Forcepoint LLC

Forcepoint® Sidewinder™

Module version: 8.3.2, firmware version: 8.3.2P07 with patch 8.3.2E106

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation

Document revision 014, July 2016

Forcepoint LLC
10900-A Stonelake Blvd.
Austin, TX 78759
United States of America

http://www.forcepoint.com/

Prepared for Forcepoint LLC by

Rycombe Consulting Limited
http://www.rycombe.com
+44 1273 476366

Contents

Figures

Tables

1 Introduction

This section identifies the cryptographic module; describes the purpose of this document; provides external references for more information; and explains how the document is organized.

1.1 Identification

Module Name	Forcepoint® Sidewinder™
Module Version	8.3.2
Firmware Version	8.3.2P07 with patch 8.3.2E106

1.2 Purpose

This is the non-proprietary FIPS 140-2 Security Policy for Forcepoint® Sidewinder™, also referred to as "the module" within this document. This Security Policy details the secure operation of Forcepoint® Sidewinder™ as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

1.3 References

For more information on Forcepoint LLC products please visit: http://www.forcepoint.com/. For more information on NIST and the Cryptographic Module Validation Program (CMVP), please visit http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.4 Document Organization

This Security Policy document is one part of the FIPS 140-2 Submission Package. This document outlines the functionality provided by the module and gives high-level details on the means by which the module satisfies FIPS 140-2 requirements. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission documentation may be Forcepoint LLC proprietary or otherwise controlled and releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Forcepoint LLC.

The Forcepoint LLC Forcepoint® Sidewinder™ Module version: 8.3.2, firmware version: 8.3.2P07 cryptographic module is a rebranding of the McAfee, Inc. McAfee Firewall Enterprise Module version: 8.3.2, firmware version: 8.3.2P07 cryptographic module. This is a cosmetic rebranding. The hardware and firmware of the two modules is identical. Some items such as the product documentation and some system software have not been rebranded and so still bear the McAfee branding. Where the "McAfee" name appears in this document it is intentional and reflects the heritage of the cryptographic module.

The various sections of this document map directly onto the sections of the FIPS 140-2 standard and describe how the module satisfies the requirements of that standard.

1.5 Document Terminology

TERM	DESCRIPTION
AC	Alternating Current
ACPI	Advanced Configuration and Power Interface
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BIOS	Basic Input/Output System
BMC	Baseboard Management Controller
CA	Certificate Authority
CAC	Common Access Card
CAST	Carlisle Adams and Stafford Tavares
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CD	Compact Disc
CD-ROM	Compact Disc – Read-Only Memory
CFB	Cipher Feedback
CLI	Command Line Interface
CLSOS	Cryptographic Library for SecureOS
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CPU	Central Processing Unit
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DES	Digital Encryption Standard
DH	Diffie-Hellman
DoS	Denial of Service
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
DVD	Digital Versatile Disc
ECB	Electronic Codebook
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HA	High Availability
HDD	Hard Disk Drive

HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IG	Implementation Guidance
IKE	Internet Key Exchange
I/O	Input/Output
IP	Internet Protocol
IPsec	Internet Protocol Security
KAT	Known Answer Test
KCLSOS	Kernel Cryptographic Library for SecureOS
KDF	Key Derivation Function
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
MD	Message Digest
MIB	Management Interface Base
NAT	Network Address Translation
NDRNG	Non-Deterministic Random Number Generator
NIA	Network Integrity Agent
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NMS	Network Management System
OFB	Output Feedback
OS	Operating System
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PKCS	Public Key Cryptography Standard
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RC	Rivest Cipher
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SQL	Structured Query Language

SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
UTM	Unified Threat Management
VGA	Video Graphics Array
VPN	Virtual Private Network

Table 1 Document terminology

2 Forcepoint® Sidewinder™

This section provides the details of how the module meets the FIPS 140-2 requirements.

2.1 Overview

Forcepoint LLC is a global leader in Enterprise Security solutions. The company's comprehensive portfolio of network security products and solutions provides unmatched protection for the enterprise in the most mission-critical and sensitive environments. Forcepoint® Sidewinder™ solutions are created to meet the specific needs of organizations of all types and enable those organizations to reduce costs and mitigate the evolving risks that threaten today's networks and applications.

Consolidating all major perimeter security functions into one system, Forcepoint® Sidewinder™ appliances are the strongest self-defending perimeter firewalls in the world. Built with a comprehensive combination of high-speed application proxies, reputation-based threat intelligence, and signature-based security services, Sidewinder™ defends networks and Internet-facing applications from all types of malicious threats, both known and unknown.

