STONESOFT

FIPS 140-2 Validation Document

StoneGate Firewall/VPN Core
FIPS 140-2 Security Policy

Product version: 4.2.2.5708.cc3.1

Date: January 20, 2010

Document version 1.2

Table of Contents

Terms and Abbreviations

Term	Description
Firewall Node	Entity consisting of the hardware platform and all software included on the StoneGate Firewall/VPN appliance, including platform software.
Firewall Cluster	Cluster of *firewall nodes*.
Management Server	Provides central management services for controlling StoneGate Firewall/VPN appliances, *Log Servers* and StoneGate *IPS*.
Management Client	Provides a graphical user interface for controlling the *firewall nodes* through the *Management Server*.
Log Server	Receives log data from the StoneGate Firewall/VPN appliance.
IPS	Stonesoft Intrusion Prevention System
StoneGate Firewall/VPN product	A system that consists of three main components: a *firewall cluster*, a *Management Server* and a *Log Server*.
Firewall Node Software, Firewall Appliance software	The software residing on a *firewall node*. Includes the hardened Debian GNU/Linux platform 4.0 (etch) with Linux 2.6.17.13 kernel, the OpenSSL software version 0.9.8, the SafeNet QuickSec Toolkit and the *StoneGate Firewall/VPN software*, the software developed by Stonesoft.
StoneGate Firewall/VPN software	*Firewall node software* excluding the Debian GNU/Linux platform, Linux kernel, OpenSSL software and SafeNet QuickSec Toolkit.

StoneGate Firewall/VPN Core FIPS module	Part of the *firewall node software*, including the *StoneGate Firewall/VPN software* and SafeNet QuickSec Toolkit. The Debian GNU/Linux platform and the OpenSSL software are excluded.
Crypto Officer Role A	Local Crypto Officer Role (has physical access to the *firewall node* and is able to use console services).
Crypto Officer Role B	Entity that uses services provided for Crypto Officer Role B

Table 1 Description of Terms

1. Introduction

This document is the non-proprietary FIPS 140-2 security policy for the StoneGate Firewall/VPN Core module.

StoneGate Firewall/VPN provides IPsec compliant VPN connectivity between two firewall clusters (site to site connectivity) and between remote VPN clients and the firewall cluster. The VPN solution is based on the IPsec standard defined in RFC 2401.

The StoneGate Firewall/VPN product consists of three main components: a firewall cluster, a Management Server and a Log Server (Figure 1). A firewall cluster consists of one or more firewall nodes. In addition to these components, it is possible to use an external StoneGate Intrusion Prevention System (IPS) with the product. All of the components operate on separate computers and communicate over a network.

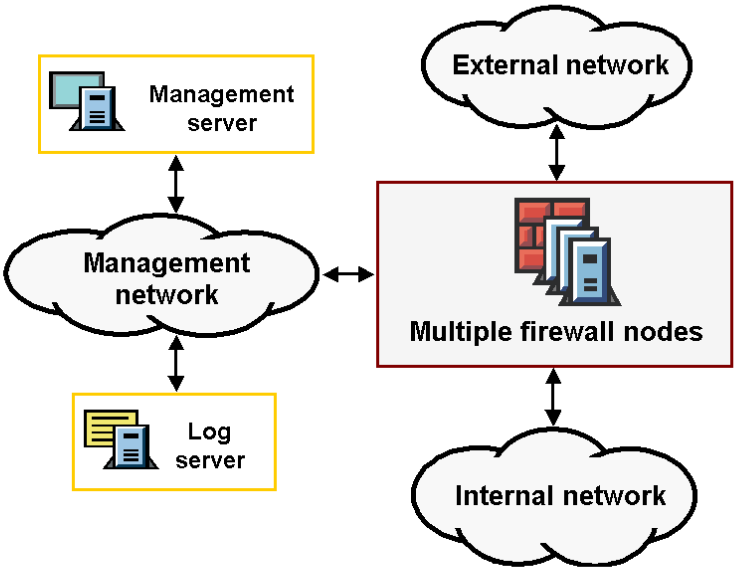


Figure 1 Example setup for the StoneGate Firewall/VPN product

2. Cryptographic Module and Cryptographic Boundary

2.1 General

In FIPS 140-2 terms, the StoneGate Firewall/VPN Core is a firmware module that is considered as a multiple-chip standalone cryptographic module for the purposes of FIPS 140-2 validation. The physical StoneGate Firewall/VPN Core FIPS module consists of a single firewall device of the StoneGate Firewall/VPN product. The StoneGate Management Server, Log Server and IPS are outside the StoneGate Firewall/VPN Core FIPS module boundary. The StoneGate Firewall/VPN Core FIPS module meets the level 1 requirements of FIPS publication 140-2.

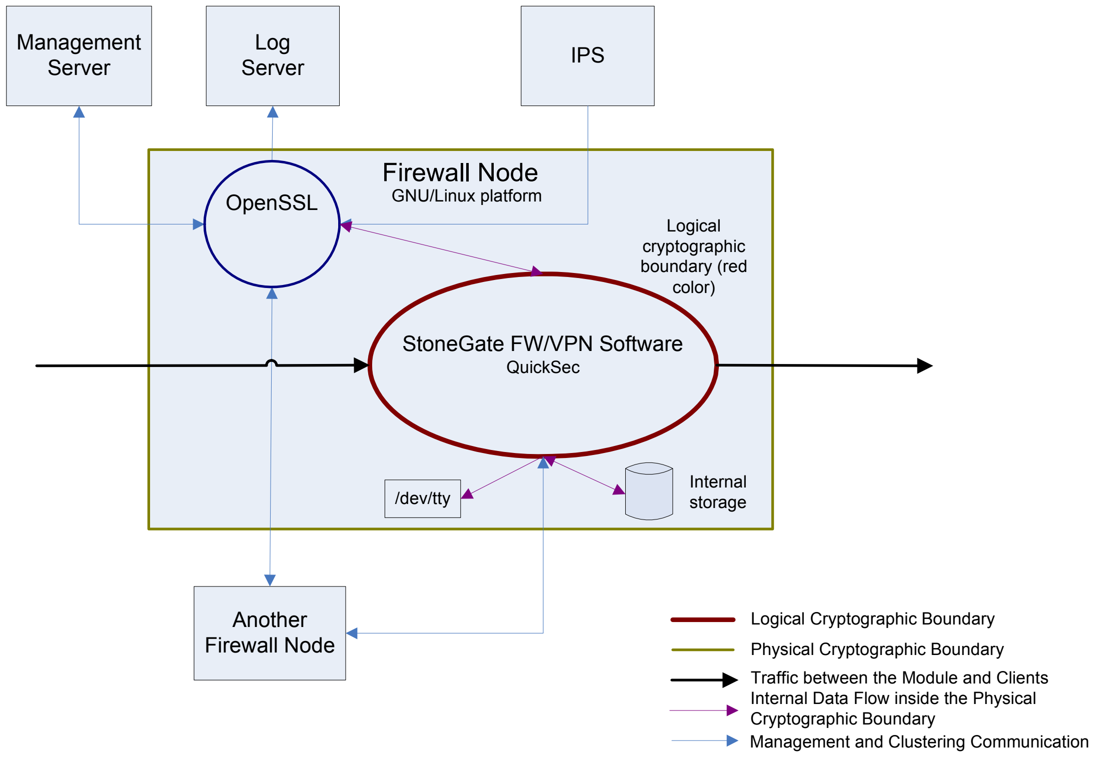
Table 2 lists the FIPS 140-2 validation level for each individual section.

Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key management	1
Electromagnetic Interface/Electromagnetic Compatibility (EMI/EMC)	1
Self-tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 2 Validation level by section

The cryptographic module can be run on standard Intel-based hardware platforms on top of a hardened Debian GNU/Linux Operating System delivered with the StoneGate Firewall/VPN product. The product can be installed from the product CD-ROM or some other mass storage device. The cryptographic module is installed as executable code.

2.2 Cryptographic Boundary


Management Server
Log Server
IPS
Firewall Node
GNU/Linux platform
OpenSSL
Logical cryptographic boundary (red color)
StoneGate FW/VPN Software
QuickSec
/dev/tty
Internal storage
Another Firewall Node
Logical Cryptographic Boundary
Physical Cryptographic Boundary
Traffic between the Module and Clients
Internal Data Flow inside the Physical Cryptographic Boundary
Management and Clustering Communication

Note: Although not presented in the diagram, both the User Traffic and the Management Traffic flow through the platform TCP/IP Stack.

Figure 2 Logical boundary of the cryptographic module

The **physical cryptographic boundary** for the StoneGate Firewall/VPN Core FIPS module is the physical computer that hosts a StoneGate firewall node. The Management Server, Log Server and IPS are outside the cryptographic boundary.

All software on the physical computer, and thus included in the physical boundary, is delivered with the StoneGate Firewall/VPN product. The delivered software includes a hardened Debian GNU/Linux platform 4.0 (etch) with the Linux 2.6.17.13 kernel, the OpenSSL software version 0.9.8, SafeNet QuickSec Toolkit and the StoneGate Firewall/VPN software version 4.2.2.5708.cc3.1, the software developed by Stonesoft.

The StoneGate Firewall/VPN Core FIPS module's **logical cryptographic boundary** includes the SafeNet QuickSec Server Toolkit 4.1 and the StoneGate Firewall/VPN software. The Debian GNU/Linux platform software and OpenSSL are outside the logical boundary.

2.3 Cryptographic Module Description

The security services of the cryptographic module are provided by the integrated software. IPsec services for the clients of the module are built using the cryptographic software primitives implemented in SafeNet QuickSec Toolkit. To provide the needed Transport Layer Security (TLS) functionality for the management communications, Stonesoft has incorporated OpenSSL into its product.

The logical StoneGate Firewall/VPN Core FIPS module boundary excludes the OpenSSL and TLS functionality. From the point of view of FIPS, the services for the Crypto Officer Role B are the services the logical cryptographic module provides to the OpenSSL module and the clustering services, which are provided directly to the other nodes of the cluster. OpenSSL acts as a mediator between the Management Server and the logical StoneGate Firewall/VPN Core FIPS module, securing traffic between these parties. OpenSSL, with cryptographic services of its own, is a self-contained module within the physical cryptographic boundary. OpenSSL is not a part of the logical StoneGate Firewall/VPN Core FIPS module, but the availability of its services is included in the additional requirements that the logical StoneGate Firewall/VPN Core FIPS module sets for the operating environment. The StoneGate Firewall/VPN Core FIPS module assumes that Crypto Officer Role B is the entity using the services that the logical StoneGate Firewall/VPN Core FIPS module provides for Crypto Officer Role B.

The communications between the firewall node and the Management Server, between the firewall node and the Log Server, as well as between the firewall node and the IPS are secured using TLS. If the firewall cluster is configured according to Stonesoft's recommendations, the communications between the nodes of the cluster are further secured by isolating them in a physically separate network. The TLS services are outside the scope of StoneGate Firewall/VPN Core FIPS module validation, because these services are outside the logical StoneGate Firewall/VPN Core FIPS module boundary. From the point of view of FIPS, the TLS services are like a wrapper on top of the services the StoneGate Firewall/VPN Core FIPS module provides to the Crypto Officer

Role B. This is shown in Figure 3.

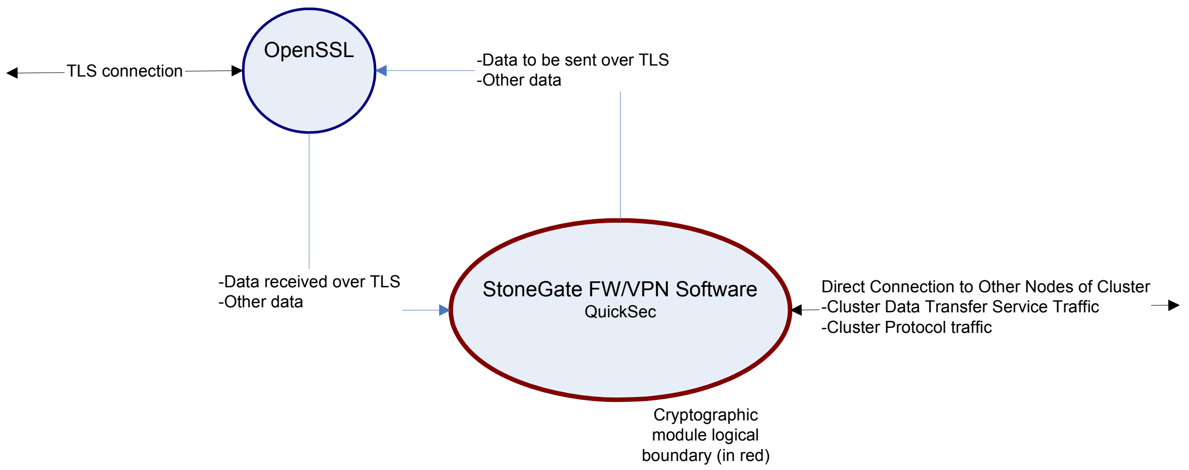

OpenSSL
TLS connection
-Data to be sent over TLS
-Other data
-Data received over TLS
-Other data
StoneGate FW/VPN Software
QuickSec
Direct Connection to Other Nodes of Cluster
-Cluster Data Transfer Service Traffic
-Cluster Protocol traffic
Cryptographic module logical boundary (in red)

Figure 3 Logical cryptographic module communicating with the Crypto Officer Role B

In addition to the OpenSSL module, the StoneGate Firewall/VPN Core FIPS module receives various data from other nodes of the cluster directly through the Linux network stack.

2.4 Rationale for Excluding OpenSSL

OpenSSL provides cryptographic services to the logical StoneGate Firewall/VPN Core FIPS 140-2 cryptographic module, but has been excluded from the logical cryptographic boundary. Communications between the physical StoneGate 140-2 cryptographic module and the Management Server, Log Server or IPS is protected using OpenSSL-provided TLS, but no CSP data is sent to these parties from the physical StoneGate 140-2 cryptographic module. Even a complete removal of the OpenSSL cryptographic services would not expose the CSP data that is transferred in the physically separate cluster network.

