Stonesoft Corporation

StoneGate Firewall/VPN

Version 4.2.2 Build 5708.cc3.1

COMMON CRITERIA

SECURITY TARGET

VERSION 1.3

19 February 2010

Stonesoft Corporation
Itälahdenkatu 22 A, FIN-0210 Helsinki, Finland

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET IDENTIFICATION

TOE Identification: Stonesoft StoneGate Firewall/VPN version 4.2.2 build 5708.cc3.1

ST Title: Stonesoft StoneGate Firewall/VPN Version 4.2.2 Build 5708.cc3.1 Common Criteria Security Target

ST Version: 1.3

Assurance level: EAL4, augmented with ALC_FLR.1, Basic flaw remediation

CC Version: 3.1 Revision 2

Keywords: Firewall, VPN, High Availability, Traffic Filter, Application Proxy

1.2 SECURITY TARGET OVERVIEW

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

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

The StoneGate Firewall/VPN 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.

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-addresses 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.

1.3 COMMON CRITERIA CONFORMANCE CLAIMS

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 2, September 2007.
  - 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 2, September 2007.
  - Part 3 conformant;
  - EAL4 augmented with ALC_FLR.1, Basic flaw remediation.

1.4 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.

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.

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

2 TOE DESCRIPTION

2.1 PRODUCT TYPE

The StoneGate firewall is a high availability firewall and VPN product for securing data communications and enabling continuous network connectivity. The firewall services include stateful packet filtering and application-level information flow control. The VPN services use a FIPS 140-2 validated cryptographic module. 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/VPN is the firewall component (or node) of the StoneGate product. The StoneGate product comprises a firewall engine, its operating system and data repository platform, cryptographic modules, and management system software. The firewall engine and its cryptographic module are included in the scope of the TOE. The management system and operating platforms are outside of the scope of the evaluation.

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 on Windows 2003, Windows XP, Red Hat Enterprise Linux (4.0 or 5.0) or Fedora Core (6 or 7).

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/VPN 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 2.1 below.

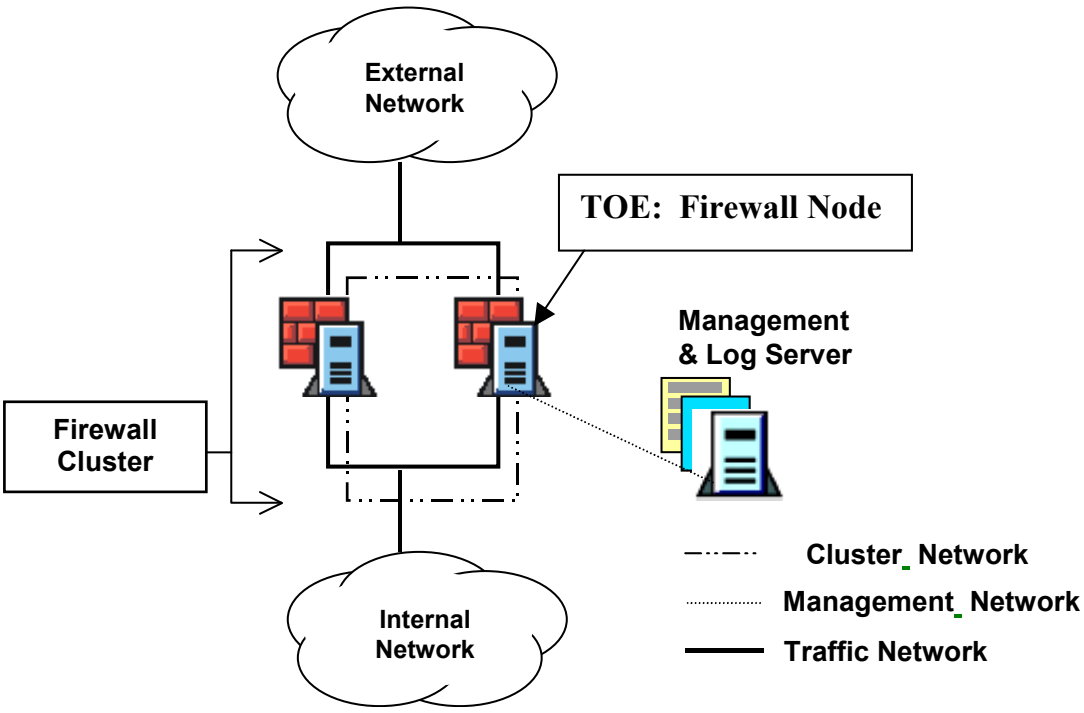

Figure 2.1 TOE Operating Environment

The following StoneGate models are included within the evaluation scope;

- FW-310 (desktop)
- FW-1020 (rackmount)
- FW-1030 (rackmount)
- FW-1050 (rackmount, same hardware as FW-1020, which is throughput-limited with license)
- FW-1200 (rackmount, faster CPU than FW-1050, otherwise same hardware)
- FW-5000 (rackmount)
- FW-5100 (rackmount, same hardware as FW-5000, which is throughput-limited with license)

2.2 TOE SECURITY FUNCTIONS

The Target of Evaluation (TOE) consists of the StoneGate Engine including the FIPS 140-2 validated StoneGate Firewall/VPN Core cryptographic module. It 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.

- **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 PUB 140-2 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 (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.

2.3 TOE SCOPE AND EVALUATED CONFIGURATION

As illustrated in Figure 2.2 below, the TOE boundary consists of:

- The Firewall/VPN Engine software application, version 4.2.2 build 5708.cc3.1; including:
- The FIPS 140-2 validated StoneGate Firewall/VPN Core cryptographic module (cert. #1263); including:
- The SafeNet QuickSec cryptographic toolkit, version 4.1.

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;
- VPN client policy download is disabled (consistent with the FIPS 140-2 validation);
- The cryptographic module is configured to be in FIPS 140-2 mode;
- The VPN policy parameters are configured to implement protocols and algorithms included in the TOE.

The IT environment for the evaluated configuration includes:

- TOE operating platform:
  - Intel Pentium 4 or higher (or equivalent) recommended
  - I GB RAM recommended,
  - Standard Linux Kernel 2.6.17.13 with minor modifications, Debian GNU/Linux 4.0 (etch) based distribution,
  - Network Interface Cards (see Annex A).
- StoneGate Management Center and supporting software, version 4.2:
  - the Management Server,
  - the Log Server;
  - the Graphical User Interface (GUI),
- OpenSSL 0.9.8 and OpenSSH (used on Firewall/VPN engine and Management Server),
- OpenLDAP client and server, version 2.3 (used on Firewall/VPN 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,
  - a third TOE used as a Security Gateway for VPN functionality.

