STONESOFT CORP.

StoneGate High Availability Firewall and VPN FIPS 140-2 Validation Security Policy

StoneGate High Availability Firewall and VPN version: 2.0.5
Author: Klaus Majewski
Date: September 2003

TABLE OF CONTENTS

1. INTRODUCTION

The StoneGate High Availability Firewall and VPN Version 2.0.5 by StoneSoft provides IPSec compliant VPN connectivity between two firewall clusters (site to site connectivity). It also provides remote VPN client connectivity to the firewall cluster.

StoneGate High Availability Firewall and VPN product consists of three main components: StoneGate Firewall management server, log server and firewall cluster as shown in Figure 1. Firewall Cluster consists of one or more firewall nodes. FIPS 140-2 testing is done for one firewall node.
The StoneGate VPN solution is based on the IPSec standard as defined in RFC 2401. The cryptographic module is designed and implemented to meet the level 1 requirements of FIPS publication 140-2.

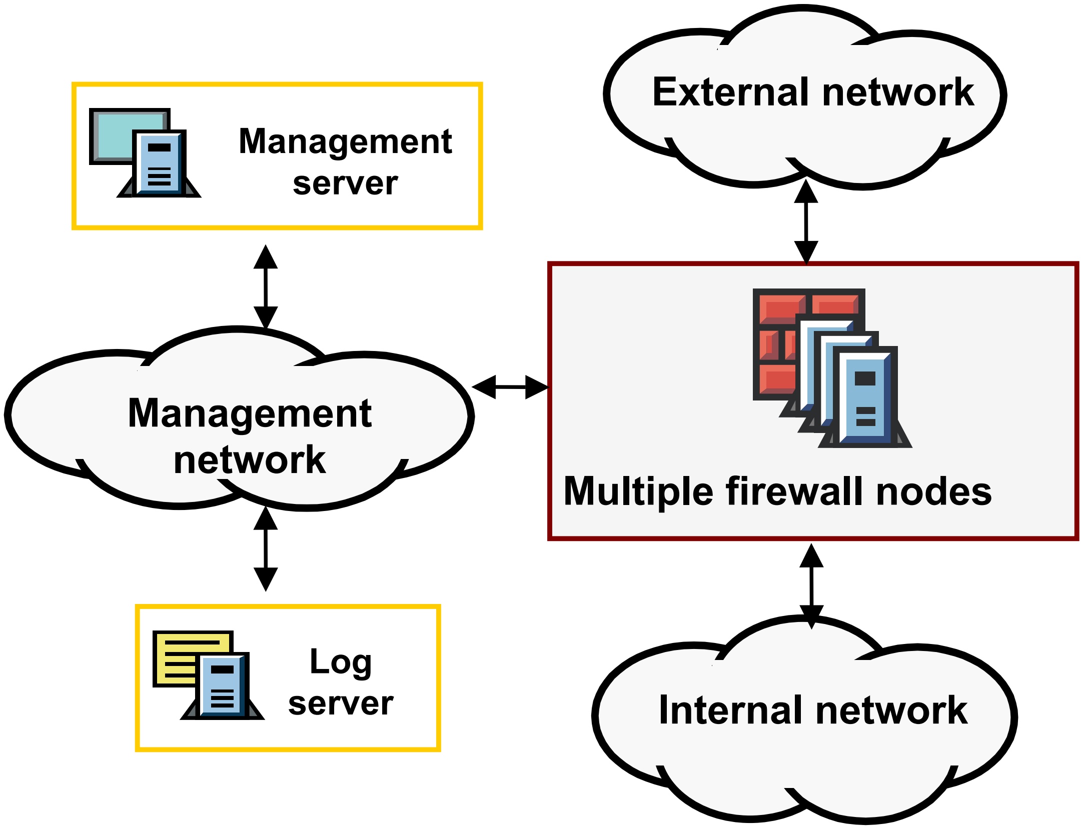


Figure 1. Example set-up for StoneGate High Availability Firewall and VPN product

The cryptographic module supports three FIPS approved encryption algorithms:

- DES[1] (FIPS 46-3)
- 3DES (FIPS 46-3)
- AES (FIPS 197)

It also supports the following non-FIPS encryption algorithms:

- Blowfish
- Twofish
- Cast-128

The cryptographic module supports one FIPS approved hash algorithm SHA-1 (FIPS 180-1). The cryptographic module also supports the use of message authentication codes (MAC) that use the SHA-1 hash function, HMAC-SHA-1.

