National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Stonesoft Corporation

StoneGate Firewall, Version 2.0.5

Report Number: CCEVS-VR-03-0043

Dated: 17 September 2003

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

James Brosey
MITRETeK Corporation
Falls Church, Virginia

Alton Lewis
National Security Agency
Linthicum, Maryland

Common Criteria Testing Laboratory

CygnaCom Solutions
McLean, Virginia 22102-3350

Table of Contents

Table of Figures

1 EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of Stonesoft StoneGate Firewall, Version 2.0.5 at EAL4 augmented with ALC_FLR.1. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by CygnaCom Solutions, McLean Virginia, and was completed 17 September 2003. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by CygnaCom and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.1, Part 2 extended and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.1, Basic flaw remediation, resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The Stonesoft StoneGate Firewall is a high availability firewall and Virtual Private Network (VPN) solution for securing data communication channels and enabling continuous network connectivity. The validated product is the StoneGate Firewall engine and VPN software application component of StoneGate.

The StoneGate Firewall is based on Mutli-Layer Inspection technology that combines both stateful and application-level inspection technology to control connectivity and information flow between internal and external networks. It provides Network Address Translation (NAT) to keep internal network addresses private. The VPN security services are based on the IPSec standard and allow users multiple cryptographic support options. As part of a firewall cluster, the StoneGate Firewall provides a high availability feature so that component firewall failures degrade the cluster to a fully functional and secure state.

The **TOE** is the StoneGate Firewall engine and VPN software application component of the StoneGate Firewall version 2.0.5, which includes the SSHToolkit Cryptographic module components, version 4.1.1. The TOE is one component of the StoneGate product (the firewall engine) and consists of the engine and the cryptographic module components only.

The StoneGate product also includes the operating system and data repository platform supporting the TOE and the management system software for configuring and monitoring the TOE. The operating system supporting the TOE is a hardened version of Debian GNU/Linux. The management system consists of a management server, a log server, and GUI client for administering the TOE via the two servers. These additional StoneGate components were not within the scope of the Firewall engine evaluation.

The evaluated security features include:

- Connection-level information flow control for IP packets, including network-through-application-level packet filtering and connection redirection for FTP, HTTP, and SMTP traffic;
- VPN data protection;
- Privacy for host IP addresses on the internal network using static NAT;
- High Availability support for network security services;
- Audit generation and
- Management and protection functions to support the security services.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- the Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated,
- the Security Target (ST), describing the security features, claims, and assurances of the product,
- the conformance result of the evaluation,
- the organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Evaluation Identifiers for Stonesoft's StoneGate Firewall, Version 2.0.5	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Stonesoft StoneGate Firewall, Version 2.0.5
Protection Profile	N/A
Security Target	Stonesoft StoneGate Firewall, Version 2.0.5, Common Criteria Security Target, Version 3.13, dated 07 August 2003
Evaluation Technical Report	Evaluation Technical Report (ETR) for a Target of Evaluation, Stonesoft StoneGate Firewall, Version 2.0.5, Proprietary ETR, Version 1.1 AVA_VLA.2,

Evaluation Identifiers for Stonesoft’s StoneGate Firewall, Version 2.0.5	
	dated 17 September 2003 [9]
Conformance Result	Part 2 extended, Part 3 conformant, and EAL4 augmented with ALC_FLR.1, Basic flaw remediation
Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable NIAP CCEVS and International Interpretations effective on March 27, 2002
Version of CEM	CEM Version 1.0 [5], [6], Supplement: ALC_FLR - Flaw Remediation [11], and all applicable NIAP CCEVS and International Interpretations effective on March 27, 2002
Sponsor	Stonesoft Corporation Itälahdenkatu 22 A FIN-00210 Helsinki, Finland
Developer	Stonesoft Corporation Itälahdenkatu 22 A FIN-00210 Helsinki, Finland
Evaluator(s)	**CygnaCom Solutions** Gary Grainger Debra Baker Peter Kukura Kris Rogers
Validator(s)	**NIAP CCEVS** James Brosey Alton Lewis Dr. Jerome Myers

3 Security Policy

The Stonesoft StoneGate Firewall is a firewall and Virtual Private Network (VPN) solution for securing data communication channels and enabling continuous network connectivity.

The StoneGate Firewall 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. It also provides a means to keep the internal hosts IP-address private from external users. The VPN security services are based on the IPSec standard and allow users multiple cryptographic support options. As part of a cluster, the StoneGate Firewall 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. Figure 1: Typical Network Configuration for TOE illustrates a typical configuration of the StoneGate Firewall in a two node cluster.