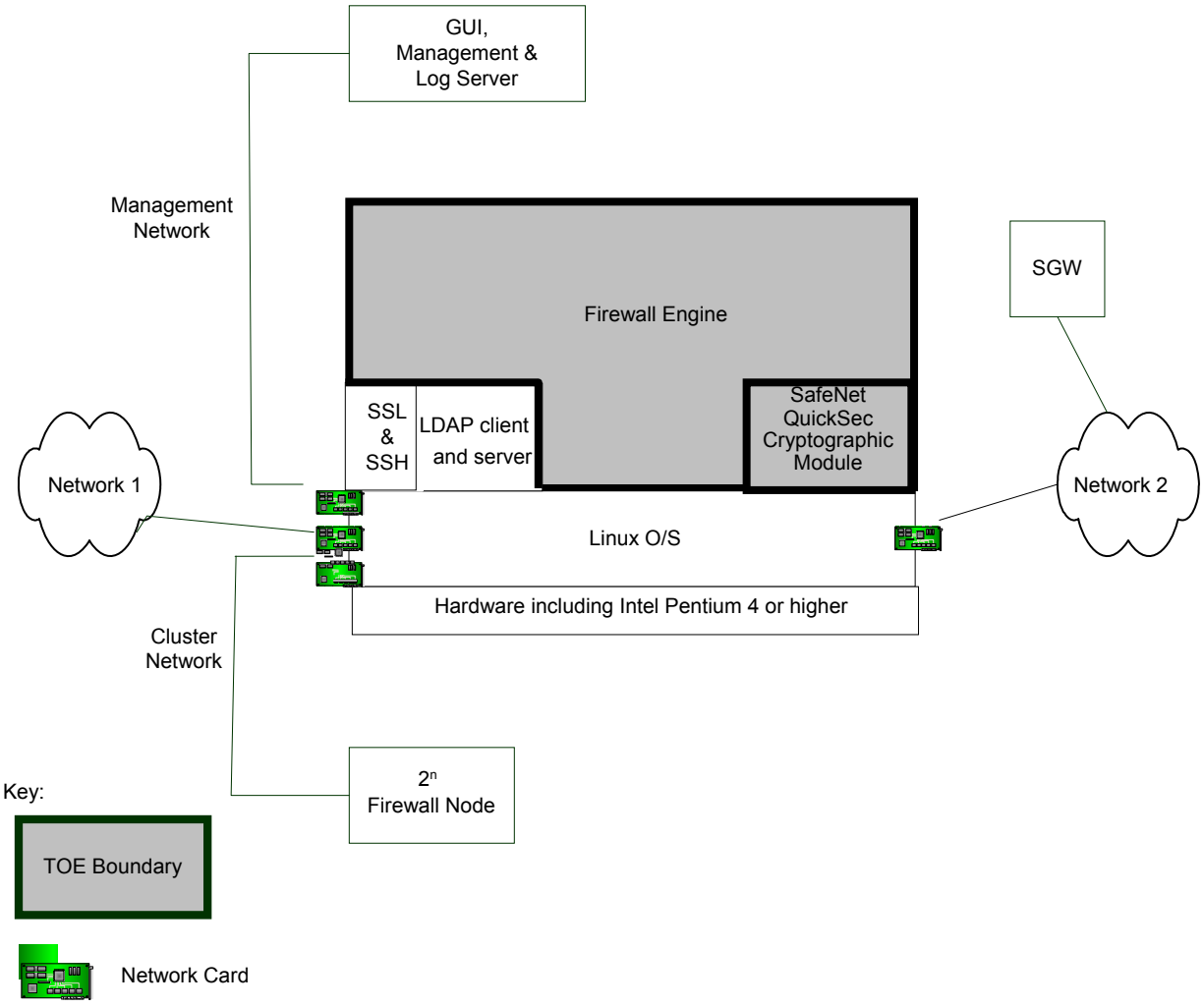

Figure 2.2 TOE Boundary and IT Environment

3 TOE SECURITY ENVIRONMENT

This section identifies the following:

- Secure usage assumptions,
- Organizational security policies, and
- Threats to Security

3.1 SECURE USAGE ASSUMPTIONS

A.ADMIN_ACCESS: Administrator Access Support Provided by the IT Environment
The administrator accesses the TOE via the trusted Management Server on a trusted and separate management network. The administrator identifies and authenticates to the Management Server application.

A.ADMINTRUSTED: Administrator Attributes
Authorized Administrators are trained, qualified, non-hostile and follow all guidance.

Application Note: If a Value Added Reseller installs the TOE, the user must establish that A.ADMINTRUSTED is applicable to the VAR. The user may also reinstall the TOE and verify its integrity using the checksums on the Stonesoft web site, www.stonesoft.com.

A.AUDITMAN: Environment Audit Procedures
Procedures shall exist to ensure that the audit trails are regularly analyzed and archived.

A.AUDIT_SUPPORT: Audit Support Provided by the IT Environment
The IT environment shall generate audit records for the security functions on which the TOE depends from its environment. It will also provide protected permanent storage of the audit trails generated by the TOE, and it will also provide reliable timestamps for the audit records.

A.MEDIAT_SUPPORT: Information Flow Control Support Provided by the IT Environment
The IT environment of the TOE must 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. It must also 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.

A.MODEXP: Attack Level
The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

A.OPERATING_ENVIRONMENT: General IT Environment Support
The node on which the TOE runs 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.SHAREDSECRETKEY: Shared Secret Key Management
The key used for Shared Secret SGW authentication will be generated and entered in the TOE in accordance with organizational security policies and follow the guidance provided in the Administrator and User Guides. The key size must be greater than or equal to 80 bits. The destruction of the key will be in accordance with the organizational security policies and follow the guidance provided in the Administrator and User Guides.

A.USER_AUTH: User Authentication for Information Flow Control
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
The IT environment will provide a trusted time source that allows the accurate time stamping of audit records.

3.2 ORGANISATIONAL SECURITY POLICIES

P.CRYPTO: Crypto Services
The TOE shall use a cryptographic module for its cryptographic operations and associated key management that are compliant with FIPS PUB 140-2 (level 1).

3.3 THREATS TO SECURITY

The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself. The assets to be protected are the information and IT resources of the network being protected.

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 impermissible 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.NOAUTH: Authorization
An unauthorized person may attempt to bypass the security of the TOE, e.g., using a masquerade attack, so as to access the VPN security functions provided by the TOE.

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.SECURE_CONNECTION_COMPROMISE: VPN Compromise
A threat agent may attempt to read and/or modify data transmitted between the TOE and another Security Gateway (SGW).

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

4 SECURITY OBJECTIVES

4.1 SECURITY 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.CRYPTOSERVICES: Cryptographic Services
The TOE shall provide cryptographic operations to support the VPN services and its associated key management functions using a cryptographic module that is FIPS 140-2 level 1 compliant.

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

O.IDAUTH: I&A
The TOE must uniquely identify and authenticate the claimed identity of SGWs before granting access to VPN functions.