3. Module Interfaces

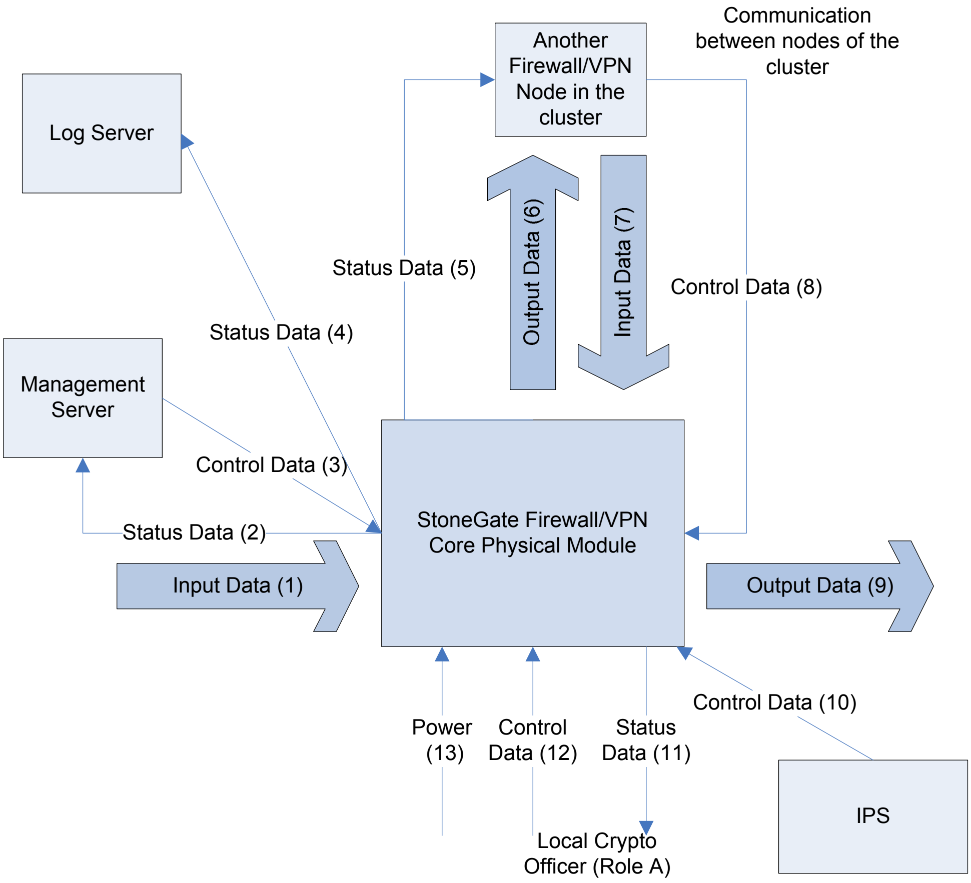


Figure 4 Data flow to the physical interfaces of the cryptographic module

Figure 4 shows the categorization of data flows between the physical cryptographic module and its counterparts.

The data input and data output flows are formed out of packets from normal clients of the module, i.e., packets that use the VPN and firewall services that the cryptographic module provides. These packets use the data input and data output interfaces of the module. The control data for the module's operation originates from the Management Server, the IPS and the other nodes of the cluster. Additionally, some control data originates from the OpenSSL module and some from the local Crypto Officer Role A. This control data as a whole is seen as Control Data from the Crypto Officers. Crypto Officers also receive status output data from the module. The traffic between the module and Crypto Officers forms the control input and status output data flows. There is an interface for normal clients, which acts as a data input and data output interface.

The management interface and the control interface for clustering functionality both act as control input and status output interfaces. Traffic between the cryptographic module and the Log Server, Management Server and IPS consists of control input and status output data only. Traffic between clustered firewall nodes consists of normal input and output data as well as control and status data. Network traffic between the cryptographic module and other parties consists of normal input data and normal output data (since remote SSH access for Crypto Officers is disabled in FIPS mode).

The cryptographic module separates network packets between the logically distinct interfaces mentioned above. The separation is based on an investigation of the packet source, destination, type and content.

The physical ports of the module are mapped to FIPS 140-2 logical interface types in Table 3. The logical interface numbers used in the table refer to the interfaces in Figure 4. In practice, the data between the module and the other parties flows mostly through the network ports.

Logical Interface	Physical Port
Data input interface (1, 7)	Network ports
Data output interface (6, 9)	Network ports
Control input interface (3, 8, 10, 12)	Network ports (3, 8, 10), serial ports, USB ports, keyboard controller port (12), power switch (12)
Status output interface (2, 4, 5, 11)	Network ports (2, 4, 5), serial ports, display controller port (11), LEDs/physical status indicators (11). LEDs indicate the following status information: • Power is being supplied to the appliance • Hard drive activity • Traffic on network interface 0 • Traffic on network interface 1 • Appliance overheating

	- Network interface activity and link status information about other network interfaces For more information about LEDs see the Appliance Installation Guide on the Stonesoft web site [6].
Power interface (13)	Power connector

Table 3 Mapping between physical ports and logical interfaces

The logical StoneGate Firewall/VPN Core FIPS module communicates with clients (normal input and normal output data) through the Linux network stack. Packets to be processed are accessed using Linux Netfilter hooks. The logical StoneGate Firewall/VPN Core FIPS module communications with OpenSSL, sending and receiving Cluster protocol service data, and sending and receiving Cluster Data Transfer service data are defined as communications with Crypto Officer Role B.

StoneGate Firewall/VPN Core FIPS module never sends any CSP data out from the appliance in plaintext form. Any CSP data that exits the logical cryptographic module is always secured through the IPsec protocol or delivered to the OpenSSL module that is within the physical cryptographic boundary.

3.1 Logical Module Interfaces

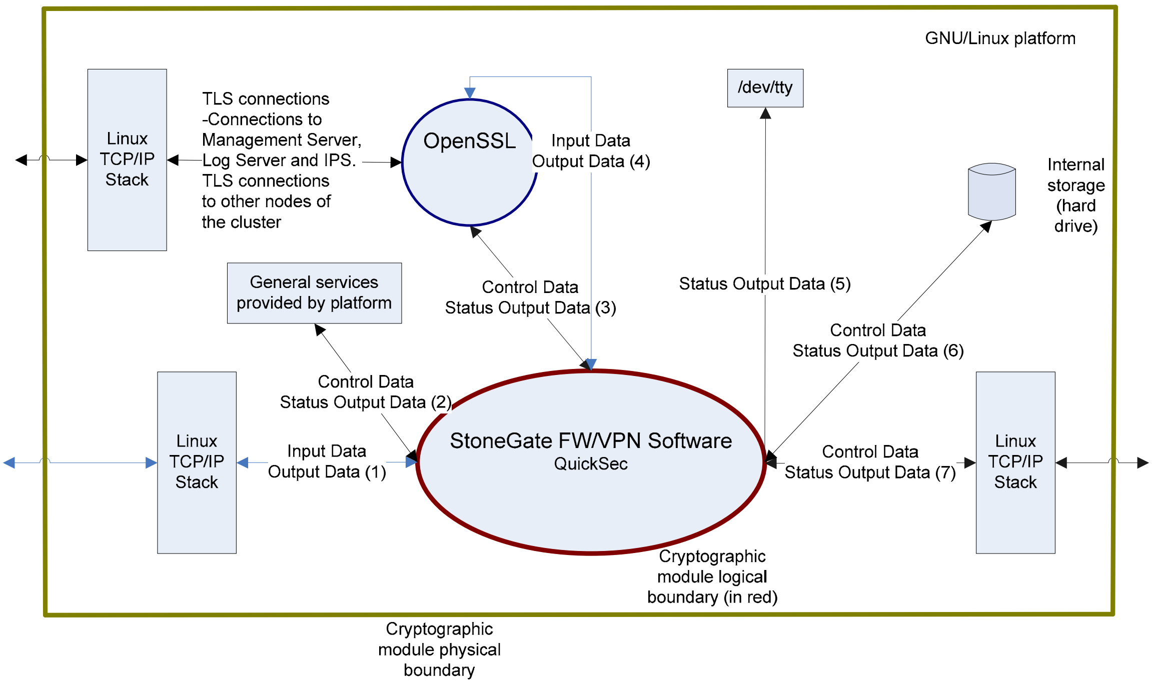

GNU/Linux platform
Linux TCP/IP Stack
TLS connections -Connections to Management Server, Log Server and IPS. TLS connections to other nodes of the cluster
OpenSSL
Input Data Output Data (4)
/dev/tty
Internal storage (hard drive)
General services provided by platform
Control Data Status Output Data (3)
Status Output Data (5)
Control Data Status Output Data (6)
Control Data Status Output Data (2)
Linux TCP/IP Stack
Input Data Output Data (1)
StoneGate FW/VPN Software
QuickSec
Control Data Status Output Data (7)
Linux TCP/IP Stack
Cryptographic module logical boundary (in red)
Cryptographic module physical boundary

Figure 5 Data flow to the logical interfaces of the cryptographic module

When providing VPN or bypass services, the StoneGate Firewall/VPN Core FIPS module communicates directly with clients of the module through the Linux network stack. Nodes in a cluster communicate directly through the Linux network stack when Cluster Protocol traffic or Cluster Data Transfer services are in question. TLS communications between the logical cryptographic module and clustered nodes as well as communications with the Management Server, Log Server, and IPS are not direct, but sent through the OpenSSL module. OpenSSL cryptographic primitives are also used directly for securing other data flows between the logical cryptographic module and other nodes of the cluster (Cluster Data Transfer).

