Stonesoft Corporation

StoneGate Firewall 5.2.5.8081.cc.2 Security Target

VERSION 2.1

2011-10-06

Stonesoft Corporation

Itälahdenkatu 22 A, FIN-0210 Helsinki, Finland

TABLE OF CONTENTS

List of Figures and Tables

Document History

Version	Date	Authors	Comment
2.0pre1	2011-02-23	Andreas Siegert, atsec	Converted from 1.3 release to exclude VPN and be conformant to CC 3.1R3
2.0pre2	2011-03-04	Jorma Levomäki, Stonesoft	Updated the TOE boundary and operating environment descriptions
2.0pre3	2011-04-11	Andres Siegert, atsec	Updated based on comments from CSEC
2.0pre4	2011-04-29	Staffan Persson, atsec	Updated based on comments from CSEC and the evaluator
2.0pre5	2011-05-09	Jorma Levomäki, Stonesoft	Updated based on comments from the evaluator
2.0pre6	2011-05-12	Staffan Persson, atsec	Minor editorial changes. Finalized version.
2.0	2011-07-13	Staffan Persson, atsec	Minor changes to audited events.
2.1	2011-10-06	Staffan Persson, atsec	Minor changes of version numbers

1 INTRODUCTION

1.1 SECURITY TARGET IDENTIFICATION

Title:	StoneGate Firewall 5.2.5.8081.cc.2 Security Target
Version	2.1
Status:	Released
Date:	2011-10-06
Sponsor:	Stonesoft Corporation
Developer	Stonesoft Corporation
Keywords:	Firewall, High Availability, Traffic Filter, Application Proxy

1.2 TOE IDENTIFICATION

Stonesoft StoneGate Firewall/VPN Version 5.2.5.8081.cc.2

1.3 TOE OVERVIEW

The Stonesoft StoneGate Firewall is the firewall part of the StoneGate Firewall//VPN product. It is a high availability firewall 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. 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.

1.3.1 TOE Type

The TOE is a firewall.

1.3.2 Required Hard- and Software

The TOE is used on standard Intel Pentium 4 or higher based hardware with

- 1 GB or more RAM and four or more network interfaces

running

- Linux kernel 2.6.32.42 with minor modifications and Debian GNU/Linux 5.0 based operating system.

Please see chapter 1.4.2.1 for the specific hardware models that are part of the evaluated configurations. A detailed list of hardware and software components that are considered part of the TOE environment is provided in chapter 1.4.2.5.

1.3.3 Intended Method of Use

The StoneGate Firewall is intended to be used as part of a firewall cluster and as the sole connection between an internal network and an external, untrusted network. The StoneGate Firewall is assumed to be in a physically protected environment, administered by trusted and trained administrators over on a trusted and separate management network.

The StoneGate Firewall product runs on a hardened Linux operating system that is shipped with the product. The product runs on a single or multi-processor Intel platform. A distributed management system comprising a Management Server, Log Server and Graphic User Interface (GUI) to support the management and operation of the firewall is supplied as a separate product.

1.3.4 Major Security Features

The security features within the scope of the ST include:

- Connection level information flow control for IP version 4 packets including network-through-application level packet filtering, and connection redirection for FTP, HTTP, and SMTP traffic.
- Privacy for hosts' IPv4 addresses on the internal network using static Network Address Translation (NAT);
- High Availability for network security services;
- Audit generation, selection and preventing of audit data loss; and
- Management and protection functions to support the security services.

1.4 TOE DESCRIPTION

1.4.1 Introduction

The StoneGate firewall is a high availability firewall for securing data communications and enabling continuous network connectivity. The firewall services include stateful packet filtering and application-level information flow control The StoneGate firewall is intended for use by organizations who need controlled, protected and audited access to services, both from inside and outside their organization's network, by encrypting, allowing, denying, and/or redirecting the flow of data through the firewall.

The StoneGate Firewall is the firewall component (or node) of the StoneGate product. The StoneGate product comprises a firewall engine, its operating system and data repository platform and management system software. The firewall engine and the VPN module is included in the scope of the TOE. However, the VPN functionality is not part of the TSF. The management system and operating platforms are outside of the scope of the evaluation.

To support the operations of the firewall engine, the separately supplied management system includes a Management Server that provides a trusted interface for administrator functions, a Log Server to store and manage (i.e., filter, sort, archive) the log records, and a GUI to facilitate administrator access. Its distributed architecture makes it flexible and scalable since it can run on single or on multiple hardware platforms, and Microsoft Windows Server 2008 SP2 and R2, Windows 7, Windows Vista SP2, Windows Server 2003 SP2 (32-bit), CentOS 5, Red Hat Enterprise Linux 5 and SUSE Linux Enterprise 11 SP1. The firewall engine uses a hardened Linux operating system based on Debian GNU/Linux. All non-essential packages have been removed from the Debian distribution.

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 optionally can have separate management networks for connectivity to the management system and the other nodes in a cluster, i.e., management network and cluster network, respectively. See Figure 1 below.