It also supports the following non-FIPS hash algorithm:

- MD5
- SHA-256 (vendor affirmed/non-compliant)

It also supports the following key agreement algorithm:

- Diffie-Hellman

The cryptographic module supports two FIPS approved digital signature algorithms:

- DSA (FIPS 186-2)
- RSA (FIPS 186-2) compliant to PKCS#1 standard

Details on validated algorithms can be found on NIST web page, http://csrc.nist.gov/cryptval/vallists.htm.

The cryptographic module uses X9.31 APPENDIX A.2.4 compliant random number generator.

[1] DES is used only for interoperability with legacy systems.

2. CRYPTOGRAPHIC MODULE AND CRYPTOGRAPHIC BOUNDARY

2.1 Module Boundary

In FIPS 140-2 terms, the StoneGate High Availability Firewall and VPN is a software module. This software module can be run on standard Intel-based hardware or Sun Microsystems UltraSPARC platforms. The StoneGate Firewall VPN module runs on Debian GNU/Linux Operating System (OS). The operating system is delivered with StoneGate High Availability Firewall and VPN product and is installed from the product CD. The cryptographic software module is installed as executable code.

In terms of FIPS 140-2, the secure cryptographic boundary is the physical computer that comprises a single StoneGate Firewall node. Multiple firewall nodes can be clustered together as depicted in Picture 1. StoneGate Firewall management server and log server are outside of the cryptographic boundary.

The cryptographic module was tested on an IBM X330 rack-optimized personal computer running the Debian GNU/Linux Version 3.0 operating system. The hardware consisted of:

- Motherboard
- Intel Pentium III 1133 MHz processor
- 256 MB System RAM
- ROM
- Standard PCI bus
- SCSI disk controller
- Display controller
- 2 RS485 ports, 2 USB serial ports
- 18.2 GB Ultra160 SCSI hard disk drive
- 24X EIDE CD-ROM Drive
- 3.5” Floppy disk drive
- Integrated keyboard/mouse controller, 2 single ports for keyboard and mouse
- 2 integrated 10/100 Ethernet ports
- 2 IBM E-Server xSeries 10/100 PCI Ethernet Adapters
- Power supply
- Rack chassis, removable cover

2.2 Software Cryptographic Module Description

The StoneGate High Availability Firewall and VPN product is a single software module. Security services of the module are provided by integrating StoneSoft developed software with third party open source programs. IPSEC services are built using the cryptographic software primitives contained in the SSH (IPSec Express) Toolkit. For VPN management functions, StoneSoft has incorporated security service software from two other software libraries, OpenSSL and OpenSSH into its product.

Figure 2 depicts the logical boundary and software architecture of the cryptographic module.