O.MEDIAT: Information Flow Control
The TOE must mediate the flow of all information between users and external IT entities, including SGWs, 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.

O.VPN: Virtual Private Network Services
The TOE must be able to protect the confidentiality of data transmitted between itself and SGWs via the use of encryption. The TOE must also be able to protect the integrity of data transmitted to a SGW and verify that the received data accurately represents the data that was originally transmitted via the use of encryption.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

The following lists the security objectives for the environment.

O.E.ADMIN_ACCESS: Administrator Access Support Provided by the IT Environment
The administrator accesses the TOE via the trusted Management Server on a trusted and separate management network. The administrator identifies and authenticates to the Management Server application.

O.E.ADMINTRUSTED: Administrator Attributes
Authorized Administrators are trained, qualified, non-hostile and follow all guidance.

O.E.AUDITMAN: Environment Audit Procedures
Procedures shall exist to ensure that the audit trails are regularly analyzed and archived.

O.E.AUDIT_SUPPORT: Audit Support Provided by the IT Environment
The IT environment shall generate audit records for the security functions on which the TOE depends from its environment. It will also provide protected permanent storage of the audit trails generated by the TOE, and it will also provide reliable timestamps for the audit records.

O.E.MEDIAT_SUPPORT: Information Flow Control Support Provided by the IT Environment
The IT environment of the TOE must 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. It must also 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.

O.E.MODEXP: Attack Level Protection
The TOE must demonstrate that it meets all of the assurance requirements defined in EAL4 augmented with ALC_FLR.1 in Part 3 of the CC. This means the TOE must be methodically designed, tested, and reviewed, and has undergone an independent vulnerability analysis to determine that it is resistant to penetration attacks performed by an attacker possessing enhanced-basic attack potential.

O.E.OPERATING_ENVIRONMENT: General IT Environment Support
The node on which the TOE runs 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.

O.E.SHAREDSECRETKEY: Shared Secret Key Management
The key used for Shared Secret SGW authentication will be generated and entered in the TOE in accordance with an organization's security policies and follow the guidance provided in the Administrator and User Guides. The key size must be greater than or equal to 80 bits. The destruction of the key will be in accordance with the organizational security policies and follow the guidance provided in the Administrator and User Guides.

O.E.USER_AUTH: User Authentication for Information Flow Control
The IT environment must provide a user authentication mechanism for the TOE to use when the firewall security policy requires users to authenticate before information can flow between the internal and external networks.

5 IT SECURITY REQUIREMENTS

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This section contains the security functional requirements (SFRs) for the TOE, listed in Table 5.1.

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

- Assignment – allows the specification of an identified parameter. Assignments are indicated by showing the value in square brackets, [assignment value].
- Selection – allows the specification of one or more elements from a list. Selections are indicated using italics in square brackets, [*selection value*].
- Refinement – allows the addition of detail to a requirement. Refinements are indicated using bold, **refinement**.
- Iteration – allows a component to be used more than once with varying operations. 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.

Table 5.1 – Functional Components

No.	Component	Component Name
Class FAU:		
1.	FAU_GEN.1	Audit data generation
2.	FAU_SEL.1	Selective Audit
3	FAU_STG.1	Protected audit trail storage
4.	FAU_STG.NIAP-0414[1]	Site-Configurable Prevention of audit loss
Class FCS: Cryptographic support		
5.	FCS_CKM.1+1	Cryptographic key generation: 3DES
6.	FCS_CKM.1+2	Cryptographic key generation: AES
7.	FCS_CKM.1+3	Cryptographic key generation: RSA
8	FCS_CKM.4	Cryptographic key destruction
9.	FCS_COP.1+1	Cryptographic operation: 3DES
10.	FCS_COP.1+2	Cryptographic operation: AES
11.	FCS_COP.1+3	Cryptographic operation: HMAC-SHA-1

[1] Extended component.

12.	FCS_COP.1+4	Cryptographic operation: RSA
13.	FCS_COP.1+5	Cryptographic operation: Diffie-Hellman
14.	FCS_COP.1+6	Cryptographic operation: SHA-1
Class FDP: User Data Protection		
15.	FDP_IFC.1	Subset information flow control
16.	FDP_IFF.1	Simple security attributes
17.	FDP_UCT.1	Basic data exchange confidentiality
18.	FDP_UIT.1	Data exchange integrity
Class FIA: Identification and Authentication		
19.	FIA_UAU.5	Multiple authentication mechanisms: For SGWs
Class FMT: Security Management		
20.	FMT_MSA.1	Management of security attributes
21.	FMT_MSA.2	Secure security attributes
22.	FMT_MSA.3	Static attribute initialization
23.	FMT_MTD.1	Management of TSF data
24.	FMT_SMF.1	Specification of management functions
25.	FMT_SMR.1	Security roles
Class FPT: Protection of the TOE Security Functions		
26.	FPT_FLS.1	Failure with preservation of secure state
Class FRU: Resource Utilization		
27.	FRU_FLT.2	Limited fault tolerance
Class FTP: Trusted path/channels		
28.	FTP_ITC.1	Inter-TSF trusted channel

5.1.1 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

c) [the events in Table 5.2].

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 5.2].

Table 5.2 – TOE Auditable Events

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
FDP_UCT.1	The identity of any user or subject using the data exchange mechanisms.	None
FDP_UIT.1		
FIA_UAU.5	Success or failure of IKE negotiation.	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
FTP_ITC.1	Failure of the trusted channel functions.	Identifier of Peer Gateway

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.]

TOE Summary Specification - 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. 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.

5.1.2 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.
- 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.

TOE Summary Specification – 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.

[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.

- 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.

5.1.3 Cryptographic Support

FCS_CKM.1+1 Cryptographic key generation: 3DES

FCS_CKM.1+1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Triple Data Encryption Standard (3DES) in TCBC mode and Keying Option 1: Three-key Triple DES] and specified cryptographic key sizes [168 bits] that meet the following: [FIPS 46-3 and FIPS 140-2 level 1].

FCS_CKM.1+2 Cryptographic key generation: AES

FCS_CKM.1+2.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Advanced Encryption Standard (AES) in CBC] and specified cryptographic key sizes [128 bits] that meet the following: [FIPS 197 and FIPS 140-2 level 1].

FCS_CKM.1+3 Cryptographic key generation: RSA

FCS_CKM.1+3.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [512-2048 bits] that meet the following: [PKCS#1 and FIPS 140-2 level 1].

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 - The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [which zeroizes all plaintext cryptographic keys] that meets the following: [FIPS 140-2, level 1].

