Swedish Certification Body for IT Security

Certification Report StoneGate FW/VPN 5.2.5

Issue: 1.0, 2012-jan-24

Authorisation: Dag Ströman, Head of CSEC , CSEC

Report Distribution: Jorma Levomäki, Stonesoft
Jerry Johansson, CSEC
Arkiv

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is a firewall with VPN capability, designed for high availability. During the evaluation, the VPN module has been considered a security non-interfering component of the TOE and has not been evaluated.

The TOE is comprised of software only, but is delivered with a hardened Debian GNU/Linux 5.0, and a hardware appliance. On delivery, the latest software is pre-installed, and the certified version is downloaded via a secure channel and then installed. Normally, the TOE is purchased as part of a firewall cluster also including a Management Server and a Log Server. An administration guide, a reference guide, an installation guide, and a configuration guide specific to the certified version also are included in the TOE.

No conformance claims to any PP is made for the StoneGate Firewall and VPN.

The StoneGate Firewall and VPN is intended for use by larger organisations, maintaining one or several clusters of firewalls from one or several Management Servers, along with Log Servers, possibly with separate maintenance networks.

The firewall functionality includes stateful packet filtering and flow control based on source address, destination address, transport layer protocol, source port, destination port, and the interface at which the packet arrives. Protocol agents provide further rules. The protocol agents for FTP, HTTP, and SMTP are included in the evaluated configuration, all others are outside the scope of the evaluation.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.

This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2011001
Name and version of the certified IT product	StoneGate Firewall and VPN, version 5.2.5.8081.cc.2
Security Target Identification	StoneGate Firewall 5.2.5.8081.cc.2 Security Target, Stonesoft Corporation, 2011-10-06, document version 2.1
EAL	EAL4 + ALC_FLR.1
Sponsor	Stonesoft Corporation
Developer	Stonesoft Corporation
ITSEF	atsec information security AB
Common Criteria version	3.1 revision 3
CEM version	3.1 revision 3
National and international interpretations	-
Certification completion date	2011-12-20

3 Security Policy

The TOE provides the following security services:

- Information Flow Control
- Network Address Translation
- High Availability
- Auditing
- Security Management

3.1 Information Flow Control

The TOE mediates the flow of all information that passes between the connected networks and enforces the firewall security policy using:

Access rules based on source IP address, destination IP address, source port, destination port, transport layer protocol, application layer protocol, and on which network interface the data arrives. The rules also considers connection status, user authentication, and connection validity time.

Protocol agents provides additional protocol specific rules based on application level data, the evaluation covers the protocol agents for FTP, HTTP, and SMTP, while others have not been covered. The TOE also has capabilities to re-direct network traffic.

3.2 Network Address Translation

The TOE supports NAT, so that the local IP addresses of internal hosts may be kept private from external users.

3.3 High Availability

When used as part of a cluster, the TOE provides failover mechanisms to increase the availability in case some nodes in the cluster fails.

3.4 Auditing

The TOE provides means to generate audit records for security relevant events, relating to the network traffic flow through the firewall, and to changes in the security policy. Authorized administrators may define criteria for which events to audit. The TOE supports the use of external audit storage servers.

3.5 Security Management

Administrators manages the firewall engine through a Management Server (outside the scope of TOE), which provides the interface to configure the firewall security policy, and other security relevant functionality.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes two assumptions on the usage of the TOE.

A.ADMINTRUSTED - the administrators are trained, qualified, non-hostile, and follow all guidance.

A:AUDITMAN - the audit trails are regularly analyzed and archived.

4.2 Environmental Assumptions

Six assuptions are made in the ST [ST] on the environment.

A.ADMIN_ACCESS - the administrator accesses the TOE via the trusted Management Server on a trusted and separate management network, and the administrator has been identified and authenticated to the Management Server before access to the TOE.

A:AUDIT_SUPPORT - the IT environment, on which TOE depends, generates proper audit records in itself, and also provides a protected permanent storage for the audit records from TOE.

A.MEDIAT_SUPPORT - networks connected to the TOE are only connected via the TOE.

A:OPERATING_ENVIRONMENT - the TOE node (i.e. the hardware and operating system, not the TOE in itself), the associated Management Server(s), and the management network are all dedicated to the trusted firewall system, and are assumed to function according to their specifications, to be physically secure, and that only autorized administrators have physical access to them.

A.USER_AUTH - the IT environment provides a user authentication mechanism which is used when the firewall security policy requires authentication before allowing an information flow.

A.TIME - the IT environment provides a reliable time source for the TOE and the TOE environment.

4.3 Clarification of Scope

The ST [ST] contains four threats, which have been considered during the evaluation.

T.AUDIT_UNDETECTED - an attacker deletes audit data or prevents the generation of audit records by exhausting the audit storage capacity, in order to mask an attack against the assets protected by the TOE.

