claimed by the developer.

3.1.2.1 Audit Reporting Tool

The reporting tool included with the SecureLogix Corporation® TeleWall® system allows extensive filters to be used to provide fine-grained and excellent visibility into the operation of the system and the use of telephone lines.

For example, if a user wished to see audit records only for modems, the user can search based on call type (which returns all voice, fax, and modem, STU III voice, STU III data, STU III generic, and unknown calls). Then the user can create a filter for voice, fax, STU III voice, STU III generic, and unknown calls thus leaving only modem records.

3.1.3 Human-Machine Interface

For all three appliance types, the SecureLogix Corporation® TeleWall® system human-machine interface (HMI) allows the administrator to perform the following functions:

- specify rules governing how telecommunication access is mediated
- specify the level of telecommunications activity displayed
- specify what telecommunication activity is logged

The HMI also provides the user with current and historical views of all calls, and their associated level of activity. Extensive reports and graphs may be generated from the historical data.

The SecureLogix Corporation® TeleWall® system provides four different user interfaces: a graphical user interface (GUI) for the Security Policy Editor, a real-time ASCII window command line for the TeleWall® Operating System (TOS), the RS232 terminal console, and a Telnet console.

The GUI includes a straightforward and highly intuitive interface for configuring and managing the SecureLogix Corporation® TeleWall® system. After a short training period for telephony concepts, the TeleWall® system can be setup and operated by administrators who are inexperienced with the TeleWall® system, within a very short period of time. Of note, the SecureLogix Corporation® TeleWall® system is capable of providing very fine-grained visibility into, and control over, the activity and traffic on telephony circuits.

The ASCII window, the RS232 terminal console and the Telnet console can be used for configuring and managing administrative functions of the TeleWall® Management Server and the appliances.

The appliances also include status lights (LEDs) that give real-time indications of their state and current activity.

4 Assumptions and Clarification of Scope

4.1 Environmental Assumptions

The environmental requirements and assumptions for this evaluation are:

- The SecureLogix Corporation® TeleWall® system is physically secure.
- Protection mechanisms (such as firewalls and intrusion detection systems) exist such that the internal TCP/IP network between the TeleWall® Management Server and appliances is trusted and considered non-hostile. These measures are used to protect the network communications between components.
- Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- The administrator is knowledgeable of both TCP/IP networking and telecommunication systems.

4.2 External Interfaces

The external interfaces for the SecureLogix Corporation® TeleWall® system are the connections to the telephone lines, and all of the human-machine interfaces, including the audit logs.

Although the SecureLogix Corporation® TeleWall® system provides an interface to integrate with TeleSweep Secure®, another SecureLogix Corporation companion product, TeleSweep Secure® is beyond the scope of this evaluation.

The external interfaces are defined in detail in the applicable ST and product documentation.

4.3 Definition of "Users" and "Administrators"

Note that the SecureLogix Corporation® TeleWall® system protects the telecommunications lines, but uses a TCP/IP network for internal communications. The use of the term "network" refers only to the TCP/IP network, not to the telecommunications lines. The term "user" refers only to individuals or IT entities who communicate over the telecommunications lines. The term "administrator" refers only to individuals who configure and operate the SecureLogix Corporation® TeleWall® system and who communicate over the internal TCP/IP network to manage TeleWall® appliances.

4.4 Cryptography

The SecureLogix Corporation® TeleWall® system can be configured to encrypt communications (using DES or Triple DES) between the TCP/IP networked components, however a formal validation of the cryptography was beyond the scope of this evaluation.

5 Architectural Information

The SecureLogix Corporation® TeleWall® system is designed to protect telecommunications lines from abuse, and provide comprehensive auditing capabilities on all telecommunications line traffic. The major TeleWall® subsystems that implement security features and the external interfaces for the SecureLogix Corporation® TeleWall® system, and form the High Level Design are:

a. TeleWall® Appliances:

- Analog appliance
- T1 appliance
- ISDN-PRI appliance

b. TeleWall® Management Server:

- Audit Reports
- Appliance Manager/Security Policy Editor

c. Client Interfaces:

- Graphical User Interface (GUI)
- ASCII windows
- Telnet Consoles
- RS232 serial interface to the appliances

The TeleWall® Management Server and GUI client are both written in the Java programming language and require a Java Virtual Machine version 1.3 or higher, to be installed on the host PC.