FCS_COP.1+1 Cryptographic operation: 3DES

FCS_COP.1+1.1 The TSF shall perform [

a) IPSec Security Association data encryption/decryption specified by IKE in RFC 2409 as defined in the TOE security policy; and

b) IPSec ESP bulk data encryption/decryption specified in RFC 2406 as defined in the TOE security policy]

in accordance with a specified cryptographic algorithm [Triple Data Encryption Standard (3DES) in TCBC mode and Keying Option 1: Three-key Triple DES] and cryptographic key sizes [168 bits] that meet the following: [FIPS 46-3 and FIPS 140-2 level 1].

FCS_COP.1+2 Cryptographic operation: AES

FCS_COP.1+2.1 The TSF shall perform [

a) IPsec Security Association data encryption/decryption specified by IKE in RFC 2409 as defined in the TOE security policy; and

b) IPsec ESP bulk data encryption/decryption specified in RFC 2406 as defined in the TOE security policy]

in accordance with a specified cryptographic algorithm [Advanced Encryption Standard (AES) in CBC mode] and cryptographic key sizes [128 bits] that meet the following: [FIPS 197 and FIPS 140-2 level 1].

FCS_COP.1+3 Cryptographic operation: HMAC-SHA-1

FCS_COP.1+3.1 The TSF shall perform [

a) Keyed secure hash computation used in authentication with a pre-shared key as specified by IKE in RFC 2409 as defined in the TOE security policy;

b) Keyed secure hash computation used in authentication with digital signature and verification using RSA as specified by IKE in RFC 2409 as defined in the TOE security policy; and

c) Keyed secure hash computation used in IPSec ESP specified in RFC 2406, as defined in the TOE security policy]

in accordance with a specified cryptographic algorithm [HMAC-SHA-1] and cryptographic key sizes [>= 80 bits] that meet the following: [FIPS 198 and FIPS 140-2 level 1].

Application note: FIPS 198 states 'the size of the key, K, shall be equal to or greater than L/2, where L is the size of the hash function output'. This implies a key size of at least 80 bits since the size of the SHA-1 output is 160 bits. This also implies that pre-shared keys should be at least 80 bits, as specified in A.SHAREDSECRETKEY.

FCS_COP.1+4 Cryptographic operation: RSA

FCS_COP.1+4.1 The TSF shall perform [authentication with digital signature and verification as specified by IKE in RFC 2409 as defined in the TOE security policy] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [512 - 2048 bits] that meet the following: [PKCS#1 and FIPS 140-2 level 1].

FCS_COP.1+5 Cryptographic operation: Diffie-Hellman

FCS_COP.1+5.1 The TSF shall perform [IPSec IKE key establishment specified in RFC 2409] in accordance with a specified cryptographic algorithm [Diffie-Hellman] and cryptographic key sizes [IKE group 1 = 768 bits, group 2 = 1024 bits, and group 5 has a modulus of 1536 bits] that meet the following: [RFC 2409, VPNC conformance and FIPS 140-2 level 1].

FCS_COP.1+6 Cryptographic operation: SHA-1

FCS_COP.1+6.1 The TSF shall perform [secure hash computation] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes [N/A] that meet the following: [FIPS 180-2 and FIPS 140-2 level 1].

TOE Summary Specification – Cryptographic functionality
The TOE includes a FIPS 140-2 validated cryptographic module that provides cryptographic support for the VPN services. The FIPS 140-2 validation addresses the detailed workings of the cryptographic functionality and provides the assurance that only secure key values are accepted for the applicable algorithms. Please refer to the FIPS 140-2 security policy for this information. The VPNC http://www.vpnc.org/ provides details of their conformance requirements.

The cryptographic support provided by the TOE is defined in the security functional requirements:

- 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.

5.1.4 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: VPN, 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 address;
- port
- user identity

b) information security attributes:

- presumed address of source subject;
- presumed 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, 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 option or match of the matched rule specifies 'vpn', and the 'VPN matching' rules defined in FDP_IFF.1.3 are 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;
- VPN matching – if the connection arrived from the VPN specified (via IP address) in the rule or if the TOE can send it via the specified VPN, VPN matching will return a succeed to the rule 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 VPN the TOE will attempt to initiate a VPN tunnel based on VPN option specified in the rule and definitions of VPN tunnels in the security policy;
- 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 authorize an information flow based on the following rules: [no explicit authorization 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
- When the 'matching part' of the rules in the rule base matches the information security attribute values and the option or match of the matched rule specifies 'vpn', and the 'VPN matching' rules defined in FDP_IFF.1.3 fail. 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.]

TOE Summary Specification - Information flow control

The StoneGate Firewall/VPN 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.

TOE Summary Specification - 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.

5.1.5 VPN User data protection

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 The TSF shall enforce the [Firewall Information Flow Control SFP] to be able to [*transmit **and** receive*] user data in a manner protected from unauthorized disclosure.

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the [Firewall Information Flow Control SFP] to be able to [*transmit **and** receive*] user data in a manner protected from [*modification, insertion**, or** replay*] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [*modification*, *insertion **or** replay*] has occurred.

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF or **SGW***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [VPN service].

TOE Summary Specification - VPN User Data Protection

The VPN service includes the creation of encrypted communication channels and the definition of encryption policies. Either the TOE or a SGW can initiate the process to establish a VPN channel.

It operates in a tunnel mode among the gateways using the IPSec protocol set as defined in RFC 2401 to integrate the following security functions:

- Authentication: public key exchanges and certificates protect the identity of communicating parties (see authentication section I&A-1).
- Access control: VPN access is restricted by the firewall traffic filter and rule bases (see information flow control above).
- Confidentiality: encryption methods protect data from unauthorized parties
- Data integrity: digital signatures ensure that unauthorized attempts to tamper with data cannot go unnoticed.

The IPsec protocol suite specifies the use of encryption to provide authentication, integrity and confidentiality security services. The TOE uses the Encapsulating Security Payload (ESP) protocol to provide confidentiality, data origin authentication, and connectionless integrity.

The Gateways negotiate to establish tunnels – two unidirectional connections called Security Associations (SAs) used to securely transmit data. SAs provide the information required to support the VPN connection, keys, algorithms, modes, and lifetimes. The SAs are negotiated during the Internet Key Exchange (IKE) phases.

IKE negotiation consists of two separate phases, IKE Phase I and IKE Phase II. During IKE Phase I the Gateways authenticate each other and create a secure channel for further negotiation (IKE Phase II). Authentication is done using a certificate based public key method (RSA signature and verification) or with a Pre-shared key (using HMAC-SHA-1). Encryption keys are generated and exchanged using the Diffie-Hellman key agreement method for encryption during the IKE negotiation.

Two modes for IKE phase 1 are available:

- Main mode: This mode protects the identity of each communicating party. With this mode, the communicating parties exchange six packets representing the initial message and its reply. The first exchanges negotiate an agreement for the SAs based on IKE proposal; the second exchanges share Diffie-Hellman public keys and some required data; and, finally, the third exchanges authenticate the identities and all previously exchanged data.