The OpenSSL module relays Control Data from the Management Server, the Log Server, the IPS and the other nodes of the cluster to the logical StoneGate Firewall/VPN Core FIPS module and the status output from the logical StoneGate Firewall/VPN Core FIPS module to the parties mentioned. The logical StoneGate Firewall/VPN Core FIPS module also relays normal input and output data through OpenSSL when there is information to be sent to the other nodes of the cluster.

Additionally, the logical StoneGate Firewall/VPN Core FIPS module writes status output data directly into the console. This status output contains all error messages that indicate state changes in cases of cryptographic or other critical errors, and messages that indicate successful completion of FIPS power-up tests.

The internal storage (hard drive or flash memory) stores data that is considered as control data when read by the module and as status output data when written by the module.

The logical StoneGate Firewall/VPN Core FIPS module uses common platform services, such as the service for rebooting the appliance. The data exchange between the platform and the logical StoneGate Firewall/VPN Core FIPS module is defined as control data and status output data.

3.2 Categorization of Exact Logical Interfaces

The exact logical interfaces of the module are categorized as four distinct logical interfaces: data input, data output, control input and status output. The logical division of data flows into these interface categories is based on analyzing the source, destination, type and content of data.

Table 4 (below) details the categorization of exact logical interfaces. The numbering of logical interfaces refers to Figure 5.

Logical Interface Category	Logical Interface	Physical Port
Data input interface	IP packet interface for data input (1) IPsec interface for data input (1) IKE interface for data input (1) User authentication communications interface for data input (1) ARP interface for data input (1) SNMP interface for data input (1) State Synchronization interface for data input (1)	Network ports (via Linux TCP/IP Stack)

	Cryptographic primitives interface for data input (4)	No physical ports (communications between logical StoneGate cryptographic module and OpenSSL)
Data output interface	IP packet interface for data output (1) IPsec interface for data output (1) IKE interface for data output (1) User authentication communications interface for data output (1) ARP interface for data output (1) SNMP interface for data output (1) State synchronization interface for data input (1)	Network ports (via Linux TCP/IP Stack)
	Cryptographic primitives interface for data output (4)	No physical ports (communications between logical StoneGate cryptographic module and OpenSSL)

Control input interface	IP packet interface for control data input (7) Management communications interface for control data input (3) Configuration interface for control data input (3) Configuration import interface for control data input (3) Blacklist interface for control data input (3) Cluster protocol interface for control data input (7) State synchronization interface for control data input (7) Data synchronization interface for control data input (3) Key exchange interface for control data input (3) Connection monitoring interface for control data input (3)	Network ports (via Linux TCP/IP Stack)
	Platform services interface for control data input (2, 6).	No physical port. General services provided by the platform etc.
	Main management communications channel interface for control data input (3). Cryptographic primitives interface for control data input (3). Cryptographic utility program interface (3).	No physical port. Control data from OpenSSL.

	Initial configuration interface for control data input (5) Configuration import interface for control data input (5, 2)	Serial port (console usage via serial port). Enabled only during initialization. Configuration import from a USB device during initialization is also possible.
Status output interface	IP packet interface for status output data (7) Management communications interface for status output data (3) Configuration interface for status output data (3) Configuration import interface for status output data (3) Blacklist interface for status output data (3) Cluster protocol interface for status output data (7) State synchronization interface for status output data (7) Data synchronization interface for status output data (3) Key exchange interface for status output data (3) Connection monitoring interface for status output data (3) Unified Log and Alert Server (ULAS) interface (3)	Network ports (via Linux TCP/IP Stack)
	Initial configuration interface for status data output (5) Configuration import interface for status data output (5)	Serial port (console usage via serial port). Enabled only during initialization.

	Main management communication channel interface for status data output (3). Cryptographic primitives interface for status data output (3). Cryptographic Utility Program Interface (3).	No physical port. Interface to OpenSSL.
	Platform services interface for status output (2, 5, 6).	No physical port except the console for informative printouts. General services provided by platform etc.
	Physical hardware status interface	LEDs
Power interface	Power interface	Power connector

Table 4 Interface Categorization

4. Rules of Operation

The following set of rules provides additions to the basic rules of FIPS 140-2. To run the StoneGate FIPS module in FIPS approved manner, the following requirements must be fulfilled:

- A compatible version of OpenSSL software must be used.
- The operating environment must be non-modifiable.
- The StoneGate Firewall/VPN product integrates the operating environment and the OpenSSL software. The StoneGate FIPS module must be used with the integrated operating environment and the integrated OpenSSL software.
- The StoneGate Firewall/VPN software must be initialized into the FIPS mode of operation according to guidance given in this document.

The last two requirements, when fulfilled, actually satisfy the preceding two requirements as well.

5. Supported Algorithms

The module supports several security levels for the IKE/IPsec services. To be FIPS compliant, a security level of at least 80 bits must be used. For the IKE/IPsec services provided to the actual users of the module, the module supports the following FIPS-approved digital signature algorithms, symmetric encryption algorithms, hash algorithms, message authentication codes and random number generators implemented in SafeNet QuickSec Toolkit:

- **DSA** (FIPS 186-2, Cert. #340). Provides 80 bits of security; non-compliant if used with less than 80 bits of security. Key size of 1024 bits corresponds to 80 bits of security.
- **RSA** (PKCS#1, authentication, Cert. #474). Provides between 80 and 112 bits of security; non-compliant if used with less than 80 bits of security. Key sizes of 1024–2048 bits correspond to 80–112 bits of security.
- **AES-128-CBC** (FIPS 197, Cert. #984).
- **AES-192-CBC** (FIPS 197, Cert. #984).
- **AES-256-CBC** (FIPS 197, Cert. #984).
- **Triple-DES-CBC** (FIPS 46-3, Cert. #772).
- **SHA-1** (FIPS 180-2, Cert. #953).
- **HMAC-SHA-1** (FIPS 198, Cert. #554).
- **X9.31** compliant **random number generator (Cert. #559)**

Algorithms that are non-approved but allowed in FIPS mode (QuickSec):

- **Diffie-Hellman** (key agreement; key establishment methodology provides between 80 and 112 bits of encryption strength; non-compliant if encryption strength is less than 80 bits). Diffie-Hellman is not approved but its use is allowed in FIPS mode. Key sizes of 1024 – 2048 bits provide 80 – 112 bits of encryption strength.

Algorithms that are non-compliant (QuickSec). These algorithms are automatically disabled in FIPS mode:

- Blowfish-CBC
- Twofish-CBC
- Cast-128-CBC
- DES-CBC
- MD5
- HMAC-MD5
- AES-XCBC-MAC
- Triple-DES-ECB (untested)

6. Test Environment

The cryptographic module was tested on the StoneGate FW-1020 appliance. As a firmware module, the cryptographic module's validation is effective on any compatible platform. See the Stonesoft web site [2] for more information on the appliances.