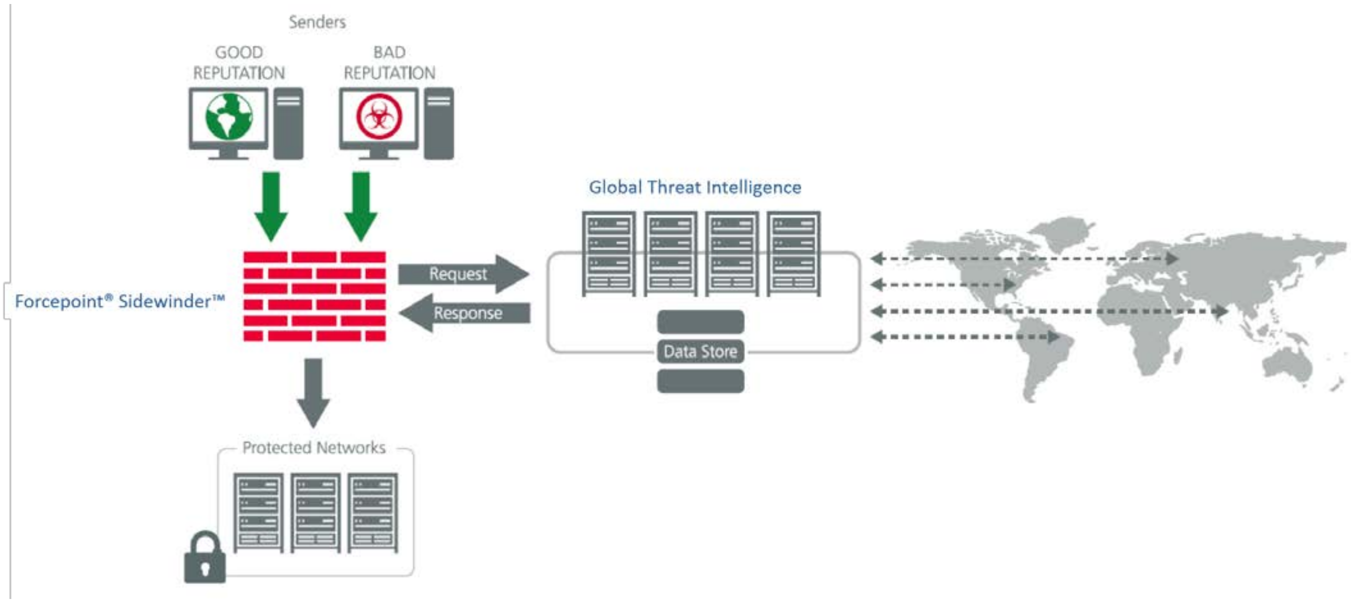


Figure 1 Typical Deployment Scenario

Sidewinder™ appliances are market-leading, next-generation firewalls that provide application visibility and control even beyond Unified Threat Management (UTM) for multi-layer security – and the highest network performance. Global visibility of dynamic threats is the centerpiece of Sidewinder™ and one of the key reasons for its superior ability to detect unknown threats along with the known. Sidewinder™ appliances deliver the best-of-breed in security systems to block attacks, including:

- Viruses
- Worms
- Trojans
- Intrusion attempts

- Spam and phishing tactics
- Cross-site scripting
- Structured Query Language (SQL) injections
- Denial of service (DoS)
- Attacks hiding in encrypted protocols

Sidewinder™ security features include:

- Firewall feature for full application filtering, web application filtering, and Network Address Translation (NAT)
- Authentication using local database, Active Directory, LDAP , RADIUS (RADIUS traffic can be sent over IPsec for added security although this is not a requirement), Windows Domain Authentication, and more
- High Availability (HA)
- Geo-location filtering
- Encrypted application filtering using TLS and IPsec protocols
- Intrusion Prevention System
- Networking and Routing
- Management via Simple Network Management Protocol (SNMP) version 3
- Per-connection auditing and policy enforcement of endpoints via DTLS protocol

Forcepoint® Sidewinder™ installed on a Forcepoint® Sidewinder™ appliance can be managed locally or remotely using one of the following management tools:

- Administration Console – The Administration Console (or Admin Console) is the graphical software that runs on a Windows computer within a connected network. Admin Console is Forcepoint's proprietary GUI management software tool that needs to be installed on a Windows-based workstation. This is the primary management tool. All Admin Console sessions are protected over secure TLS channel.

- Command Line Interface (CLI) – A UNIX-based CLI is also available for configuring the firewall and performing troubleshooting functions. It can be used as an alternative to the Admin Console to perform most administration tasks. The CLI is accessed locally over the serial port or by a direct-connected keyboard and mouse, while remote access is via Secure Shell (SSH) session.

- Forcepoint® Sidewinder™ SNMP Agent –Forcepoint® Sidewinder™ installed on a Forcepoint® Sidewinder™ appliance can use the SNMP v3 protocol for remote management, and to provide information about the state and statistics as part of a Network Management System (NMS).

  Although SNMP v3 can support AES encryption, the protocol employs a non-approved key generation method. However, the module's SNMP Agent does not support "set" requests, preventing the modification of any critical security parameters (CSPs) through this interface. Additionally, because the module's CSPs are not defined in the Firewall's MIB, information about those CSPs is not made available to be transmitted or viewed over this interface. Thus, this interface provides management for non-FIPS-relevant information only, and offers no ability to alter or view CSPs.

- Forcepoint® Sidewinder™ Control Center – Sidewinder™ Control Center is an enterprise-class management appliance that enables scalable centralized management and monitoring of Forcepoint® Sidewinder™ solutions, allowing network administrators to centrally define firewall policy, deploy updates, inventory their firewall products, generate reports, and demonstrate regulatory compliance. Sidewinder™ Control Center is designed to run on an administrator's workstation, and allows network administrators to fully manage their firewall solutions from the network edge to the core. Management communications between the Forcepoint® Sidewinder™ and Sidewinder™ Control Center are secured over a TLS session.