All appliances are designed by SecureLogix Corporation using commercially available components, and these appliances run an operating system also created by SecureLogix Corporation. The types of appliances that are selected and used for specific installations (e.g. analog, T1 or ISDN/PRI) depend on the type of incoming telephony lines. The security policy enforcement logic within each of the appliance types is the same, with the only fundamental differences between the appliances being the signal and waveform conditioning for analog, T1 or ISDN/PRI.

The SecureLogix Corporation® TeleWall® system mediates access between local and external telecommunication users based on rules defined by the administrator. Rulesets are created on the TeleWall® Management Server, then pushed down to the appliances. The appliances allow or deny calls based on their respective rulesets. The default behaviour is to allow any calls not explicitly denied.

A hardware setting exists to determine the default failure-mode behaviour should the SecureLogix Corporation® TeleWall® system fail (due to a power outage, for example). The SecureLogix Corporation® TeleWall® system can be configured to fail-safe (allow all calls), or fail-secure (deny all calls).

Ethernet network links are used to facilitate the following communication channels between:

- the appliances and the TeleWall® Management Server
- the GUI and the TeleWall® Management Server
- the administrator and appliances (telnet)

Administrators may also communicate directly to the appliances though a serial port located on the appliances.

The SecureLogix Corporation® TeleWall® system has three security modes to administer the communications with its appliances. The appliances can be set to communicate at Low, Medium or High security modes. The appliance security mode determines whether Telnet access to the appliance is enabled, and controls the means by which modifications may be made to several security-related configuration items, including those related to networking (e.g., IP address, IP port), encryption (e.g., encryption key, encryption algorithm), and the appliance security mode itself.

In Low security mode, Telnet access to the appliance is enabled and the security-related configuration items can be modified over Telnet, the serial port, or via the TeleWall® Management Server. In Medium security mode, Telnet access is disabled. In High security mode, Telnet is disabled and the security-related configuration items can only be modified using the serial port. High security mode requires physical access to the appliance via the serial port to modify the security-related configuration items.

In all security modes, the non security-related settings can be changed from Telnet, the serial port, or from the TeleWall® Management Server, provided that the communications type is allowed by the security mode. The user must supply a password before any configuration item, whether security-related or non security-related, can be modified via Telnet or the Serial port.

6 Evaluated Configuration

The final evaluation version of the SecureLogix Corporation® TeleWall® system was version 2.0, and it included the TeleWall® Management Server version Washington 33 and applicable appliances, version 2.0.18 with Digital Signal Processor 2.07. The operating system was Windows NT 4.0.

The major TeleWall® components are:

- the TeleWall® Management Server running on an Intel based PC with Windows NT 4.0 as the operating system
- the administrator graphical user interface (GUI) client version 2.0 running on an Intel based PC with Windows NT 4.0
- hardware analog appliances, model TW 1010[1]
- hardware T1 appliances, model TW 1020[1]
- hardware ISDN/PRI appliances, model TW 1030[1]

A SecureLogix Corporation® TeleWall® system consists of a management server and associated appliances that are matched to an organization's telephone system. The appliances are actually installed on the telephone circuits and a single management server can manage multiple appliances or arrays of appliances. The appliances are available in different types: analog for traditional analog phone lines, and T1 and ISDN/PRI for digital types of telephone lines. The basic processing for security policy enforcement and management for all appliance types is similar, with the main differences being telephony signal processing within the appliances.

[1] These appliances are programmable and the evaluated configuration is identified as version 2.0.18 with DSP 2.07.