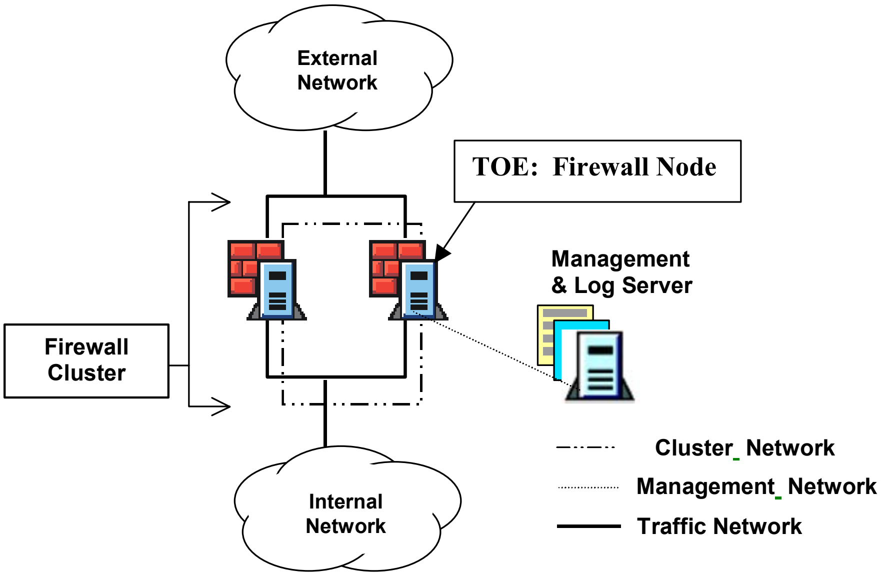

Figure 1: Typical Network Configuration for TOE

The security features within the scope of the ST include:

- Connection level information flow control for IP packets including network-through-application level packet filtering, and connection redirection for FTP, HTTP, and SMTP traffic.
- VPN data protection;
- Privacy for hosts IP-address on the internal network using static Network Address Translation (NAT);
- High Availability for network security services;

- Audit generation; and Management and protection functions to support the security services.

The StoneGate Firewall and VPN support the enforcement of nine security policies that are described in this section.

3.1 Information Flow Control Policy

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 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.
- VPN matching rules to decide whether to accept or discard encrypted and unencrypted connections.
- Protocol Agents providing additional rules based on application level information and mechanisms to redirect connections. While the firewall engine supports many protocol agents, the evaluation is limited to protocol agents for FTP, HTTP, and SMTP.
- Network Address Translation (NAT) between external IT entities that pass traffic through the TOE, ensuring the IP-addresses of hosts on internal networks are kept private from external users.

3.2 Identification and Authentication Policy

Identification and authentication of remote peer (security gateway) is started always when StoneGate engine receives a packet that matches a rule requiring VPN connection or remote peer proposes a VPN connection to the TOE. Mechanisms used for authentication are listed in the ST. The mechanism to be chosen for each specific connection is decided based on StoneGate engine configuration.

3.3 Encryption/VPN Policy

The TOE provides VPN network security services based on the IPSec protocol. This includes certificate-based authentication and data confidentiality and integrity protection using its FIPS PUB 140-2 certified cryptographic module described below. IPSec manual key exchange is an available configuration option but is not included in the evaluation.

- **I&A to support VPN:** The TOE includes authentication mechanisms for SGWs to establish VPN connections. SGWs can authenticate with the Internet Key Exchange (IKE) to establish a VPN connection using a certificate-based mechanism using RSA, or using pre-shared key.

- **Crypto Functions supporting the VPN:** The TOE includes a FIPS PUB140-2 certified cryptographic module to provide the following cryptographic operations and key management services:
  - Cryptographic Operations:
    - 3DES encryption/decryption
    - AES encryption/decryption
    - RSA signature/verification
    - SHA-1 Secure Hash
    - HMAC-SHA-1 Keyed-Hash Message Authentication Code
    - Diffie-Hellman Key Exchange
  - Cryptographic Key Management:
    - Key generation of symmetric 3DES and AES keys
    - Key generation of RSA keys;
    - Cryptographic Key Destruction by zeroization.

3.4 Audit/Logging Policy

The audit policy mandates that the TOE:

- Provide a means to generate audit records of security-relevant events relating to the IP traffic through the firewall and firewall security policy changes,
- Allow only authorized administrator to define the criteria used for the selection of events to be audited, include or exclude auditable events from the set of audited events based on specified attributes,
- Recognize and creates an audit record resulting from a change of management functions,
- Recognize malformed or unrecognizable security policies for the firewall engine, and
- Provide mechanisms to prevent audit data loss such as loss of audit records due to audit storage failure.

The Audit policy also mandates that all audit records include the following attributes: date and time of the event, type of event, subject identity (if applicable), event outcome, and other event-specific data.

When the TOE receives a new firewall security policy, it generates an audit record identifying the date, time, and configuration identification.

Firewall Information Flow Control policy forces all packets to be processed by configured security policy rules. Audit of security relevant events is defined with same configurable rules.

3.5 Log Spooling Policy

The Log Spooling Policy, defined by an authorized administrator, specifies the behavior of the TOE whenever its local log spool is filled.

TOE audit entries are first stored on cache buffers on each node and then forwarded to a log server. When new log information is received, the log server stores it as database files. An audit entry is removed from cache buffers after the TOE has received confirmation from log server that the entry has been successfully stored.

The policy mandates that the TOE provide a means for the management server to prioritize log data. The firewall engine stops producing designated log entries before applying the selected log spooling policy.