7. Roles and Services

The cryptographic module implements the Crypto Officer roles and a User role (but no maintenance role):

- Crypto Officer Role A is assumed when the root user is doing the initial configuration of the StoneGate Firewall/VPN product. Crypto Officer A can update or remove StoneGate Firewall/VPN product software from the firewall node. Crypto Officer A is authenticated by the operating system when the officer logs in locally on the firewall node. Authentication is based on the “root” user name and password (role-based authentication). User “root” can also log in remotely using the SSH service (note: the SSH service is disabled in FIPS mode). Crypto Officer A cannot log in on the firewall node if the FIPS mode has been set. In FIPS mode, Crypto Officer A is only able to read the local console printouts and see the appliance status LEDs.

- Crypto Officer Role B is assumed when there is data flow between the logical StoneGate Firewall/VPN Core FIPS module and the OpenSSL module that is within the physical cryptographic boundary. Crypto Officer Role B sends commands and VPN security policy parameters to the cryptographic module and receives status information from the module. Crypto Officer Role B is also assumed when direct control data or status data packet exchange between the logical StoneGate Firewall/VPN Core FIPS module and some other node in the cluster has been established. To be accurate, Crypto Officer Role B is implicitly applied to any entity that can access services that are only provided for Crypto Officer Role B.

- The User of the StoneGate Firewall/VPN Core FIPS module is the StoneGate Firewall/VPN application. As a server application, StoneGate Firewall/VPN is able to provide services to a large number of clients simultaneously. The data streams between the clients and the StoneGate Firewall/VPN Core FIPS module are encrypted, decrypted or bypassed by the StoneGate Firewall/VPN Core FIPS module depending on the VPN security policy. If required by the VPN security policy, the source of an encrypted data stream may be initially identified using digital certificates or a pre-shared key according to IPsec standards. The individual packets in the data stream are authenticated using the HMAC-SHA-1 message authentication code according to IPsec standards.

The services available to the Crypto Officer and clients are listed in Table 5.

Service	Input	Output	Crypto Officer Roles	Client
1) IKEv1 services Standard session key negotiations, authentication.	Standard IKE inputs.	Standard IKE outputs.		X
2) IPsec services Securing the network traffic. Manual key feeding is not supported.	Standard IPsec inputs.	Standard IPsec outputs.		X
3) Perform bypass service (no IPsec services applied to the packet) The security policy (installed into the cryptographic module using General Configuration service) defines the rules according to which the IPsec services are applied to the network packets. If the rules do not apply IPsec services to a packet, the packet is bypassed. Decision is based on the IP address information etc. Services for both Crypto Officer and clients may use the perform bypass service (depends on the installed security policy).	Packets that do not use cryptographic services of the module according to policy settings.	The data input to the module.	B	X
4) Primary management communication channel service The main channel established for communication between Crypto Officer Role B and the cryptographic module. In practise, the Crypto Officer Role B (in the form of the OpenSSL module) uses this service of the cryptographic module as an endpoint to TLS connections. This service is used by the TLS connections between the physical Firewall Node and the Management Server, the Log Server, the IPS and the other nodes of the cluster.	Various data (several other services use this communication channel for data input to the cryptographic module).	Various data (several other services use this communication channel for output).	B	
5) File encryption service Encryption of files on the node’s hard disk. The policy encryption option in the Management Client is used for setting the encryption of files on/off. Disabled in FIPS mode.	Configuration commands to the module through the interface between the cryptographic module and OpenSSL (configuration originates from the Management Server).	Status output through the interface between the cryptographic module and OpenSSL.	B	

6) Perform Self-tests service Operator can execute the power-up self-tests by rebooting the node.	Policy file and commands through the interface between the cryptographic module and OpenSSL.	Status output through the interface between the cryptographic module and OpenSSL.	B	
7) Show status service The module provides various types of status information to the Crypto Officer Role B through the Primary Management Communication Channel service (actually, the data flows to the Management Server and to the Log Server). Particularly, the following information is provided: - If the module boots in FIPS mode, a log indicating this is printed and sent to the Log Server. - It is also possible to check if the module is in FIPS mode by installing a firewall policy that contains non-approved algorithms for IKE/IPsec configuration. In FIPS mode, the policy installation does not succeed and an informative error message is printed by the Management Client. - The active firewall policy determines the state of the bypass capability. The log printouts sent to Log Server indicate which connections are encrypted by IKE/IPsec and which are not. The log printouts provide accurate information about the state of the alternating bypass capability the module provides.	Commands for controlling the status output. Given to the module through the interface between the cryptographic module and OpenSSL (command data originates from the Management Server).	System status data through the interface between the cryptographic module and OpenSSL	B	
8) Console services for Crypto Officer Note that login at console is disabled in FIPS mode, but the console provides some limited services without a need to log in to the system: - The system restore service that overwrites the hard disk several times with random data (executed before maintenance) - The status output service that prints the indicators of error states.	Input data from the console	Console outputs	A	
9) SSH remote login service (disabled in FIPS mode) This service is not actually provided by the logical StoneGate Firewall/VPN Core FIPS module but by the platform.	SSH connection input data	SSH connection outputs	A	
10) General Management command service General management commands: reboot, go	Commands through the interface between	Status data to OpenSSL,	B, A (in FIPS mode	

offline/online, etc. (Console and SSH login are disabled in FIPS mode.)	the cryptographic module and OpenSSL. Commands from the console.	console or SSH	only B)	
11) IPsec certificate generation service Commands the module to generate a private key and certificate request (to be used with IPsec authentication) and send the certificate request to the Management Server (to be signed by the CA). Install the CA signed IPsec gateway certificate on the appliance.	Commands through OpenSSL (commands originate from the Management Server). Signed certificate is stored on the appliance's hard disk.	Status data through OpenSSL. Certificate request is sent to the Management Server.	B	
12) IPsec CA certificate install service Installs IPsec CA certificates and remote certificates on the node through the Management Server connection.	Certificates, commands through OpenSSL (data originates from the Management Server).	Status data through OpenSSL, signed certificates installed on the hard disk.	B	
13) TLS certificate install service Installs the Management Server (TLS CA) signed TLS node certificate (the node's own TLS certificate) on the node. During initialization, the node generates a private key and a certificate request (TLS keys). The node sends the certificate request to the Management Server and receives a CA signed certificate from the Management Server. The signed certificate is installed on the node's hard disk.	Signed TLS certificate, commands through OpenSSL (data originates from the Management Server).	Certificate request, status data through OpenSSL	B	
14) TLS CA certificate install service Installs a TLS CA certificate on the node.	Certificate, commands through OpenSSL (data originates from the Management Server)	Status data through OpenSSL	B	
15) General configuration service Configures and manages the system (firewall configuration, VPN configuration). Configures clustering. Configures firewall nodes' usage of log servers and IPS.	Configuration files and commands through OpenSSL (data originates from the Management Server), or from the platform	Status data through OpenSSL interface. Configuration installed on the appliance's hard disk.	B	
16) Blacklisting service Receives blacklist commands and disables user connections based on the commands. Blacklisting source may be a separate IPS (StoneGate	Blacklist commands through OpenSSL (data originates from the IPS or	Status data through OpenSSL	B	