For more information regarding Sidewinder™ Control Center, please refer to Forcepoint's Sidewinder™ Control Center product documentation.

2.2 Module Specification

Forcepoint® Sidewinder™ cryptographic module is a firmware module with a multi-chip standalone embodiment. The module meets overall Level 1 FIPS 140-2 requirements. The module was tested and found compliant on a Forcepoint® Sidewinder™ 1402-C3 appliance.

2.2.1 Hardware, Software and Firmware components

The module is a firmware module and has no hardware or software components. The module implements three firmware cryptographic libraries to offer secure networking protocols and cryptographic functionalities. The firmware libraries for the module are:

- Forcepoint® Sidewinder™ 32-bit Cryptographic Engine v8.3.2
- Forcepoint® Sidewinder™ 64-bit Cryptographic Engine v8.3.2
- Kernel Cryptographic Library for SecureOS® (KCLSOS) v8.2

2.2.2 Cryptographic Boundary

The cryptographic boundary of Forcepoint® Sidewinder™ is defined by all the firmware that runs on the Forcepoint® Sidewinder™ appliance hardware, operating within the Forcepoint® Sidewinder™ enclosure. The physical cryptographic boundary of the module is the hardware appliance, from this point forward referred to as the 'host appliance', that it runs on. The logical cryptographic boundary is drawn around the module code that runs entirely on the host appliance's CPU.

The processor of this platform executes all firmware. All firmware components of the module are persistently stored within the device and, while executing, are stored in the device local RAM.

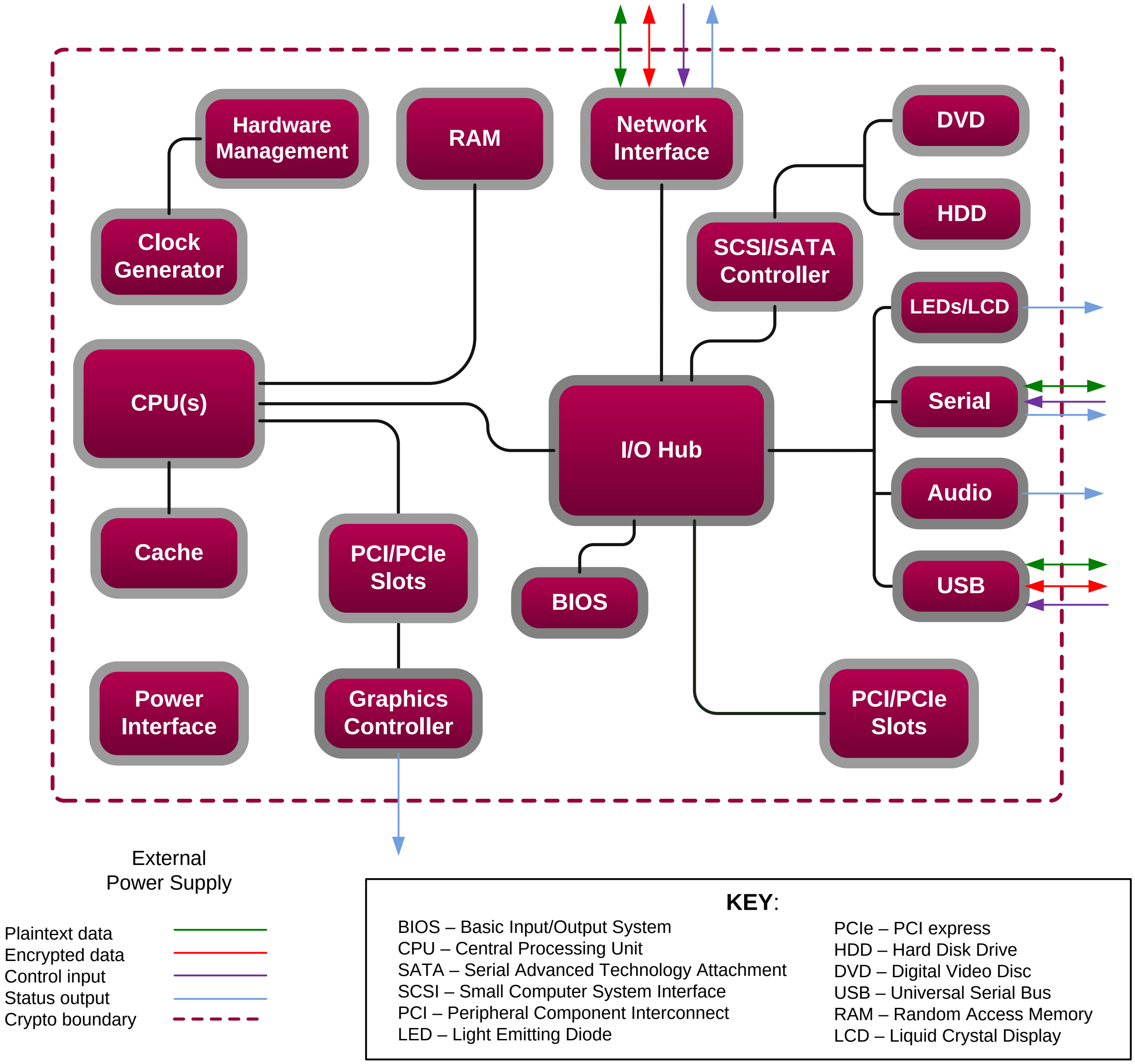


Figure 2 Hardware Block Diagram

The logical cryptographic boundary of the module (shown by the red dotted line in Figure 3 below) consists of the Forcepoint® Sidewinder™ firmware including three cryptographic libraries and Forcepoint's SecureOS® v8.3 firmware running on the host appliance.