3.6 TOE Security Functions Protection Policy

When the physical environment of the TOE is secure, the only way to access TOE is to send packets to it. StoneGate engine captures and handles all packets received from OS and all packets are handled based on rules in the rulebase. StoneGate is started up and shut down in a manner that ensures that packets do not bypass the rules of rulebase.

3.7 High Availability/Fault Tolerance Policy

The StoneGate Firewall can operate as a single firewall or as part of a firewall cluster consisting of 2-16 firewall nodes. The firewall cluster is required for high availability of security services. Each node has internal and external network connections for which it provides its security services, and separate management networks for connectivity to the management system and the other nodes in a cluster, i.e., management network and cluster network, respectively. In the event of hardware malfunction, packets will not be passed through a failed node. Other nodes of the cluster will process packets destined to the cluster after failure of one node. In the event of network failures StoneGate engine continues to operate according to configured rules (security policy). If applying a new security policy fails, StoneGate engine continues to operate according to previously successfully installed security policy.

3.8 Communication Policy

StoneGate engine communicates with remote security gateway through encrypted communication channels, VPN tunnels. Either the engine or a remote peer can initiate the process to establish a VPN. The IKE protocol is used in negotiation and the parameters must follow configured policy of StoneGate engine. User data is protected from unauthorized disclosure by encryption, decryption and authentication of it using ESP protocol of the IPSec protocol suite.

3.9 Management Policy

Ability to modify the security attributes is restricted only to the management server. Initial default values are restrictive and only values that follow configuration syntax are allowed.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The evaluation made the following assumption concerning product usage:

Administrators access the TOE via the trusted management server on a trusted and separate management network. Administrators identify and authenticate to the management server application.

Authorized administrators are trained, qualified, non-hostile and follow all guidance.

Procedures exist to ensure the audit trails are regularly analyzed and archived.

The IT environment will:

- Generate audit records for the security functions on which the TOE depends on from its environment.
- Provide protected permanent storage of the audit trails generated by the TOE, and provide reliable timestamps for the audit records.
- Ensure that information cannot flow among the internal and external networks unless it passes through the TOE, and it must provide residual information protection for those packets.
- Provide secure storage of and access to the network security policy and user authentication data, and it must provide a reliable timestamp to support time-based information flow control decisions.
- Protect itself against attempts by unauthorized user to bypass, deactivate, or tamper with its security functions.
- 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

The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

The TOE (firewall engine), its associated management servers and the management networks are dedicated to the trusted firewall system, function according to their specifications, and are physically secure, only allowing trusted administrators physical access.

The key used for Shared Secret SGW authentication will be generated and entered in the TOE in accordance with organization security policies and follow the guidance provided in the Administrator and User Guides. The key size will be greater than or equal to 10 bytes.

The destruction of the key will be in accordance with the organization security policies and follow the guidance provided in the Administrator and User Guides.

4.2 Clarification of Scope

The StoneGate Firewall that a customer would purchase includes more than the just the evaluated TOE. The additional components of the product are treated in this evaluation as part of the IT Environment. Some requirements were placed upon the configuration of the IT Environment to support the analysis and conclusions reached by this evaluation. The general StoneGate Firewall product supports configurations that are outside the scope of this evaluation. This section highlights some of the restrictions upon the product configuration and the implications of some product components not being within the scope of the evaluation.

Important architectural components of the overall StoneGate product that are considered to be part of the IT Environment include the base platform (hardware and operating system) for the StoneGate Firewall, and the management and logging servers with their associated platforms.

The analysis of the TOE was based upon a requirement that general network users could not gain physical or logical access to certain network interfaces to the TOE. A typical configuration of the TOE is shown in Figure 1: Typical Network Configuration for TOE. There are four separate networks shown in that figure: the internal network, the external network, the management network, and the firewall engine cluster (Heartbeat) network. The general architecture of the StoneGate product has unevaluated support for encrypted separation of the management and heartbeat networks from the internal and external networks rather than requiring physical separation of the four networks. The evaluated configuration requires that the four networks be physically separated. As a result, the evaluated configuration of the TOE cannot be easily used with distributed network management. Rather it is anticipated that the TOE will be used in configurations where multiple nodes of a cluster and the management workstations are in close physical proximity so the management network and the heartbeat network can be isolated and physically protected. This is not necessarily a limitation upon the capabilities of the product, but rather it is a statement of the limitations on the scope of the analysis that was performed for this evaluation.

StoneGate supports DSS signature authentication. However, the implementation of DSS signature authentication is not compatible with the "FIPS mode", and hence, is not available in the evaluated configuration.

5 Architectural Information

Stonesoft StoneGate is a high availability firewall and Virtual Private Network (VPN) solution for securing data communication channels and enabling continuous network connectivity. The validated product is the StoneGate Firewall engine and VPN software application component of StoneGate.

The StoneGate Firewall engine 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. It provides Network Address Translation (NAT) to keep internal network addresses private. The VPN security services are based on the IPSec standard and allow users multiple cryptographic support options. As part of a firewall cluster, the StoneGate Firewall engine provides a high availability feature, so that component firewall failures degrade the cluster to a fully functional and secure state.