- Aggressive mode: This mode does not protect the identity of the communicating parties. With this mode only three packets are exchanged in a more compact format. The first exchanges negotiate an agreement for the SAs, share Diffie-Hellman public keys with some required data, send unencrypted identities, and authenticate the remote party. The negotiation is concluded with a second unidirectional exchange that authenticates the initiator of the negotiation.

IKE Phase 2 negotiation establishes the encryption/decryption procedures for protecting the IP data traffic between the Gateways. It generates a pair of SAs, which contains information for protecting the IP traffic. The negotiation of IPsec SAs is encrypted using the keys already agreed in the IKE SAs. The generated IPsec tunnels are used for conveying securely the actual data traffic between security gateways. The SA specified for this phase sets the lifetime of the IPsec SAs.

VPN Policy Parameters

The security associations generated for the IKE and IPsec SAs broadly represent the encryption policy to be implemented. To add granularity to the encryption policy, authorized firewall administrators can specify the negotiation degree of security associations; Security Associations can be negotiated for each pair of communicating networks, hosts, protocols, or ports.

Symmetric Encryption Parameters: symmetric encryption is used to provide confidentiality of data during the SA negotiation based on IKE proposals and is used for encrypting/decrypting bulk data. The following symmetric algorithms can be specified:
- 3DES;
- AES;
- (DES is included in the product for interoperability but is not included in the evaluation.)

Data Integrity Parameters: the HMAC-SHA-1 keyed hash function is used to ensure the integrity of the data exchanged.

Authentication Parameters: certificate based public key methods are used to authenticate the Gateways to each other. The following algorithms can be specified for Gateway authentication:
- RSA signature;
- Pre-shared key.

Diffie-Hellman Parameters: The following two parameters can be set for computing Diffie-Hellman values in the IKE negotiation mode and the IPsec mode:
- Diffie-Hellman group for IKE;
- Diffie-Hellman group for Perfect Forward Secrecy (PFS).

Lifetime Parameters: the lifetime of the IKE and IPsec tunnels can be specified in terms of elapsed time and transferred data. Lifetime (minutes or KB) represents the overall time (or data volume) after which the opened tunnels are closed. If a new tunnel is needed, the negotiation process is started over again. When an IPsec tunnel expires, only Phase II negotiation is performed again based on the settings of the IPsec proposal and through the IKE negotiated tunnel. This process generates new key material to be used for the IPsec traffic. Similarly, IKE SAs are set to expire, but their lifetime is typically much longer than that of the IPsec SA since IKE SA negotiation is more complex.

5.1.6 Identification and Authentication

FIA_UAU.5 Multiple authentication mechanisms: For SGWs

FIA_UAU.5.1 The TSF shall provide [

a) Certificate-based, or

b) IKE authentication with Pre-shared key]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [the mechanism defined in the VPN Policy authentication parameters; and the following rules:

a) SGWs must be authenticated before granting access to VPN services;

b) The TSF performs no authentication on External IT entities or human users initiating information flow through the TOE. When required by the Firewall Security Policy the TOE uses the mechanisms from its IT environment to authenticate these users.]

TSS – Identification and authentication
The TOE provides the following Identification and Authentication mechanisms for SGWs to establish a VPN connection with the TOE:
Certificated-based using RSA digital signatures; and
IKE authentication with Pre-shared key.
SGWs and the TOE authenticate each other when establishing a VPN connection, i.e., tunnel. This is done during the IKE Phase 1of the IKE protocol. The certificate-based authentication method options are RSA signatures. The pre-shared key method uses the HMAC_SHA-1 cryptographic algorithm. Either side can initiate the connection, and based on the configuration setting, the appropriate authentication method is used. The FIPS 140-2 cryptographic module within the Gateway performs the required cryptographic operations.

5.1.7 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.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [access as listed in Table 5.3] the [data list in Table 5.3] to [roles in Table 5.3].

Table 5.3 – TSF Data Management

TSF DATA	Management Server Access	Other Users
Auditable events, log levels, and log spool policy;	*modify*	*none*
Security policy attributes	*modify*	*None*
NAT IP address translation table;	*modify*	*none*
Actions to be taken in case of audit storage failure;	*modify*	*none*
IP address for SGWs for VPN services;	*modify , delete*	*none*
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*	*none*
Cryptographic key management attributes;	*modify , delete*	*none*

The VPN Policy Parameters: • Confidentiality parameters • Integrity parameters; • Authentication parameters.	*modify , delete*	*none*

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) The VPN Policy Parameters including specifying cryptographic operations and the associated key management functions;

h) Configuring Firewall Information Flow policy including NAT, VPN matching, authentication matching;

i) Configuring information for SGW authentication for VPN access (i.e., IP addresses).]

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.

TOE Summary Specification - 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. An authorized human administrator must successfully log into the Management Server to modify the configuration to permit the flow of information.

The certification that the embedded cryptographic module is FIPS 140-2 compliant will provide the assurance that only secure key values are accepted for the cryptographic keys.

5.1.8 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.]

TOE Summary Specification – 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 and VPN services.

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:

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

5.2 TOE SECURITY ASSURANCE REQUIREMENTS

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 4 (EAL4) augmented with ALC_FLR.1, Basic flaw remediation.

Table 5.5 - Assurance Components

Assurance Class	Assurance Component ID	Assurance Component Name
Development		
5.2.1	ADV_ARC.1	Security architecture description
5.2.2	ADV_FSP.4	Complete functional specification
5.2.3	ADV_IMP.1	Implementation representation of the TSF
5.2.4	ADV_TDS.3	Basic modular design
Guidance Documents		
5.2.5	AGD_OPE.1	Operational user guidance
5.2.6	AGD_PRE.1	Preparative procedures
Life Cycle Support		
5.2.7	ALC_CMC.4	Production support, acceptance procedures and automation
5.2.8	ALC_CMS.4	Problem tracking CM coverage
5.2.9	ALC_DEL.1	Delivery procedures
5.2.10	ALC_DVS.1	Identification of security measures
5.2.11	ALC_FLR.1	Basic flaw remediation **(augmentation)**
5.2.12	ALC_LCD.1	Developer defined life-cycle model
5.2.13	ALC_TAT.1	Well-defined development tools
Tests		

5.2.14	ATE_COV.2	Analysis of coverage
5.2.15	ATE_DPT.2	Testing: security enforcing modules
5.2.16	ATE_FUN.1	Functional testing
5.2.17	ATE_IND.2	Independent testing – sample
Vulnerability Assessment		
5.2.18	AVA_VAN.3	Focused vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 PP CLAIMS

None.

7 RATIONALE

This section provides the rationale for completeness and the consistency of the Security Target.

