CSEC

Swedish Certification Body for IT Security

Certification Report- Stonesoft FW-VPN o IPS V5.5

Issue: 1.0, 2014-jun-27

Authorisation: Dag Ströman, Head of CSEC , CSEC

Report Distribution:

Arkiv

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is Stonesoft Firewall/VPN & IPS Security Engine 5.5 with the following elements:

- Stonesoft Firewall/VPN & IPS Security Engine, version 5.5.4.9869.cc.2
- INSIDE Secure QuickSec IPsec Toolkit, version 5.2

The TOE is a network protection software component running on an appliance. It may be operated either as a Layer 3 Firewall with VPN or as a transparent Layer 2 Intrusion Prevention System (IPS).

Operated as Firewall/VPN it provides a Multi-Layer Inspection technology that combines both stateful and application-level inspection technology to control connectivity and information flow between internal and external networks. It also provides a means to keep the internal hosts' IP-address private from external users. As part of a cluster, the Stonesoft Firewall/VPN & IPS Security Engine provides high availability of these firewall security services for the users and servers protected by the cluster of firewalls when a node in the cluster or a network connection to a node fails.

Operated as IPS, it provides Multi-Layer Inspection technology combined with evasion-proof threat protection and flexibility in network deployment.

No claims to Protection Profile conformance were made.

There are ten assumptions made in the ST regarding the secure usage and environment of TOE. The TOE relies on these being met to counter the six threats, and to fulfil the three organisational security policies (OSP) in the ST. The assumptions, the threats and the organisational security policies are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information security AB in Danderyd, Sweden, and was completed on 2414-06-19. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1 R4, and the Common Methodology for IT Security Evaluation, version 3.1 R4. The evaluation was performed at the evaluation assurance level EAL4, augmented by ALC_FLR.1 Basic Flaw Remediation.

The certifier audited the activities of the evaluator by reviewing all evaluation reports and by overseeing the evaluators performing site visit and testing. The certifier determined that the evaluation results showed that the product satisfied all functional and assurance requirements stated in the Security Target [ST]. The evaluator concluded that the common criteria requirements for evaluation assurance level EAL4 augmented by ALC_FLR.1 have been met.

The technical information included in this report has been compiled from the Security Target [ST] and from the final evaluation report produced by atsec information security AB.

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	CSEC2013003
Name and version of the certified IT product	Stonesoft Firewall/VPN & IPS Security Engine 5.5
Security Target Identification	McAfee NGFW and McAfee NGFW-IPS 5.5 Security Target, document version 2.0, 2014-05-27
EAL	EAL4 augmented by ALC_FLR.1, CC part 3 conformant.
Sponsor	McAfee, Inc. (An Intel Company)
Developer	McAfee, Inc. (An Intel Company)
ITSEF	atsec information security AB
Common Criteria version	Common Criteria version 3.1R4 [CCp1], [CCp2], [CCp3]
CEM version	Common Methodology for Information Technology Security Evaluation, version 3.1R4, [CEM],
National and international interpretations	-
Scheme version	QMS 1.16.1 QMS 1.16 2014-02-13 QMS 1.15 2013-10-23 The changes have had no impact on the certification.
Certification completion date	2014-06-27

3 Security Policy

The security features within the scope of the ST when operated in the Firewall/VPN role are:

- Information Flow Control on the traffic that passes through the TOE. The TOE mediates the flow of all information that passes through its internal and external network connections to enforce the firewall security policy using:
  - Access rules based on the IP source address, destination address, transport layer protocol, application layer protocol, source port, destination port, and the interface on which the packet arrives; connection tracking; user authentication results; and the validity time.
  - Protocol Agents providing additional rules based on application-level information and mechanisms to redirect connections. The evaluation is limited to protocol agents for FTP, HTTP, and SMTP. All other protocol agents are not part of the evaluated configuration.
- Network Address Translation (NAT) between external IT entities that pass traffic through the TOE, ensuring that the IP addresses of hosts on internal networks are kept private from external users.
- Virtual Private Network: IPsec compliant VPN (tunnel mode only) using IKE for key establishment with certificate based authentication. SSL-based VPN connections are not included in the evaluated configuration.
- High Availability: In case of a total node failure, failure in one component or loss of connectivity to a network connected to a node, the firewall engine in a cluster is capable of failing over all sessions to other nodes. This provides continuous enforcement of the firewall security policy, including information flow control.

