122-B

CERTIFICATION REPORT No. CRP249

StoneGate Firewall/VPN
Version 4.2.2 Build 5708.cc3.1

running on the StoneGate appliance models FW-310, FW-1020, FW-1050, FW-1200, FW-5000 and FW-5100

Issue 1.0

March 2009

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.

Sponsor:	Stonesoft Corporation
Developer:	Stonesoft Corporation
Product and Version:	StoneGate Firewall/VPN Version 4.2.2 Build 5708.cc3.1
Platform:	StoneGate appliance models FW-310, FW-1020, FW-1050, FW-1200, FW-5000 and FW-5100
Description:	The Stonesoft StoneGate Firewall/VPN is a high-availability firewall and Virtual Private Network solution for securing data communication channels and enabling continuous network connectivity.
CC Part 2:	Extended with FAU_STG.NIAP-0414
CC Part 3:	Conformant
EAL:	EAL4 augmented by ALC_FLR.1
PP Conformance:	None
CLEF:	BT
CC Certificate:	CRP249
Date Certified:	13 March 2009

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOG-IS MRA logo which appears below:

- confirms that the certificate has been issued under the authority of a party to an international Mutual Recognition Agreement (MRA) [MRA] designed to ensure that security evaluations are performed to high and consistent standards;
- indicates that it is the claim of the evaluating party that its evaluation and certification processes meet all the conditions of the MRA.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo of this Agreement does not imply acceptance by other Members of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

Common Criteria

IT Security Certified

CCRA logo **CC logo** **SOG-IS MRA logo**

[1] All judgements contained in this Certification Report, are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

CERTIFICATION STATEMENT 2
TABLE OF CONTENTS 3
I. EXECUTIVE SUMMARY 4
Introduction 4
Evaluated Product and TOE Scope 4
Security Claims 4
Evaluation Conduct 5
Conclusions and Recommendations 5
Disclaimers 5
II. TOE SECURITY GUIDANCE 7
Introduction 7
Delivery 7
Installation and Guidance Documentation 7
III. EVALUATED CONFIGURATION 9
TOE Identification 9
TOE Documentation 9
TOE Scope 9
TOE Configuration 9
Environmental Requirements 10
Test Configuration 11
IV. PRODUCT ARCHITECTURE 14
Introduction 14
Product Description and Architecture 14
TOE Design Subsystems 15
TOE Dependencies 16
TOE Interfaces 16
V. TOE TESTING 19
TOE Testing 19
Vulnerability Analysis 20
Platform Issues 20
VI. REFERENCES 21

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of StoneGate Firewall/VPN Version 4.2.2 Build 5708.cc3.1 to the Sponsor, Stonesoft Corporation, as summarised on page 2 'Certification Statement' of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to ***CC EAL4 augmented by ALC_FLR.1*** on 04 March 2009:

> **StoneGate Firewall/VPN, Version 4.2.2, Build 5708.cc3.1, running on the StoneGate appliance models FW-310, FW-1020, FW-1050, FW-1200, FW-5000 and FW-5100.**

4. The Developer was Stonesoft Corporation.

5. The Stonesoft StoneGate Firewall/VPN is a high availability firewall and VPN solution for securing data communication channels and enabling continuous network connectivity.

6. The StoneGate Firewall/VPN is based on Multi-Layer inspection technology that combines both stateful and application-level inspection technology to control connectivity and information flow between internal and external networks.

7. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

8. An overview of the TOE and its product architecture can be found in Chapter IV 'Product Architecture' of this report. Configuration requirements are specified in Section 2 of [ST].

Security Claims

9. The Security Target [ST] fully specifies the TOE's Security Objectives, the threats and organisational security policies (OSPs) which these Objectives meet and the Security Functional Requirements (SFRs) that refine the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products. There is one SFR (FAU_STG.NIAP-0414) which is not taken from CC Part 2 [CC2] – see [ST] for more details.

10. The TOE security policies are detailed in the Security Target [ST]. The OSP that must be met is specified in [ST] Section 3.2.

11. The environmental assumptions related to the operating environment are detailed in Chapter III (in ‘Environmental Requirements’) of this report.

Evaluation Conduct

12. The Certification Body monitored the evaluation which was performed by the BT Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in March 2009, were reported in the Evaluation Technical Report [ETR].