7.1 SECURITY OBJECTIVES RATIONALE

This section includes the following:

- Table 8.1 shows that all of the secure usage assumptions, organizational security policies, and threats to security have been addressed by the objectives.
- Table 8.2 shows that each objective counters at least one assumption, policy, or threat.
- The rationale for each of these mappings.

Table 7.1 - Mapping the Security Environment to the Security Objectives

Policy/Threat/Assumptions	Objectives
T.AUDIT_UNDETECTED	O.AUDIT, O.E.AUDIT_SUPPORT, O.E.AUDITMAN
T.MEDIAT	O.MEDIAT, O.NETADDRHIDE, O.VPN, O.E.MEDIAT_SUPPORT, O.E.USER_AUTH
T.NOAUTH	O.IDAUTH
T.NODE_FAILURE	O.HIGHAVAILABILITY
T.SECURE_CONNECTION_COMPROMISE	O.MEDIAT, O.VPN, O.CRYPTOSERVICES
T.SELPRO	O.SECFUN, O.E.ADMIN_ACCESS
P.CRYPTO	O.CRYPTOSERVICES
A.ADMIN_ACCESS	O.E.ADMIN_ACCESS
A.ADMINTRUSTED	O.E.ADMINTRUSTED
A.AUDITMAN	O.E.AUDITMAN
A.AUDIT_SUPPORT	O.E.AUDIT_SUPPORT
A.MEDIAT_SUPPORT	O.E.MEDIAT_SUPPORT
A.MODEXP	O.E.MODEXP
A.OPERATING_ENVIRONMENT	O.E.OPERATING_ENVIRONMENT
A.SHAREDSECRETKEY	O.E.SHAREDSECRETKEY
A.USER_AUTH	O.E.USER_AUTH
A.TIME	O.E.AUDIT_SUPPORT

Table 7.2 - All IT Security Objectives for the TOE are Necessary

Objectives	Policy/Threat/Assumptions
Security Objectives for the TOE	
O.AUDIT	T.AUDIT_UNDETECTED
O.CRYPTOSERVICES	P.CRYPTO, T.SECURE_CONNECTION_COMPROMISE
O.HIGHAVAILABILITY	T.NODE_FAILURE
O.IDAUTH	T.NOAUTH
O.MEDIAT	T.MEDIAT, T.SECURE_CONNECTION_COMPROMISE

O.NETADDRHIDE	T.MEDIAT
O.SECFUN	T.SELPRO
O.VPN	T.MEDIAT, T.SECURE_CONNECTION_COMPROMISE
Security Objectives for the Environment	
O.E.ADMIN_ACCESS	A.ADMIN_ACCESS, T.SELPRO
O.E.ADMINTRUSTED	A.ADMINTRUSTED
O.E.AUDITMAN	A.AUDITMAN, T.AUDIT_UNDETECTED
O.E.AUDIT_SUPPORT	A.AUDIT_SUPPORT, T.AUDIT_UNDETECTED, A.TIME
O.E.MEDIAT_SUPPORT	A.MEDIAT_SUPPORT, T.MEDIAT
O.E.MODEXP	A.MODEXP
O.E.OPERATING_ENVIRONMENT	A.OPERATING_ENVIRONMENT
O.E.SHAREDSECRETKEY	A.SHAREDSECRETKEY
O.E.USER_AUTH	A.USER_AUTH, T.MEDIAT

7.1.1 Policies

P.CRYPTO: Crypto Services
The TOE shall use a cryptographic module for its cryptographic operations and associated key management that are compliant with FIPS PUB 140-2 (level 1).

P.CRYPTO is satisfied by ensuring that the cryptographic operations of the TOE are implemented using a cryptographic module that is FIPS 140-2 level 1 compliant, (O.CRYPTOSERVICES).

7.1.2 Threats

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.

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 (O.E.AUDIT_SUPPORT),
- An audit trail that can be effectively reviewed (O.E.AUDITMAN), and
- Reliable timestamps being available for the audit trail (O.E.AUDIT_SUPPORT).

T.MEDIAT: Information Flow Control
An unauthorized person may send impermissible 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 O.E.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),

- Confidentiality and integrity services are available for the information passing between the internal and external networks (O.VPN),
- No residual information is transmitted (O.E.MEDIAT_SUPPORT),
- Reliable timestamps being available for time-based information flow control decisions (O.E.MEDIAT_SUPPORT), and
- User authentication services available for information flow control decisions (O.E.USER_AUTH).

T.NOAUTH: Authorization
An unauthorized person may attempt to bypass the security of the TOE, e.g., using a masquerade attack, so as to access the VPN security functions provided by the TOE.

This threat is diminished by VPN functions only being available to SGWs after they have been identified and authenticated using a mechanism that protects against masquerade attacks (O.IDAUTH).

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 not available.

This threat is diminished high availability mechanisms for the information flow control and VPN services when the TOE is deployed as part of a firewall cluster (O.HIGHAVAILABILITY).

T.SECURE_CONNECTION_COMPROMISE: VPN Compromise
A threat agent may attempt to read and/or modify data transmitted between the TOE and another Secure Gateway (SGW).

This threat is diminished by:
- Ensuring VPN services are applied according to the firewall security policy to all information that flows between the internal and external networks (O.MEDIAT),
- Providing confidentiality and integrity services to all information transmitted between itself and SGWs when required by the firewall security policy (O.VPN), and
- Using cryptographic mechanisms to provide the integrity and confidentiality services (O.CRYPTOSERVICES).

T.SELPRO: Self Protection
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, O.E.ADMIN_ACCESS),

7.1.3 Assumptions

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.

7.2 SECURITY REQUIREMENTS RATIONALE

This section includes the following:

- Table 8.3 shows that all of the objectives have been met by the requirements.
- Table 8.4 shows that each requirement addresses at least one objective.
- The rationale for each of these mappings.

Table 7.3 - Security Objective to Requirements Mapping

Objectives	Requirements
O.AUDIT	FAU_GEN.1, FAU_SEL.1, FAU_STG.1, FAU_STG.NIAP-0414
O.CRYPTOSERVICES	FCS_CKM.1+1 through FCS_CKM.1+3, FCS_CKM.4 FCS_COP.1+1 through FCS_COP.1+6
O.HIGHAVAILABILITY	FPT_FLS.1, FRU_FLT.2
O.IDAUTH	FIA_UAU.5
O.MEDIAT	FDP_IFC.1, FDP_IFF.1
O.NETADDRHIDE	FDP_IFC.1, FDP_IFF.1
O.SECFUN	FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1
O.VPN	FDP_UCT.1, FDP_UIT.1, FTP_ITC.1

Table 7.4 - All Security Requirements for the TOE are Necessary

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
FCS_CKM.1+1	O.CRYPTOSERVICES
FCS_CKM.1+2	O.CRYPTOSERVICES
FCS_CKM.1+3	O.CRYPTOSERVICES
FCS_CKM.4	O.CRYPTOSERVICES
FCS_COP.1+1	O.CRYPTOSERVICES
FCS_COP.1+2	O.CRYPTOSERVICES
FCS_COP.1+3	O.CRYPTOSERVICES
FCS_COP.1+4	O.CRYPTOSERVICES
FCS_COP.1+5	O.CRYPTOSERVICES
FCS_COP.1+6	O.CRYPTOSERVICES
FDP_IFC.1	O.MEDIAT, O.NETADDRHIDE
FDP_IFF.1	O.MEDIAT, O.NETADDRHIDE
FDP_UCT.1	O.VPN
FDP_UIT.1	O.VPN
FIA_UAU.5	O.IDAUTH
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
FTP_ITC.1	O.VPN

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.