The security features within the scope of the ST when operated in the IPS role are:

- Deep packet inspection for the following protocols: Ethernet, IPv4, TCP, UDP, DNS, and HTTP
- Context-aware inspection, in which the inspection is protocol specific Fingerprinting

Both the Firewall/VPN and the IPS provides the following major security features:

- Audit generation: The TOE provides a means to generate audit records of security-relevant events relating to the IP traffic through the firewall and firewall security policy changes. The TOE also provides a means for the administrator to define the criteria used for the selection of the IP traffic events to be audited. It also provides a mechanism for preventing audit data loss.
- Security manageability and protection of security functions: Administrators access the TOE using certificate based authentication and protected communication between the Stonesoft Management Center (not part of the TOE) and TOE. The Stonesoft Management Center provides the interface for managing the security policy and authentication attributes, the TSF data, and security functions of the TOE. The TOE also ensures the trusted security functions are always invoked and cannot be bypassed.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes three assumption on the usage of the TOE:

A.ADMIN	It is assumed that the administrator only can access the TOE via the trusted Management Server on a trusted and separate management network and that the administrator has been identified and authenticated to the Stonesoft Management Center.
A.ADMINTRUST	It is assumed that administrators are trained, qualified, non-hostile and follow all guidance.
A.AUDITMAN	It is assumed that audit trails are regularly analyzed and archived.

4.2 Environmental Assumptions

Seven assumptions are made in the Security Target [ST] on the environment:

A.AUDITSUPP	It is assumed that the environment provides protected permanent storage of the audit trails generated by the TOE.
A.MEDIATSUPP	It is assumed that data cannot flow between the internal and external networks unless it passes through the TOE. In the cluster case (Firewall/VPN role only), traffic only needs to pass through one of the cluster nodes, which is just another instance of the TOE.
A.ENVIRON	It is assumed that the underlying hardware of the TOE node and the TOE's associated Management Servers and management and cluster networks are dedicated to the TOE usage, function according to their specifications, and are physically secure, only allowing administrators physical access.
A.TIME	It is assumed that the IT environment will provide a reliable time source to the TOE and the TOE environment.
A.USERAUTH {Firewall/VPN}	It is assumed that the IT environment will provide a user directory and a user authentication mechanism for the TOE to use when the firewall security policy requires users to authenticate before information can flow between the internal and external networks.
A.VPN {Firewall/VPN}	Peer external IT entities in trusted VPN channels must be able to protect the integrity and confidentiality of data transmitted to the TOE via encryption and provide authentication for such data. Upon receipt of data from the TOE, the peer external IT entity must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.
A.PLACEMENT {IPS}	The IPS must be placed in such a way to ensure adequate coverage of network segments where critical assets are located.

4.3 Clarification of Scope

The following Stonesoft Firewall/VPN & IPS Security Engine appliance models are included within the evaluation scope:

- Stonesoft MIL-320 (Firewall/VPN only)
- Stonesoft 5206

- Stonesoft 3206
- Stonesoft 3202
- Stonesoft 1402
- Stonesoft 1065
- Stonesoft 1035

Hardware and software components that are considered part of the TOE environment:

- TOE operating platform:
  - Intel Pentium 4 or higher (or equivalent) recommended,
  - 2 GB RAM or more recommended,
- Standard Linux Kernel 3.5.7 with Stonesoft specific modifications, Debian GNU/Linux 6.0 (squeeze) based distribution,
  - Network Interface Cards (see [ST]Annex D).
- Stonesoft Management Center, version 5.5:
  - the Management Server,
  - the Log Server,
  - the Management Client,
- OpenSSL 1.0.1 and 0.9.8,
- OpenSSH 5.5,
- OpenLDAP client and server, version 2.4,
- Architecture and System support:
  - at least 2 network interfaces,
  - 1 management network interface,
  - 1 cluster network interface (applicable only for Firewall/VPN),
  - a second TOE to form a cluster (applicable only for Firewall/VPN), and
  - a third TOE used as a Security Gateway for VPN functionality (applicable only for Firewall/VPN).

5 Architectural Information

The Target of Evaluation (TOE) is Stonesoft Firewall/VPN & IPS Security Engine, version 5.5.4.9869.cc.2.

In the evaluated configuration the TOE is provided and running as part of a Stonesoft appliance with hardware and underlying operating system consisting of

- a standard Intel Pentium 4 or higher based hardware platform with 2 GB or more RAM with four or more network interfaces, and
- a Debian GNU/Linux 6.0 based operating system including a Linux kernel 3.5.7 with Stonesoft specific modifications.

The Stonesoft Firewall/VPN & IPS Security Engine may be used either as a Firewall/VPN or as an IPS.

The Stonesoft Firewall/VPN & IPS Appliance product in IPS role is intended to be used for network traffic deep inspection and threat protection. The intended IPS deployment scenarios are (but not limited to) network perimeter, network core and internal network segments.

The Stonesoft Firewall/VPN & IPS Appliance is assumed to be installed and operated within a physically protected environment, administered by trusted and trained administrators over a trusted and separate management network.