The StoneGate Firewall engine runs on a hardened Linux operating system that is integrated with the engine. StoneGate includes a distributed management system comprising a management server, a log server and a graphical management client for administering the engine via the two servers.

Security features of the StoneGate Firewall engine include:

- Information flow control
  - Stateful information flow control for IP packets
  - Filtering on network level through application level information
  - Connection redirection for FTP, HTTP, and SMTP traffic
- VPN
  - Confidentiality and integrity of information exchanged with security gateways
  - IPSec-based authentication of security gateways
  - FIPS 140-2 certified cryptographic functions
- Static NAT to protect internal network addresses from disclosure
- High Availability for engine security services through support of firewall clustering
- Auditing
- Management and protection of engine security functions.

5.1 Subsystems

The high level design of the StoneGate Engine decomposes the TOE into eleven subsystems. The specific allocation of TOE functionality to the subsystems is considered to be proprietary to Stonesoft. Hence, further details of the system architecture are not described in this document.

6 Delivery and Documentation

The TOE hardware and software for the TOE may be separately acquired. The TOE software is bundled with the TOE documentation and is distributed as the "Media Kit". The Media Kit includes hardcopy documentation, installation CDs, and softcopy documentation on CDs. The underlying operating system for the TOE is included in the StoneGate Firewall product and hence is included in the software distribution. The ST provides further details on the TOE delivery process and the appropriate actions to take to ensure that a complete evaluated TOE has been received.

The following is a list of Hardcopy Documentation provided with the TOE media kit for Stonesoft StoneGate Version 2.0.5:

StoneGate VPN Client Installation and User's Guide, Version 2.1, revision SGVCG-211111002
StoneGate Installation Guide, version 2.0, revision SGInstG-213090802
StoneGate Administrator's Guide, version 2.0 , revision SGAG-202090802
Booklet "*StoneGate High Availability Firewall VPN*" (17 pages)

The TOE media kit also provides softcopy documentation. The following Softcopy Documentation is provided on the Common Criteria User's Guide Version 2.0.5 Intel Platform CD:

StoneGate Common Criteria Certification User’s Guide, version 2.0 as SGCC_180080803.pdf

The following Softcopy Documentation is provided on the Management System VPN Client Version 2.0.7 CD:

StoneGate Administrator's Guide	as	SGAGBook.pdf
How_Tos	as	HOWTOvpnonly.pdf
StoneGate Installation Guide	as	SGInstGBook.pdf
VPN_Client_Guide	as	SGVCG.pdf
VPN_Client_Installer	as	VPNC2.0.7-RLNT.pdf
Training Documentation	***as***	***StoneGate - Advanced Training Outline.pdf***
	and	***StoneGate - Fundamentals Training Outline.pdf***

The Management System VPN Client Version 2.0.7 CD also includes SGONLINEHELP 2.0.

7 IT Product Testing

7.1 Developer Testing

The developer maintains a suite of tests for confirming that the StoneGate Firewall product meets its advertised functional requirements. Testing is performed at a developer facility in Finland. Since the TOE boundary does not match the boundary of the vendor product, some of the vendor’s normal functional testing was not applicable to the TOE and some evaluation specific test documentation and tests were developed by the vendor. The developer tested the product on a variety of platforms and configurations, some of which were outside the scope of the evaluated configuration. The basic test configuration for the evaluated configuration testing was same as the one illustrated in Figure 2 Evaluation Test Configuration and described in the following section for the evaluation team test configuration.

The developers Test Plan and Test Procedures were documented in the “StoneGate Test Cases and Test Procedures.” The Test Cases provide a high level description of the functionality tested and test setup The Test Cases were mapped to one or more Test Procedures. The Test Procedures provided detailed instructions for the tester as well as expected and actual test results.

Test documentation including test plans, test procedures, a description of the test configuration, test coverage documentation, expected test results, and actual test results were provided to the CCTL for review. The evaluators reviewed the developers tests and test results to ensure that the developers testing and test results were appropriate for the evaluated configuration. The developer's test documentation showed that at least one test case was mapped to every external interface. Many of the interfaces were exercised by multiple tests. An evaluation team review of all of the security functions and the mapping between security functions and tests confirmed that security functions were appropriately tested by the developer tests.

7.2 Evaluator Testing

Evaluation team testing was conducted from June 24 to August 9, 2003 at the CygnaCom Solutions CCTL facility in McLean, VA. The evaluation team performed the following activities during testing:

1. Installation of the TOE in its evaluation configuration
2. Execution of a sample of the developer's functional tests
3. Independent Testing
4. Vulnerability Testing (AVA_VLA.2)

The TOE was tested in the specific configuration illustrated in Figure 2 Evaluation Test Configuration. The test configuration consisted of two StoneGate firewall nodes configured into a cluster. Physically separate networks were used for the management network and the heartbeat network. A single management server was configured on the management network and that same host was also configured as the logging server. In the test configuration a single host was configured on the internal network to drive tests and to accept traffic from tests. The external network was configured with one host that communicated directly with the external interfaces of the two StoneGate test nodes and also a third StoneGate firewall was configured on the external network with another host behind it to test some of the VPN capabilities. The host that was directly connected to the external network was used to drive most of the testing of the external firewall interfaces .