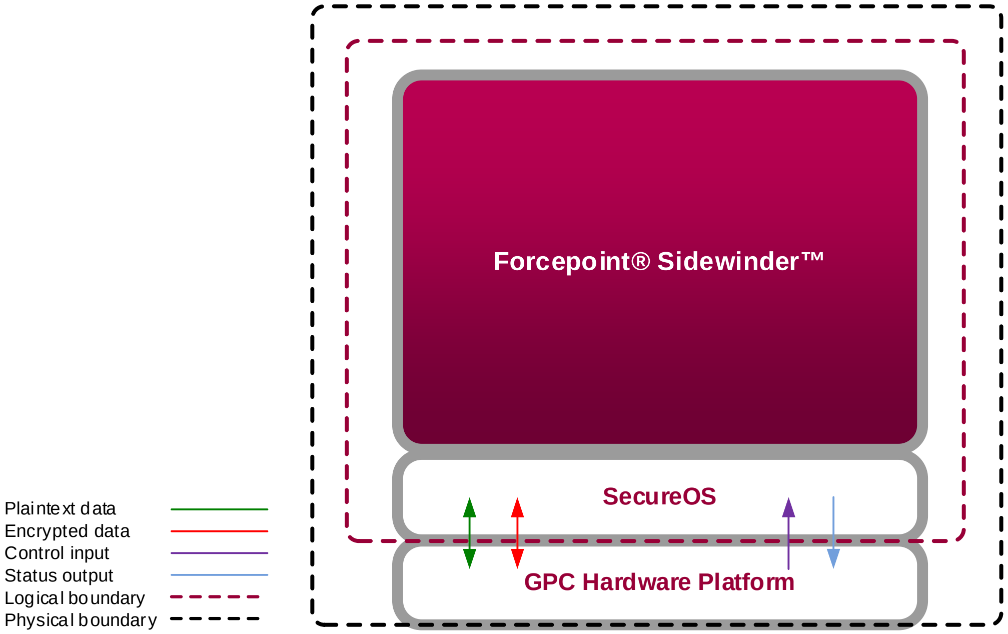


Figure 3 Logical Block Diagram

The Forcepoint® Sidewinder™ cryptographic module was tested on the Forcepoint® Sidewinder™ 1402-C3 appliance and was found to conform to FIPS 140-2 Level 1 requirements. The validated firmware version is 8.3.2P07.

The cryptographic module is also vendor affirmed to be FIPS 140-2 compliant on the following Forcepoint® Sidewinder™ appliance models however no claim is made as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not on the validation certificate:

- FWE-S1104
- FWE-S2008
- FWE-S3008
- FWE-S4016
- FWE-S5032
- FWE-S6032

2.2.3 Scope of Evaluation

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2, with both Design Assurance and Cryptographic Module Specification at Level 3.

SECURITY REQUIREMENTS SECTION	LEVEL
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 Security Level specification per individual areas of FIPS 140-2

2.2.4 Cryptographic Algorithms

2.2.4.1 Approved Algorithms

The following table provides details of the approved algorithms that are included within the module:

Approved Security Function	Certificate #		
	32-Bit	64-Bit	KCLSOS
Symmetric Key			
Advanced Encryption Standard (AES) 128/192/256-bit in CBC, ECB, OFB, CFB128 modes and 256-bit in CTR mode	#2711	#2713	-
AES 128/192/256-bit in CBC, ECB modes	-	-	#1833
Triple Data Encryption Standard (DES) 3-key options in CBC, ECB, OFB, CFB64 modes	#1628	#1630	-
Triple-DES 3-key option in CBC mode	-	-	#1185
Asymmetric Key			
RSA ANSI X9.31 key generation: 2048/3072/4096-bit	#1407	#1409	-
RSA PKCS #1 signature generation: 2048/3072/4096-bit	#1407	#1409	-
RSA PKCS #1 signature verification: 1024/1536/2048/3072/4096-bit	#1407	#1409	-
DSA PQG generation: 2048-bit	#828	#830	-
DSA PQG verification: 1024/2048/3072-bit	#828	#830	-
DSA key generation: 2048/3072-bit	#828	#830	-
DSA signature generation: 2048/3072-bit	#828	#830	-
DSA signature verification: 1024/2048/3072-bit	#828	#830	-
ECDSA key generation (2048-bit); signature generation/verification (2048/256-bit)	#472	#474	-
Secure Hash Standard			
SHA-1, SHA-256, SHA-384, and SHA-512	#2276	#2278	#1612
Message Authentication			
HMAC using SHA-1, SHA-256, SHA-384, and SHA-512	#1690	#1692	#1086
Random Number Generators (RNG)			
SP 800-90 Counter-based DRBG	#448	#450	-

Table 3 Approved Algorithms

Notes:

DSA 1024-bit signature verification is allowed for legacy use.