Conclusions and Recommendations

13. The conclusions of the Certification Body are summarised on page 2 ‘Certification Statement’ of this report.

14. Prospective consumers of StoneGate Firewall/VPN Version 4.2.2 Build 5708.cc3.1 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

15. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II ‘Toe Security Guidance’ of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

Disclaimers

16. This report is only valid for the evaluated TOE. This is specified in Chapter III ‘Evaluated Configuration’ of this report.

17. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the Certification Body’s view at the time of certification.

18. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

19. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

20. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

II. TOE SECURITY GUIDANCE

Introduction

21. The following sections provide guidance that is of particular relevance to purchasers of the TOE.

Delivery

22. On receipt of the TOE hardware, the consumer is recommended to check that instructions for installing and configuring the evaluated version have been supplied, and to check that the security of the TOE hardware has not been compromised during delivery.

23. TOE consumers should download the Common Criteria Certification User's Guide [CCCUG] and the following guidance from the www.stonesoft.com website:

a. StoneGate Installation Guide – SMC 4.2 and Firewall/VPN 4.2 [IG]

b. StoneGate Administrator's Guide – SMC 4.2, Firewall/VPN 4.2 and IPS 4.2 [AG]

c. StoneGate Reference Guide – SMC 4.2 and Firewall/VPN 4.2 [RG]

24. TOE consumers must download the TOE software from Stonesoft's website at www.stonesoft.com, as detailed in the Common Criteria Certification User's Guide [CCCUG]. All administration guidance for the TOE is available on the website. A consumer is required to authenticate, using information sent to them when they placed their order, before they can access the secure area of the website and download the TOE.

25. Once consumers have downloaded the TOE, they are required to validate the MD5 and SHA-1 checksum, which are provided on the www.stonesoft.com website.

Installation and Guidance Documentation

26. The Installation and Secure Configuration documentation is as follows:

- [IG]
- [CCCUG]

27. The User Guide and Administration Guide documentation is as follows:

- [RG]
- [AG]
- [CCCUG]

28. The Common Criteria Certification User's Guide [CCCUG] describes the procedures that must be followed to install and configure the product in its evaluated configuration, and to operate it securely. It also describes the procedures that must be followed to configure the environment. Hence it is recommended that these procedures are read first.

29. The intended audience of the installation and guidance documents is the administrator.

III. EVALUATED CONFIGURATION

TOE Identification

30. The TOE is StoneGate Firewall/VPN Version 4.2.2 Build 5708.cc3.1, which consists of the firewall/VPN engine software application, Version 4.2.2 Build 5708.cc3.1 including the SafeNet QuickSec cryptographic toolkit Version 4.1[2].

TOE Documentation

31. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report.

TOE Scope

32. The TOE Scope is defined in the Security Target [ST] Section 2. Functionality that is outside the TOE Scope is defined in [ST] Section 2.3.

33. The evaluation was constrained by the functionality available in StoneGate Firewall/VPN Version 4.2.2 Build 5708.cc3.1 identified as outside the scope of the evaluation in section 2.3 of [ST]. Software and hardware features outside the scope of the defined TOE Security Functions and thus not evaluated are:

a. StoneGate Management Server, Version 4.2

b. StoneGate Log Server, Version 4.2

c. OpenSSL 0.9.8 and OpenSSH (used on the Firewall/VPN engine and Management Server)

d. OpenLDAP client and server, Version 2.3 (used on the Firewall/VPN engine and Management Server).

TOE Configuration

34. The evaluated configuration of the TOE is defined in [ST] Section 2.

35. The evaluated TOE configuration comprises any of the following StoneGate appliance hardware platforms running StoneGate Firewall/VPN Version 4.2.2 Build 5708.cc3.1:

FW-310	FW-1020	FW-1050
FW-1200	FW-5000	FW-5100

[2] An assumption is made that the Cryptographic Module within the TOE is FIPS PUB 140-2 [FIPS 140-2] Level 1 validated.

Environmental Requirements

36. The environmental assumptions for the TOE are stated in [ST] Section 3.1.

37. The TOE was evaluated running on the hardware platforms detailed in paragraph 35 above.

38. The evaluated configuration (as detailed in section 2.3 of [ST]) is shown in Figure 1 below and consists of:

a. at least 2 network interfaces

b. 1 cluster network interface

c. 1 management network interface

d. a second TOE to form a cluster

e. a third TOE used as a security gateway for VPN functionality.