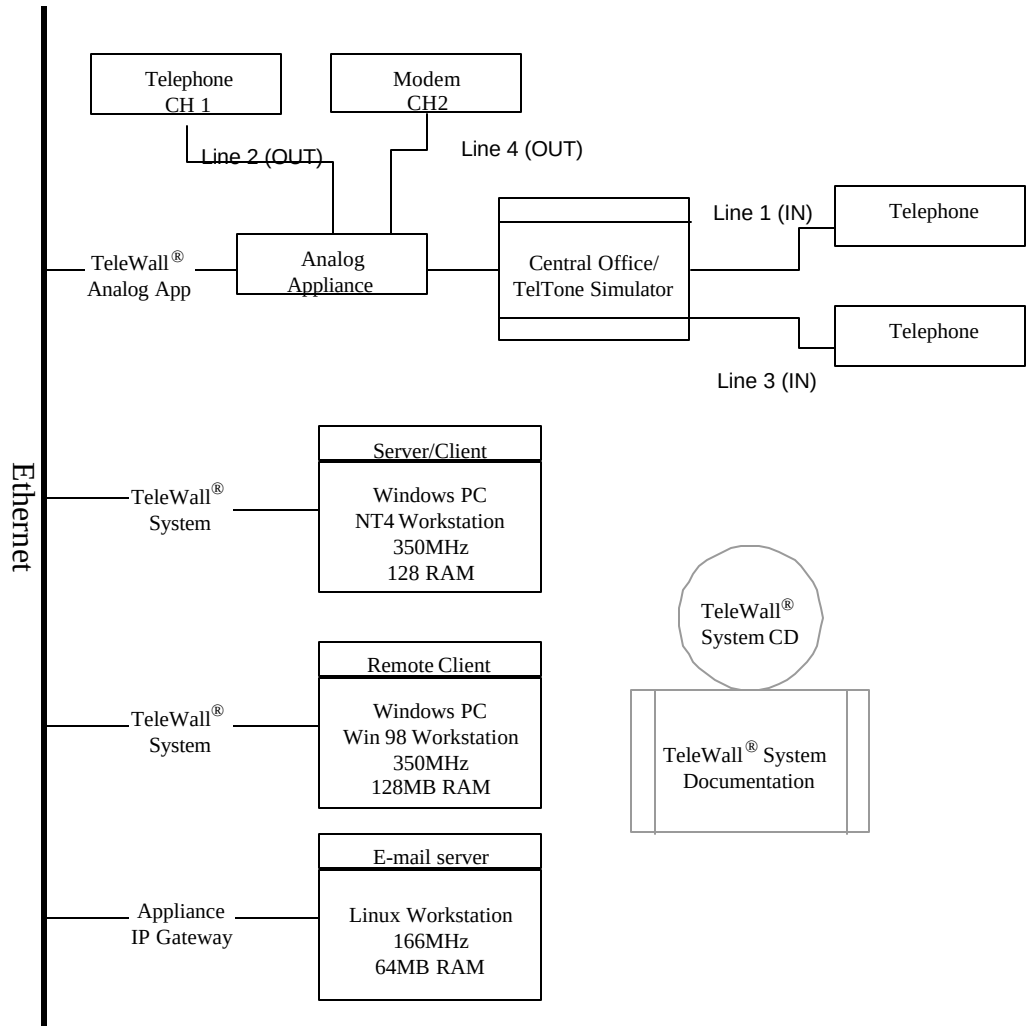

Figure 2: Test Configuration – Analog Appliance

7 Documentation

7.1 Evaluation Documents

The documents and associated reference numbers produced as a result of this evaluation are:

- Evaluation Work Plan 1362-001-D001
- Security Target 1362-002-D001
- Evaluation Technical Report 1362-001-D002
- Preliminary Certification Report 1362-001-D003

7.2 Consumer Documents

The documents and associated versions are found in the table below:

TeleWall® FireWall for Telephone Lines, Version 2.0	Part # 84-0027-2.0 1 – About SecureLogix.pdf	7 July 2000
Users Guide	Part # 84-0027-2.0 2 – Users Guide.pdf	7 July 2000
Administration Overview and Installation Guide	Part # 84-0027-2.0 3 – Admin Overview & Install.pdf	7 July 2000
System Administration Guide	Part # 84-0027-2.0 4 – Sys Admin.pdf	7 July 2000
Dialogs Reference	Part # 84-0027-2.0 5 – Dialog Reference.pdf	7 July 2000
TOS Commands	Part # 84-0027-2.0 6 – TOS Commands.pdf	7 July 2000
Glossary	Part # 84-0027-2.0 7 – Glossary.pdf	7 July 2000
Site Survey	Part # 84-0027-2.0 8 – Site Survey.pdf	7 July 2000
Technical Bulletin SecureLogix Corporation® TeleWall® System 2.0 Release Notes	#137 (Revision A)	7 July 2000

Table 2: Consumer Documents

8 Evaluation Analysis Activities

8.1 Scope of Evaluation Analysis Activities

The evaluation involved an analysis of the developer's processes used to develop and support the SecureLogix Corporation® TeleWall® system and associated documentation. The product documentation and design were considered from a security perspective, along with the associated operational user's manuals and administrative guidance documentation.

The evaluation analysis activities specifically involved a structured evaluation of the product documentation in the following areas:

- Configuration Management
- Product Delivery and Operation, including secure installation and start-up
- Development documentation (specifications, design and requirements traceability)
- Administrator and User Guidance documentation
- Testing (developer's coverage and depth and functional testing)
- Strength of Function (for password mechanisms)
- Vulnerability Assessment for the product
- Development Security documentation

8.2 Quality of SecureLogix Corporation® TeleWall® System Documentation

All of the product documentation associated with the SecureLogix Corporation® TeleWall® system was found to be of very high quality in terms of completeness, level of detail, accuracy, usefulness and comprehensiveness.

9 Product Testing

9.1 Testing Philosophy

In general there are three aspects to evaluation testing:

- assessing developer tests
- performing independent tests
- performing penetration tests

For this particular evaluation, the evaluators chose to develop a suite of independent tests by:

- examining the developer's exhaustive test documentation
- witnessing and sampling the developer tests
- independently developing test documentation (e.g., test plan, test procedures, expected results)
- conducting independent evaluator testing based on the evaluator test plans and procedures and documenting test results

The test philosophy used in this evaluation was to test and evaluate the security features of the SecureLogix Corporation® TeleWall® system, as defined in the functional specifications. In general, the philosophy used in the establishment of test procedures for the security evaluation of the SecureLogix Corporation® TeleWall® system was to prove or disprove the security claims made by the vendor through positive- and negative-oriented "functional type" testing. Also, the evaluators attempted to defeat the SecureLogix Corporation® TeleWall® system and its programmed security policies through telecom "penetration type" testing based on defined Telecom Attacks and Vulnerabilities.

9.2 Testing Coverage

The evaluator's approach to independently testing the SecureLogix Corporation® TeleWall® system was to develop and document tests that covered all security requirements specified in the ST, with emphasis in the form of rigorous testing for a subset of the security requirements. Rigorous testing of a subset of security functionality (an approach compliant to the CEM) was appropriate since:

- The SecureLogix Corporation test documentation was extremely comprehensive and it was highly efficient to make maximum use of witnessing developer testing.

- The developer's laboratory had additional special-purpose telephony test equipment beyond what was available at the EWA-Canada lab.