Intrusion Prevention System) or the Management Server.	the Management Server).			
17) Log data output service Log data output to the Log Server.	Commands, status data through OpenSSL. Log data output configuration data originates from the Management Server.	Log data and status data through OpenSSL	B	
18) Cluster data transfer service Transfers data between nodes of the cluster. Data is sent in encrypted form (encrypted and signed packets, no TLS). OpenSSL is used to encrypt and decrypt the data. The logical cryptographic module sends the encrypted data through the Linux TCP/IP Stack. The module should be configured to use physically separate networks for management and clustering communications.	Encrypted data that originates from other nodes of the cluster, Encrypted data from OpenSSL. Decrypted Data from OpenSSL. IPsec and IKE related data (security associations, local IKE secrets, notifications, and status data).	Encrypted data sent to other nodes of the cluster. Encrypted data given to OpenSSL to be decrypted. Plaintext data given to OpenSSL to be encrypted. IPsec and IKE related data (security associations, local IKE secrets, notifications, status data).		
19) Cluster protocol service Shares various load balancing and status data between nodes of the cluster. Required for cooperation between the nodes of the cluster. The module should be configured to use a physically separate network for cluster protocol services. The cluster protocol service does not transfer any CSP data between nodes of the cluster.	Load balancing data, system status data. The cryptographic module receives the data directly from the Linux network stack.	Similar types of data as the input data. Cryptographic module sends the data directly to the Linux network stack.	B	

Table 5 Security services available to the Crypto Officer

8. Critical Security Parameters

The critical security parameters and corresponding services for normal users of the module are listed in Table 6.

Critical Security Parameters	Algorithms, Implementation	Services that Access the Critical Security Parameters	Access Type
IKE pre-shared secret	HMAC-SHA-1 QuickSec implementation	**1)** IKE services Authentication in IKE key establishment negotiations	Read
IKE certificate(s)	RSA DSA QuickSec implementation	**1)** IKE services Authentication in IKE key establishment negotiations	Read
IKE private key(s)	RSA DSA QuickSec implementation	**1)** IKE services Authentication in IKE key establishment negotiations	Read
IKE Certification Authority Certificates	RSA DSA QuickSec implementation	**1)** IKE services Authentication of peer certificates in IKE negotiations	Read
IKE-negotiated IPsec encryption keys	Triple-DES-CBC AES-128-CBC, AES-192-CBC, AES-256-CBC QuickSec implementation	**2)** IPsec services Encryption and decryption of data	Read, Write
IKE-negotiated IPsec authentication keys	HMAC-SHA-1 QuickSec implementation	**2)** IPsec services Authentication of bulk data	Read, Write
Key agreement method keys	Diffie-Hellman QuickSec implementation	**1)** IKE services Session key material generation.	Read, Write

Table 6 Critical security parameters and corresponding services for users

The critical security parameters, certificates and corresponding services for Crypto Officers are listed in Table 7. Presented algorithm implementations are within the StoneGate Firewall/VPN Core FIPS module logical boundary.

Critical Security Parameters	Algorithms, Implementation	Services that Access the Critical Security Parameters	Crypto Officer Roles Using the Services, Access Type
IKE pre-shared secret	HMAC-SHA-1 QuickSec implementation	**15)** General configuration service Crypto Officer Role B is able to install IKE pre-shared secrets. Installation is done through the Management Server.	Role B (Write)
IKE certificates	RSA DSA QuickSec implementation	**11)** IPsec certificate generation service **12)** IPsec CA certificate install service	Role B (Write)
		18) Cluster data transfer service	Role B (Read, Write)
IKE private keys	RSA DSA QuickSec implementation	**11)** IPsec certificate generation service	Role B (Write)
		18) Cluster data transfer service	Role B (Read, Write)
IKE-negotiated IPsec encryption keys	Triple-DES-CBC AES-128-CBC, AES-192-CBC, AES-256-CBC QuickSec implementation	**18)** Cluster data transfer service	Role B (Read, Write)
IKE-negotiated IPsec authentication keys	HMAC-SHA-1 QuickSec implementation	**18)** Cluster data transfer service	Role B (Read, Write)

Table 7 Critical security parameters, certificates and corresponding services for Crypto Officers within the logical boundary

The critical security parameters, certificates and corresponding services for Crypto Officers are listed in Table 8. Presented algorithm implementations are outside the StoneGate Firewall/VPN Core FIPS module logical boundary.

Critical Security Parameters	Algorithms, Implementation	Services that Access the Critical Security Parameters	Crypto Officer Roles Using the Services, Access Type
TLS certificate of the firewall node (used for authentication of network connections between the firewall node and the Management Server, between the firewall node and the Log Server, between the firewall node and the IPS, and authentication of data synchronization services between the nodes of the cluster)	RSA OpenSSL implementation is outside the StoneGate Firewall/VPN Core FIPS module logical boundary.	**4)** Primary management communication channel service **13)** TLS certificate install service	Role B (Read, Write)
TLS private key of the firewall node (authentication of network connections between the firewall node and the Management Server, between the firewall node and the Log Server, between the firewall node and the IPS, and authentication in data synchronization services between the nodes of the cluster)	RSA OpenSSL implementation is outside the StoneGate Firewall/VPN Core FIPS module logical boundary.	**4)** Primary management communication channel service	Role B (Read)
TLS CA certificate Authentication of network connections between the firewall nodes and the	RSA OpenSSL implementation is outside the StoneGate Firewall/VPN Core FIPS module logical boundary.	**14)** TLS CA certificate install service	Role B (Write)

Management Server, between the firewall node and the Log Server, between the firewall node and the IPS, and authentication in State synchronization services between the nodes of the cluster		**4)** Primary management communication channel service	Role B (Read)
TLS encryption keys (separate key for each session) Encryption of network connections between the firewall nodes and the Management Server, between the firewall node and the Log Server, between the firewall node and the IPS, and encryption in data synchronization services between the nodes of the cluster	Triple-DES-CBC OpenSSL implementation is outside the StoneGate Firewall/VPN Core FIPS module logical boundary.	**4)** Primary management communication channel service	Role B (Read, Write)
TLS authentication key (separate key for each session) Authentication of data connections between the firewall nodes and the Management Server, between the firewall node and the Log Server, between the firewall node and the IPS, and authentication in data synchronization services between the nodes of the cluster	HMAC-SHA-1 OpenSSL implementation is outside the StoneGate Firewall/VPN Core FIPS module logical boundary.	**4)** Primary management communication channel service	Role B (Read, Write)
Secret keys shared between nodes of the cluster	AES-128-CFB HMAC-SHA1	**18)** Cluster data transfer service Keys are stored in the cryptographic module. Crypto	Role B (Read, Write)

Keys are used to protect Cluster data transfer service packets that are sent between the nodes of the cluster.	OpenSSL implementations are outside the StoneGate Firewall/VPN Core FIPS module logical boundary.	Officer Role B writes the keys in the cryptographic module or reads the keys from the cryptographic module. The OpenSSL module (that is within the same physical cryptographic boundary) is the party that actually writes or reads the keys to/from the cryptographic module.	
Crypto Officer password	No cryptography applied	**8)** Console services for Crypto Officer The password that the Crypto Officer supplies when logging in to the console.	Role A (Write)

Table 8 Critical security parameters, certificates and corresponding services for Crypto Officers outside the logical boundary

The other critical security parameters are listed in Table 9.

Critical Security Parameter	Algorithm
The checksum used for module integrity check during start-up.	SHA-1
Seed and seed key for the RNG.	ANSI X9.31 compatible PRNG

Table 9 Other critical security parameters

9. Operating Environment

When the FIPS mode has been set, nobody can log in to the operating environment or execute arbitrary commands. The operating environment is trustworthy; there is no cron or other processes that could start arbitrary services. The logical FIPS module checks the validity of the whole operating environment software by calculating a checksum of the disk partition in which the module and the operating environment is stored. For the reasons mentioned, the operating environment is non-modifiable. Because of this fact, the requirements for the operating environment defined in FIPS 140-2 are fulfilled.