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.CRYPTOSERVICES: Cryptographic Services

The TOE shall provide cryptographic operations to support the VPN services and its associated key management functions using a cryptographic module that is FIPS PUB 140-2 level 1 compliant.

This objective is satisfied by requiring a FIPS 140-2 compliant cryptographic module that performs the cryptographic operations 3DES, AES, HMAC-SHA-1, RSA, Diffie-Hellman, SHA-1 (FCS_COP.1+1 through 6). To support these operations cryptographic key destruction is required (FCS_CKM.4), and key generation for 3DES, AES, RSA (FCS_CKM.1+1 through 3).

O.HIGHAVAILABILITY: High Availability

The TOE when operating as part of a firewall cluster must provide high availability of information flow control and VPN services, 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.IDAUTH: I&A

The TOE must uniquely identify and authenticate the claimed identity of SGWs before granting access to VPN functions.

This objective is satisfied by requiring SGWs to authenticate using either certificates or IKE with a pre-shared key (FIA_UAU.5).

O.MEDIAT: Information Flow Control

The TOE must mediate the flow of all information between users and external IT entities, including SGWs, 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: Hide Internal Network Addresses

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: Management Functions

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).

O.VPN: Virtual Private Network Services

The TOE must be able to protect the confidentiality of data transmitted between itself and SGWs via the use of encryption. The TOE must also be able to protect the integrity of data transmitted to a SGW and verify that the received data accurately represents the data that was originally transmitted via the use of encryption.

This objective is satisfied by requiring a communication channel with a SGW be available to provide a means for data to be transmitted and received in a manner that protects it from unauthorized disclosure, modification, insertion or replay (FTP_ITC.1, FDP_UCT.1 and FDP_UIT.1).

7.2.1 Assurance Rationale

The assurance level selected for the TOE EAL4 augmented with ALC_FLR.1 because it provides appropriate assurance measures for the expected application of the product. EAL4 ensures a product that is methodically designed, tested, and reviewed with maximum assurance from positive

security engineering based on good commercial development practices. It also requires a moderate to high level of independently assured security.

ALC_FLR.1 is an augmentation to the EAL4 requirements. ALC_FLR.1 is included to add assurance for flaw remediation which is a standard part of a product's life cycle.

7.2.2 Security Requirements are Justified

Table 7.5 – Functional Component Dependencies

No.	Component	Dependencies	Reference
1.	FAU_GEN.1	FPT_STM.1	IT-Environment
2.	FAU_SEL.1	FAU_GEN.1	1
		FMT_MTD.1	23
3	FAU_STG.1	FAU_GEN.1	1
4.	FAU_STG.NIAP-0414	FMT_MTD.1	23
		FAU_STG.1	3 and IT-Environment
5.	FCS_CKM.1+1:3DES	FCS_CKM.2 or	
		FCS_COP.1,	9
		FCS_CKM.4,	8
		FMT_MSA.2	21
6.	FCS_CKM.1+2:AES	FCS_CKM.2 or	
		FCS_COP.1,	10
		FCS_CKM.4,	8
		FMT_MSA.2	21
7.	FCS_CKM.1+3:RSA	FCS_CKM.2 or	
		FCS_COP.1	12
		FCS_CKM.4	8
		FMT_MSA.2	21
8.	FCS_CKM.4	FCS_CKM.1	5-7
		FMT_MSA.2	20
9.	FCS_COP.1+1:3DES	FCS_CKM.1	5
		FCS_CKM.4	8
		FMT_MSA.2	21
10.	FCS_COP.1+2:AES	FCS_CKM.1	6
		FCS_CKM.4	8
		FMT_MSA.2	21
11.	FCS_COP.1+3:HMAC-SHA-1	FCS_CKM.1	N/A. See A.SHAREDSECRETKEY Pre-shared key is manually entered.
		FCS_CKM.4	8
		FMT_MSA.2	21
12.	FCS_COP.1+4:RSA	FCS_CKM.1	7
		FCS_CKM.4	8
		FMT_MSA.2	21
13.	FCS_COP.1+5:Diffie-Hellman	FCS_CKM.1	N/A – DH includes key generation.
		FCS_CKM.4	8
		FMT_MSA.2	21
14.	FCS_COP.1+6:SHA-1	FCS_CKM.1	N/A – SHA-1 does not use keys

		FCS_CKM.4	N/A
		FMT_MSA.2	21
15.	FDP_IFC.1	FDP_IFF.1	16
16.	FDP_IFF.1	FDP_IFC.1	15
		FMT_MSA.3	22
17.	FDP_UCT.1	FTP_ITC.1	28
		FDP_IFC.1	15
18.	FDP_UIT.1	FDP_IFC.1	15
		FTP_ITC.1	28
19.	FIA_UAU.5	None	N/A
20.	FMT_MSA.1	FDP_IFC.1	15
		FMT_SMR.1	25
		FMT_SMF.1	24
21.	FMT_MSA.2	FDP_ACC.1 or	
		FDP_IFC.1	15
		FMT_MSA.1	20
		FMT_SMR.1	25
22.	FMT_MSA.3	FMT_MSA.1	20
		FMT_SMR.1	25
23.	FMT_MTD.1	FMT_SMR.1	25
		FMT_SMF.1	24
24.	FMT_SMF.1	None	N/A
25.	FMT_SMR.1	FIA_UID.1	IT-Environment
26.	FPT_FLS.1	None	N/A
27.	FRU_FLT.2	FPT_FLS.1	26
28.	FTP_ITC.1	None	N/A

7.2.3 Justification for explicit requirements

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 nearly full. The format of the new component follows the Part 2 model. The extended component is a member of the class FAU, and is hierarchical to FAU_STG.4.

7.2.4 Rationale for SAR Dependencies

EAL4 augmented with ALC_FLR.1 Basic flaw remediation. ALC_FLR.1 has no dependencies.

7.3 RATIONALE FOR PP CONFORMANCE

This ST makes no claims of conformance with any PP.

8 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

9 REFERENCES

Stonesoft Documentation

[1] Stonesoft StoneGate Administrator's Guide, Version 4.2.