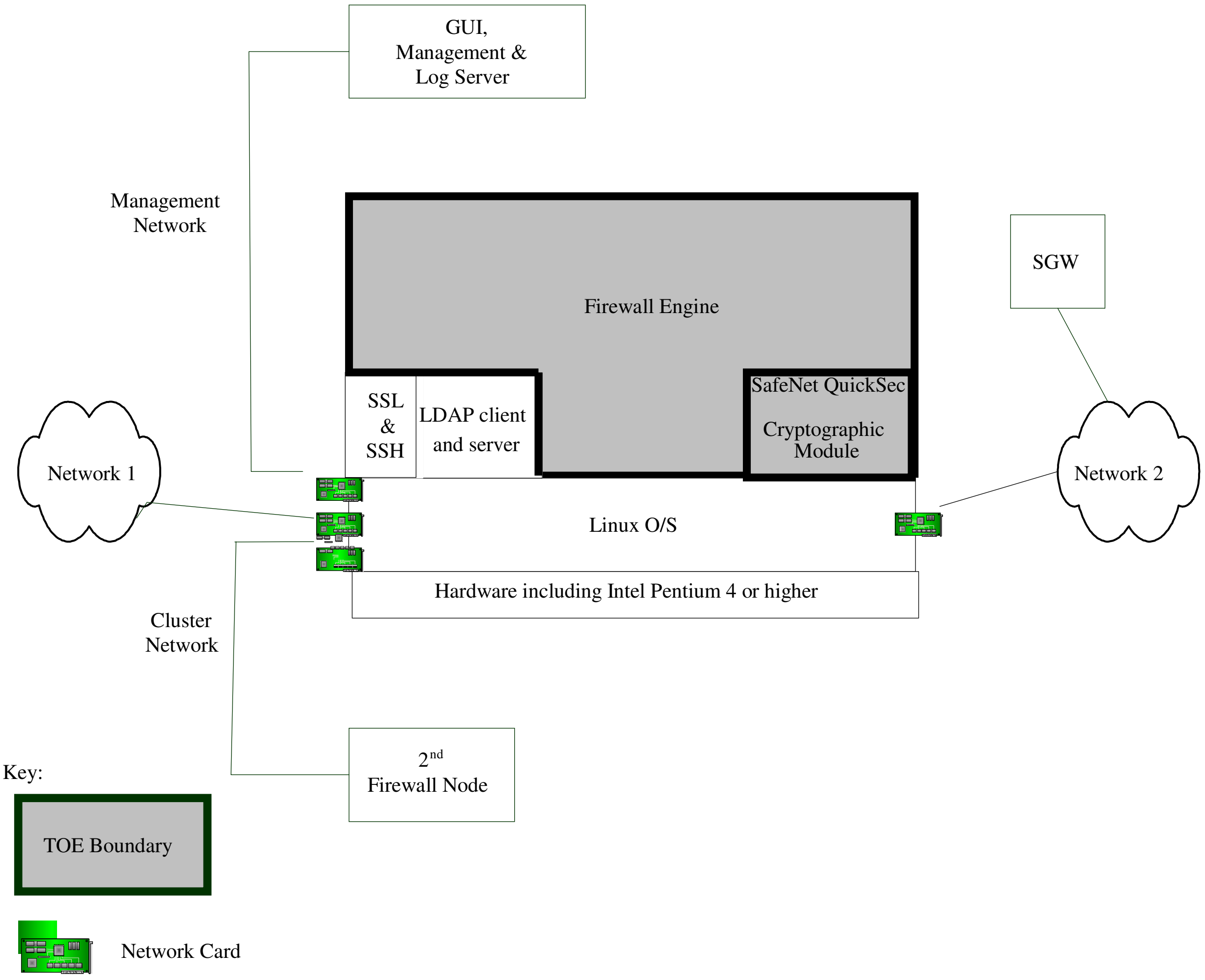

Figure 1 - TOE Configuration

Test Configuration

39. The environmental configuration used by the developer to test the TOE is summarised in Figure 2, supported by the table below which gives more information (such as description, operating system and memory) about the network components (named in bold text). The Evaluators used a subset of this network as detailed in Figure 3.