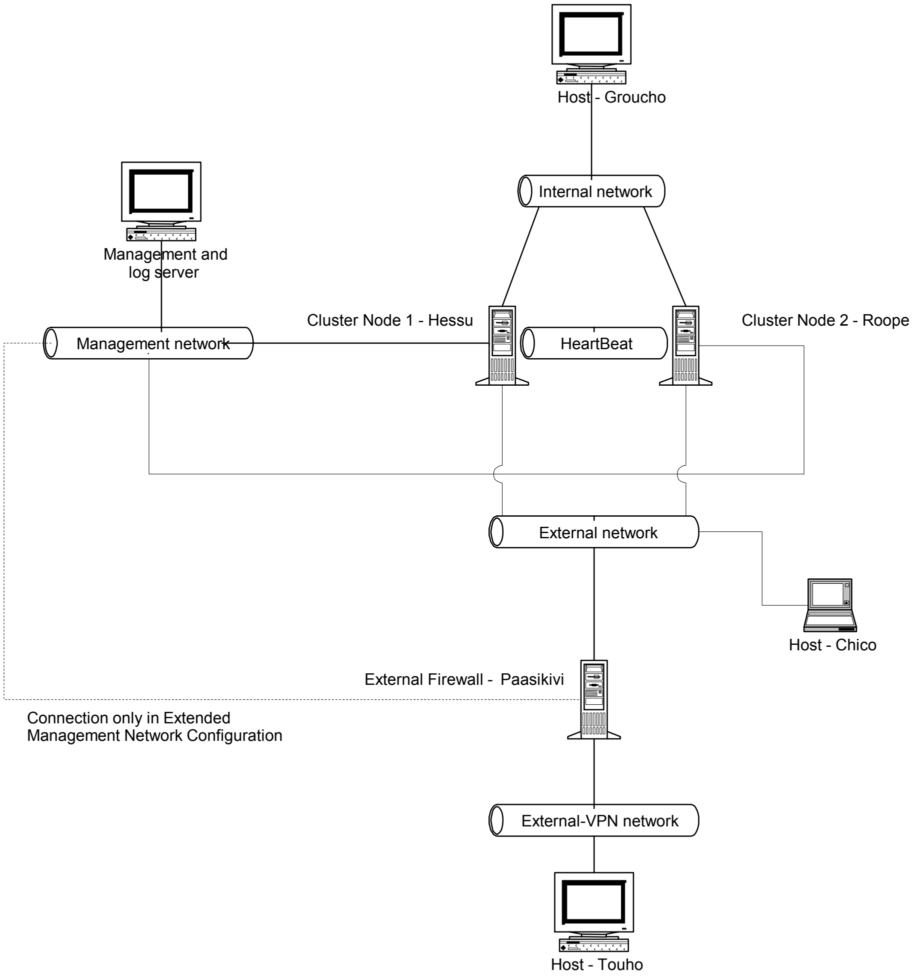

Figure 2 Evaluation Test Configuration

Most of the developers test procedures were manual. The tests required that the testers perform a relatively long sequence of steps to set up the tests. Moreover, the test results involved visual observation and interpretation of information presented by the management GUI or displayed logs. Although test results were often observed through a GUI, the actual test result was also captured in the firewall logs or by logging the network traffic at all of the interfaces that were being exercised by the specific tests. Hence, sufficient information was captured in the network traffic logs and the firewall logs to reproduce any analysis of test results that was performed by visual inspection. The manual procedures needed to set up the individual tests were very time consuming and the evaluators were very thorough in carefully documenting every step that they performed and the system responses to those steps. As a result, testing progressed very slowly.

A vendor representative was available to facilitate some of the testing. The primary role of the vendor representative was to facilitate the resolution of any apparent discrepancies between the evaluator's test results and the expected test results. Discrepancies between the expected and actual results were addressed by having the developer extract copies of firewall logs and associated diagnostic data and deliver that data to the developer test facilities in Atlanta and in Finland, where the information was analyzed and the discrepancies resolved.

The evaluators conducted testing using a sample of tests found in the developer test plan and procedures. The evaluators' tests were selected based upon a review of Stonesoft's test evidence and the evaluators' understanding of the TOE's design. The strategy used to devise the test set was to choose a few tests that cover as many TOE security functions a possible and then add tests to exercise key TOE security functions for information flow policy, VPN, and high-availability in greater depth. Stonesoft had one automated test procedure that tested a large set of security functions and a collection of additional test procedures that were manual. The evaluator selected the automated test procedure and a set of manual tests that covered:

- TCP, UDP, and ICMP packet filtering;
- NAT;
- Spoofing;
- Audit storage exhaustion; and
- VPN.