Multiple installations of the Stonesoft Firewall/VPN & IPS Security Engine may be used in combination to obtain the functionality of both the Firewall/VPN or the IPS role.

The Stonesoft Firewall/VPN & IPS Security Engine runs on a hardened Linux operating system that is shipped with the product. The software runs on a single or multiprocessor Intel platform, which is also part of the Stonesoft Firewall/VPN & IPS Appliance product.

6 Documentation

The following user guidence are part of the TOE:

- Common Criteria Certification User's Guide, version SGCC_20140417
- Stonesoft Firewall/VPN Installation Guide, version SGFIG_20130624
- Stonesoft Firewall/VPN Reference Guide, version SGFRG_20131126
- Stonesoft IPS and Layer 2 Installation Guide, version SGIIG_20130618
- Stonesoft IPS and Layer 2 Reference Guide, version SGIRG_20130624
- Stonesoft Administrator's Guide, version SGAG_20131202

7 IT Product Testing

7.1 Test Configuration

Firewall/VPN evaluation testing environment includes two Stonesoft Firewall/VPN-role clusters with two nodes in each cluster. Additional hosts include SMC (Stonesoft Management Center) for controlling and configuring the security engine nodes and receiving log data, ATF (Automated Testing Framework) control host for executing automated tests and six hosts and two routers for miscellaneous functions depending on executed test. Additionally, evaluation test environment includes three Firewall/VPN single nodes each having two client/server host machines which run on ESX virtual machines.

IPS role test environment has six single security engines. Each are cabled so that recording replay machine can replay traffic capture recordings through them using one inline pair. Three hosts are on different sides (one left and two right) so that traffic between sides go through security engine inline pair and by changing used addresses (and VLAN) traffic can go through selected security engine.

7.1.1 Developer Testing

Testing Effort

The developer uses an automated test framework (ATF) for most of the test cases. It allows the execution of single or batches of test cases. The ATF controls local test networks that consists of various test clients (PCs), as well as all supported TOE hardware platforms.

The test cases are written in XML and instruct the ATF on

- how to configure the involved clients
- how to configure the TOEs that are to be tested
- which commands to perform on which device
- how to investigate for the expected results

Each test case consists of several test steps, which have unique identifiers. Each test step contains one specific task to perform, e.g., to configure an IP address on a specific device, or to perform a PING command from one device to another.

Approach

The testing approach of the developer was to demonstrate that all test cases ran successfully and that all ST claims, interfaces, and subsystems were verified by the tests. 101 test cases (including several test steps) were used for this task.

The ATF can be instructed on which TOE hardware platform to use for a specific test. All platforms run the same software binary; the developer tests therefore run a subset of the tests on each platform to cover all functionalities of the binary. The test cases also include testing of the clustering functionality (where applicable).

Configuration

The ATF environment contains two test networks, one for the Firewall/VPN role and one for IPS. Both contain all applicable hardware platforms. In summary, all supported TOE hardware platforms are included in the tests:

- Stonesoft MIL-320 (Firewall/VPN only)
- Stonesoft 1402

- Stonesoft 1035
- Stonesoft 1065
- Stonesoft 3202
- Stonesoft 3206
- Stonesoft 5206

This allows for automated testing of all hardware and role (Firewall/VPN and IPS) combinations, without the need for manual rewiring.

Each of the two test networks contains several sub-networks to perform various network tests such as NAT, VPN or clustering.

Results

The developer has provided the results of all test cases that were performed, as well as the associated low level log files from the ATF framework. All tests were successfull.

7.1.2 Evaluator Testing Effort

Test effort

The evaluator executed 56 developer test suites where each test suite is comprised of multiple subtests.

The evaluator further performed evaluator tests to verify the requirements of FCS_CKM.4 {Firewall/VPN}. This was done in form of a source code review, together with the developer and certifier. All relevant call trees in the code were inspected.

Test approach

The independent evaluator testing followed the CEM guidance to test every security function, without striving for exhaustive testing. For their own test, the evaluators determined that a source code audit is the most suitable approach.

The evaluators tested a sample of the supported hardware platforms, in single and cluster mode (sample). The test environment of the developer was used, including the proprietary Automated Testing Framework (ATF). The ATF allowed to perform most of the test automated, and produced detailed log files of the test results.

The evaluators also performed various manual tests. The actual execution was done by developer personnel, under close supervision of the evaluators and the certifier.

The evaluator also performed negative tests by manually modifying the ATF test cases. All such tests were found to behave as expected.

All security functionality defined in the ST has been tested.

Test configuration

The evaluators executed a sample of the developer test suites. The testing environment consisted of two networks, one for the Firewall/VPN role and one for IPS. The Firewall/VPN network contained two Firewall/VPN clusters, with two nodes in each cluster, as well as single devices. The IPS network contained multiple IPS devices. Additional hosts included SMC for controlling and configuring the Security Engine nodes and receiving log data, ATF control host for executing automated tests and multiple clients for miscellaneous functions depending on the executed test.

