Certification Report

EAL 1 Evaluation of ConSeal Private Desktop

Version 1.4

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 1999-EWA-03
Version: 1.00 Final
Date: 13 May, 1999
Pagination: i to iv, 1 to 19

DISCLAIMER

The 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 Certification Scheme using the Common Methodology for Information Technology Security Evaluation, Version 0.6, for conformance to the Common Criteria for IT Security Evaluation, Version 2.0. 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 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 for short) provides a third-party evaluation service for determining the trustworthiness of IT security products. Evaluation is performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the 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 CCS CB for approval to perform Common Criteria evaluations. A significant requirement for such approval by the 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.

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 also defines and scopes the evaluation activities. A consumer of certified IT products should review the ST, in addition to the certification report, to gain an understanding of any assumptions made during 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 ConSeal Private Desktop (EAL 1)
EWA File number: 1351-013-D001
Issue number: 1.01
Dated: March 31, 1999

TABLE OF CONTENTS

EXECUTIVE SUMMARY

ConSeal Private Desktop firewall (*CPD*) version 1.4 for Windows 95/98, from Signal 9 Solutions Canada Inc., is the Target of Evaluation (TOE) for this EAL 1 evaluation. *CPD* provides distributed host-based network access control and audit security functionality at the level of the personal computer (PC) desktop.

The Common Criteria Evaluation Facility (CCEF) conducting the evaluation was EWA-Canada, Ltd. Evaluation work took place over an eleven-week period from 1 Feb 1999 to 16 April 1999.

The evaluation of *CPD* has determined that the TOE can be trusted, to a level of assurance of **EAL 1**, to conform to the requirements of the Security Target (ST) [5]. The TOE is CC Part 2 conformant (functional requirements from CC Part 2 only) and CC Part 3 conformant (assurance requirements from CC Part 3 only).

The evaluated configuration for *CPD* is a PC running the Microsoft Windows 98 operating system, including all of the standard suites of office and network software applications usually found on this platform (see section 8 for further details). No special or unusual restrictions about the operating environment apply.

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 that is managed by the Communications Security Establishment (CSE). The evaluation was performed using the Common Criteria (CC) [1], applied using the Common Methodology for Information Technology Security Evaluation (CEM) [3][4].

The scope of the evaluation is defined by the ST, which identifies 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. Consumers of CPD are advised to verify that their own environment is consistent with the ST [5], and to give due consideration to the comments, observations and recommendations stated in this report.

The information contained in this document is supported by evidence contained in the detailed Evaluation Technical Report (ETR) [6].

1 Identification of target of evaluation

This report pertains to the *ConSeal Private Desktop* (*CPD*) firewall security product, version 1.4. This product is intended for use on personal computers in the Windows 95 (with WinSock 2 upgrade) or Windows 98 environment, although formal testing was completed using only Windows 98.

2 Security target

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

Security Target for ConSeal Private Desktop (EAL 1)
EWA File number: 1351-013-D001
Issue number: 1.01
Dated: March 31, 1999

3 Security policy

CPD allows users to define rules constraining the network traffic flowing to and from individual PCs. It provides easy-to-use mechanisms for control, audit and display in order to permit users to allow or block software application communications and protocol traffic. *CPD* is intended to protect both corporate and private personal computing environments against a variety of threats including unauthorised access attempts, network-based attacks, and rogue applications (such as viruses or trojan horses).

CPD is fundamentally a *hybrid* security product that provides some of the functionality typically associated with traffic-filter and application-filter firewalls, but in a distributed host-based context. Unlike "traditional" firewalls, CPD protects (and is configured) at the level of the individual PC. It is specifically designed to be easy to use and therefore, as a design trade-off, the developer has simplified the human-machine interfaces, and the product provides the user with only a limited granularity of control in defining filtering rules. *CPD* is intended to complement other PC based security applications such as virus scanners.