The effort required to verify Stonesoft's test results influenced the size of the test subset. Most of Stonesoft's test procedures were manual. Many entailed significant setup. Hence, the subset was devised to maximize the scope and effectiveness of testing, while being as small as possible in order to be consistent with the effort expended on other evaluation activities. All security functions were tested, as well as almost all external interfaces. Testing of internal subsystem interfaces was done implicitly.

The evaluation team's independent testing included automated and manual tests. The automated tests consisted of port and vulnerability scans to test TOE security functions for information flow policy. These scans addressed known public domain weaknesses commonly associated with firewalls. The evaluator devised additional tests to augment and supplement the automated tests. The independent tests were selected with the following objectives:

- Augment Stonesoft tests by consolidating information flow and audit checks into a single procedure
- Augment Stonesoft tests with additional test cases tailored to TOE security functional requirements
- Augment Stonesoft tests with different types of information flow policies
- Supplement Stonesoft tests with negative cases and complex cases

The evaluation team also inspected the tests that were performed for the IPSEC interoperability/conformance claims documented at the third party web site and used the evaluator supplemental testing to strengthen the case for the conclusions from those third party claims.

Finally, the evaluator performed tests for hypothesized vulnerabilities. Other than the port and vulnerability scans, all of the evaluator's test procedures were manual. The evaluator team determined that the vendor's own vulnerability analysis was very thorough and appropriately tested. As a result, there were only a few additional vulnerabilities hypothesized and tested by the evaluators.

The end result of the testing activities was that all tests gave expected (correct) results. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities.

The evaluation team tests and penetration tests substantiated the security functional requirements in the ST.

7.3 Third Party Testing

The ST claimed compliance with some standards that are not normally part of a CCTL testing activity. Whenever possible, the developer relied upon third party testing that is associated with those standards. Hence, the analysis and testing for the FIPS 140-2 certification was performed by an accredited FIPS laboratory, which in this case was a separate part of CygnaCom also located within its the McLean, VA home office. Supporting testing for compliance with the IPSEC VPN standards was in part performed and documented by the Virtual Private Network Consortium (VPNC) on their web site at www.vpnc.com. However, neither of these two third parties performs complete testing for the standards. In particular, the FIPS –140-2 standard does not have FIPS testing to determine compliance with Diffe-Hellman key management or the RSA algorithm. Similarly, the VPNC certification tests interoperability with two reference servers and does not explicitly test that the IPSEC implementation meets the standards. In such cases, a combination of vendor testing and evaluator testing were used to supplement the third party testing that determined compliance with the standards. Identification of the methods used to determine compliance with specific standards are specified in the ST where the compliance claims are asserted.

8 Evaluated Configuration

8.1 TOE

This section documents the configuration of the IT product during the evaluation. The administrator and installation guides provide the necessary details for the correct configuration of the IT product in its evaluated configuration.

It is important for potential users to realize that if the evaluated configuration differs from the intended operational use, the differences must be factored into the final risk assessment.

The TOE includes both physical and logical boundaries.

8.1.1 Physical Boundaries of TOE

The **TOE** is the StoneGate firewall engine software version 2.0.5 build 888, which includes the SSHToolkit Cryptographic module components version 4.1.1. The TOE is configured in FIPS mode in the evaluated configuration. FIPS mode requires:

- SSH daemon disabled on the underlying platform;
- Root account disabled on underlying operating system;
- Connection tracking enabled;
- Log spooling policy set to stop traffic;
- VPN client policy download disabled; and
- FIPS mode enabled in Security Gateway settings.

8.1.2 Platform for TOE

The underlying operating system for the TOE is Debian GNU/Linux v.3.0 as modified by Stonesoft. The underlying operating system is part of the StoneGate Firewall product and hence it is delivered along with the evaluated TOE. The underlying hardware for the TOE is:

- IBM eServer xSeries 330, Type 8674 Server,
- Intel Pentium III 1133 MHz,
- Network Interface Cards, Fast Ethernet or Gigabit Ethernet Interfaces to support architecture defined below. The cards must be based on the Intel 82557, 82558 or 82559 chipset. The specific cards used in the test configuration are the IBM eServer xSeries 10/100 Ethernet Adapter.

8.1.3 IT Environment of TOE

The relationship of the TOE with its IT environment is show in Figure 3 IT Environment of TOE.