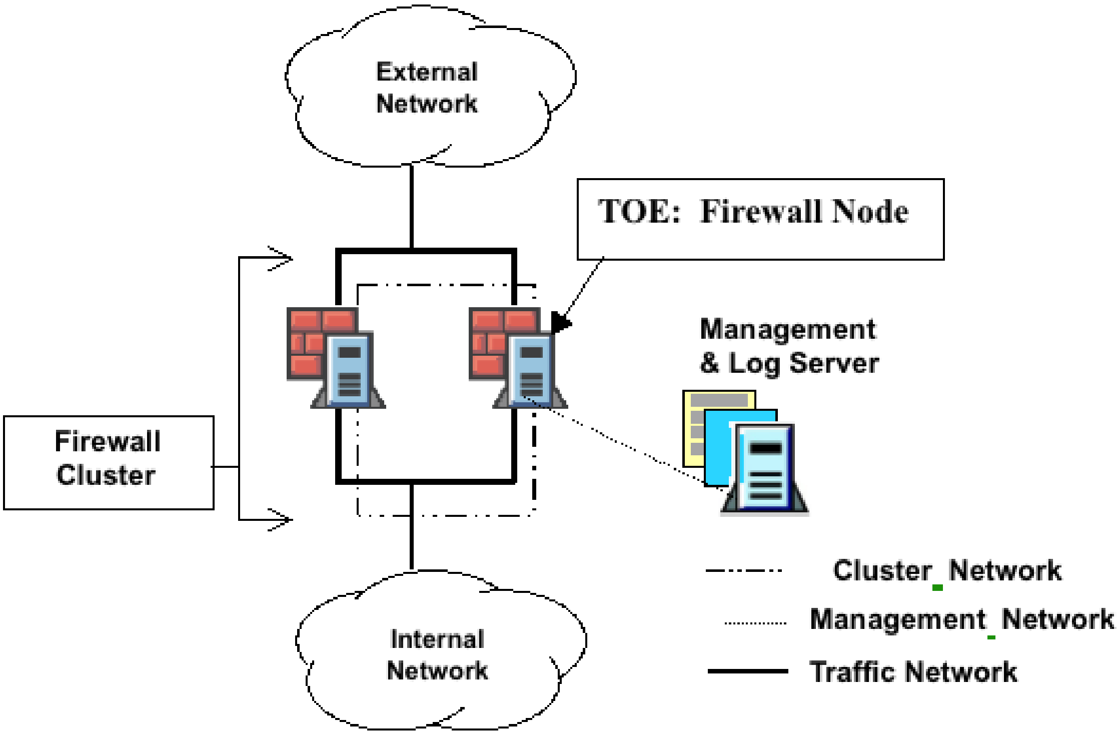

Figure 1 TOE Operating Environment

1.4.2 **TOE Scope**

1.4.2.1 Hardware Platforms

The following StoneGate models are included within the evaluation scope;

- FW-315 (desktop)
- FW-1301 (rackmount)
- FW-3201 (rackmount)
- FW-3205 (rackmount)

1.4.2.2 Physical

As illustrated in Figure 2 below, the physical TOE scope comprises:

- The Firewall Engine software application, version 5.2.5.8081.cc.2
- The AuthenTec QuickSec IPsec Toolkit, version 5.1

running on one of the platforms indicated in chapter 1.4.2.1.

The documentation is included with the scope of the TOE and consists of the Installation Guide, the Administrator's Guide and a Reference Guide. The documentation is available for download from the web side of the developer.

1.4.2.3 Logical

The Target of Evaluation (TOE) consists of the StoneGate Engine and the VPN module. The Stone Gate Engine 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.
    - 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 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.
- 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 (out of scope) 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.

Even though the TOE does contain a VPN module, the VPN functionality is not part of the evaluated TSF.

1.4.2.4 Configurations

The TOE evaluated configuration specifies:

- Connection tracking enabled;
- Log spooling policy set to ‘stop traffic’;
- Access to the command line interface to the Firewall Engine from the operating system is disabled as specified in the installation documentation;

1.4.2.5 TOE Environment

The operational environment for the evaluated configuration includes:

- TOE operating platform:
    - Intel Pentium 4 or higher (or equivalent) recommended,
    - 1 GB RAM or more recommended,
    - Standard Linux Kernel 2.6.32.42 with minor modifications, Debian GNU/Linux 5.0 (lenny) based distribution,
    - Network Interface Cards (see Annex D).
- StoneGate Management Center and supporting software, version 5.2:
    - the Management Server,
    - the Log Server,
    - the Graphical User Interface (GUI),
- OpenSSL 0.9.8 (used on Firewall engine and Management Server),
- OpenSSH 5.1,
- OpenLDAP client and server, version 2.4 (used on Firewall engine and Management Server),
- Architecture and System support:
    - at least 2 network interfaces,
    - 1 cluster network interface,
    - 1 management network interface,
    - a second TOE to form a cluster.