CPD mediates access between the host PC and its network interfaces based on *static*, *hidden* and *user-defined* rules. User control of rules is constrained to simply whether an application is declared as trusted or blocked, or whether a particular protocol is allowed or blocked. The hidden portion of the rules is not user-configurable and provides protection against a variety of known network-based attacks, as summarized below (a more comprehensive description of these access control, filtering and audit logging rules, along

with their respective user controls, is provided in the product documentation and extensive on-line help). The system services and protocols that can be controlled include:

- NetBIOS shares of TOE resources;
- NetBIOS access of remote, shared network resources;
- TCP Identification requests;
- ICMP traffic;
- ARP traffic;
- UDP/DHCP traffic;
- TCP RIP traffic;
- TCP PPTP traffic;
- IP protocols, other than TCP, UDP or ICMP; and
- non-IP protocols, other than ARP.

In addition to the above network access control, *CPD* blocks fragmented IP packets, and IP packets with the same destination and source address.

At an individual application level, *CPD* monitors Winsock applications for network access requests. When trusted applications need to access a network, *CPD* manages network access to transparently permit that application's traffic. When non-trusted (i.e. blocked) applications try to access a network, *CPD* blocks all traffic to and from that application. Apart from declaring the application itself to be trusted or blocked, *CPD* affords the user no control over what the application specifically does once it has access to the network or the Internet. Otherwise stated, once an application is declared by the user to be trusted (or blocked), the application is allowed (or denied) full network access control.

CPD is also capable of "hiding" the host system. A computer protected by *CPD* will not respond to any unexpected network connections, such as a port scan, requiring the initiating system to wait for a timeout period. If a system does not respond to a network request during a scan, it is inherently less exposed and therefore less at risk.

CPD can use a password to protect the configuration files. This password does not protect the file from deletion within the operating system, but it does restrict the

modification of the firewall configuration. If the configuration file is removed the user/administrator is warned the next time that *CPD* is started.

4 Assumptions and clarification of scope

The security aspects of the environment/configuration in which the IT product is expected to be used are included in this section.

4.1 IT environment

CPD can operate on any typical PC running the Microsoft Windows 98 (or Windows 95 with Winsock 2) operating system, and it supports all of the standard suites of office communications and network software applications usually found on these platforms. It supports a wide variety of network configurations and dial-up modem connections (including Ethernet-like network devices, but excludes Token Ring, FDDI, Frame Relay and X.25 network devices).

4.2 Environment and usage assumptions

The ST for this product defines the following assumptions:

- The PC is physically secure;
- The PC is functioning as a single-user, networked workstation. The sharing of PC resources with external network IT entities is limited to the peer-to-peer file and print sharing capabilities provided by the underlying PC operating system;
- The user of the PC is also the administrator who manages PC security functions locally (no remote administration);
- Users are non-hostile and follow all administrator guidance; however, they are capable of error;
- Only network devices compatible with the *CDP* product are installed and functioning within the PC. This includes Ethernet-like network devices, but excludes Token Ring, FDDI, Frame Relay and X.25 network devices;
- The user is knowledgeable of PC applications that require network access;
- The PC does not route traffic between network interfaces (that is, it does not act as a router);

- Users do not execute applications on the PC that communicate over network interfaces, but bypass the Winsock protocol stack (and thus the security that CPD provides);

- The TOE cannot protect against an external network user or IT entity that exploits flaws in authorized application or service implementations to read, modify, or destroy internal TOE data.

4.3 Threats

CPD is designed for a non-technical user (someone without a detailed knowledge of network protocols and services). It provides security functionality intended to protect corporate and private personal computing environments against a variety of threats including unauthorised access attempts, network-based attacks, and rogue applications such as viruses and trojan horses. The ST [5] contains the detailed threat information.

4.4 Clarification of scope

CPD is not a traditional firewall and potential customers need to clearly appreciate some of the security relevant strengths and deliberate limitations of this product, as compared with more traditional firewalls. Although *CPD* does provide much of the functionality typically associated with traffic-filter and application-level firewalls, sophisticated users may be disappointed by the lack of fine-grained control over user-defined rules that might normally be expected from a more traditional firewall product. For users requiring full fine-grained traditional control over complex rule definitions, (for example by protocol, and specific source and destination ports) the sister product developed by Signal 9 Solutions Canada, Inc., known as *PC ConSeal Firewall* may be a preferred product.

CPD is designed for a non-technical user (someone without a detailed knowledge of network protocols and services). *CPD* will not prevent a user from carelessly configuring *CPD* such that network protection is compromised, however the product will provide the user with information on insecure states and configurations so that informed decisions may be made regarding configuration and use.