Resulting from this test coverage approach is the following list of test goals:

1. Test Goal A - TeleWall® Management Server Installation Procedures
2. Test Goal B - Analog Appliance Setup Procedures
3. Test Goal C - T1 Appliance Setup Procedures
4. Test Goal D - ISDN Appliance Setup Procedures
5. Test Goal E - TeleWall® Management Server Administration
6. Test Goal F - Definition of Security Policy Rulesets
7. Test Goal G - Enforcement of Security Policy (Information Flow)
8. Test Goal H - Access Control Tests
9. Test Goal I - Audit of TeleWall® Management Server Management
10. Test Goal J - Audit of Appliance Configurations
11. Test Goal K - Audit of Security Policy Enforcement
12. Test Goal L - Alarm Triggering
13. Test Goal M - Log File Management
14. Test Goal N - Report Generation
15. Test Goal O - Report Filtering
16. Test Goal P - Password Protections
17. Test Goal Q - Log File Protections
18. Test Goal R - Different user interfaces - telnet, ASCII interface, serial console
19. Test Goal S - Load Testing
20. Test Goal T - Variation of telephony conditions - DTMF tone variations etc.
21. Test Goal U - Audit failures - rollover loss of data
22. Test Goal V - Self protection mechanisms
23. Test Goal W - Test security posture [Hi, Med, Low]
24. Test Goal X - TeleWall®-TeleSweep Secure® interface
25. Test Goal Y - VLA-1 Hook Flash Detection
26. Test Goal Z - VLA-2 Pulse Digits
27. Test Goal AA - VLA-3 DTMF Digits

28. Test Goal BB - VLA-10 Dead Call State
29. Test Goal CC - VLA-X ADSL LP Filters
30. Test Goal DD - Fail Safe/Fail Secure
31. Test Goal EE - Negative Testing

9.3 Detailed Test plan and Procedures

Annex B of the ETR contains a comprehensive discussion of the detailed test goals, objectives, plan and detailed test procedures, along with the actual test results.

9.4 Conduct of the Testing

EWA-Canada Ltd. informally tested three different developmental versions of the SecureLogix Corporation® TeleWall® system, to gain product familiarity and to facilitate the evaluation planning process.

The final evaluation version of the SecureLogix Corporation® TeleWall® system was subjected to an extensive and comprehensive suite of formally documented tests during a three-month period. The actual testing took place at the Developer's facility in San Antonio, Texas and EWA-Canada Ltd.'s Ottawa laboratory.

The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are defined and documented in the ETR.

9.5 Testing Results

For all formal tests, the actual results matched the expected results and confirmed that the security claims, telephony access controls, audit mechanisms and the external interfaces of the product operate as claimed and documented.

In summary, the results of the independent testing by EWA-Canada Ltd. confirmed the following:

- All claims made by SecureLogix Corporation related to the ability of the SecureLogix Corporation® TeleWall® system to mediate access control and traffic on the telephone circuits (by allowing, blocking and auditing calls) were confirmed to be valid, for all types of access control functions.

- All claims made by SecureLogix Corporation related to the ability of the SecureLogix Corporation® TeleWall® system to enforce fine-grained security policy on telephone lines based on source number, destination number, time of day/day of week, call direction (inbound, outbound), and call type (voice, modem, fax or STU III) were confirmed.

- All claims made by SecureLogix Corporation that related to the ability of the SecureLogix Corporation® TeleWall® system to audit traffic activity and other events on different telephone circuits were confirmed to be valid for all types of audit events.

- The SecureLogix Corporation® TeleWall® system is straightforward to configure, use and integrate into a corporate telephone network.
- For calls that conform to corporate security policy, the fact that the SecureLogix Corporation® TeleWall^{T}® system is installed and operating is completely transparent to users.
- The SecureLogix Corporation® TeleWall® system effectively terminates and/or audits and logs calls that violate orporate security policy.
- The reporting capabilities of the SecureLogix Corporation® TeleWall® system are extensive and useful.
- The configurable fail-safe (allow all calls), and fail-secure (deny all calls) failure modes for the SecureLogix Corporation® TeleWall® system were confirmed to operate as claimed.
- The SecureLogix Corporation® TeleWall® system can be securely installed on a corporate telephone network (trunk or station side) and managed via a TCP/IP network. It does not introduce any new, known or obvious vulnerabilities on either the telephone or TCP/IP networks.
- In order to ensure that SecureLogix Corporation® TeleWall® system properly enforces security policy without leaving vulnerabilities due to ruleset processing logic, it is important that administrators carefully read and understand the applicable administrative guidance information published by SecureLogix Corporation.