RSA 1024/1536-bit signature verification is allowed for legacy use.

For details regarding algorithm transition, please refer to NIST Special Publication 800-131A.

ECDSA is used only for SSH. The NIST supported curves are P-256, P-384, and P-521. These are used for both signature generation and signature verification.

The following table lists the key derivation functions (and their associated CVL certificate numbers) implemented by the module.

Approved KDF	32-Bit Protocol Engine	64-Bit Protocol Engine
Transport Layer Security (TLS) v1.0	#168	#171
Secure Shell (SSH)	#168	-
Internet Key Exchange (IKE) v1 and v2	#168	-
Simple Network Management Protocol (SNMP) v3	-	#171

Table 4 Approved Key Derivation Functions

For each of these approved Key Derivation Functions the module supports or uses the corresponding protocol. These protocols can be used in the approved mode of operation, but have not been reviewed or tested by the CAVP and CMVP as testing such protocols is not within the scope of CMVP or CAVP activities.

The module includes mostly 32-bit executables and a few 64-bit executables. There are two separate crypto libraries to support these two classes of executables. For example, IKE and SSH are 32-bit, and SNMP is 64-bit. There are both 32-bit and 64-bit executables that use TLS.

The TLS implementation used in this module is not subject to the Heartbleed bug.

2.2.4.2 Non-approved algorithms allowed in approved mode

The module utilizes the following non-compliant algorithm implementation, which is allowed for use in a FIPS-approved mode of operation:

- Diffie-Hellman 2048 bit (key agreement; key establishment methodology provides 112 bits of encryption strength

The module employs an NDRNG that provides the entropy used to seed the approved SP 800-90 Counter-based DRBG.

The module also includes two library/executable collections that provide the key derivation function (KDF) implementations for the various protocols. These engines provide KDF functionality to both 32-bit and 64-bit applications resident on the module. They are:

- Forcepoint® Sidewinder™ 32-bit Protocol Engine v8.3.2
- Forcepoint® Sidewinder™ 64-bit Protocol Engine v8.3.2

2.2.5 Components excluded from the security requirements of the standard

There are no components excluded from the security requirements of the standard.

2.3 Physical ports and logical interfaces

The module is classified as a multi-chip standalone module for FIPS 140-2 purposes. The module's physical boundary is that of the device on which it is installed. The device shall run a supported operating system (OS) and supporting sufficient interfaces to allow operators to initiate cryptographic operations and determine the module status.

The module provides its logical interfaces via the physical interfaces of its host appliance. These logical interfaces provide the module services (described in section 2.4.2).

The logical interfaces provided by the module are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output as follows:

FIPS 140-2 Logical Interface	Module Interface Mapping
Data Input	Connectors (Ethernet)
Data Output	Connectors (Ethernet)
Control Input	Connectors (Ethernet, USB, serial) and button (power)
Status Output	Connectors (VGA, Ethernet, serial), and LED indicators (power-on, drive activity, system status, network activity)
Power Interface	Connectors (power)

Table 5 Module Interfaces

2.4 Roles, Services and Authentication

The following sections described the authorized roles supported by the module and the services provided for those roles.

2.4.1 Roles

The Cryptographic Module implements both a Crypto Officer role and a User role. Section 2.4.2 summarizes the services available to each role.

Role	Description
Crypto Officer	A Crypto-Officer performs administrative services on the module, such as initialization, configuration, and monitoring of the module.
User	A User employs the services of the module for establishing VPN or TLS connections via Ethernet.

Table 6 Roles

2.4.2 Services

The services that require operators to assume an authorized role (Crypto-Officer or User) are listed in Table 7 below. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 7 use the following indicators to show the type of access required:

- R (Read): The CSP is read
- W (Write): The CSP is established, generated, modified, or zeroized
- X (Execute): The CSP is used within an approved or allowed security function or authentication mechanism

Service	Description	CO	User	CSP and Type of Access
Authenticate to the Admin Console	Allows administrators to login to the appliance using the Sidewinder™ Admin Console	x		Administrator Password - R
Authenticate to the Admin Console using Common Access Card (CAC)	Allows administrators to login to the appliance with CAC authentication to access the Sidewinder™ Admin Console	x		Common Access Card One-Time Password - R
Authenticate to the Admin CLI	Allows administrators to login to the appliance using the Sidewinder™ Admin CLI	x		Administrator Password - R
Authenticate to the Admin CLI using CAC	Allows administrators to login to the appliance with CAC authentication to access the Sidewinder™ Admin CLI	x		Administrator Password - R
Authenticate to the local console	Allows administrators to login to the appliance via the local console	x		Administrator Password - R
Change password	Allows external users to use a browser to change their Sidewinder™, SafeWord PremierAccess, or LDAP login password	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W Administrator Password - R/W
Manage network objects	Allows administrators to view, create, and maintain network objects, manage netgroup memberships, and manage access control rules' time periods	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W