Test depth

The evaluators tested all security functions for appropriate coverage; since the evaluators already determined that the developer testing was sufficiently exercising all relevant subsystems, the evaluators did not need to exhaustively test all interfaces and subsystems. Especially, the evaluators did cover management functions mainly by using them. Their exposure to potentially malicious users is minimal (actually non-existent) when the system is operated in the evaluated configuration in an environment fulfilling the assumptions from the ST.

Test results

The subset of developer tests re-run by the evaluator performed successfully. All manual and automated evaluator tests were performed successfully - expected and actual results were consistent.

7.1.3 Evaluator Penetration Testing

Testing effort

The testing was performed on the external TOE network interfaces. The evaluator tested network traffic handling, filtering, routing and inspection. Security Management and logging was tested indirectly during testing, e.g., the evaluator edited firewall rules, configured interfaces and observed logging events. The cluster functionality was not tested during independent testing as only one firewall node was used.

Testing approach

The evaluator analysed the developer design and guidance documentation in order to identify the attack surface of the TOE. The evaluator came to the conclusion that the attack surface consists of the external network interface, i.e., data that are sent or received on these interfaces. The evaluator also used publicly documented vulnerabilities in CVE database and used general search engines. The analysis of potential attack surfaces was performed according to the ISO/OSI layer model, i.e., for Ethernet, IP, TCP etc.

Testing configuration

The TOE was installed on the 1035 and 1065 hardware models. The configuration was performed according to the provided documentation, starting with the acquisition of the software from the developer. The TOE was tested in the Firewall/VPN and IPS role (as applicable for the particular test).

Testing depth

The following areas were considered for vulnerability testing:

- Ethernet parsing
- IPv4 and IPv6 parsing
- IPv4 routing, with and without a VPN tunnel involved
- ICMPv4 and ICMPv6 parsing
- TCP parsing
- UDP parsing
- HTTP parsing and redirection
- FTP parsing and redirection
- SMTP parsing and redirection

- ARP parsing
- IPsec, IKEv1 and IKEv2 parsing
- IPsec traffic handling
- Discarding of "Loose Source and Record Route" and "Strict Source and Record Route" IP options.
- Protection of the administrative interface from external access
- Browser-based user authentication

In addtion, a TCP and UDP port scan of the external interface was performed to detect any further potential attack surfaces.

Testing results

The evaluator performed the penetration tests described above. None of the performed penetration tests revealed any exploitable vulnerability in the TOE.

8 Evaluated Configuration

In the evaluated configuration, the Stonesoft Firewall/VPN & IPS Security Engine may be operated in one of two roles (modes of operation), each providing a different set of security functionality. The Stonesoft Firewall/VPN & IPS Security Engine may be used either as a Firewall/VPN or as an IPS. Multiple installations of the Stonesoft Firewall/VPN & IPS Security Engine may be used in combination to obtain the functionality of both the Firewall/VPN or the IPS role.

Operated in the Firewall/VPN role it provides information flow control using multi-layer inspection (layer 3) including packet filtering, virtual private network connections (VPN) authenticating and encrypting data traffic to remote nodes over untrusted networks.

Operated in the IPS role it provides intrusion detection and prevention (IDS/IPS) using a range of different intrusion detection mechanisms including protocol decoding and normalization on all protocol layers. Connection state, protocol specific inspection modules and file contexts provide accurate signature matching context in the normalized data stream.

Independent of the role, the Stonesoft Firewall/VPN & IPS Security Engine is centrally managed and generates audit records for security critical events.

A distributed management system comprising a Management Server, Log Server and Graphical User Interface (GUI) to support the management and operation of the firewall is supplied as a separate product.

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 Security Target [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 of the evaluation 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
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
Derived security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Life-cycle support	ALC	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Flaw remediation	ALC_FLR.1	Pass
Development	ADV	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	AGD	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Tests	ATE	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	AVA	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

10 Evaluator Comments and Recommendations

The evaluators have no remaining comments, observations, or recommendations.

11 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation

12 Bibliography

[ST] McAfee NGFW and McAfee NGFW-IPS 5.5 Security Target, document version 2.0, 2014-05-27

[CCp1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1, revision 4, September 2012, CCMB-2012-09-001

[CCp2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version 3.1, revision 4, September 2012, CCMB-2012-09-002

[CCp3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, version 3.1, revision 4, September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, version 3.1, revision 4, September 2012, CCMB-2012-09-004

[SP-002] Evaluation and Certification, SP-002, Issue: 20.0, 2013-09-30, 13FMV7990-2:1, FMV/CSEC