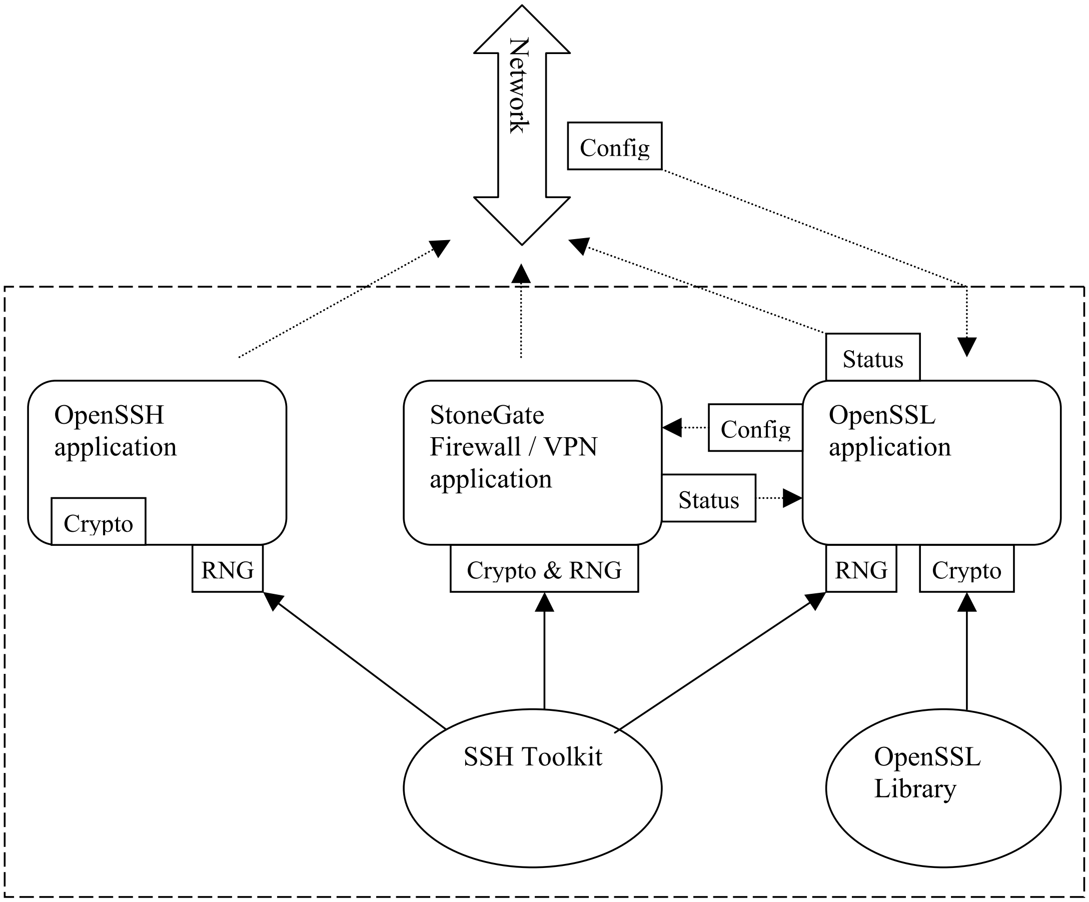
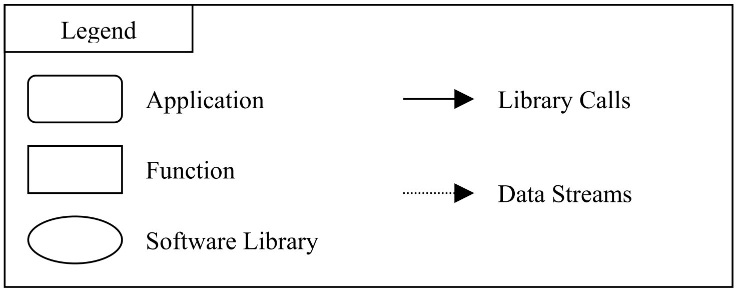


Figure2. Module Boundary



The software module is comprised of these components:

1. The StoneGate Firewall/VPN application program developed by StoneSoft manages data flow and firewall/VPN services; IPSec related cryptographic functions are performed by programs in the SSH Toolkit.

2. The SSH (IPSec Express) Toolkit is an open source cryptographic software library that provides all the cryptographic functions needed to support IPSec services.

3. The OpenSSL application is a third party open source executable used by StoneSoft to establish TLS communication with the management server for the purpose of securely inputting control information or outputting status information. The OpenSSL program library supplies the code for cryptographic functions used by the OpenSSL application.

4. The OpenSSH application provides the capability for a system administer to login remotely to monitor the performance of the node.

The cryptographic services can be configured through an Application Program Interface (API). The cryptographic module receives its configuration commands from the StoneGate Firewall management server using TLS encrypted communication channel.

3. ROLES AND SERVICES

The cryptographic module implements two different Crypto Officer roles and a User role. There is no maintenance role.