The *CPD* product is intended to complement other PC-based security applications such as virus scanners.

5 Architectural information

CPD consists of three main software components:

- the CPD.EXE application;
- a highly robust and well proven packet filter; and
- the ConSeal Service Layered Service Provider.

These components and the principal data flows are described in detail in the evaluation documentation.

CPD operates at two levels within the protocol stack. At an upper level, *CPD* inserts itself as a Layered Service Provider (LSP) between the Winsock layer and the Transport Provider layer (TCP/IP, NetBIOS, etc.), and mediates Winsock application access to the network at this interface. At a lower level, *CPD* inserts itself between the Transport Providers and network device drivers, and mediates incoming and outgoing network packets.

CPD mediates access between the host PC and its network interfaces based on rules defined by the user. At an individual application level, *CPD* monitors Winsock (Windows Sockets) applications for network access requests. When trusted applications need to access a network, *CPD* manages network access to transparently permit that application's traffic. When non-trusted applications try to access a network, *CPD* blocks all traffic to and from that application. The user selects whether *CPD* trusts an application or not.

In addition to application network access, *CPD* also intercepts all inbound network packets as they are passed from the network device driver (Ethernet, Ethernet-like, dial-up, etc.), and allows or blocks them in accordance with a set of user-defined rules and the proprietary hidden static rules. Mediation of all protocols (e.g., TCP/IP, UDP/IP, ICMP/IP, ARP, NBT, IPX, NetBEUI, IPSec/IP and Gre/IP) is supported at this level.

The *CPD* user interface (UI) enables the user to specify how network access is mediated, the level of network activity displayed and what network activity is logged. The UI also provides the user with current and historical views of Winsock application network access, and their associated level of activity. As selected by the user, application network activity and mediated incoming network traffic are logged to a separate ASCII text file. This file can be reviewed using standard text editors.

5.1 System requirements

CPD requires Windows 95 (with Winsock 2 update) or Windows 98 as the underlying PC operating system. All of the standard suites of office communications and network software applications usually found on these platforms are supported, including a wide

variety of network configurations and dial-up modem connections (Ethernet-like network devices, but excluding Token Ring, FDDI, Frame Relay and X.25 network devices).

6 Documentation

6.1 Product documentation

The standard product documentation consists simply of two instructional e-mails and extensive on-line help accessible from within the *CPD* product itself. The e-mails provide information regarding step-by-step instructions for installing and licensing the product, information regarding upgrades, support and mailing lists.

Comprehensive information that is traditionally found in user and administrator guidance documents is contained within the on-line help files.

6.2 Evaluation documentation

The following proprietary reference documents were provided by the developer to support the evaluation.

- *ConSeal Private Desktop* Private Desktop Design
- *ConSeal Private Desktop* Thread Inputs
- *ConSeal Private Desktop* Access Controls
- *ConSeal Private Desktop* Requirements, Functional and Design Specification
- *ConSeal Private Desktop* Messages
- *ConSeal Private Desktop* Files
- *ConSeal Private Desktop* Hidden and Static Rules
- *ConSeal Private Desktop* WSP Calls
- *ConSeal Private Desktop* Version History
- *ConSeal Private Desktop* Specification
- *ConSeal Private Desktop* Error Messages

- *ConSeal Private Desktop* Port Mapping
- *ConSeal Private Desktop* Licensing description
- *ConSeal Private Desktop* Help Files
- *ConSeal Private Desktop* Design of Password Protection
- *ConSeal Private Desktop* Network Attacks

7 ITS product testing

This section discusses the evaluation testing effort.

7.1 Independent Testing Philosophy

The evaluators considered three aspects related to *CPD* testing:

- informally assessing Signal 9 Solution's development tests;
- performing their own independent tests; and
- performing penetration tests.

Based on the general types of tests normally applied to firewall products, the evaluators used the following general categories of testing:

- General functionality;
- Packet Filter oriented;
- Application oriented (including trojan horses);
- User Controllable options oriented; and
- Attacks and Penetration.