atf_cc-1 StoneGate Firewall FW-5100	**atf-cc-host-4** O/S Linux CentOS 5 RAM 4 GB
atf_cc-2 StoneGate Firewall FW-5000	**atf-cc-host-5** O/S Linux CentOS 5 RAM 4 GB
atf_tampere StoneGate Firewall FW-1020	**atf-cc-control** O/S Linux CentOS 5 RAM 4 GB
atf_turku StoneGate Firewall FW-1200	**atf-cc-smc** O/S Linux CentOS 5 RAM 4 GB
atf-cc-host-0 O/S Linux CentOS 5 RAM 4 GB	**atf-cc-kvm** KVM Switch Dell PowerEdge 2161DS-2
atf-cc-host-1 O/S Linux CentOS 5 RAM 4 GB	**GUI Client** O/S Linux CentOS 5 RAM 512 MB
atf-cc-host-2 O/S Linux CentOS 5 RAM 4 GB	**Dell 6248 Switch/Router** Dell PowerConnect 6248
atf-cc-host-3 O/S Linux CentOS 5 RAM 4 GB	**atf-router-6** O/S Linux CentOS 5 RAM 4 GB

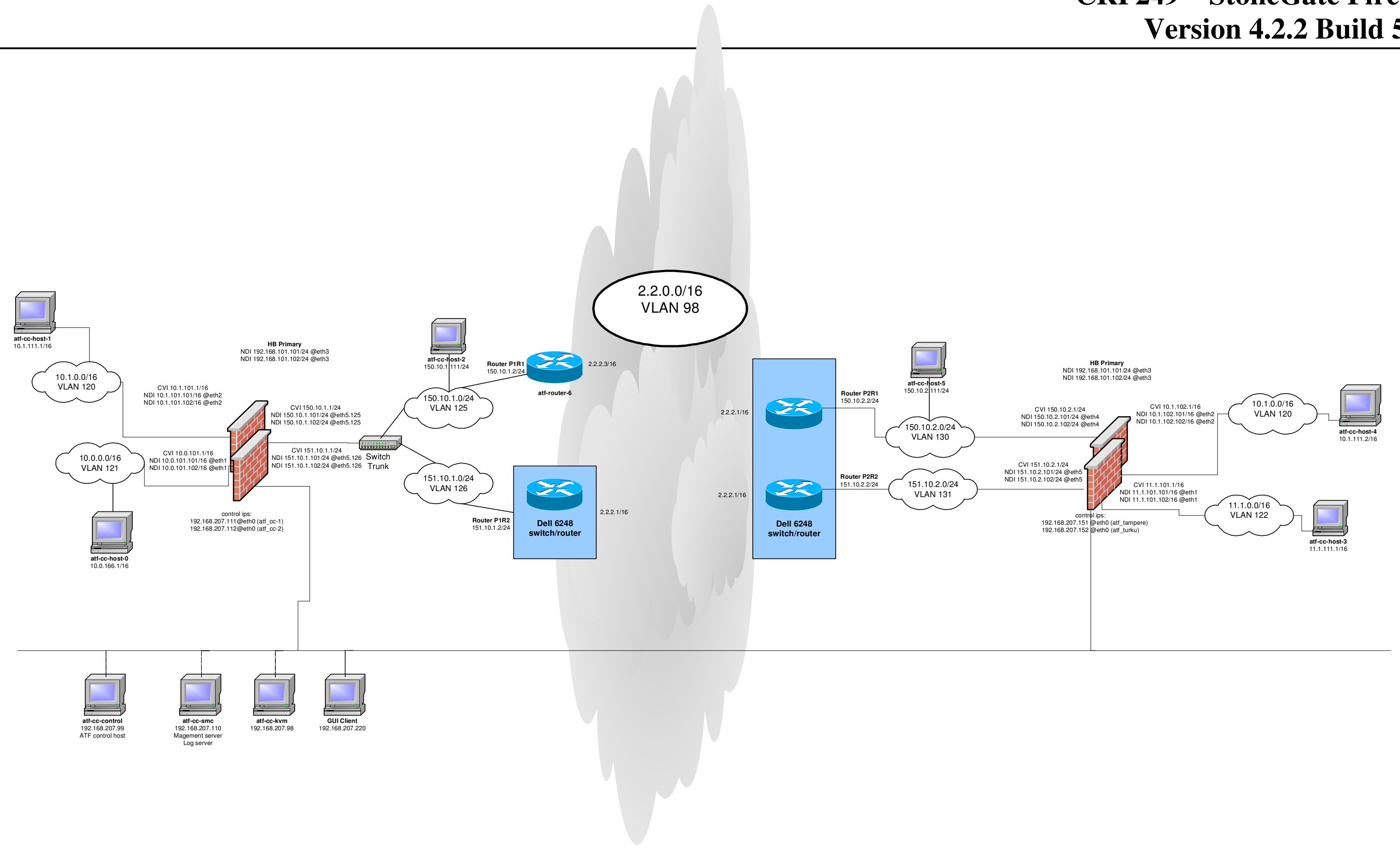

Figure 2 - Developer Test Network

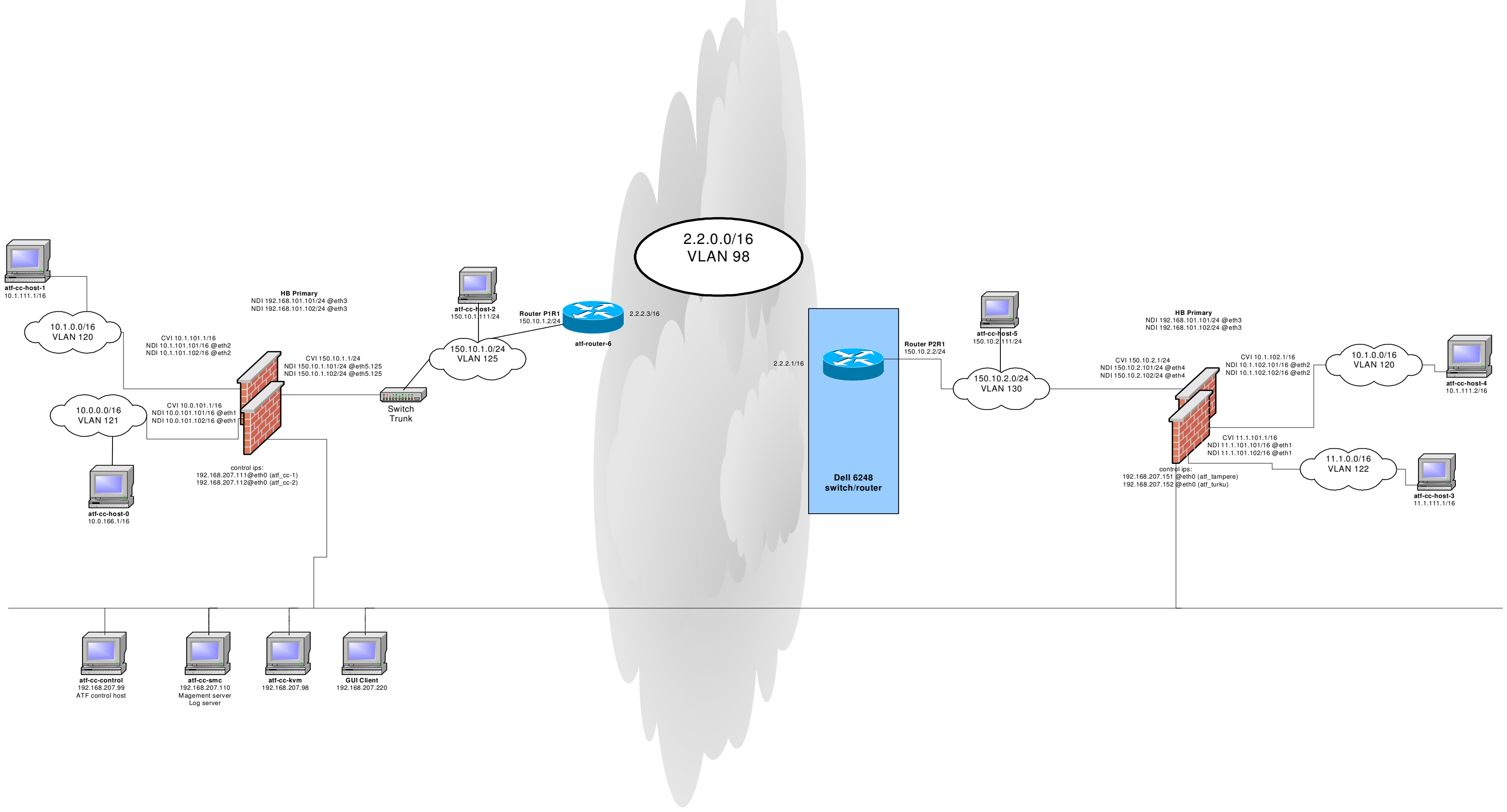

Figure 3 Evaluators Test Network

IV. PRODUCT ARCHITECTURE

Introduction

40. This Chapter gives an overview of the main TOE architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