There are two Crypto Officer instances:

- Crypto Officer role (CO Role A) is assumed when the root user is loading the StoneGate High Availability Firewall and VPN product from the CD-ROM to the firewall node. The Crypto Officer can update or remove StoneGate High Availability Firewall and VPN product from the firewall node. The Crypto Officer can locally log into the VPN node and see module status information. In this role, the Crypto Officer is authenticated using the "root" userid and password for the operating system (Role-based authentication). Even though the module provides SSH service for the "root" user to login remotely, this capability is disabled in the FIPS mode to maintain single operator environment.

- Another Crypto Officer role (CO Role B) is entered when a connection is established between the VPN and the management application residing on an external management server. Using TLS encrypted connection, the module receives from the management server VPN security policy parameters and creates/updates VPN configuration through the module's API interface; the module also sends status information to the management server. Both the management server and the firewall node are authenticated using digital certificates. (Identity-based authentication)

  To restrict the module to a single-user mode of operation, the Crypto Officer role A is disabled after the installation is complete, and only Crypto Officer role B can be used to configure the module. Crypto Officer role A and role B are not simultaneously available.

- User Role: Users are data streams that flow through the cryptographic module. They use encrypt, decrypt, or bypass services of the cryptographic module based on VPN security policy. Role-based authentication is used for data packets. Packets are authenticated using the IPSec protocol where the Authentication Header (AH) authenticates the identity of the source host. IPSec address in the AH are authenticated when the VPNs are established. Digital certificates and the use of pre-shared secrets are both acceptable methods of authentication.

Although authentication methods are provided they do not meet all the authentication requirements of FIPS 140-2. Therefore only FIPS 140-2 Level 1 authentication requirements are met.

The security services available to the Crypto Officer and users are listed in Table 1.

Service	**Crypto Officer**	**User**
Authentication in IKE key establishment negotiations		X
Encryption and decryption of data in connections that do not use IKE for key establishment (preshared secret)		X
Authentication of peer certificates in IKE negotiations		X
IKE Key Establishment		X
Encryption and decryption of data in connections that use IKE for key establishment		X
Authentication of data in connections that use IKE for key establishment		X
Perform bypass		X
TLS - Authentication of internal connections between the firewall nodes and management server	X (Role B)	
TLS - Encryption of internal connections between the firewall nodes and management server	X (Role B)	
Encryption of files in node’s hard disk	X (Role A,B)	
Authentication of files in node’s hard disk	X (Role A,B)	
Crypto officer login at console.	X (Role A)	
Show status	X (Role A,B)	
Create/update VPN Configuration	X (Role B)	
Show mode	X (Role B)	
Self-Tests	X (Role A,B)	
Generate certificate request	X (Role A)	
SSH remote login (non-Approved)	X (Role A)	

Table 1. Security services

4. CRITICAL SECURITY PARAMETERS

4.1 Symmetric Keys

User (IPSec) Services
Symmetric keys (DES[2], 3DES, and AES in FIPS mode) are used to provide confidentially of data both during negotiation of IPSec security associations and for protecting bulk data during transmission.

Crypto Officer Services
3DES keys are used to protect Crypto Officer (Role B) communications originated from the management server (in TLS protocol, as specified in IETF RFC 2246). Files containing critical security parameters are protected using FILESEC utility that uses 3DES.

4.2 Message Digest

User (IPSec) Services
A keyed hash signature, generated using the SHA-1 algorithm, is used in the authentication header (AH) for authenticating the sender and verifying the integrity of AH data. In the Encapsulating Security Payload (ESP), a keyed hash signature, using the SHA-1 signature, is also used for this segment of data.

Crypto Officer Services
Files containing critical security parameters are authenticated using FILESEC utility that uses HMAC-SHA-1.