7.2 Testing goals

The following test goals were used in the *CPD* product testing:

- Test the delivery and installation procedures;

- Test the access control mechanisms;
- Test audit mechanisms;
- Test the hidden rules;
- Test the usability in a real-world environment;
- Perform some standard penetration tests;
- Perform some standard vulnerability scans;
- Perform some independent exploitation attacks using tools from the EWA-Canada library;
- Test that the program can display and terminate any network application, including a trojan application;
- Test the password mechanism;
- Test the detection of corrupted or deleted configuration files;
- Test the display of error codes and warnings; and
- Test the human-machine interface.

7.3 Testing coverage and depth

Informally, for some time prior to the actual evaluation, the evaluators familiarized themselves with early versions of the emerging *CPD* product. This activity allowed them to act as impartial, beta testers, permitted early insight into the developing functionality of the product, and also afforded the opportunity to provide to the developer any relevant comments which could be used to better posture the product and its documentation for success, both in the market and during the evaluation itself. This approach also allowed the evaluation planning and execution to be done in a compressed, resource efficient timeframe.

The EWA-Canada ITSET facility informally tested five different developmental versions of the *CPD* product. The final evaluation version of *CPD* was subjected to a comprehensive suite of formally documented tests during a two-week period. The detailed tests are defined in the ETR.

The evaluation testing documentation explicitly refers to the distinct goals identified in section 7.2 above. A large suite of some fifty-three subordinate objectives and tests, each with documented procedures, specific test configurations and test cases, supports each of these goals. All testing activities are designed in a manner such that they are fully repeatable and traceable to Common Criteria Security Functional requirements and components.

The testing covered all external interfaces, including network access control and all of the controls and displays associated with the human machine interface. The audit and logging functionality of the product was examined extensively and confirmed in conjunction with other tests. All of the product's proprietary hidden, static and default filtering rules were tested. All of the supported protocols were examined and/or explicitly tested.

Test cases were selected such that as many of the internal interfaces and as much of the internal design of the product as possible were exercised and stressed.

7.4 Testing results

The following high-level statements summarize the results for *CPD* that were confirmed during testing:

- the installation process for *CPD* is straightforward, correct and well documented;
- as claimed in the product documentation and extensive on-line help, the product provides protection and security functionality in the areas of access mediation, access display, access control; and security event audit logging;
- the product is highly useable in a real-world context by novice users, for both network operations on a LAN and Internet operations;
- *CPD* proves the concept of distributed firewalls can be used as cost-effective tools in an arsenal of security products;
- The hard-coded hidden static filtering rules within *CPD* do provide the claimed protection against, and auditing of, well-known network-based attacks, including those based on flooding the host with fragmented packets;
- The product proved to be highly robust in the face of real-world denial-of-service (DoS) attacks and stress testing;
- *CPD* provides exceptional protection against many kinds of attacks and means of vulnerability exploitation;

- *CPD* provides a highly intuitive means to gain insight into the behavior of software applications that communicate (or attempt to, if they are not trusted). The actual behavior of the system can be a major revelation for many users who are blissfully unaware that a growing number of commercially available applications acquire network or Internet access and communicate without their knowledge or explicit consent;

- *CPD* further provides the user with a means to detect and manage (by identifying, locating, allowing/blocking or stopping) rogue applications such as trojan horses, or new applications which the user may not be aware are attempting to access a network or the Internet in violation of a user's preference or an organizational security policy;

- *CPD* informs the user of, and provides good protection against, network scanning activities and, in fact, does hide the host (including things like open-application services) from the network or the Internet;

- *CPD* facilitates password protection of the system settings;

- *CPD* alerts the user of, and can automatically recover from, corrupted/deleted software configurations that may compromise security; and

- *CPD* does provide the user with extensive, useful and understandable error codes and warnings.

7.5 Test environment

The suite of software applications used during the evaluation testing effort is listed in Table 1, below. Figure 1 shows the network setup that was used during testing and Table 2 describes the configuration of each test system.