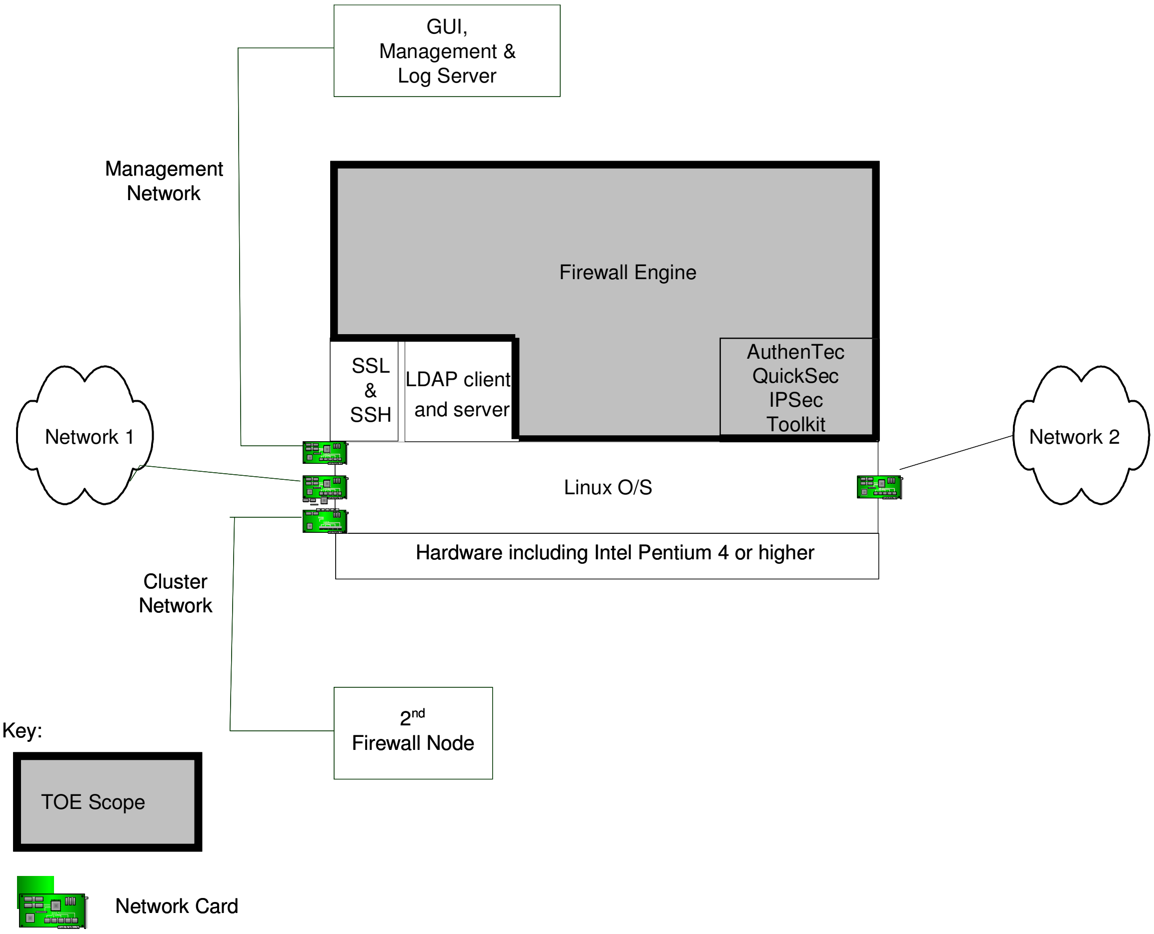

Figure 2 TOE Boundary and IT Environment

2 CC CONFORMANCE CLAIM

This TOE conforms to the following CC specifications:

Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009. Part 2 extended - component FAU_STG.NIAP-0414 is used to express additional functionality contained within NIAP interpretation 0414.

Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, Revision 3 July 2009. Part 3 conformant;

Evaluation Assurance level 4 (EAL4) augmented with ALC_FLR.1, Basic flaw remediation.

3 SECURITY PROBLEM DEFINITION

3.1 THREAT ENVIRONMENT

3.1.1 Assets

The assets to be protected are the information and IT resources of the network being protected by the TOE.

3.1.2 Threat Agents

The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself

3.1.3 Threats Countered by the TOE

T.AUDIT_UNDETECTED:
Audit Events Go Undetected
A threat agent may attempt to compromise the assets without being detected. This threat includes a threat agent causing audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.

T.MEDIAT: **Information Flow Control**
An unauthorized person may send information through the TOE, which results in the exploitation and/or compromise of IT assets. This threat includes an unauthorized person attempting to by-pass the information flow control policy by sending an IP packet with a fake source address.

T.NODE_FAILURE:
Denial of Service Prevention
A failure of a node or a network connection to a node caused by a threat agent or due to the normal lifecycle of components could cause denial of service, making IT assets unavailable.

T.SELPRO: **Self Protection**
An unauthorized person may access TOE management functions, and read, modify, or destroy security critical TOE data.

3.2 ASSUMPTIONS

3.2.1 Operational Environment of the TOE

A.ADMIN_ACCESS:
Administrator Access Support provided by the IT Environment
It is assumed that the administrator accesses 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 Management Server application.

A.ADMINTRUSTED:
Administrator Attributes
It is assumed that authorized Administrators are trained, qualified, non-hostile and follow all guidance.

A.AUDITMAN: **Environment Audit Procedures**
It is assumed that audit trails are regularly analyzed and archived.

A.AUDIT_SUPPORT:
Audit Support Provided by the IT Environment
It is assumed that the IT environment generates audit records for the security functions on which the TOE depends from its environment and provides protected permanent storage of the audit trails generated by the TOE.

A.MEDIAT_SUPPORT:
Information Flow Control Support Provided by the IT Environment
It is assumed that the TOE is the only connection between internal and external networks.

A.OPERATING_ENVIRONMENT:
General IT Environment Support
It is assumed that TOE node and the TOE's associated Management Servers and management networks are dedicated to the trusted firewall system, function according to their specifications, and are physically secure, only allowing trusted administrators physical access.

A.USER_AUTH: **User Authentication for Information Flow Control**
It is assumed that the IT environment will 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.

A.TIME: **Trusted time source**
It is assumed that the IT environment will provide a reliable time source to the TOE and the TOE environment.

3.3 ORGANISATIONAL SECURITY POLICIES

This ST does not define any operational security policies for the TOE.

4 SECURITY OBJECTIVES

4.1 OBJECTIVES FOR THE TOE

O.AUDIT: **Detect and Record Audit Events**
The TOE must provide a means to accurately detect and record security-relevant events in audit records, and prevent audit data loss by prioritizing and preventing security-relevant events when the audit storage capacity fills.

O.HIGHAVAILABILITY:
High Availability
The TOE when operating as part of a firewall cluster must provide high availability of information flow control, ensuring continuation of service when firewall nodes or their interfaces fail.

O.MEDIAT: **Information Flow Control**
The TOE must mediate the flow of all information between users and external IT entities on the internal and external networks connected to the TOE in accordance with its security policy.

O.NETADDRHIDE:
Hide Internal Network Addresses
The TOE must provide a means to hide the IP addresses of hosts on its internal network.

O.SECFUN: **Management Functions**
The TOE must provide a means for an administrator via the Management Server to manage the TOE security functions.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

OE.ADMIN_ACCESS:
Administrator Access Support provided by the IT Environment
The environment has to ensure that the administrator accesses 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 Management Server application..

OE.ADMINTRUSTED:
Administrator Attributes
The environment has to ensure that authorized Administrators are trained, qualified, non-hostile and follow all guidance..

OE.AUDITMAN: **Environment Audit Procedures**
The environment has to ensure that audit trails are regularly analyzed and archived.