Product Description and Architecture

41. The StoneGate Firewall/VPN is the firewall component of the StoneGate product. The StoneGate product comprises a firewall engine, its operating system and data repository platform, cryptographic modules and management system software. The firewall engine and its cryptographic module are included in the scope of the TOE. The management system and operating platforms are outside of the scope of the evaluation. See Figure 1 for more details.

42. The TOE can operate as a single firewall or as part of a cluster. In cases of 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 and VPN services. Figure 4 shows the TOE as a cluster in a network environment:

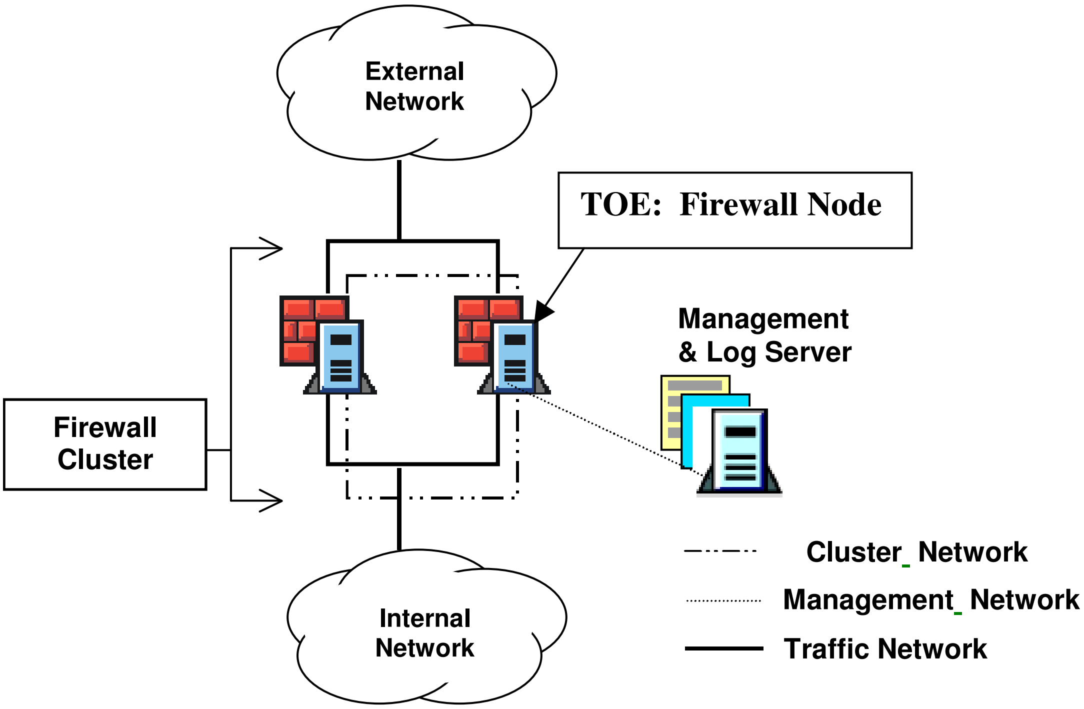

Figure 4 – TOE Operating Environment

43. The TOE performs Information Flow Control on all traffic that passes through it. The TOE mediates the flow of all information to enforce the firewall security policy using:

a. Access rules based on the source address, destination address, transport layer protocol, application layer protocol, source port, destination port, the interface on which the packet arrives, connection tracking, user authentication results and the validity of time.

b. VPN matching rules to decide whether to accept or discard encrypted and unencrypted connections.

44. Protocol Agents provide additional rules which are based on application-level information and mechanisms. While the firewall engine supports many protocol agents the evaluation is limited to protocol agents for FTP, HTTP and SMTP.

45. The TOE also provides VPN network security services based on the IPSec protocol. This includes certificate-based authentication and data confidentiality and integrity protection using (see Footnote 2 on Page 9) a FIPS PUB 140-2 [FIPS 140-2]certified cryptographic module.

