National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Safend Protector
Version 3.0

Report Number: **CCEVS-VR-10177-2008**

Dated: **August 13, 2008**
Version: **1.1**

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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers, Aerospace
Scott Shorter, Orion Security Solutions

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of **Safend Protector 3.0** was performed by SAIC, in the United States and was completed in August 2008. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Safend Protector 3.0 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3 and International Interpretations effective on 12, January 2007. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is the EAL 2 family of assurance requirements. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Safend Protector 3.0 Security Target.

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Safend Protector 3.0 product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, examined evaluation testing procedures, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The validation team notes that the claims made and successfully evaluated for the product represent a more limited set of requirements than what might be used for a "normal" product deployment. Specifically, no claims are made for protection of data transmission between the TOE and non –TOE components such as the web browser and the network devices in spite of the fact that it will mostly likely be configured and setup in a distributed fashion over a network whose traffic could well be less than benign. It then becomes quite necessary for the administrators to fulfill the requirements levied on the environment.

The technical information included in this report was obtained from the Evaluation Technical Report for Safend Protector 3.0 (ETR) Parts 1 and 2 produced by SAIC.

1.1 Evaluation Details

Evaluated Product: **Safend Protector 3.0**

Sponsor & Developer:	Safend Ltd. 2 Penn Center, Suite 300 Philadelphia, PA 19102
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Completion Date:	August 2008
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation, Version 2.3
Evaluation Class:	EAL 2
Description	Safend Protector™ Version 3.0 is a software product that complements enterprise data security and network/server-based security products by controlling access to external physical, wireless and storage device interfaces on network endpoints (e.g., workstations, laptops). Safend Protector enables IT security administrators to design and implement an enterprise-wide security policy (Protection Policy) regulating the peripheral devices and storage media to which enterprise endpoints can connect and communicate with. Safend Protector controls access to physical ports (USB, FireWire, PCMCIA, SecureDigital (SD), serial, parallel, modem), wireless ports (Bluetooth, WiFi, IrDA), and storage media (CD/DVD Drives, flash drives, floppy drives, tape drives). Safend Protector can also identify and restrict USB, FireWire, and PCMCIA devices by their class, vendor, model, or unique serial number, and can identify and restrict storage devices based on their storage capacity, type, model, or unique serial number. It can also identify and restrict WiFi network connections based on the network identity (MAC address or SSID), authentication mode and encryption mode. Multiple customized Protection Policies, specifying different access rights for different user groups, can be created and automatically distributed according to the organizational units (computers and users) already defined in the enterprise

	Active Directory. By controlling access to these endpoint interfaces, Safend Protector prevents data leakage and theft, enterprise penetration, and introduction of malware. Safend Protector provides central control over enterprise interfaces, devices and storage devices and ensures that users will only be able to use permitted devices through permitted interfaces.
Disclaimer	The information contained in this Validation Report is not an endorsement of the Safend Protector 3.0 product by any agency of the U.S. Government and no warranty of the Safend Protector 3.0 product is either expressed or implied.
PP:	none
Evaluation Personnel	Eve Pierre, SAIC Gary Grainger, ASL
Validation Team:	Scott Shorter, Orion Security Solutions Jerome Myers, Aerospace

1.2 Interpretations

The Evaluation Team determined that there were no NIAP Interpretations applicable to this evaluation:

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 1 - Threats

Threat	TOE Threats
T.UA-ACCESS	An unauthorized user may gain access to or modify TOE data, whether stored in the TOE components or in transit between distributed parts of the TOE, in order to acquire knowledge of and/or circumvent the protection afforded by the TOE.
T.UA-ACTION	An authorized user may exceed his or her privileges and gain access to or perform unauthorized modifications of TOE data which go undetected, in order to acquire knowledge of and/or circumvent the protection afforded by the TOE.

Threat	TOE Threats
T.DISABLE	An attacker may disable or delete the TOE Client or modify its behavior and thus expose the protected machine (and through the compromise machine, the network as well) to attack. Note that the attacker described here may well be the authorized user of the TOE.
T.ATTACK	An attacker may gain access to the protected machine (the TOE Client) via the machine's physical interfaces, using a variety of well-known attack methods, and thereby gain access to and/or modify user data, or install malware on the endpoint machine or in the protected network.
T.DISCLOSURE	An endpoint user accidentally or deliberatey exposes user data by writing it to a removable storage device or media, or sending it to an insecure device or network.

2 Identification

The product being evaluated is Safend Protector 3.0. Note that the actual target of evaluation is defined to be the entire product.

3 Security Policy

Table 2 - Policies

P.MANAGE	IT Systems are protected from unauthorized access and modification.

4 Assumptions

4.1 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

Table 3– Personnel Assumptions

A.ADMIN	The administrators assigned to manage the TOE: • Are competent and properly trained; • Are neither careless, willfully negligent, nor hostile; • Follow the guidance and instruction provided in the TOE documentation; • Install and administer the TOE in a manner consistent with organizational policies.