Service	Description	CO	User	CSP and Type of Access
Configure identity validation method	Allows administrators to select identity validation settings	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure cluster communication	Provides services required to communicate with each other in Sidewinder™ multi-appliance configurations	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure and monitor Virtual Private Network (VPN) services	Generates and exchanges keys for VPN sessions	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W IKE Preshared key - W IPsec Session Key - W IPsec Authentication Key - W
Create and configure bypass mode	Creates and monitors IPsec policy table that governs alternating bypass mode	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage web filter	Manages configuration with the SmartFilter	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage Sidewinder™ Control Center communication	Verifies registration and oversees communication among the Sidewinder™ Control Center and managed Sidewinder™ appliances	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure Network Integrity Agent (NIA) settings	Configures NIA authentication and certificate settings, enable agent discovery, modify connection settings, and create explicit NIA communication rules	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W

Service	Description	CO	User	CSP and Type of Access
Configure content inspection settings	Configures settings for content inspection methods	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage applications and Application Defense information	Manages applications, application groups, and Application Defense settings	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage access control rules	Manages rules enforcing policy on network flows to or through the firewall	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage SSL rules	Manages SSL rules for processing SSL connections	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Process audit data	Allows administrators to view and export audit data, transfer audit records, and manage log files.	x		Firewall Authentication Keys - R Key Agreement Key - R DTLS Session Authentication Key - R/W DTLS Session Key - R/W
Manage attack and system responses	Configures how the firewall should respond to audit events that indicate abnormal and potentially threatening activities	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure network defenses	Customizes audit output for attacks on specific networks stopped by the firewall	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
View active hosts	Provides a method to view active hosts connected to a Sidewinder™ appliance	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Configure the SNMP Agent	Configures the SNMP Agent for status monitoring of non-FIPS-relevant information	x		SNMP v3 Session Key - R

Service	Description	CO	User	CSP and Type of Access
Configure networking	Configures and manages network characteristics, security zones, and Quality of Service profiles.	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Manage email services	Manages email options and 'sendmail' features	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Load package	Downloads available firmware update or patch	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Perform self-tests	Run self-tests on demand via reboot	x		None
Enable FIPS mode	Configures the module in FIPS mode	x		Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W
Show status	Allows Crypto-Officer to check whether FIPS mode is enabled	x		None
Zeroize	Resets the module to its factory default state	x		Common Access Card Authentication keys - R/W Firewall Authentication public/private keys - R/W Peer public keys - R/W Local CA public/private keys - R/W IKE Preshared Key - R/W IPsec Session Authentication Key - R/W Administrator Passwords - R/W SSL CA key - R/W SSL Server Certificate key - R/W
Establish an authenticated TLS connection	Establish a TLS connection (requires operator authentication)		x	Firewall Authentication Keys - R Key Agreement Key - R TLS Session Authentication Key - R/W TLS Session Key - R/W SSL CA key - R SSL Server Certificate key - R

Service	Description	CO	User	CSP and Type of Access
Establish a VPN connection	Establish a VPN connection over IPsec tunnel		x	Firewall Authentication Keys - R Key Agreement Key - R IKE Session Authentication Key - W IKE Session Key - W IKE Preshared Key - R IPsec Session Key - R/W IPsec Authentication Key - R/W

Table 7 Authorized Operator Services

In addition to the services listed in Table 7 Authorized Operator Services, the module provides non-security relevant services. The non-security relevant services provided by the module can be found in the module's product guide: *McAfee Firewall Enterprise 8.3.2P03 and later Product Guide Revision B*. The document is publicly available for download at https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25204/en_US/fe_832P03_pg_b_en-us.pdf.

2.4.3 Authentication

The module has been evaluated at FIPS 140-2 level 1 and no claims are made for authentication.

2.5 Physical Security

The Cryptographic Module is a firmware-only cryptographic module and therefore the physical security requirements of FIPS 140-2 do not apply.

2.6 Operational Environment

The requirements in this section are not applicable, as the module does not provide a general-purpose operating system (OS) to module operators. Forcepoint's proprietary SecureOS version 8.3 provides a limited operational environment, and only the module's custom-written image can be run on the OS. The module provides a method to update the firmware in the module with a new version. This method involves downloading a digitally-signed firmware update to the module.

2.7 Cryptographic Key Management

2.7.1 Random Number Generators

The module contains an approved counter-mode SP800-90 approved DRBG. Checks are made to ensure that the quality of the entropy remains high enough to be used to seed the DRBG.

Entropy is collected from user key presses and mouse events, interrupts and network packets. The entropy seeds the DRBG via the /dev/random library.

2.7.2 Key Generation

The module generates keys using an approved key generation mechanism made up of an SP 800-90A CTR_DRBG and available entropy conditioned by /dev/random.

2.7.3 Key Table

The following tables list all of the keys and CSPs within the module, describe their purpose, and describe how each key is generated, entered and output, stored and destroyed.