OE.AUDIT_SUPPORT:
Audit Support Provided by the IT Environment
The environment has to ensure that the IT environment generates audit records for the security functions on which the TOE depends from its environment and provides protected permanent storage of the audit trails generated by the TOE..

OE.MEDIAT_SUPPORT:
Information Flow Control Support Provided by the IT Environment
The environment has to ensure that the TOE is the only connection between internal and external networks .

OE.OPERATING_ENVIRONMENT:
General IT Environment Support
The environment has to ensure that the TOE node and the TOE's associated Management Servers and management networks are dedicated to the trusted firewall system, function according to their specifications, and are physically secure, only allowing trusted administrators physical access.

OE.USER_AUTH:
User Authentication for Information Flow Control
The environment has to 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.

OE.TIME: **Trusted time source**
The environment has to provide a reliable time source to the TOE and the TOE environment.

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats, showing that each TOE objective addresses at least one threat.

Objective	Threats
O.AUDIT	T.AUDIT_UNDETECTED
O.HIGHAVAILABILITY	T.NODE_FAILURE
O.MEDIAT	T.MEDIAT
O.NETADDRHIDE	T.MEDIAT
O.SECFUN	T.SELPRO

Table 1 Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the operational environment to assumptions and threats, showing that each objective addresses at least one assumption or threat.

Objective	Assumptions / Threats
OE.ADMIN_ACCESS	T.SELPRO, A.ADMIN_ACCESS
OE.ADMINTRUSTED	A.ADMINTRUSTED
OE.AUDITMAN	T.AUDIT_UNDETECTED, A.AUDITMAN
OE.AUDIT_SUPPORT	T.AUDIT_UNDETECTED, A.AUDIT_SUPPORT
OE.MEDIAT_SUPPORT	T.MEDIAT, A.MEDIAT_SUPPORT
OE.OPERATING_ENVIRONMENT	A.OPERATING_ENVIRONMENT
OE.USER_AUTH	T.MEDIAT, A.USER_AUTH
OE.TIME	T.MEDIATE, T.AUDIT_UNDETECTD, A.TIME

Table 2 Mapping of security objectives for the operational environment to assumptions, threats and policies.

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T.AUDIT_UNDETECTED	A threat agent may attempt to compromise the assets without being detected. This threat includes a threat agent causing audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker’s actions. This threat is diminished by: ▪ Audit records which record security relevant events (O.AUDIT), ▪ Security relevant events are prioritized and prevented as audit storage capacity fills (O.AUDIT), ▪ Administrator actions being auditable (OE.AUDIT_SUPPORT),

	▪ An audit trail that can be effectively reviewed (OE.AUDITMAN), and ▪ Reliable timestamps being available for the audit trail (OE.TIME).
T.MEDIAT	An unauthorized person may send information through the TOE, which results in the exploitation and/or compromise of IT Assets. This threat includes an unauthorized person attempting to by-pass the information flow control policy by sending an IP packet with a fake source address. This threat is diminished by: ▪ Applying the firewall security policy to all information that passes through the networks between users and external IT entities (O.MEDIAT and OE.MEDIAT_SUPPORT), ▪ Preventing information flow for any packet that uses the source routing option (O.MEDIAT), ▪ Information on the IP addresses of the hosts on the internal networks is not available to the external network (O.NETADDRHIDE), ▪ No residual information is transmitted (OE.MEDIAT_SUPPORT), ▪ Reliable timestamps being available for time-based information flow control decisions (OE.TIME), and ▪ User authentication services available for information flow control decisions (OE.USER_AUTH).
T.NODE_FAILURE	A failure of a node or a network connection to a node caused by a threat agent or due to the normal lifecycle of components could cause denial of service making IT assets not available. This threat is diminished high availability mechanisms for the information flow control when the TOE is deployed as part of a firewall cluster (O.HIGHAVAILABILITY).
T.SELPRO	An unauthorized person may read, access TOE management functions, and read, modify, or destroy security critical TOE data. This threat is diminished by providing a means for only authorized administrators to manage the security functions and trusted data (O.SECFUN, OE.ADMIN_ACCESS).

Table 3 Sufficiency of objectives countering threats

The rationale for assumptions is addressed by a direct mapping of each assumption to an environment objective with corresponding name and description, and is therefore self-explanatory apart from A.TIME explained below:

Assumption	**Rationale for security objectives**
A.ADMIN_ACCESS	OE.ADMIN_ACCESS
A.ADMINTRUSTED	OE.ADMINTRUSTED
A.AUDITMAN	OE.AUDITMAN
A.AUDIT_SUPPORT	OE.AUDIT_SUPPORT
A.MEDIAT_SUPPORT	OE.MEDIAT_SUPPORT
A.OPERATING_ENVIRONMENT	OE.OPERATING_ENVIRONMENT
A.USER_AUTH	OE.USER_AUTH
A.TIME	OE.TIME

Table 4 Sufficiency of objectives holding assumptions

5 EXTENDED COMPONENTS DEFINITION

The explicit requirement, FAU_STG.NIAP-0414 is used for compliance with NIAP interpretation 0414. It imposes no additional assurance requirements.

FAU_STG.NIAP-0414 has been used to express functionality configurable by the administrator related to prioritization of audit records when audit trail storage is full.

5.1 CLASS FAU: AUDIT

5.1.1 Site-Configurable Prevention of Audit Loss

Family behavior

This family defines the requirements for the TSF to be able to create and maintain a secure audit trail. Stored audit records refers to those records within the audit trail, and not the audit records that have been retrieved (to temporary storage) through selection.

Component Leveling

FAU_STG.NIAP-0414 is hierarchically to component FAU_STG.4.

Management

The following actions could be considered for the management functions in FMT:

Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.

Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

1. Basic: Actions taken due to the audit storage failure.

2. Basic: Selection of an action to be taken when there is an audit storage failure.

5.1.1.1 FAU_STG.NIAP-0414 Site-Configurable Prevention of Audit Loss

Hierarchical to:	FAU_STG.4
Dependencies:	FAU_STG.1 Protected Audit Trail Storage FMT_MTD.1 Management of TSF Data

FAU_STG.NIAP-0414-1
The TSF shall provide the administrator the capability to select one or more of the following actions [selection: 'ignore auditable events', 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records'] and [assignment: other actions to be taken in case of audit storage failure] to be taken if the audit trail is full.

FAU_STG.NIAP-0414-2
The TSF shall [selection: 'ignore auditable events', 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records', assignment: other actions to be taken in case of audit storage failure]] if the audit trail is full and no other action has been selected.

User Application Notes:

This component specifies the set of administrator selectable actions that the TSF must be capable of performing when the audit trail is full and allows the administrator to specify which action is to be performed by the TSF. It also provides a default action to take if the administrator does not select one of the actions.

6 SECURITY REQUIREMENTS

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

The following are the conventions used for the operations applied to the Security Functional Requirements:

Assignment — Assignments are indicated by showing the value in square brackets, [assignment value].

Selection — Selections are indicated using italics in square brackets, [*selection value*].

Refinement — Refinements are indicated using bold, **refinement**.

Iteration — Iteration is indicated by a plus sign and a number at the end of the component and additional text after the component name, e.g., FCS_COP.1+1 Cryptographic key generation: 3DES.

Class	Component	Component Name
Class FAU – Security Audit		
	FAU_GEN.1	Security audit data generation
	FAU_SEL.1	Selective Audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.NIAP-0414[1]	Site-Configurable prevention of audit loss
Class FDP – User Data Protection		
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Class FMT – Security Management		
	FMT_MSA.1	Management of security attributes
	FMT_MSA.2	Secure security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Class FPT – Protection of the TOE Security Functions		
	FPT_FLS.1	Failure with preservation of secure state
Class FRU – Resource Utilization		
	FRU_FLT.2	Limited fault tolerance

Table 5 Functional Components

6.1.1 Audit selection and generation

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*not specified*] level of audit; and

[1] Extended component.

c) [the events in Table 6].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three in Table 6].

Functional Component	Auditable Event	Additional Audit Record Contents
FAU_STG.NIAP-0414	Actions taken due to the audit storage failure.	None
FDP_IFF.1	All decisions on requests for information flow except denial of packets with the IP source route option set, (i.e., the TOE denies all source route packets but does not record the denial in the audit log.)	Source IP address of request
FMT_SMF.1	Use of the management functions. When a change is made via the Management Server, the Management Server generates audit records of this change. The TOE records that a change has been made and includes the identifier of the Management Server record.	Policy identifier (which is the reference to the management audit record.
FPT_FLS.1	Failure from security policy not being recognized, and loss of connectivity to user or management networks.	None

Table 6 TOE Auditable Events

FAU_SEL.1 Selective Audit

FAU_SEL.1.1 The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes:

a) [*user identity, subject identity, event type*]

b) [all attributes used for the rules defined in FDP_IFF.1.1 except TOE interface on which traffic arrives.]

6.1.2 Preventing audit data loss

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit trail records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.NIAP-0414 Site-Configurable Prevention of Audit Loss

FAU_STG.NIAP-0414.1

The TSF shall provide the administrator the capability to select one or more of the following actions [*prevent* ***audited***[2] *events, except those taken by the authorized user with special rights*] and [the capability to prioritize **audited** events that get spooled on the local node while space is available on the node:

Alert: Generated with an alert status and are always stored.

[2] "auditable" is changed to "audited" in this component to make the NIAP interpretation consistent with a corresponding wording change in CC Version 3.1, Revision 2.

Essential: Always generated even if the firewall engine is running out of disk space.

Stored: Stored to the audit log database if alert and essential log entries have already been stored.

Transient: Not stored to database but kept in firewall log cache.

] to be taken if the audit trail is full.

FAU_STG.NIAP-0414.2 The TSF shall [*prevent **audited** events, except those taken by the authorized user with special rights*] if the audit trail is full and no other action has been selected.

6.1.3 Information flow control and NAT

FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [Firewall Information Flow Control SFP] on [

a) subjects: IT entities on the internal or external networks that send and receive information through the TOE to one another, and human users;

b) information: connections over IP sent through the TOE from one subject to another;

c) operations: pass information and initiate the following services: NAT, authentication check, and opening related connections.]

FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [Firewall Information Flow Control SFP] based on the following types of subject and information security attributes: [

a) subject security attributes:

- presumed IP address;
- port number
- user identity

b) information security attributes:

- presumed IP address of source subject;
- presumed IP address of destination subject;
- TOE interface on which traffic arrives;
- transport layer protocol information
- service (protocol and port);
- time/date of service request.]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and **another controlled subject** via a controlled operation if the following rules hold: [

- When the ‘matching part’ of the rules in the rule base matches the information security attribute values and the ‘action part’ of the matched rule is ‘allow’. The rules may be composed from all possible combinations of the values of the information security attributes, created by the authorized administrator, and
- When the ‘matching part’ of the rules in the rule base matches the information security attribute values and the ‘action part’ of the matched rule is ‘allow’ and the ‘authentication matching’ defined in the rule, as specified in FDP_IFF.1.3, is successful. The rules may be composed from all possible combinations of the values of the information security attributes, created by the authorized administrator]

FDP_IFF.1.3 The TSF shall enforce the [following additional information flow control rules:

- Authentication matching – when a match in a rule requires authentication, if the user identity is successfully authenticated by the external authentication method defined in the rule, authentication matching will return a succeed to the rules defined in FDP_IFF.1.2 and FDP_IFF.1.5, else it will return a fail, and

- Source route protection - the TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject.
- To support NAT, static IP address translation will translate the source and/or destination IP address to another IP address as defined in the rule.
- To support authentication matching, the TSF initiates a request to the authentication service specified by the rule to obtain the authentication of the identity.
- When configured, the TOE will redirect FTP packets, based on RFC 959, to a proxy type of software
- When configured, the TOE will redirect SMTP, based on RFC 821, packets to a proxy type of software,
- When configured, the TOE will redirect HTTP, based on RFC 2616, packets to a proxy type of software.]