4.2 Physical Assumptions

The following physical assumptions are identified in the Security Target:

Table 4 – Physical Assumptions

A.LOCATE	The TOE Management Server and TOE Management Console and other components on which they rely (for example, the Active Directory Server) are located in a physically secured area, protected from unauthorized physical access.
A.PROTECT	The endpoint devices that host the TOE Client are physically protected to the degree necessary to ensure that the TOE Client cannot be uninstalled or otherwise disabled by direct physical interaction with the endpoint device.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made; and meets them with only a certain level of assurance (EAL 2 in this case).
2. As with all EAL 2 evaluations, this evaluation did not specifically search for vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM); or seriously attempt to find counters to them; nor find vulnerabilities related to objectives not claimed in the ST.
3. Encryption of communications using SSL between the TOE Client and the TOE Management Server components and between the Management Console and the Management Server is required on the IT environment. The evaluation team did verify that communication between the components is encrypted. Testing confirmed the presence of encrypted communication.

5 Architectural Information

Safend Protector enables IT security administrators to design and implement an enterprise-wide security policy (Protection Policy) regulating the peripheral devices and storage media to which enterprise endpoints can connect and communicate with. Safend Protector controls access to physical ports (USB, FireWire, PCMCIA, SecureDigital (SD), serial, parallel, modem), wireless ports (Bluetooth, WiFi, IrDA), and storage media (CD/DVD Drives, flash drives, floppy drives, tape drives). Safend Protector can also identify and restrict USB, FireWire, and PCMCIA devices by their class, vendor, model, or unique serial number, and can identify and restrict storage devices based on their storage capacity, type, model, or unique serial number. It can also identify and restrict WiFi network connections based on the network identity (MAC address or SSID), authentication mode and encryption mode.

Safend Protector operates at the lowest level of the kernel, just above the TOE Client machine's hardware. With the understanding that every endpoint has a different set of external interfaces, based on differing standards but all employing similar architectures – Safend has created a unique kernel-level protocol inspection engine on the TOE Client machine that analyses in real time all inbound and outbound communication for a given port or interface. Safend Protector monitors and controls all incoming and outgoing traffic for each device, blocking or allowing access or data based on the Protection Policy defined in the Safend Protector Management Console.

5.1.1 Hardware/Software Components

The TOE consists of the following components:

- **Protector Management Server** (TOE Management Server), the repository for the TOE database (Protection Policies, integrated logs, *etc*.), downloads Protection Policies to the Protector Clients (via Active Directory), receives logs from the Protector Clients, and manages and displays the centralized log file.
- **Protector Management Console** (TOE Management Console), the graphic interface by which TOE administrators maintain the TOE.
- **Protector Client** (TOE Client), installed on the protected machine (the endpoint), enforces the policy downloaded to it by Protector Management Server (via Active Directory), writes logs (audit records) locally, and periodically uploads those logs to Protector Management Server.

6 Documentation

Following is a list of useful documents supplied by the developer and shipped with the product.

- Safend Protector v3.0 – Release Notes, August 28, 2006
- Safend Protector Installation Guide Version 3.0
- Safend Protector User Guide Version 3.0

The security target used is:

- Safend Protector Security Target, Version 1.98, 21 July, 2008.

7 IT Product Testing

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a subset of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST. The tests were conducted using:

- Management Server running on Windows 2003
- Management Console running on Windows 2003
- TOE Client installed on Windows 2003, Windows XP, and Windows 2000
- The TOE Client machines had the following ports: USB, FireWire, PCMCIA, SecureDigital, Serial, Parallel, Modem, WiFi, Bluetooth, and IrDA.

The developer test suite was examined and found to provide adequate coverage of the security functions; where the vendor test suite provided insufficient coverage, the evaluation team devised additional test cases to adequately test the security functions. For example: The vendor test did not adequately test the following: access control enforcement based on a user policy; port access control enforcement when no policy is applied on the client machine; and the restrictions on management console based on role; the evaluation team devised test cases to validate these aspects of the Policy enforcement and security management security functions. In addition the vendor tested access control to the serial port by checking Windows Manager, the team tested this by connecting a device to the serial port and ensuring that the SFP is enforced; the vendor did not test access control to tape drive devices, the evaluation team tested that the SFP is enforced for access to these devices.

A subset of the developer tests were run and the results were found to be consistent with the results generated by the developer.

No vulnerabilities in the TOE were found during a search of vulnerability databases.

8 Evaluated Configuration

The evaluated configuration is the Management Server installed on a machine running Windows 2003, The Management Console running on a Windows 2003 machine, and the TOE Client installed on several Windows machines including Windows XP, Windows 2000, and Windows 2003.

9 Results of the Evaluation

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s performance of the vendor tests suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

Administrators should be alert for unexpected “Policy Update” audit events, as these may indicate the actions of malicious users attempting to circumvent the policy by copying policy files from one machine to another. This issue can be mitigated by following the vendors advice to prevent local users from administering their own computers.

The TOE relies on OpenSSL version 0.9.8a which has a number of potential public known vulnerabilities, but none of them have been demonstrated to have an impact on the evaluated product.

Note that there is no claim in the Security Target that the TOE will protect the audit log from filling up. The administrator should therefore monitor the system to ensure that sufficient storage space remains to store the logs. Also, the TOE relies on the IT environment for the delivery of alert messages.

11 Annexes

Not applicable.

12 Security Target

The security target for this product's evaluation is **Safend Protector Security Target, version 1.98, 21 July 2008**.

13 Glossary

There were no definitions used other than those used in the CC or CEM.

Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.

[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 2005, Version 2.3.

[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 2005, version 2.3.

[7] Evaluation Technical Report for Safend Protector 3.0 Part II, version 1.0, October 26, 2007

[8] Security Target for Common Criteria: Safend Protector 3.0, version 1.98, 21 July 2008.

[9] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001