Name	Version	Purpose	Comment
MS Windows	98	Operating System	Default installation with MS Network client, and TCP/IP, NetBIOS over TCP/IP (NBT) and NetBEUI network protocols.
MS Telnet	98	Telnet client included with Windows 98	Included with Windows 98. Representative network application.
MS FTP	98	FTP client included with Windows 98	Included with Windows 98. Representative network

Name	Version	Purpose	Comment
			application.
MS Internet Explorer	4.0	Web browser	Included with Windows 98. Representative network application.
MS Outlook Express	4.0	E-mail, newsreader client	Representative network application.
MS Office	97 Pro SR 2a	Word processor, spreadsheet, presentation, database application	Default installation less Outlook. Representative office application.
Netscape Communicator	4.5	Web browser, E-mail, newsreader, FTP client	Representative network application.
Eudora Light	3.06	E-mail client	Representative network application.
Free Agent	1.11	Newsreader	Representative network application.
WS FTP Pro	5.00	FTP client	Representative network application.
mIRC	5.51	IRC client	Representative network application.
ICQ	99a	ICQ client	Representative network application.
Real Player	G2	Streaming audio/video client	Representative network application.
Terra Term	1.4	Telnet client	Representative network application.
ConSeal Private Desktop	1.4	Desktop Security	TOE security application

Table 1: TOE Software Environment

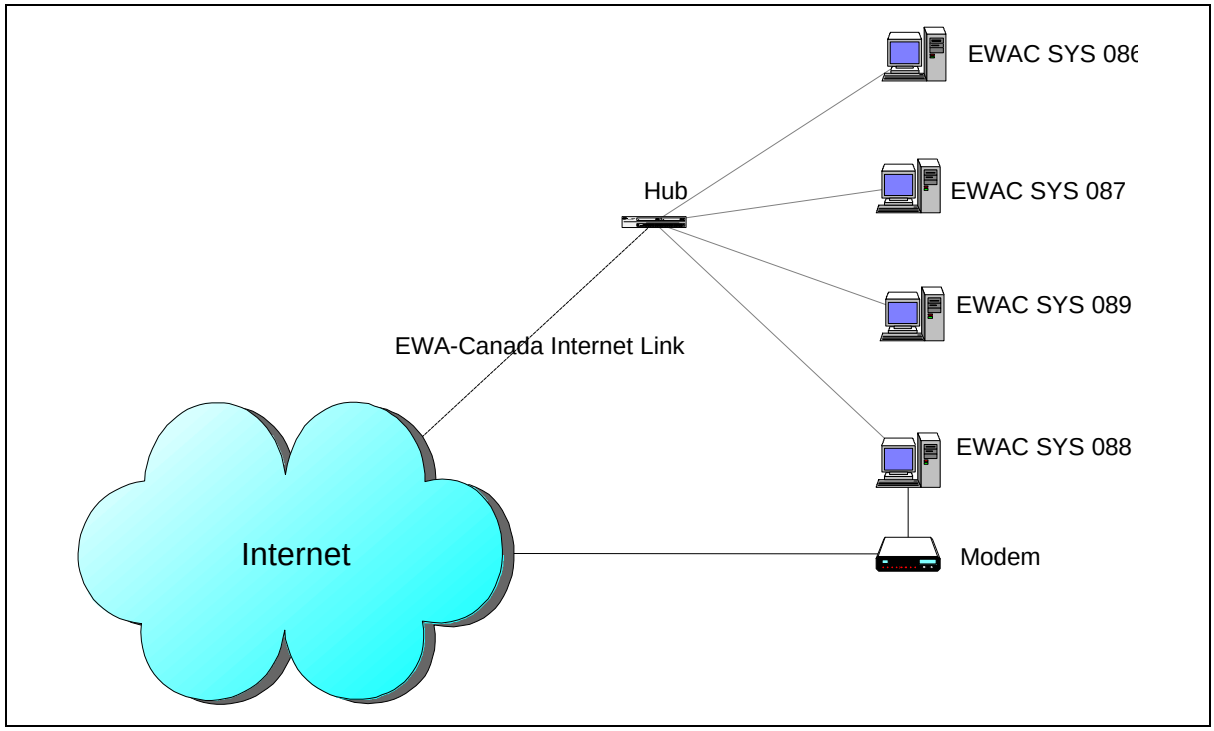

Figure 1 *CPD* Test Network

EWA System Identification	Hardware Description	Operating System	Applications
EWAC-SYS-086	Acer Pentium 133 2 Gbyte fixed disk 64 Mbyte RAM Artisoft Noderunner NIC	Microsoft Windows 95	
		RedHat Linux 5.2	Nessus Teardrop Winnuke
EWAC-SYS-087	Acer Pentium 133 2 Gbyte fixed disk 64 Mbyte RAM Intel eepro NIC	Microsoft Windows 98 NetBIOS File Sharing	Netscape Internet Explorer Eudora Light Free Agent Netcat
		Red Hat Linux 5.2	