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [no explicit authorisation rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [

- When the ‘matching part’ of the rules in the rule base matches the information security attribute values and the ‘action part’ of the matched rule is ‘discard’ or ‘refuse’. The rules may be composed from all possible combinations of the values of the information security attributes, created by the authorized administrator; and
- When the ‘matching part’ of the rules in the rule base matches the information security attribute values and the ‘authentication matching’ is defined in the rule, as specified in FDP_IFF.1.3, fails. The rules may be composed from all possible combinations of the values of the information security attributes, created by the authorized administrator; and
- The following rules can be deduced from the above rules but are explicitly included for clarity:
  - The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;
  - The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;
  - The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;
  - The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.]

6.1.4 Security Management

FMT_MSA.1 - Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Firewall Information Flow Control SFP] to restrict the ability to [*modify*] the security attributes [

a) Attributes from a rule in the firewall security policy;

b) The rules in the firewall security policy.]

to [the Management Server].

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [all security attributes].

FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Firewall Information Flow Control SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

Application Notes: It is not possible for any user role to specify alternative initial values.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [access as listed in Table 7] the [data list in Table 7] to [roles in Table 7].

TSF DATA	Management Server
Auditable events, log levels, and log spool policy;	modify
Security policy attributes	modify
NAT IP address translation table;	modify
Actions to be taken in case of audit storage failure;	modify
For cluster definition for high availability including: ▪ Interface data: NIC number mapping the StoneGate interface number to the physical network address, CVI, NDI internal IP address and mask, NDI specifying interface network type (management, heartbeat, outgoing); ▪ Network element data: cluster name, Log server ID; ▪ Routing information.	modify, delete

Table 7 TSF Data Management

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) Defining auditable events for information flow control auditing;

b) Defining Log Spool Policy;

c) Modifying log levels;

d) Modifying actions to be taken in case of audit storage failure;

e) Configuring access for Management Server interface for administrator;

f) Configuring cluster definition for high availability with the following:

- Interface data: NIC number mapping the StoneGate interface number to the physical network address, CVI, NDI internal IP address and mask, NDI specifying interface network type (management, heartbeat, outgoing);
- Network element data: cluster name, Log server ID
- Routing information.

g) Configuring Firewall Information Flow policy including NAT and authentication matching.]

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [Management Server].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5 High Availability

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [

a) node hardware malfunction;

b) security policy not recognized;

c) interface to internal, external, management or cluster networks fails.]

FRU_FLT.2 Limited fault tolerance

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [

a) node hardware malfunction;

b) security policy not recognized;

c) interface to internal, external, management or cluster networks fails.]

6.2 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Requirement(s)	**Objective(s)**
FAU_GEN.1	O.AUDIT
FAU_SEL.1	O.AUDIT
FAU_STG.1	O.AUDIT
FAU_STG.NIAP-0414	O.AUDIT
FDP_IFC.1	O.MEDIAT, O.NETADDRHIDE
FDP_IFF.1	O.MEDIAT, O.NETADDRHIDE
FMT_MSA.1	O.SECFUN
FMT_MSA.2	O.SECFUN
FMT_MSA.3	O.SECFUN
FMT_MTD.1	O.SECFUN
FMT_SMF.1	O.SECFUN
FMT_SMR.1	O.SECFUN
FPT_FLS.1	O.HIGHAVAILABILITY
FRU_FLT.2	O.HIGHAVAILABILITY

Table 8 Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Objective	**Threats**
O.AUDIT	The TOE must provide a means to accurately detect and record security-relevant events in audit records, and prevent audit data loss by prioritizing and preventing security-relevant events when the audit storage capacity fills.

	This objective is satisfied by requiring the following: ▪ An audit record can be generated for security-relevant events (FAU_GEN.1), ▪ Unauthorized deletion of audit records is prevented (FAU_STG.1), ▪ Security-relevant events can be included or excluded from the audit log based on selected attributes, and can be prioritized when the audit storage nears capacity (FAU_SEL.1 and FAU_STG.NIAP-0414), and When the audit log is full, auditable events are prevented from occurring (FAU_STG.NIAP-0414).
O.HIGHAVAILABILITY	The TOE when operating as part of a firewall cluster must provide high availability of information flow control, ensuring continuation of service when firewall nodes or their interfaces fail. This objective is satisfied by requiring a secure state is preserved and ensuring operation, when node hardware malfunctions, the security policy is not recognized, or there is a failure on the internal, external or cluster network interfaces (FRU_FLT.2, and FPT_FLS.1).
O.MEDIAT	The TOE must mediate the flow of all information between users and external IT entities on the internal and external networks connected to the TOE in accordance with its security policy. This objective is satisfied by requiring a firewall security policy to control the information flow (FDP_IFC.1 and FDP_IFF.1), and requiring that the policy is applied to all traffic between the internal and external interfaces.
O.NETADDRHIDE	The TOE must provide a means to hide the IP addresses of hosts on its internal network. This objective is satisfied by requiring a firewall security policy that provides IP address translation services (FDP_IFC.1 and FDP_IFF.1).
O.SECFUN	The TOE must provide a means for an administrator via the Management Server to manage the TOE security functions. This objective is satisfied by requiring there to be security management functions for the administrative roles (FMT_SMF.1 and FMT_SMR.1), and protection of the related trusted data and attributes (FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1).