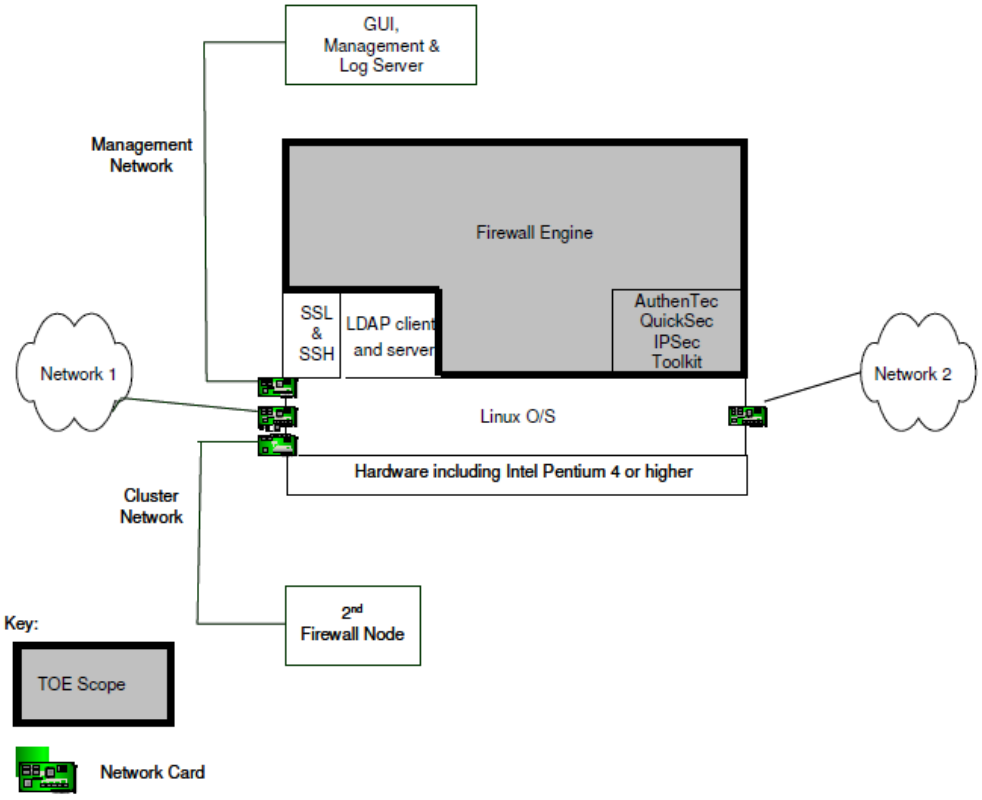
T.MEDIAT - an attacker sends information through the TOE, potentially compromising protected IT resources, thus violating the configured firewall security policy. This includes using forged source IP addresses.

T.NODE_FAILURE - an attacker causes a denial of service attack, rendering protected IT resources unavailable. Spontaneous hardware failure is considered a special case of this attack.

T.SELPRO - an unauthorized person accesses the TOE management functions to read, modify, or destroy critical TSF data, in order to get access to protected IT resources.

5 Architectural Information

The TOE consists of the firewall engine software, version 2.5.2.8081.cc.2, the AuthenTec QuickSec IPsec Toolkit, version 5.1, and documentation. The TOE is part of a product, which also includes hardware and an operating system.



6 Documentation

The following documents are included in the scope of the TOE:

- StoneGate 5.2 Firewall/VPN Reference Guide [REFGUIDE]
- StoneGate 5.2 Firewall/VPN Installation Guide [INSTALL]
- StoneGate 5.2 Administrator's Guide [ADMIN]
- StoneGate 5.2 Common Criteria Certification User's Guide [CCGUIDE]

7 IT Product Testing

7.1 Developer Testing

The developer has developed an Automated Testing Framework (ATF) which was used during the testing of the TOE. The ATF runs scripted test suites and collects test result. The test scope include testing of:

- Information flow control
- Network Address Translation (NAT)
- High availability
- Audit
- Security Management

All hardware appliances were tested, FW-3201 (64 bit) and FW-315 (32 bit) were tested extensively (i.e. every test case was used on each of these). This also means that both the 32-bit binary and the 64-bit binary (the same source code is used for both, but the compiler generates different binaries for 32/64 bit processors) were tested extensively. For the FW-3201 and FW-1301 hardware, subsets of the test cases were used.

The tests were divided into test suites, with consists of a number of test cases, each of which tests one or many functions using one or several data sets.

The evaluators verified that every TSFI function and subsystem was tested with focus on security relevant behaviour, and with a fine-grained coverage of TSFI and subsystem functionality.

The testing was successful for all TOE configurations.

7.2 Evaluator Testing

The evaluators verified the developer testing by re-running 6 test suites, each comprised of multiple subtests. Both 32-bit and 64-bit TOEs were tested.

Additionally, the evaluators executed manual tests on the 32-bit platform, covering "definition of a cluster", "secure start-up", and "installation", in order to verify the auditing and security management functionality.