EWA System Identification	Hardware Description	Operating System	Applications
EWAC-SYS-088	Acer Pentium 350 6.4 Gbyte fixed disk 64 Mbyte RAM Intel eepro NIC	Microsoft Windows 98 NetBIOS File Sharing	Netscape Internet Explorer Eudora Light Free Agent Mirc ICQ MS-Office WS-FTP RealPlayer Terra-Term Outlook Express
		RedHat Linux 5.2	
EWAC-SYS-089	Acer Pentium 350 6.4 Gbyte fixed disk 64 Mbyte RAM Intel eepro NIC	Microsoft Windows NT 4.0	
		RedHat Linux 5.2	Tcpdump

Table 2 *CPD* Evaluation Laboratory System Configuration

8 Evaluated configuration

The evaluated configuration of *CPD* is version 1.4 for PCs running the Microsoft Windows 98 operating system, in an Ethernet-based networked environment, and includes a standard modem dial-up and a representative suite of office and network applications.

9 Results of the evaluation

The evaluation of CPD has determined that the TOE can be trusted, to an **EAL 1** level of assurance, to conform to the requirements of its ST. The TOE is CC Part 2 conformant (functional requirements from CC Part 2 only) and CC Part 3 conformant (assurance requirements from CC Part 3 only).

EAL 1 provides a basic level of assurance by an analysis of the security functions described in a functional specification and guidance documentation to understand the security behavior. Independent testing of the TOE security functions supports the analysis.

10 Comments, observations and recommendations

10.1 Requirement for source code review

During the course of this evaluation, to increase their comprehension and understanding of certain critical functionality for this product, the evaluators requested whether it might be possible to have additional explanation in two areas of the product design. The first area related to the product default "Hidden and Static Rules", and in particular, the packet filtering and network access control rules which apply to user-transparent protection against common network-based attacks such as "LAND". The second area related to the requirement for the developer to make extensive product improvements in the area of audit recording as a result of this evaluation.

Discussions between the evaluators and the developer resulted in agreement that the best approach, in terms of both efficiency and increased credibility for the evaluation, would be for the evaluators to review a portion of the actual product source code, along with the benefit of relevant explanations.

Information gained from the source code review (along with the numerous other verbal explanations and considerably more low level design information which was continuously and cooperatively provided to the evaluators during the course of the evaluation), was invaluable in ascertaining the precise functionality of the product in certain security-critical areas.

Although these requests went well beyond what is normally carried out at EAL 1, and despite the fact that the source code is very tightly controlled as valuable intellectual property, the developer agreed to provide this information, under conditions of non-disclosure. The evaluators would like to acknowledge the exceptional co-operation of the developer in their assistance and co-operation throughout this evaluation, including making all design documentation and source code available upon request.

10.1.1 Developer's implementation coding standards

In addition to the source code itself, the developer provided the evaluators with general written guidelines as to the proprietary coding standards and practices followed by the company for this product line. The evaluators informally inspected the code with full knowledge of these standards.

In their limited code review, the evaluators found that the developer appeared to adhere to the company documented coding guidelines and standards, as expected. Much of the *CPD* product is written in high order languages (C, and C++) which makes for ease of maintenance over the product lifecycle and which facilitates design and code reviews.

Although the documented coding standards were fairly general in scope and minimal in coverage (with respect to all of the variables, which might be standardized), they do represent documented evidence of good practices which would tend to support Common Criteria coding standard requirements that enter at higher assurance than EAL 1.

10.2 Significant results of the source code review

10.2.1 Increased evaluator knowledge and confidence

As a direct result of the source code review, the detailed product-specific knowledge of the evaluators increased considerably in the two key security areas of interest. In particular, the review confirmed the simplicity and elegance of the design of the *CPD* packet filter, the core component of the product.