Table 9 Security objectives for the TOE rationale

6.2.3 Security Requirements Dependency Analysis

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	**Dependencies**	**Resolution**
FAU_GEN.1	FPT_STM.1	IT-Environment
FAU_SEL.1	FAU_GEN.1	FAU_GEN.1
	FMT_MTD.1	FMT_MTD.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.NIAP-0414	FMT_MTD.1	FMT_MTD.1
	FAU_STG.1	FAU_STG.1 and IT-Environment
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1	FDP_IFC.1 FMT_MSA.3
	FMT_MSA.3	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1
	FMT_SMR.1	FMT_SMR.1

Security Functional Requirement	Dependencies	Resolution
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1
	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	No role can change the default values, so no such dependeny exist
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	IT-Environment
FPT_FLS.1	None	
FRU_FLT.2	FPT_FLS.1	FPT_FLS.1

Table 10 TOE SFR dependency analysis

6.3 TOE SECURITY ASSURANCE REQUIREMENTS

The target Evaluation Assurance Level for this TOE is EAL4 augmented by ALC_FLR.1.

6.4 SECURITY ASSURANCE REQUIREMENTS RATIONALE

The evaluation assurance requirements were selected from an EAL to provide a balanced level assurance and to be appropriate with this assurance level for this type of product and consistent with the security objectives of the TOE, the TOE should withstand an attacker with an attack potential of Enhanced-Basic.

The Common Criteria authors have ensured that EAL4 is a sound selection of assurance components where all dependencies have been resolved. Since the augmentation of ALC_FLR.1 does not have any dependencies, there is no need to verify the consistency of the assurance component selection.

7 TOE SUMMARY SPECIFICATION

7.1 AUDIT

7.1.1 Audit Selection and Generation

The TOE provides an audit mechanism that cannot be disabled. The startup and shutdown of the audit function is synonymous with the start-up and shutdown of the TOE. The set of potential audit events and record information are defined in FAU_GEN.1.

The audit mechanism is the 'logging' operation which is triggered using the logging option of a rule in the firewall security policy. The TOE applies the matching mechanism for packet filtering, and for each match a logging option can be defined that generates an audit record. The TSF selects the audited events based on the defined logging options. In addition to the logging operation, the TOE provides an audit record when the firewall security policy (i.e., active file) changes. When the TOE receives new firewall security policy it generates an audit record identifying the date, time, and configuration identification. Note: the audit record generated by the TOE for component FMT_SMF.1 provides the link between the two sets of audit records.

The TOE relies on the operating system to provide the time for the audit records and for the Management Server to generate audit records providing the details on the use of the security management functions.

7.1.2 Preventing audit data loss

The TOE provides a mechanism to prevent audit data loss. TOE audit entries are first stored on cache buffers on each node. The size of this cache depends on the size of the hard disk. The proprietary protocol for synchronizing and managing the data among the distributed components notifies the Log Server that there is new log information and sends the log entry to the Log Server. The log information is stored by the Log Server as database files which are only accessible to an authorized firewall administrator via the Management Server. 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 administrator defines the log spooling policy. This specifies the behavior of the TOE whenever its local log spool is filled as one of the following:

- Stop traffic (required in the evaluated configuration): TOE automatically goes to an offline state and connections going through TOE are transferred to other nodes in a cluster (please see information on high availability). Once the spool situation has improved, the node returns automatically to online state.
- Discard log: (the default setting and needs to be changed to the evaluated configuration) the cluster overlooks new log entries without any means of retrieval. This log spooling policy should be used only if the traffic is more important than the logs.

The TOE also provides a means for the Management Server to prioritize log data. The mechanism is based on the following log level:

Alert:	generated with an alert status and are always stored;
Essential:	always generated even if the firewall engine is running out of disk space;
Stored:	stored to the audit log database if alert and essential log entries have already been stored;
Transient:	not stored to database but kept in firewall log cache.

Before applying the selected log spooling policy, the engine stops producing transient logs. If insufficient, it can drop all but the essential log entries. As a last resort, the engine applies the selected log spooling policy.

7.2 FIREWALL

7.2.1 Information flow control

The StoneGate Firewall provides an information flow control mechanism using a rule base that comprises a set of security policy rules, i.e., the firewall security policy. The TSF applies the firewall security policy to all traffic that passes through via its internal or external network interfaces. The traffic is TCP, UDP, ICMP, IPSec connections over IP. The TSF only permits traffic to pass through that has been explicitly allowed by the firewall security policy, and implements packet defragmentation to enforce the policy on entire IP packets. Authorized administrators using the Management Server define the firewall security policy rules.

The TSF implements connection tracking to manage the information flow control decisions for connections rather than packets, providing increased performance and support for firewall features that require packet information above the IP level. The connection tracking mechanism stores the state information of each connection to allow packets belonging to an established connection to pass.

Connection tracking works closely with the protocol agents to manage the information flow control decisions based on information attributes at the different networking layers through the application layer to decide whether a packet should be granted access or not. The following protocol agents and their security function are within the scope of the evaluation: FTP, HTTP, and SMTP redirection.

The TSF follows a specific orderly algorithm to traverse the rule base for matching and filtering the traffic between its internal and external networks. Any traffic that is not explicitly accepted by the security policy is rejected by the firewall. The structure of the rule base and the capabilities of its associated protocol agents enable the TSF to make the information flow control decisions defined in FDP_IFF.1.2 through FDP_IFF.1.5.

Each rule comprises matching criteria and target actions. If the matching criteria is verified (i.e., a comparison matches) the TSF applies the target actions. The TSF compares the information attributes defined in FDP_IFF.1.1 with the matching criteria of the rule to determine whether apply the rule. If applied the target actions are implemented and the additional capabilities and flow control rules defined in FDP_IFF.1.2 through FDP_IFF.1.5 are applied.

The rulebase is read from top down, and when the first matching rule is encountered the search stops and the TOE executes the matching rule. There are two exceptions to this:

a) jump rule - this makes the search jump to a sub-rulebase if the jump rule matches. The search will continue inside the sub-rulebase until it either finds a matching rule or comes back empty-handed from the sub-rulebase and continues searching through the main rulebase;

b) continue rule - when it matches, it will set some variables and then the search continues.