All test results were consistent with the expectations.

7.3 Evaluator Penetration Testing

The evaluator's performed penetration testing using a 32-bit TOE.

The penetration testing was done using OpenVAS, Nmap, and Python scripts, from a dedicated test laptop. The testing covered the following areas:

- NAT traversal
- ARP poisoning
- Sending valid and malformed UDP, TCP, and ICMP messages
- HTTP block
- Port scanning
- Vulnerability scan

The testing did not reveal any exploitable vulnerability of the TOE.

8 Evaluated Configuration

The TOE is delivered with hardware and Debian GNU/Linux 5.0 (Lenny) with a slightly modified Linux 2.6.32.28 kernel. The hardware is one of the following:

- FW-315 with a 32-bit Intel processor
- FW-1301 with a 64-bit Intel processor
- FW-3201 with a 64-bit Intel processor
- FW-3205 with a 64-bit Intel processor

All of these are of standard PC type.

In the firewall node, OpenSSL 0.9.8, OpenSSH 5.1, and OpenLDAP client and server version 2.4 were present (but not part of the TOE).

The TOE was set up in two-node clusters, with several different hardware combinations, during the testing.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the ST [ST] for an attack potential of Enhanced-Basic.

The certifier reviewed the work of the evaluator to determine that the evaluation was conducted in accordance with the requirements of the Common Criteria [CC].

The evaluators overall verdict is: PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional specification	ADV_FSP.4	PASS
Implementation representation	ADV_IMP.1	PASS
TOE design	ADV_TDS.3	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Life-cycle support	ALC	PASS
CM capabilities	ALC_CMC.4	PASS
CM scope	ALC_CMS.4	PASS
Delivery	ALC_DEL.1	PASS
Development security	ALC_DVS.1	PASS
Flaw remediation	ALC_FLR.1	PASS
Life-cycle definition	ALC_LCD.1	PASS
Tools and techniques	ALC_TAT.1	PASS
Security Target evaluation	ASE	PASS
ST introduction	ASE_INT.1	PASS
Conformance claims	ASE_CCL.1	PASS
Security problem definition	ASE_SPD.1	PASS
Security objectives	ASE_OBJ.2	PASS
Extended components definition	ASE_ECD.1	PASS
Security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS
Depth	ATE_DPT.1	PASS
Functional tests	ATE_FUN.1	PASS
Independent testing	ATE_IND.2	PASS
Vulnerability assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.3	PASS

10 Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product or using the product.

11 Glossary

ARP	Address Resolution Protocol, protocol for binding an IP address to the MAC address of a physical network interface card
CC	Common Criteria for Information Technology Security, set of three documents, CC Part 1-3, standard for security evaluation of IT products
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
FTP	File Transfer Protocol, part of TCP/IP, protocol used for transfer of data files
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol, protocol used for communication between web browsers and web servers
IP	Internet Protocol, part of TCP/IP, low-level communication protocol
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
LDAP	Lightweight Directory Access Protocol, protocol for accessing directory databases
NAT	Network Address Translation, technique used in firewalls to connect a private IP network to a public IP network, letting all private nodes share one public IP address
NMAP	Utility for portscanning
OpenLDAP	Open source software, implementing LDAP
OpenSSH	Open source software, implementing SSH
OpenSSL	Cryptography toolkit, open source software
OpenVAS	Utility for vulnerability scanning
PP	Protection Profile, document containing evaluation requirements and specifications for a product category
Python	Interpreted, high level programming language
SSH	Secure Shell, protocol for secure communication
SSL	Secure Sockets Layer, protocol for cryptographic protection of transmitted data
SMTP	Simple Mail Transfer Protocol, part of TCP/IP, protocol used for transfer of e-mail
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TCP	Transmission Control Protocol, part of TCP/IP, connection oriented communication protocol
TOE	Target of Evaluation
TSFI	TOE Security Functional Interface
UDP	User Datagram Protocol, part of TCP/IP, datagram (connectionless) communication protocol
VPN	Virtual Private Network

12 Bibliography

ST	StoneGate Firewall 5.2.5.8081.cc.2 Security Target, Stonesoft, 2011-10-06, document version 2.1
ADMIN	StoneGate 5.2 Administrator's Guide, Stonesoft, 2011-05-25, document id SGAG_20101027
REFGUIDE	StoneGate 5.2 Firewall/VPN Reference Guide, Stonesoft, 2011-05-25, document id SGFRG_20101015
INSTALL	StoneGate 5.2 Firewall/VPN Installation Guide, Stonesoft, 2011-05-25, document id SGFIG_20101231
CCGUIDE	StoneGate 5.2 Common Criteria Certification User's Guide, Stonesoft, 2011-09-30, document id SGCC_20110930
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, CCMB-2009-07-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, CCMB-2009-07-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, CCMB-2009-07-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, CCMB-2009-07-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2011-11-11, document version 16.0