10.2.2 Analytical confirmation of the proprietary hidden and static filtering rules

The evaluator's line-by-line inspection of the *CPD* product default hidden and static packet filtering and network access control rules revealed no syntax or logic errors (some minor syntax errors had understandably been present in early beta versions). All hidden and static filtering rules were comprehensively inspected. Filtering logic based on user settings (where applicable) was also reviewed. Adequate comments appear in the code, which document the applicable filtering variables (e.g. port numbers and protocol types, etc.) and related design structures. The results of this inspection and analysis both supported, and were consistent with, the results of actual testing of these rules and logic.

Regarding the area of code controlling the logging of security-relevant audit records, the evaluators found that the new design additions had been well introduced into contained areas of the product code, without apparent adverse impact on other areas (confirmed during testing). These controlled changes had been facilitated by the highly modularized design of the *CPD* product. The logic confirmed the expected functionality and corroborated the sequencing of the audit log records actually reviewed during informal and formal product testing, and the audit log examples in the on-line help file.

10.2.3 No backdoors or security compromising features found

In the sampling of the source code reviewed by the evaluators (which represents a relatively small portion of the product, albeit in critical areas), the evaluators found no evidence of backdoors, illogical structures, weak interfaces or similar security-compromising features.

10.3 Developer's CM procedures

At EAL 1, the CC does not require the developer to have a formal Configuration Management system with documented procedures or automated tools. However, Signal 9 Solutions Inc. has a documented, (albeit minimally detailed), CM procedure for controlling the *CPD* product line. The responsibility for implementing the CM procedures is vested primarily in a single engineer (for control within the company), and the procedure itself generally focuses on control of the code and associated libraries. Prior to and during the course of the evaluation activities, all early beta versions of the *CPD* product and the associated documentation were observed to be uniquely identified and procedurally controlled by Signal 9. The distribution of the product (by e-mail) was always clearly accompanied by version-specific configuration identification information.

As a useful audit trail, the company also generally documents the version description information describing the product evolution, and distributes this information to beta testers and customers, as appropriate. User-oriented extracts of this information are provided in the product on-line help. A detailed example of this is included in the ETR [6].

The recommendation has been made to the developer that, if they wish to further improve their software development environment in the future, a code management system may be a reasonable and logical addition. This will provide a significant increase in product management capabilities that can support a larger development team, and represents an important investment in another higher level assurance family.

11 Glossary

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

11.1 Abbreviations and acronyms

CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CPD	ConSeal Private Desktop
CR	Certification Report

CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TOE	Target of Evaluation

11.2 Vocabulary

Traffic Filter: refers to filtering of network traffic on the basis of information found at the network layer, typically port number and other information associated with connections and individual packets.

Application Filter: refers to filtering done on the basis of information specific to each individual application protocol. For example, the ability to allow or disallow specific commands during a FTP session.

Virus: a virus is a program that implants itself to other executable files and spreads systematically from one file to another.

Trojan horse: a program that appears to be trustworthy, possibly even performing a useful function, but which is in fact malicious.

12 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, Version 2.0, May 1998;
2. CCS#4, Technical oversight, Canadian Common Criteria Evaluation and Certification Scheme (CCS), version 0.82 - Draft;
3. Common Methodology for Information Technology Security Evaluation, CEM-97/017, Part 1: Introduction and general model, Version 0.6, 11 January 1997;
4. Common Methodology for Information Technology Security Evaluation, CEM-99/008, Part 2: Evaluation methodology, Version 0.6, January 1999;
5. Security Target for Signal 9 Solutions ConSeal Private Desktop (EAL 1), 1351-013-D001, issue number 1.01, March 31, 1999;

6. Evaluation Technical Report, D1351-0130-D003, March 31, 1999;
7. Preliminary Certification Report for ConSeal Private Desktop (EAL 1), 1351-013-D002, 31 March 1999.
8. ConSeal VPN and Firewall Security, VPNs Much more than Encryption, Authentication and Remote Access.
9. ConSeal VPN and Firewall Security – ConSeal PC Firewall™ – Securing your Backdoor.