KEY/CSP	PURPOSE	32-BIT VERSION	64-BIT VERSION
SNMPv3 Session Key	Provides secured channel for SNMPv3 management	-	X
Common Access Card Authentication keys	Common Access Card Authentication for generation of one-time password	X	X
Firewall Authentication public key	- Peer Authentication of TLS, IKE, and SSH sessions - Audit log signing	X	X
Firewall Authentication private key	- Peer Authentication of TLS, IKE, and SSH sessions - Audit log signing	X	X
Peer public key	Peer Authentication for TLS, SSH, and IKE sessions	X	X
Local CA public key	Local signing of firewall certificates and establish trusted point in peer entity	X	X
Local CA private key	Local signing of firewall certificates and establish trusted point in peer entity	X	X
Key Agreement Key	Key exchange/agreement for DTLS, TLS, IKE/IPsec and SSH sessions	X	X
TLS Session Authentication Key	Data authentication for TLS sessions	X	X
TLS Session Key	Data encryption/decryption for TLS sessions	X	X
DTLS Session Authentication Key	Data authentication for DTLS sessions	X	X

Key/CSP	Purpose	32-bit Version	64-bit Version
DTLS Session Key	Data encryption/decryption for DTLS sessions	X	X
IKE Session Authentication Key	Data authentication for IKE sessions	X	-
IKE Session Key	Data encryption/decryption for IKE sessions	X	-
IKE Preshared Key	Data encryption/decryption for IKE sessions	X	-
IPsec Session Authentication Key	Data authentication for IPsec sessions	X	X
IPsec Session Key	Data encryption/decryption for IPsec sessions	X	X
IPsec Preshared Session Key	Data encryption/decryption for IPsec sessions	X	X
SSH Session Authentication Key	Data authentication for SSH sessions	X	-
SSH Session Key	Data encryption/decryption for SSH sessions	X	-
Package Distribution Public Key	Verifies the signature associated with a firewall update package	X	X
License Management Public Key	Verifies the signature associated with a firewall license	X	X
Administrator Password	Standard Unix authentication for administrator login	X	X
Common Access Card One-Time Password	Common Access Card authentication for administrator login	X	X
SSL CA Key	Signing temporary server certificates for TLS re-encryption	X	X
SSL Server Certificate Key	Peer authentication for TLS sessions (TLS re-encryption)	X	X
DRBG Entropy Input	Provides entropy input to the DRBG	X	X
DRBG seed	Seeds the DRBG	X	X
DRBG V	The DRBG "V" parameter, DRBG internal state value	X	X
DRBG Key	The DRBG "Key" parameter, DRBG internal state value	X	X

Table 8 Module Cryptographic Keys and CSPs

Key/CSP	Key//CSP type	Generation/Input	Output
SNMPv3 Session Key	AES 128-bit CFB key	Internally generated using a non-compliant method	Never exits the module
Common Access Card Authentication keys	RSA 2048-bit key DSA 2048-bit key	Imported electronically in plaintext	Never exits the module
Firewall Authentication public key	RSA 2048-bit key	Internally generated	Output in encrypted form via network port or in plaintext form via local management port
	RSA 2048-bit key	Imported electronically in plaintext via local management port	Never exits the module
Firewall Authentication private key	RSA 2048-bit key	Internally generated	Never exits the module
Peer public key	RSA 2048-bit key	Imported electronically in plaintext during handshake protocol	Never exits the module
Local CA public key	RSA 2048-bit key	Internally generated	Public key certificate exported electronically in plaintext via local management port
Local CA private key	RSA 2048-bit key	Internally generated	Never exits the module
Key Agreement Key	Diffie-Hellman 2048-bit key RSA 2048/3072-bit key	Internally generated	Public exponent electronically in plaintext, private component not exported
TLS Session Authentication Key	160-bit HMAC SHA-1 key	Internally generated	Never exits the module
TLS Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module
DTLS Session Authentication Key	160-bit HMAC SHA-1 key	Internally generated	Never exits the module
DTLS Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module
IKE Session Authentication Key	160-bit HMAC SHA-1 key	Internally generated	Never exists the module
IKE Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module

KEY/CSP	KEY//CSP TYPE	GENERATION/INPUT	OUTPUT
IKE Preshared Key	Triple-DES, AES-128, AES-256 key	- Imported in encrypted form over network port or local management port in plaintext - Manually entered	Never exits the module
IPsec Session Authentication Key	160-bit HMAC SHA-1 key	- Imported in encrypted form over network port or local management port in plaintext - Internally generated - Manually entered	Never exits the module
IPsec Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exits the module
IPsec Preshared Session Key	Triple-DES, AES-128, AES-256 key	- Imported in encrypted form over network port or local management port in plaintext - Manually entered	Exported electronically in plaintext
SSH Session Authentication Key	160-bit HMAC SHA-1 key	Internally generated	Never exists the module
SSH Session Key	Triple-DES, AES-128, AES-256 key	Internally generated	Never exists the module
Package Distribution Public Key	DSA 1024-bit public key	Externally generated and hard coded in the image	Never exits the module
License Management Public Key	DSA 1024-bit public key	Externally generated and hard coded in the image	Never exits the module
Administrator Password	PIN	Manually or electronically imported	Never exits the module
Common Access Card One-Time Password	8-character (minimum) ASCII string	Internally generated; Manually or electronically imported	Exported electronically in encrypted form over TLS
SSL CA Key	RSA 2048-bit key DSA 2048-bit key	Internally generated	Exported electronically in ciphertext via network port or in plaintext via local management port

KEY/CSP	KEY//CSP TYPE	GENERATION/INPUT	OUTPUT
SSL Server Certificate Key	RSA 2048-bit key DSA 2048-bit key	Internally generated or imported electronically in plaintext via local management port	Exported electronically in ciphertext via network port or in plaintext via local management port
DRBG Entropy Input	256-bits	SP 800-90 CTR_DRBG	N/A
DRBG seed	384-bits	SP 800-90 CTR_DRBG	N/A
DRBG V	128-bits	SP 800-90 CTR_DRBG	N/A
DRBG Key	256-bits	SP 800-90 CTR_DRBG	N/A

Table 9 Key Table Part 1

Notes:

The management port is provided via the network interface using the combination of the control input port for input and the status output port for output.