The TOE relies on the operating system to provide the time for making the control decisions on the time-based information flow.

7.2.2 Network Address Translation (NAT)

When configured for static mapping NAT, the TOE provides a mechanism to ensure the real addresses on the internal networks are hidden. Static mapping is a one to one mapping and provides a means to determine the IP address number that is chosen.

Activation of NAT is done per connection based on the rule base. The TOE rewrites the headers of IP packets. It is a two-way process and keeps track of the source and destination addresses and can do a reverse translation to returning packets.

The NAT manipulation occurs after a connection has been accepted so that connection decisions are based on the original addresses. Routing takes place after the connection has been modified. NAT rules can be defined independently of access rules.

7.2.3 Management of TOE functions and data

Security management defines the protection and management mechanisms of the TOE. The management interface to the TOE is via the Management Server (a non-human user from the TOE perspective). This interface provides the functionality required for administrators to manage the trusted data and security attributes for the security functions. The TOE maintains a single role, Management Server, and the use of its interface implicitly defines the role.

The TOE implements consistency checking on the trusted data received through the Management Server interface to ensure only consistent values are accepted. The Management Server authenticates the human administrator.

The TOE enforces restrictive default values for information flow security attributes. Any traffic that is not explicitly accepted by the security policy is rejected by the firewall. The TSF applies the security policy to restrict the ability to modify the security attributes and the TSF data to the Management Server. An authorized human administrator must successfully log into the Management Server to modify the configuration to permit the flow of information.

7.2.4 High availability

As part of a firewall cluster the TOE provides high availability of the firewall security services defined in the firewall security policy. Up to 16 firewall nodes can form a cluster. The evaluated configuration assumes the cluster uses a dedicated and secure network. In case a firewall node in a cluster has a hardware malfunction, or can't recognize its security policy, or a failure of an interface to an internal, external, management or cluster network, the firewall engine is capable of failing over all sessions to other nodes. This provides continuous enforcement of the firewall security policy including information flow control.

The TOE's clustering subsystem implements the high availability security feature. The clustering subsystem includes a set of proprietary protocols to communicate among the nodes of a cluster to communicate the following state information:

- Which nodes are online;
- What is the capacity of each online node;
- What is the load of each node;
- The following firewall state is exchanged:
    - Current connections
    - Active authentications

ANNEX A ACRONYMS

3DES	Triple DES (Data Encryption Standard)
AES	Advanced Encryption Standard
CA	Certificate Authorities
CBC	Cipher Block Chaining
CC	Common Criteria for IT Security Evaluation
CM	Configuration Management
CVI	Cluster Virtual interface
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FIPS	Federal Information processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
GNU	GNU’s Not Unix (recursive)
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation
NIAP	National Information Assurance Partnership
NIC	Network interface Card
NDI	Node Detected Interface
PFS	Perfect Forward Secrecy
PKCS	Public Key Cryptography Standards
RFC	Request For Comments
RSA	Rivest, Shamir and Adleman
SF	Security Function
SHA	Secure Hashing Algorithm
SFP	Security Function Policy
SGW	Security Gateway
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions

TSP	TOE Security Policy
UDP	User Datagram Protocol
VAR	Value-Added Reseller
VPN	Virtual Private Network
VPNC	VPN Consortium

ANNEX B TERMINOLOGY

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 decrypt 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, which 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.

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.

ANNEX C REFERENCES

Stonesoft Documentation

[1] Stonesoft StoneGate Administrator’s Guide, Version 5.2.

[2] Stonesoft StoneGate Reference Guide, Version 5.2.

[3] Stonesoft StoneGate Installation Guide, Version 5.2.

Standards

[4] Common Criteria for Information Technology Security Evaluation, CCMB-2009-07, Version 3.1, Revision 3, July 2009.

[5] NIAP Interpretation 0414, Site-configurable prevention of audit loss, Effective date 4 January 2002

[6] Internet Engineering Task Force, File Transfer Protocol, RFC 959, October 1985.

[7] Internet Engineering Task Force, Simple Mail Transfer Protocol, RFC 959, August 1982.

[8] Internet Engineering Task Force, Hypertext Transfer Protocol, RFC 2616, June 1999.

ANNEX D NETWORK INTERFACE CARDS

The following network interface cards are available with appliances that are within the scope of the evaluation:

FW-315

4 x 10/100/1000 Mbit/s Intel 82574L ports

FW-1301

4 x 10/100/1000 Mbit/s Intel 82574L and 2 x 10/100/1000 Mbit/s Intel 82576EB ports

In addition to that there is one PCI Express expansion slot for modules presented in the table below.

FW-3201

2 x 10/100/1000 Mbit/s Intel 82576EB ports onboard

In addition to that there are three PCI Express expansions slots for modules presented in the table below.

FW-3205

2 x 10/100/1000 Mbit/s Intel 82576EB ports onboard

In addition to that there are three PCI Express expansions slots for modules presented in the table below.

Module	**Ports**	**Code**
GE6	6 x 10/100/1000 Mbit/s Intel 82576EB	MOD-EM1-GE-6
GE4SFP	4 x SFP transceiver openings for SFP transceivers presented in the table below	MOD-EM1-GE-SFP-4
10GSFP2	2 x SFP+ transceiver openings for SFP+ transceivers presented in the table below	MOD-EM1-10G-SFP-2

Transceiver	**Port**	**Code**
TX SFP	10/100/1000 Mbit/s copper	MOD-SFP-GE-TX
SX SFP	1000 Mbit/s multi-mode fiber	MOD-SFP-GE-SX
LX10 SFP	1000 Mbit/s single-mode fiber	MOD-SFP-GE-LX10
SR SFP+	10 Gbit/s multi-mode fiber	MOD-SFP-10G-SR
LR SFP+	10 Gbit/s single-mode fiber	MOD-SFP-10G-LR