9.1 Access to the CSP and Certificates

Since the operating environment is non-modifiable, unauthorized parties have no access to the CSP and certificates of the cryptographic module. The CSP and certificates can only be accessed through services provided by the module.

The Clients and Crypto Officer are not able to directly access the CSP and certificates of the module (Crypto Officer Role A using root account is an exception, but cannot log in to the system when the FIPS mode is set). Clients and the Crypto Officer have access to the CSP and certificates only through services provided by the cryptographic module. Normal users access the CSP and certificates of the module through standard IPsec and IKE services. Crypto Officer Role B can access CSP and certificates through the interfaces that the cryptographic module provides to OpenSSL.

The Cluster Protocol service and the Cluster Data Transfer service provide a way to communicate directly with the cryptographic module from outside the physical cryptographic boundary (through the Linux network stack). However, the Cluster Protocol service does not transfer any CSP data and the Cluster Data Transfer service transfers CSP data in encrypted format. CSP data transferred by the Cluster Data Transfer service is encrypted using OpenSSL. It is required that these services have a physically separate network for their traffic (from the network used by clients of the module).

The Crypto Officer (Role B) is able to install, read and remove the IPsec remote certificates and IPsec CA certificates of the node. The Crypto Officer (Role B) is able to install IPsec certificates and private keys of the nodes of the cluster, secret keys shared between the nodes of the cluster, IPsec security associations and local IKE secrets. The Crypto Officer (Role B) is also able to install the TLS CA certificate and the CA certified TLS certificate of the node. Similarly, the Crypto Officer (Role B) is able to install the CA certified IPsec certificate of the node. The node has generated its own node certificates (IPsec certificates, one TLS certificate) and corresponding private keys itself, but it passes the certificates to the Crypto Officer Role B who handles the signing of the certificates. After signing, the Crypto Officer Role B “installs” the certificates to the module through the interface the module provides to OpenSSL.

10. Zeroization of Keys

Zeroization of the keys on the hard drive is done by the Crypto Officer Role A, who either formats the hard drive or uses the “system restore” feature to wipe or delete the information on the hard drive’s data partition. Using “system restore” feature destroys all the keys and CSP in the module.

Crypto Officer Role A can use the “system restore” feature by rebooting the module and choosing “System restore options” in the boot menu. Crypto Officer Role A is able to delete the information or use the overwriting functionality. At least one overwrite is required for zeroization of keys. More overwrites are more secure, but may take a considerable amount of time depending on the appliance’s storage capacity.

Using “system restore” restores the factory settings. The module cannot be used after performing “system restore” without re-doing the initial configuration.

All data output from the module is inhibited whilst the module is being zeroized. Crypto Officer zeroizing the module must not leave the module until zeroization has been finished.

Zeroization of keys must be done before maintenance of the module.

In addition to zeroization initiated by Crypto Officer, the module performs continuous automatic key zeroization. Automatic zeroization overwrites Diffie-Hellman shared secrets and derived key material with zeros when they are no longer needed.

11. Usage of Keys and Algorithms

Client (IPsec) Services:

- Symmetric keys (Triple-DES and AES in FIPS mode) are used to provide confidentiality of data both during negotiations of IPsec security associations and during bulk data transmissions. The symmetric session keys are generated by the IKE protocol.

- HMAC-SHA-1 message authentication code is used in the authentication header (AH) and in the Encapsulating Security Payload (ESP) for authenticating the sender and verifying the integrity of AH data.

- SHA-1 hash algorithm is used for authentication together with the public key algorithms used in the IKE negotiations.

- DSA or RSA algorithms are used for authenticating the parties in the IPsec Internet Key Exchange (IKE) process. The IKE key exchange can also be authenticated with a pre-shared secret. The method for authenticating the IKE key exchange is selected by the Crypto Officer (Role B) when configuring the cryptographic module. The IPsec node certificate and private key or the pre-shared secret is needed in the authentication process. The pre-shared secret is used as a part of the MAC key that authenticates the IKE phase 1 exchange.

- During IKE phase 1 negotiations, VPN nodes establish a Security Association (SA) that defines the methods for protecting future communications. The Diffie-Hellman method is used to generate key material to encrypt and authenticate further IKE negotiations and to generate keying material for user IPsec services.

- IPsec session keys are generated during IKE phase 2 negotiations. The session keys are derived from the keying material established with the Diffie-Hellman exchange in IKE phase 1. If the Crypto Officer Role B has configured the module to use IKE perfect forward secrecy, the session keys are established using a Diffie-Hellman exchange. Session keys have a lifetime that Crypto Officer Role B can set. When the set lifetime is reached, new session keys are negotiated.

Crypto Officer Services:

- Services to Crypto Officer Role B are mostly provided through the interface between the cryptographic module and OpenSSL. Crypto Officer Role A can access no services if the FIPS mode has been set (except the status output in the console without login possibility, and except the possibility to wipe the hard disk before maintenance). The services provided to Crypto Officer Role B through the interface between OpenSSL and the cryptographic module require no authentication or encryption of service data flow, since the actual module using the interface is within the physical cryptographic boundary.

- Cluster Data transfer service contains data (provided by Crypto Officer Role B) for the purpose of distributing the data to all nodes of the cluster. Accessing the data provides no access to the CSP because the data has been encrypted using OpenSSL services.

- Crypto Officer Role B is able to access most parts of the CSP data in the cryptographic module through the provided services. However, accessing the CSP is possible only through those services that can be used within the physical cryptographic boundary. There is no leakage of CSP from the non-modifiable operating environment.

12. Random Number Generation

The cryptographic module uses X9.31 compatible pseudo-random number generator in order to generate random data in FIPS 140-2 approved mode. The pseudo-random number generator is fed with entropy from several sources.

13. Key Generation

The types of keys generated by the module are shown in Table 10. Other types of keys have been mentioned in this document as CSP data, but are not listed in the table that follows, because they are inserted into the cryptographic module by the Crypto Officer, not generated in the module. See the chapter “Usage of Keys and Algorithms” for additional information about the keys.

Key Type, Usage	Algorithm	Generation Method	Other Information.
IKE private key, certificate Used for authenticating the IPsec session between client and the cryptographic module.	RSA, DSA	Generated by the module or inserted into the module by the Crypto Officer. QuickSec Toolkit services are used for key generation. Approved X9.31 prng fed from several entropy sources is used in the key generation.	Stored on the hard drive. Keys are zeroized before maintenance by the Crypto Officer. If clustering is in use, the keys are given to Crypto Officer Role B (OpenSSL module within the physical cryptographic boundary) in plaintext form.
IKE-negotiated IPsec encryption keys Used for encrypting and decrypting IPsec session data between clients and the cryptographic module.	Triple-DES AES	Generated by the module or inserted into the module by the Crypto Officer (Crypto Officer Role B is able to install IPsec security associations of the other nodes of the cluster). Derived according to IPsec standards.	Automatically zeroized after use (by overwriting with zeroes). Stored in the memory. If clustering is in use, the keys are given to the Crypto Officer Role B in plaintext form.
IKE-negotiated IPsec authentication keys Used for authenticating IPsec session data between clients and the cryptographic module.	HMAC-SHA-1	Generated by the module or inserted into the module by the Crypto Officer. Derived according to IPsec standards.	Automatically zeroized after use (by overwriting with zeroes). Stored in the memory. If clustering is in use, the keys are given to Crypto Officer Role B in plaintext form.
Key agreement method keys	Diffie-Hellman	Generated according to PKCS#3 standards. Approved X9.31 prng is used and fed from various entropy sources.	Automatically zeroized after use (by overwriting with zeroes). Stored in the memory. If clustering is in use, the keys are given to Crypto Officer Role B in plaintext form.