[2] Stonesoft StoneGate Reference Guide, Version 4.2.

[3] Stonesoft StoneGate Installation Guide, Version 4.2.

[4] StoneGate Firewall/VPN Core FIPS 140-2 Security Policy, Version 1.2, January 20, 2010.

Standards

[5] *Common Criteria for Information Technology Security Evaluation,* CCMB-2007-09, Version 3.1, Revision 2, September 2007.

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

[7] Federal Information Processing Standard Publication (FIPS-PUB) 46-3, *Data Encryption Standard (DES),* October 1999.

[8] Federal Information Processing Standard Publication (FIPS-PUB) 140-2, *Security Requirements for Cryptographic Modules,* May 25, 2001.

[9] Federal Information Processing Standard Publication (FIPS-PUB) 180-2, *Secure Hash Standard,* August 1, 2002.

[10] Federal Information Processing Standard Publication (FIPS-PUB) 186-2, *Digital Signature Standard,* June 27, 2000.

[11] Federal Information Processing Standard Publication (FIPS-PUB) 197, *Advanced Encryption Standard,* November 26, 2001.

[12] Internet Engineering Task Force, *IP Encapsulating Security Payload (ESP),* RFC 2406, November 1998.

[13] Internet Engineering Task Force, *Internet Key Exchange (IKE),* RFC 2409, November 1998.

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

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

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

[17] RSA Security Inc., *PKCS #1, version 2.0*, July 2000.

ANNEX A – NETWORK INTERFACE CARDS

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

FW-310
4 x 10/100/1000 Intel 82573L ports

FW-1020
Motherboard 4 integrated NICs
http://www.supermicro.com/products/motherboard/Xeon3000/3000/PDSMi-LN4+.cfm
in addition to that there is one dual NIC card
PWLA8492MT (PCI-X)
http://www.intel.com/products/server/adapters/pro1000mt-dualport/pro1000mt-dualport-overview.htm

FW-1030
6 x 10/100/1000 Intel 82573L ports

FW-1050
http://www.supermicro.com/products/motherboard/Xeon3000/3000/PDSMi-LN4+.cfm
in addition to that there is one quad NIC card
PWLA8494GT (PCI-X)
http://www.intel.com/network/connectivity/products/pro1000gt_quadport_server_adapter.htm
or fiber version of it
PWLA8492MF (PCI-X)
http://www.intel.com/network/connectivity/products/pro1000mf_dual_server_adapter.htm

FW-1200
http://www.supermicro.com/products/motherboard/Xeon3000/3000/PDSMi-LN4+.cfm
in addition to that there is one dual NIC card
PWLA8494GT (PCI-X)
http://www.intel.com/network/connectivity/products/pro1000gt_quadport_server_adapter.htm
or fiber version of it
PWLA8492MF (PCI-X)
http://www.intel.com/network/connectivity/products/pro1000mf_dual_server_adapter.htm

FW-5000
Two Intel onboard NICs
X7DBE
http://www.supermicro.com/products/motherboard/Xeon1333/5000P/X7DBE.cfm
and in addition several NICs as presented in table below.

FW-5100
Two Intel onboard NICs
X7DBE
http://www.supermicro.com/products/motherboard/Xeon1333/5000P/X7DBE.cfm
and in addition several NICs as presented in table below.

Motherboard	Copper	Fiber	Total	Code
FW-5000 **(2 x PCI-X and 3 x PCIe)**				
2 copper ports	20 ports 3 x Intel 4-port (EXPI9404PT) (PCIe) 2 x Intel 4-port (PWLA8494GT) (PCI-X)	0 ports	22 ports (0 fiber) (5C0F)	APP-FW-5000
2 copper ports	16 ports 3 x Intel 4-port (EXPI9404PT) (PCIe) 1 x Intel 4-port (PWLA8494GT) (PCI-X)	2 ports 1 x Intel 2-port (PWLA8492MF) (PCI-X)	20 ports (2 fiber) (4C1F)	APP-FW-5000F1
2 copper ports	12 ports 3 x Intel 4-port (EXPI9404PT) (PCIe)	4 ports 2 x Intel 2-port (PWLA8492MF) (PCI-X)	18 ports (4 fiber) (3C2F)	APP-FW-5000F2
2 copper ports	8 ports 2 x Intel 4-port (EXPI9404PT) (PCIe)	6 ports 2 x Intel 2-port fiber (PWLA8492MF) (PCI-X) 1 x Intel 2-port fiber (EXPI9402PF) (PCIe)	16 ports (6 fiber) (2C3F)	APP-FW-5000F3
2 copper ports	4 ports 1 x Intel 4-port (EXPI9404PT) (PCIe)	8 ports 2 x Intel 2-port fiber (PWLA8492MF) (PCI-X) 2 x Intel 2-port fiber (EXPI9402PF) (PCIe)	14 ports (8 fiber) (1C4F)	APP-FW-5000F4
2 copper ports	12 ports 3 x Intel 4-port (EXPI9404PT)	0 ports	14 ports (0 fiber) (3C0F)	APP-FW-5000L
2 copper ports	4 ports 1 x Intel 4-port (EXPI9404PT)	4 ports 2 x Intel 2-port fiber (EXPI9402PF)	10 ports (4 fiber) (1C2F)	APP-FW-5000LF2

FW-5100 **(1 x PCI-X and 3 x PCIe)**				
2 copper ports	16 ports 3 x Intel 4-port (EXPI9404PT) (PCIe) 1 x Intel 4-port (PWLA8494GT) (PCI-X)	0 ports	18 ports (0 fiber) (4C0F)	APP-FW-5100
2 copper ports	12 ports 3 x Intel 4-port (EXPI9404PT) (PCIe)	2 ports 1 x Intel 2-port fiber (PWLA8492MF) (PCI-X)	16 ports (2 fiber) (3C1F)	APP-FW-5100F1
2 copper ports	8 ports 2 x Intel 4-port (EXPI9404PT) (PCIe)	4 ports 1 x Intel 2-port fiber (PWLA8492MF) (PCI-X) 1 x Intel 2-port fiber (EXPI9402PF) (PCIe)	14 ports (4 fiber) (2C2F)	APP-FW-5100F2
2 copper ports	4 ports 1 x Intel 4-port (EXPI9404PT) (PCIe)	6 ports 1 x Intel 2-port fiber (PWLA8492MF) (PCI-X) 2 x Intel 2-port fiber (EXPI9402PF) (PCIe)	12 ports (6 fiber) (1C3F)	APP-FW-5100F3
2 copper ports	0 ports	8 ports 1 x Intel 2-port fiber (PWLA8492MF) (PCI-X) 3 x Intel 2-port fiber (EXPI9402PF) (PCIe)	10 ports (8 fiber) (0C4F)	APP-FW-5100F4