4.3 Authentication[3] and Digital Signature Parameters

User (IPSec) Services
Digital Signature Algorithm (DSA) or Rivest, Shamir and Adleman (RSA) algorithms are used for the authentication of parties in the IPSec Internet Key Exchange (IKE) process. The IKE key exchange can also be authenticated with a pre-shared secret. The method used for authenticating the IKE exchanges is selected by the Crypto Officer (Role B), when configuring the crypto module. IKE local secret is used for VPN anticlogging protection.

Crypto Officer Services
As part of the system initialization process, the module generates a public-private key pair. The public key is sent, in a certificate request, to the management server. The certificate (TLS certificate), signed with the Certificate Authority's private key, is returned and stored in the module. The digital certificates associated with the servers are used for authenticating both parties in the TLS session.

[2] DES is to be used only for interoperability with legacy systems.

[3] Although authentication methods are provided they do not meet all the authentication requirements of FIPS 140-2. Therefore only FIPS 140-2 Level 1 authentication requirements are met.

4.4 IKE Pre-shared Secret and Crypto Officer Supplied IPSec keys

User (IPSec) Services
The cryptographic module uses the IKE protocol (RFC-2409) for key establishment. IKE authentication of the VPN peers can be done with digital certificates using the RSA or DSA signature algorithm, or a pre-shared secret. The pre-shared secret is used as a part of the MAC key authenticating the phase-I exchange.

Crypto Officer Services
IPSec encryption keys at the connection level may be supplied through the management server interface. The management server interface uses authenticated and encrypted TLS communications.

4.5 Session Keys

User (IPSec) Services
During IKE Phase 1 negotiation, VPN nodes establish Security Association (SA) that defines 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 lifetime expires, new session keys are negotiated.

Crypto Officer Services
The session keys for TLS connections between the module and the management server are generated by a method that is provided by the TLS protocol. The method is specified in IETF RFC 2246.

4.6 Crypto Officer Password

Crypto Officer Services
The Crypto Officer (Role A) password is entered during initial software load. It is active during the installation and disabled after the installation.

4.7 Random Number Generation

The cryptographic module uses X9.31 APPENDIX A.2.4 compatible random number generator in order to generate random keys in FIPS 140-2 approved mode.

5. ACCESS CONTROL POLICY

User access to the VPN and its associated critical security parameters is through the execution of module's code only. The Crypto Officer (Role B) has no access to user keys with the exception of the instance when the Crypto Officer (Role B) is supplying an IKE pre-shared secret or IPSec key

. Table 2. Service's Access to All Security-relevant Information

Critical Security Parameters	**Key Type (If it is a key)**	**Service**	**Role**	**Type of access**
IKE pre-shared secret	HMAC-SHA-1	Authentication in IKE key establishment negotiations	User Crypto Officer (Role B)	Read Write
IKE certificate(s)	RSA DSA	Authentication in IKE key establishment negotiations	User Crypto Officer (Role B)	Read Write
IKE private key(s)	RSA DSA	Authentication in IKE key establishment negotiations	User Crypto Officer (Role B)	Read Write
IKE local secret	HMAC-SHA-1	Key used for VPN anti-clogging protection, established during IKE negotiation	User	Write
Crypto Officer supplied IPSec encryption keys	DES 3DES AES	Encryption and decryption of data in connections that do not use IKE for key establishment	User Crypto Officer (Role B)	Read Write
Certification Authority Certificates	RSA DSA	Authentication of peer certificates in IKE negotiations	User	Read
IKE-negotiated IPSec encryption keys	DES 3DES AES	Encryption and decryption of data in connections that use IKE for key establishment	User	Write
IKE-negotiated IPSec authentication keys	HMAC-SHA-1	Authentication of data in connections that use IKE for key establishment	User	Write
TLS certificate /	RSA	Authentication of	Crypto Officer	Read

Critical Security Parameters	**Key Type (If it is a key)**	**Service**	**Role**	**Type of access**
private key		internal connections between the firewall nodes and management server	(Role B)	
TLS certificate of management server	RSA	Authentication of internal connections between the firewall nodes and management server	Crypto Officer (Role B)	Read
TLS encryption key	3DES	Encryption of internal connections between the firewall nodes and management server	Crypto Officer (Role B)	Read
TLS authentication key	HMAC-SHA-1	Authentication of internal data connections between the firewall nodes and management server	Crypto Officer (Role B)	Read
File encryption key (filesec)	3DES	Encryption of files in node's hard disk	Crypto Officer (Role B)	Read
File authentication key (filesec)	HMAC-SHA-1	Authentication of files in node's hard disk	Crypto Officer (Role B)	Read
Crypto officer password	No cryptography applied	Password crypto officer supplies, when login in at console.	Crypto Officer (Role A)	Write

Please note, that TLS private key and TLS certificate are created when system is installed.