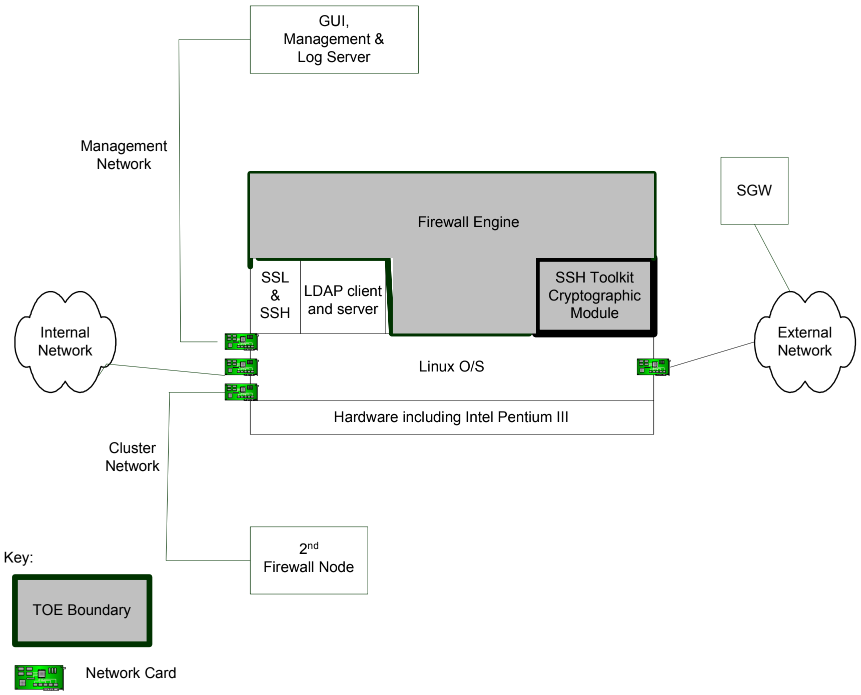

Figure 3 IT Environment of TOE

The TOE is connected to four networks: External, Internal, Management, and Heartbeat networks as shown in Figure 1: Typical Network Configuration for TOE located on page 7.

The support software running on the TOE platform is:
OpenSLL, SSLeay 1995-1998, Stonesoft FIPS PUB 140-2 certified version;
OpenSSH, Stonesoft FIPS PUB 140-2 certified version; and
OpenLDAP client and server, version 2.3, 28 July 2000

8.1.4 Logical Boundaries of TOE

The TOE provides the following security services:

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 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.

- VPN matching rules to decide whether to accept or discard encrypted and unencrypted connections.
- Protocol Agents providing additional rules based on application level information and mechanisms to redirect connections. While the firewall engine supports many protocol agents, the evaluation is limited to protocol agents for FTP, HTTP, and SMTP.

VPN data protection between the TOE and another trusted Security Gateway (SGW). The TOE provides VPN network security services based on the IPSec protocol. This includes certificate-based authentication and data confidentiality and integrity protection using its FIPS PUB 140-2 certified cryptographic module described below. IPSec manual key exchange is an available configuration option but is not included in the evaluation.

- **I&A to support VPN:** The TOE includes authentication mechanisms for SGWs to establish VPN connections. SGWs can authenticate with IKE, to establish a VPN connection using a certificate-based mechanism using RSA, or using pre-shared key.

- **Crypto Functions supporting the VPN:** The TOE includes a FIPS PUB140-2 certified cryptographic module to provide the following cryptographic operations and key management services:

- Cryptographic Operations:
  - 3DES encryption/decryption
  - AES encryption/decryption
  - RSA signature/verification
  - SHA-1 Secure Hash
  - HMAC-SHA-1 Keyed-Hash Message Authentication Code
  - Diffie-Hellman Key Exchange
- Cryptographic Key Management:
  - Key generation of symmetric 3DES and AES keys
  - Key generation of RSA keys;
  - Cryptographic Key Destruction by zeroization.

Network Address Translation (NAT) between external IT entities that pass traffic through the TOE ensuring the IP-address of hosts on internal networks are kept private from external users.

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 and VPN services.

Auditing: 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 authorized administrator to define the criteria used for the selection of the IP traffic events to be audited. The TOE provides mechanism to prevent audit data loss.

Security Management and Protection of Security Functions: administrators access the firewall engine through the management server which provides the interface for managing the security policy and authentication attributes, the TSF data and security functions of the firewall engine. The firewall engine also ensures the trusted security functions are always invoked and cannot be bypassed.

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC, Version 2.1; CEM, Version 1.0, and all applicable NIAP CCEVS and International Interpretations in effect on March 27, 2002.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component and for the augmented assurance component: ALC_FLR.1. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the document *Evaluation Technical Report for a Target of Evaluation, Stonesoft StoneGate Firewall Version 2.0.5, ETR Version 1.1 AVA_VLA.2, dated 17 September 2003*, contains the verdicts of "PASS" for all the work units.

The evaluation determined the product to be Part 2-extended and, as well, meeting the requirements for Part 3, and EAL 4 augmented by Flaw Remediation (ALC_FLR.1). The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom Solutions.

10 Validator Comments

The base platform (hardware and operating system) for the StoneGate product is considered to be part of the IT Environment rather than the TOE. The fact that this component was excluded from the TOE is sufficient cause for the product evaluation to not make any claims of compliance with the U.S. DoD Protection Profiles for Medium Robustness Firewalls.

The validators concur with the following evaluation team recommendation that is not already discussed in other sections of this report.

> "The TOE supports connection filtering based on user identity.
> User identity is established using authentication server(s) in
> the IT environment, either LDAP (password), TACACS+, or RADIUS.
> Users may telnet to port 2543 on the TOE to initiate
> authentication.
>
> The evaluator recommends against using the LDAP password function
> with unsecured telnet, because passwords would be observable in
> transit to the TOE. Instead, TACACS+ or RADIUS one-time passwords should
> be used. Alternatively, telnet sessions to the TOE should be via
> a VPN connections, such as provided by the StoneGate VPN client.
> However, the StoneGate VPN client was not within the scope of
> this evaluation."