Table 10 Key Generation information

Other key material is not generated by the cryptographic module, but given to it by the Crypto Officer (the cryptographic module does not generate keys for OpenSSL).

14. Design Assurance

Stonesoft uses configuration management software (BitKeeper [5]) for software source code management. Documentation is managed with both BitKeeper and Lotus Notes. The configuration management software provides access control and versioning. Each version of the cryptographic module and its components, the operating system, user guidance and security policy are assigned and labeled with a unique identification number.

The guides referred to in this document provide, together with this document, procedures for secure installation, initialization and startup of the cryptographic module.

The integrity of the cryptographic module is checked during installation. The preinstalled image on StoneGate appliances is not FIPS compliant, but must be upgraded to a FIPS compliant version. Similarly, CD-ROM installations on a standard PC must be upgraded to a FIPS compliant version. The upgrade calculates the SHA-1 checksum of the image that is to be used for the upgrade. The calculated checksum must be verified and must match the one provided by Stonesoft’s technical support. See the Crypto Officer guidance [3] for details.

The cryptographic module checks the integrity of the module and platform software during power-up tests by calculating a SHA-1 checksum of the whole rootfs partition (including all of the components of the logical cryptographic module), therefore the user of the module can be sure that the software has not changed and operates as intended by the vendor.

15. Self-tests

The module performs power-up self-tests during module initialization and continuous tests during module operation.

Power-up tests contain the following tests:

- Cryptographic algorithm tests
- Random number generator test
- Software/firmware integrity test
- Critical functions test

Conditional tests contain the following tests:

- Pairwise consistency tests
- Continuous random number generator test
- Bypass test

Software/firmware load test is not applicable. External modules are not loaded into the cryptographic module.

Manual key entry test is not applicable. Cryptographic keys are not entered into the module manually.

Power-up self-tests are initiated automatically if the cryptographic module is in FIPS mode and the appliance boots. Self-test errors are reported on the system console or on the system log. If the power-up self-test fails, an error message is displayed on the console followed by a system reboot.

Algorithm (QuickSec Toolkit Implementation)	Performed Tests
AES-128, AES-192, AES-256	Known answer tests during power-up
Triple-DES	Known answer tests during power-up
Diffie-Hellman	Simulated Diffie-Hellman key exchange during power-up.
RSA	Known answer test during power-up, key consistency tests when keys are generated.
DSA	Consistency test during power-up (sign and verify test), key consistency tests when keys are generated.
SHA-1	Known answer test during power-up.
HMAC-SHA-1	Known answer test during power-up.
ANSI X9.31 prng	Known answer test during power-up, continuous prng tests.

Table 11 Self-tests for algorithms implemented by the cryptographic module.

Additionally, there is a certmake utility program within the cryptographic boundary that uses its own instance of the QuickSec Toolkit. This program executes all of the tests mentioned when the program is used (power-up tests and continuous tests). If a cryptographic error occurs in the certmake utility, the whole cryptographic module enters an error state that causes the appliance to reboot.

The cryptographic module checks the integrity of the module and platform software during power-up tests. The SHA-1 implementation of the OpenSSL command line tool is used to calculate the checksum and to compare the result to the value stored in the cryptographic module.

There are additional power-up tests for critical functions of the platform. The OpenSSL ciphers, public-key algorithms, hash and MAC algorithms are tested during the module power-up. If these tests fail, the cryptographic module enters an error state that causes the appliance to reboot.

16. Authentication

The IPsec implementation of the module provides authentication that consists of RSA or DSA certificates for authenticating the parties of the VPN session during Phase 1 and HMAC-SHA-1 for authenticating the bulk data according to the IPsec standard. The module's IPsec implementation provides encryption strength of 112 bits for authentication if 2048-bit asymmetric keys are used with certificates.

2048-bit RSA certificates are used for authenticating TLS communications between the physical cryptographic module and its counterparts. The Management Server, Log Server and IPS each have their own certificate identity that is checked during authentication.

SSH connections and console login use password based authentication. If the length of the password is n characters, there are more than n^26 passwords to choose from. SSH and console login are disabled in the FIPS mode.

17. Operating Modes

The cryptographic module has two operating modes:

- FIPS 140-2 Approved mode
- FIPS 140-2 Non-Approved mode

In FIPS 140-2 Approved mode, only the FIPS 140-2 approved encryption algorithms can be used and the cryptographic module rejects any attempts to use non-approved algorithms.

The cryptographic module generates a log entry each time it enters or exits the FIPS 140-2 Approved mode.

See chapter "Guidance" for more information on how to invoke the FIPS mode.

18. Guidance

18.1 Crypto Officer Guidance

Enabling FIPS 140-2 Approved mode requires completing the following steps. For a detailed description, refer to the guidance [3]:

1. Crypto Officer Role A selects the "Restricted FIPS-compatible operating mode" when doing the initial configuration.

2. In the Management Client, Crypto Officer Role B selects the FIPS-compatible operating mode (the FIPS-compatible operating mode option on the Advanced Settings tab of the firewall or firewall cluster properties).

3. To disable the File encryption service, disable "Encrypt configuration data" in the Advanced Settings of the firewall properties in the Management Client. This is required for the module to operate in the FIPS Approved mode. The algorithm used to encrypt configuration data is non-approved.

4. Crypto Officer Role B must only enable the FIPS approved algorithms (RSA, DSA, Diffie-Hellman, Triple-DES, AES-128, AES-192, AES-256, SHA-1) and key lengths representing at least 80 bits of encryption strength.

5. Crypto Officer Role B must not configure the RADIUS service for use.

6. Clustering must be configured to use encryption and authentication (AES-128 and HMAC-SHA-1) for state synchronization packets.

7. There must be a physically separate network reserved for communications between the physical StoneGate Firewall/VPN nodes of the cluster (if clustering is in use).

8. FIPS requires that the module does not generate keys in non-approved mode and then switch back to approved mode and continue using the keys. Therefore, while in FIPS mode, do not switch to non-approved mode (do not set any option that is not compliant with FIPS anywhere) if you wish to maintain the FIPS approved state of operation.

18.2 User Guidance

In addition to the information presented in this document, refer to the guidance [3].

19. Physical Security

The module was tested on a StoneGate FW-1020 appliance consisting of industrial grade components with standard passivation. The components are entirely enclosed within a production-grade enclosure that includes removable covers. As a firmware module, the cryptographic module's validation is effective on any compatible platform. See the Stonesoft web site [2] for more information on StoneGate appliances.

Prior to performing physical maintenance, all CSP material contained within the cryptographic module must be zeroized by the cryptographic officer.

20. Mitigation of Other Attacks

The vendor makes no assertions on the Mitigation of Other Attacks.

21. References

[1] http://csrc.nist.gov/groups/STM/cavp/index.html

[2] http://www.stonesoft.com/en/products_and_solutions/products/fw/appliances/

[3] Common Criteria Certification User’s Guide (http://www.stonesoft.com/)

[4] RFC 2246, “The TLS Protocol Version 1.0”

[5] BitKeeper (http://www.bitkeeper.com/)

[6]
http://www.stonesoft.com/en/support/technical_support_and_documents/manuals/appliances/

Copyright

Stonesoft Corporation
Itälahdenkatu 22 A
FIN-00210 Helsinki, Finland
tel. +358 9 476 711
fax +358 9 4767 1234
info.finland@stonesoft.com

Stonesoft Inc.
1050 Crown Pointe Parkway,
Suite 900, Atlanta, GA 30338, USA
tel. +1 866 869 4075
fax +1 770 668 1131
info.americas@stonesoft.com

www.stonesoft.com