The Crypto Officer (Role B), beyond selecting FIPS Approved mode, can select encryption algorithm, if there are several encryption algorithms available in FIPS 140-2 Approved mode. Table 3 shows cryptographic algorithms that are used in cryptographic module.

SSH Toolkit Algorithms used for IPSec Services	**Algorithms in OpenSSL used for TLS Services**	**Algorithms Used in OpenSSH Used for SSH Services**
FIPS Approved	***FIPS Approved***	***FIPS Approved***
DES (#194) [ECB, CBC, CFB, OFB modes]		
3DES (#147) [ECB, CBC, CFB, OFB modes]	3DES (#145) [CBC mode]	3DES (#146) [CBC mode]
AES (#40) [ECB, CBC, CFB, OFB modes]		AES (#39) [CBC mode]
SHA-1 (#132)	SHA-1 (#131)	Uses OpenSSL implementation
HMAC-SHA-1 (#132, vendor affirmed)		
DSA (#78)	DSA (#77)	DSA, Uses OpenSSL implementation
RSA (PKCS#1, vendor affirmed)	RSA (PKCS#1, vendor affirmed)	RSA, Uses OpenSSL implementation
PRNG (X9.31 Appendix A.2.4 compliant)	PRNG, Uses SSH Toolkit Implementation	PRNG, Uses SSH Toolkit Implementation
Non-Approved		
Diffie-Hellman		
SHA-256		
Blowfish		
Twofish		
Cast-128		
MD5		

Table 3. Cryptographic algorithms used in StoneGate High Availability Firewall VPN Module

Zeroization of keys

The keys are stored in the CPU's memory only for the time they are used. When the keys are no longer needed, the corresponding memory area is overwritten with null data. Zeroization of keys on the hard drive (e.g. certificates) is done by the Crypto Officer, who formats the hard drive.

6. OPERATING MODES

The cryptographic module has two operating modes:

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

Enabling FIPS 140-2 Approved mode is four step procedure:

1. Crypto Officer (Role A) must disable root account from cryptographic module after the installation of the cryptographic module is complete.
2. Cryptographic Officer Role B must only enable the FIPS approved algorithms.
3. Crypto Officer (Role A) must disable OpenSSH remote connection possibility when installing cryptographic module from CD.
4. Crypto Officer (Role B) must also disable VPN Client policy download possibility from the cryptographic module.

The operating system is not modifiable in FIPS 140-2 Approved mode, because there is no user accounts on the operating system level that could perform login to the operating system.

Detailed instructions can be found on StoneGate How-To Guidelines: Implementing a FIPS-compliant VPN.

When using FIPS 140-2 Approved mode only FIPS 140-2 approved encryption algorithms can be used. In FIPS 140-2 Approved mode the cryptographic module will reject any attempt to configure non-FIPS approved algorithms. The cryptographic module generates a log entry every time it enters or exits the FIPS 140-2 Approved mode.

OpenSSL component operates always in FIPS 140-2 Approved mode and its configuration is predefined.

7. PHYSICAL SECURITY

The software module was tested on a standard IBM X330 rack-optimized PC. In FIPS 140-2 terms, the cryptographic hardware module is a “multi-chip stand alone module.” consisting of industrial grade components with standard passivation and is entirely enclosed within a production-grade enclosure that includes removable covers.

Prior to performing physical maintenance, all plaintext secret and private keys and other unprotected CSPs contained in the cryptographic module shall be zeroized by the cryptographic officer.

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