46. The TOE performs 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.

47. The TOE provides a means to generate audit records of security-related events relating to the IP traffic through the firewall and firewall security policy changes.

TOE Design Subsystems

48. The TOE subsystems, and their security features/functionality, are as follows:

a. Logging and Monitoring Subsystem. This subsystem receives log and monitoring data from other subsystems and generates audit records from this data.

b. General Subsystem. This subsystem is a collection of utilities which ensure that the system is started up and shut down in a secure manner.

c. Basic Firewall Functionality Subsystem. This subsystem handles all incoming packets that are processed by the TOE. It receives a packet from the operating system, processes it by communication with other subsystems and then routes the packet to the correct interface.

d. Authentication Subsystem. This subsystem is responsible for managing connections that require user authentication.

e. Protocol Agents Subsystem. This subsystem provides packet filtering based on application-level content. If an FTP, HTTP or SMTP packet is received, the Basic Firewall Functionality subsystem routes this packet to the Protocol Agents Subsystem which inspects the protocol data and enforces the relevant protocol standards.

f. Blacklisting Subsystem. This subsystem allows the StoneGate Management System to terminate or block connections for a period of time based on IP addresses and, optionally, protocol ports.

g. VPN Subsystem. The VPN subsystem is responsible for managing VPN tunnels which provide for secure communication between the TOE and another trusted IT product.

h. Configuration Subsystem. This subsystem allows an administrator to change the behaviour of the TOE. The Configuration Subsystem is called each time changes made by an administrator are required to be enabled.

i. Clustering Subsystem. This subsystem improves performance and provides high-availability within the TOE by distributing the load around a number of nodes.

j. StoneGate Common Subsystem. This subsystem contains the Sendlog Daemon which is used by the Log Sending Module to read data from the Log Spool files and send it to an external Log Server.

k. Management Communications Subsystem. This subsystem consists of a set of modules that enable secure communication between the Firewall Engine and the Management Server.

l. Installation Subsystem. This subsystem enforces a restrictive default security policy allowing only management and administrative connections.

TOE Dependencies

49. The TOE dependencies are as follows:

a. The administrator must access the TOE via the trusted management server on a trusted and separate management network.

b. The IT environment shall provide protected permanent storage of the audit trails generated by the TOE.

c. The operating system and hardware platform on which the TOE operates are physically secure allowing physical access only to administrators.

d. The IT environment must provide 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.

TOE Interfaces

50. The external TOE Security Functions Interface (TSFI) is described as follows:

a. Configuration Interface. The audit configuration for the TSF is constructed on the Management Server and transferred to the TSF through the Configuration Interface.

b. Management Communications Interface. The administrator configures the Log Spool policy through the Management Server. This information is then passed to the TSF via the Management Communications Interface.

c. Unified Log and Alert Server (ULAS). Audit Data is sent from the TOE to an external Log Server using the proprietary ULAS interface.

d. IP Security (IPSec) Protocol. The TOE uses its cryptographic functionality to establish IPSec VPN connections.

e. Internet Key Exchange (IKE). VPN tunnels are created using the IKE protocol.

f. IP Packet Interface. The IP packet interface binds the packet flow of the Linux operating system and the packet flow of the TOE.

g. IP Datagram Interface. The TSF sends and receives standard IPv4 datagrams using this interface.

h. Transmission Control Protocol (TCP) Connection Interface. This interface maintains details of the presumed address and port of a connection as well as the transport layer protocol and service associated with the connection.

i. Unreliable Datagram Protocol (UDP) Datagram Interface. This interface maintains details of the source address, destination address and port for UDP connections.

j. Internet Control Message Protocol (ICMP) Message Interface. This interface inspects ICMP messages received.

k. File Transfer Protocol (FTP) Interface. This interface inspects FTP packets that are received.

l. Hypertext Transfer Protocol (HTTP) Interface. This interface inspects HTTP packets that are received.

m. Simple Mail Transfer Protocol (SMTP) Interface. This interface inspects SMTP packets that are received.

n. User Authentication Communications Interface. This interface is used when communicating with a client if a connection requires authentication.

o. Address Resolution Protocol (ARP) Interface. This interface is used to resolve network-layer addresses to hardware addresses.

p. Blacklisting Interface. This interface allows administrators to add Blacklist entries as part of the configuration of the TSF.

q. Initial Configuration Interface. This interface is required to supply the TSF with the necessary information for establishing a secure connection with the Management Server.

r. Configuration Import Interface. This interface allows an administrator to import a configuration from a floppy disk or USB key.

s. Cluster Protocol Interface. This interface provides a reliable way to distribute load balancing information and status information between firewalls in a cluster.

t. State Synchronisation Interface. This interface is used to synchronise the hash values that are used for load balancing between nodes in a cluster.

u. Data Synchronisation Interface. This interface is used to synchronise the certificates used in VPN tunnels between nodes in a cluster.

v. Key Exchange Interface. This interface is used for distributing keys that are used to encrypt and decrypt communications between clustered firewalls.