10 Results of the Evaluation

The evaluation clearly demonstrated that the SecureLogix Corporation® TeleWall® system merits an Evaluation Assurance Level (EAL) 2+ rating against the requirements of the Common Criteria (ISO 15408) and can be trusted, to an EAL2 + level of assurance.

The evaluators found, and documented, compelling evidence that the SecureLogix Corporation® TeleWall® system provides the claimed security protection.

The evaluation of the SecureLogix Corporation® TeleWall® system has determined that it is conformant with the functional requirements specified in Part 2 of the CC. The SecureLogix Corporation® TeleWall® system is conformant to the assurance requirements for Evaluation Assurance Level (EAL) 2+, as specified in Part 3 of the CC, with the following augmentations:

- ACM_CAP.3 – Authorisation controls
- ACM_SCP.1 – TOE Configuration Management coverage
- ALC_DVS.1 – Identification of security measures

11 Evaluator Comments, Observations and Recommendations

11.1 Developer Briefings

The developer briefings were extremely detailed and comprehensive with respect to the information presented on the product requirements, design and the corporate processes used to develop and support the product.

11.2 Recommendation

Corporate users looking for technology to fill a gap in their security protection requirements to include enforcement of security policy on telephone lines are encouraged to consider the SecureLogix® TeleWall® system.

11.3 Comment on SecureLogix Corporation Process Maturity

Although it is a relatively young company, SecureLogix Corporation has instituted a very mature set of development processes for their products, which bodes very well for future product development and support. Their systems and software engineering teams are composed of highly experienced, motivated and disciplined staff, most of whom have come from very disciplined and demanding standards-based environments.

The engineering efforts of the company are extremely efficient and are highly focused on adopting and integrating world-class best practices and processes into every aspect of their corporate culture for product development, testing and support. The documentation produced by the company is outstanding in quality and comprehensiveness. As an example of this, SecureLogix Corporation has a well-developed and efficient system for highlighting and aggressively tracking and managing all bugs, deficiencies and problem rectification issues. The comprehensiveness of this tracking system, along with a tight coupling of engineering and marketing cooperation on formally refining product and test requirements, is a matter of corporate culture that is efficient and works well.

This translates directly into improved quality attributes for their products and documentation.

12 Glossary

This section expands upon abbreviations and acronyms, and defines vocabulary used in a special way to help increase the readability of this report.

12.1 Abbreviations and acronyms

CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
CSE	Communications Security Establishment
DES	Data Encryption Standard
DSP	Digital Signal Processor
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HMI	Human-Machine Interface
ISDN	Integrated Services Digital Network
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MAC	Media Access Control
NFAS	Non-Facility Associated Signaling
PALCAN	Program for the Accreditation of Laboratories Canada
PBX	Private Branch Exchange
PC	Personal Computer
PLD	Programmable Logic Device
POTS	Plain Old Telephone System
PRI	Primary Rate Interface
SMDR	Station Message Detail Recording
SNMP	Simple Network Management Protocol
ST	Security Target
STU III	Secure Telephone Unit III
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation

TOS TeleWall® Operating System

13 References and bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

1. Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999
2. Common Methodology for Information Technology Security Evaluation, CEM-97/017, Part 1: Introduction and general model, Version 0.6, January 1997
3. Common Methodology for Information Technology Security Evaluation, CEM-99/008, Part 2: Evaluation and Methodology, Version 1.0, August 1999
4. CCS#4, Technical Oversight, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 0.84, 13 April 2000
5. Security Target for the SecureLogix Corporation® TeleWall® System Version 2.0, 1362-002-D001, Version 1.4, 10 November 2000
6. Evaluation Technical Report, 1362-001-D002, Version 1.8, 30 October 2000
7. Preliminary Certification Report for SecureLogix Corporation® TeleWall® System, 1362-001-D003, Version 1.3, 11 September 2000