11 Security Target

The Security Target, "Stonesoft StoneGate Firewall Version 2.0.5 Common Criteria Security Target, Version 3.13, dated 7 August 2003" is included here by reference.

12 Glossary

12.1 Definition of Terms

Certificate, Digital
An electronic identification card for a user or device. Digital certificates are distributed, or granted, by certificate authorities (CAs), and ensure that the user or device is who/what they claim to be. Digital certificate holders have a public and private key pair, which can be used to sign messages (authenticate the sender), and decrypting incoming messages (ensuring only the certificate holder can decode the encrypted message).

Clustering Technology
A set of methods and algorithms used to implement highly scalable solutions where more than one machine handles the work load. The advantages of clustering technology include increased performance, availability, and reliability.

Connection Tracking
The set of data maintained for a connection. Used for relating incoming packets to existing connections. Connection tracking also includes information to support features like NAT, Load Balanced Routing and Protocol Agents. May also contain accounting information.

Firewall
A barrier or choke point between two or more networks, which examines, controls and/or blocks the flow of data between those networks. Often thought of as a defense between a corporate network and the Internet, firewalls can also protect internal networks from each other.

Firewall Cluster
A group of firewalls that, through clustering technology, process the work normally performed by a single firewall machine.

Firewall Engine
The application software or processes that run on a firewall, performing the actual examination and access control of data.

Firewall Node
A single device, often a specialized PC or router, that runs firewall software, and performs the functions of a firewall as part of a firewall cluster.

Firewall Security Policy
A rule base that defines the policies implemented by the firewall for securing network and computer resources.

Firewall System
A collection of applications used to implement security policies and monitor network traffic at one or more sites. A firewall system consists of firewall engines, management servers, log servers and GUIs.

High Availability
The implementation of clustering technology, hot standby technology, or general redundancy in a system to increase the availability of an application, service, or network beyond what a single system is capable of providing. Increased availability is achieved by eliminating all single points of failure, with clustering technology providing the highest level of availability.

IPSec (IP Security)
A set of protocols supporting secure exchange of packets. Used for the implementation of VPNs, it provides transport and tunnel encryption modes. IPSec is defined in RFC 2401.

Multi-Layer Inspection
A hybrid firewall technology that incorporates the best elements of application level and network level firewalls, with additional technology to enable the secure handling of many connection types.

NAT (Network Address Translation)
A mechanism for assigning local networks a set of IP addresses for internal traffic and another for external traffic. NAT was originally described in RFC 1631 as a means for solving the rapidly diminishing IP address space. It provides a supplemental security purpose by hiding internal IP addresses.

Packet
A unit of data sent across a network.

Packet Filtering
A method of controlling access to a network, or set of networks, by examining packets for source and destination address information, and permitting those packets to pass, or halting them based on defined rules.

Protocol
An agreed-upon format for transmitting data between two or more devices. Protocols typically define how to check for errors, how the sender will announce they have completed the sending of data, how the receiver will acknowledge receipt of the data, and how they will compress the data (if applicable).

Protocol Agent
A module that assists the firewall engine in handling a particular protocol. Protocol agents ensure that related connections for a service are properly grouped and evaluated by the firewall engine, as well as assisting the engine with content filtering or network address translation tasks.

Route

The set of routers or gateways a packet travels through in order to reach its destination. In TCP/IP networks, individual packets for a connection may travel through different routes to reach the destination host.

Security Gateway (SGW)
A remote trusted device that is IPSec compatible and is able to implement a VPN with the TOE.

Traffic Filter Firewall
A type of firewall that looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules.

Virtual Private Network (VPN)
A set of devices connected to one or more public networks that encrypt communications amongst themselves. Effectively, the devices create a tunnel over the public network(s) as if they were connected by private lines instead.

12.2 Definition of Acronyms

CA	Certificate Authorities
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Items
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transport Protocol
I&A	Identification and Authentication
I/O	Input/Output
IP	Internet Protocol
IT	Information Technology
MAC	Mandatory Access Control
NAT	Network Address Translation
NIAP	National Information Assurance Program
NIST	National Institute of Science & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OR	Observation Report
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SGW	Security Gateway
SMTP	Simple Mail Transfer Protocol

SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol
VPN	Virtual Private Networking
VPNC	Virtual Private Networking Consortium

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[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 1999, Version 2.1.

[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 1999, version 1.0.

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

[8] Common Criteria Evaluation and Validation Scheme for Information Technology Security Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, February 2002

[9] Evaluation Technical Report for a Target of Evaluation Stonesoft StoneGate Firewall version 2.0.5, Proprietary ETR Version 1.1 AVA_VLA.2, 17 September 2003

[10] Stonesoft StoneGate Firewall v.2.0.5 Common Criteria Security Target, Version 3.13, 7 August 2003

[11] Supplement: ALC_FLR - Flaw Remediation, CEM-2001/0015, Version 1.0, August 2001