V. TOE TESTING

TOE Testing

51. During their on-site testing, the Evaluators used the Common Criteria Certification User's Guide [CCCUG] in order to check that the TOE was installed and configured in a secure manner.

52. The environmental configuration used by the Evaluators to test the TOE was equivalent to that used by the developers to test the TOE, as summarised in 'Test Configuration' above.

53. The Developer's tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;
- the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

54. The Developer's tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly.

55. The Developer tested on all platforms within the scope of the evaluation (StoneGate appliance models FW-310, FW-1020, FW-1050, FW-1200, FW-5000 and FW-5100) using the developer test network detailed in Figure 2 of this report.

56. Most developer tests were automated and driven through a set of scripts. In addition some manual tests were performed.

57. The Evaluators performed a sample of the Developer's tests in order to validate the developer's testing. Both automated and manual test samples were repeated.

58. The Evaluators devised and ran a total of 7 independent functional tests, different from those performed by the Developer. No anomalies were found.

59. The Evaluators also devised and ran a total of 11 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

60. The Evaluators used the following tools in order to perform the functional and penetration tests:

a.	Nmap	Version 4.6
b.	Wireshark	Version 0.99.4-3
c.	Sing	Version 1.1

d.	Packit	Version 1.0
e.	Fuzzball 2	Version 0.7

61. The Evaluators performed their functional and penetration tests on the FW-5000 platform using the evaluation network detailed in Figure 3 of this report.

62. The Evaluators finished running their penetration tests on 13 February 2009.

Vulnerability Analysis

63. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables, in particular the developer's vulnerability analysis.

Platform Issues

64. 'TOE Configuration' in Chapter III lists the hardware platforms that are within the scope of the evaluation.

65. Developer tests were performed across all hardware platforms. Exactly the same results were generated on all platforms and no parts of the TSF were identified that behaved differently on different hardware platforms. The Evaluators performed their testing on the FW-5000 platform.

VI. REFERENCES

[AG] StoneGate Administrator's Guide - SMC 4.2, Firewall/VPN 4.2 and IPS 4.2,
Stonesoft Corporation,
SGAG_20080123, Issue 4.2, January 2008.

[CC] Common Criteria for Information Technology Security Evaluation
(comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2006-09-001, Version 3.1 R1, September 2006.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2007-09-002, Version 3.1 R2, September 2007.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2007-09-003, Version 3.1 R2, September 2007.

[CCCUG] Common Criteria Certification User's Guide,
StoneGate Management Center 4.2 and Firewall/VPN 4.2,
SGCG_20090123, Version 4.2, January 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
May 2000.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2007-09-004, Version 3.1 R2, September 2007.

[ETR] Evaluation Technical Report,
BT CLEF,
LFS/T536/ETR, Issue 1.0, March 2009.

[FIPS 140-2] Federal Information Processing Standard Publication,
Security Requirements for Cryptographic Modules,
National Institute of Standards and Technology,
FIPS-PUB 140-2, May 25, 2001.

[IG] StoneGate Installation Guide – SMC 4.2 and Firewall/VPN 4.2,
Stonesoft Corporation,
SGIG_20080108, Issue 4.2, January 2008.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee of Agreement Group,
Senior Officials Group – Information Systems Security,
Version 2.0, April 1999.

[RG] StoneGate Reference Guide - SMC 4.2 and Firewall/VPN 4.2,
Stonesoft Corporation,
SGRG_20071119, Issue 4.2, November 2007.

[ST] StoneGate Firewall/VPN Version 4.2.2 Build 5708.cc3.1 Security Target,
Stonesoft Corporation,
Issue 1.0, February 2009.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.5, October 2008.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.2, October 2008.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.1, October 2008.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.3, October 2008.