KEY/CSP	STORAGE	ZEROIZATION
SNMPv3 Session Key	Resides in volatile memory in plaintext	Power cycle or session termination
Common Access Card Authentication keys	Stored in plaintext on the hard disk	Erasing the system image
Firewall Authentication public key	Stored in plaintext on the hard disk or Resides in volatile memory in plaintext	Erasing the system image
Firewall Authentication private key	Stored in plaintext on the hard disk	Erasing the system image
Peer public key	Stored in plaintext on the hard disk	Erasing the system image
Local CA public key	Stored in plaintext on the hard disk	Erasing the system image
Local CA private key	Stored in plaintext on the hard disk	Erasing the system image
Key Agreement Key	Resides in volatile memory in plaintext	Power cycle or session termination
TLS Session Authentication Key	Resides in volatile memory in plaintext	Power cycle or session termination
TLS Session Key	Resides in volatile memory in plaintext	Power cycle or session termination
DTLS Session Authentication Key	Resides in volatile memory in plaintext	Power cycle or session termination
DTLS Session Key	Resides in volatile memory in plaintext	Power cycle or session termination
IKE Session Authentication Key	Resides in volatile memory in	Power cycle or session

KEY/CSP	STORAGE	ZEROIZATION
	plaintext	termination
IKE Session Key	Resides in volatile memory in plaintext	Power cycle or session termination
IKE Preshared Key	Stored in plaintext on the hard disk	Erasing the system image
IPsec Session Authentication Key	- Stored in plaintext on the hard disk - Resides in volatile memory	Power cycle
IPsec Session Key	Resides in volatile memory in plaintext	Power cycle
IPsec Preshared Session Key	Stored in plaintext on the hard disk	Power cycle
SSH Session Authentication Key	Resides in volatile memory in plaintext	Power cycle or session termination
SSH Session Key	Resides in volatile memory in plaintext	Power cycle or session termination
Package Distribution Public Key	Hard coded in plaintext	N/A
License Management Public Key	Hard coded in plaintext	N/A
Administrator Password	Stored on the hard disk through one-way hash obfuscation	Erasing the system image
Common Access Card One-Time Password	Resides in volatile memory inside the CAC Warder process	Password expiration, session termination, or power cycle
SSL CA Key	Stored in plaintext on the hard disk	Erasing the system image
SSL Server Certificate Key	Stored in plaintext on the hard disk	Erasing the system image
DRBG Entropy Input	Stored in plaintext on the hard disk	Power cycle
DRBG seed	Stored in plaintext on the hard disk	Power cycle
DRBG V	Stored in plaintext on the hard disk	N/A
DRBG Key	Stored in plaintext on the hard disk	N/A

Table 10 Key Table Part 2

2.7.4 Key Destruction

All key material managed by the module can be zeroized using the key zeroization service.

In this way all key material and CSPs are zeroized. There are no user-accessible plaintext keys or CSPs in the module.

2.8 Self-Tests

The module implements both power-up and conditional self-tests as required by FIPS 140-2. The following two sections outline the tests that are performed.

2.8.1 Power-up self-tests

SELF-TEST	32/64-BIT	KCLSOS
HMAC SHA-256 firmware integrity check	✓	✓
AES KAT for encrypt	✓	✓
AES KAT for decrypt	✓	✓
Triple-DES KAT for encrypt	✓	✓
Triple-DES KAT for decrypt	✓	✓
RSA KAT for sign	✓	-
RSA KAT for verify	✓	-
RSA KAT for encrypt	✓	-
RSA KAT for decrypt	✓	-
DSA pairwise consistency check	✓	-
ECDSA pairwise consistency check	✓	-
SHA-1 KAT	✓	✓
SHA-256 KAT	✓	✓
SHA-384 KAT	✓	✓
SHA-512 KAT	✓	✓
HMAC KAT with SHA-1	✓	✓
HMAC KAT with SHA-256	✓	✓
HMAC KAT with SHA-384	✓	✓
HMAC KAT with SHA-512	✓	✓
DRBG KAT	✓	-

Table 11 Power-up self-tests

If any of the tests listed above fails to perform successfully, the module enters into a critical error state during which all cryptographic operations and output of any data is inhibited. An error message is logged for the CO to review and requires action on the Crypto-Officer's part to clear the error state.

2.8.2 Conditional self-tests

EVENT	TEST	CONSEQUENCE OF FAILURE	32/64-BIT	KCLSOS
Module requests a random number from the NDRNG	Continuous RNG Test (CRNGT) for NDRNG	Critical error state	-	✓
Module requests a random number from the FIPS approved SP800-90 DRBG	Continuous RNG Test (CRNGT) for DRBG	Soft error state	✓	-
RSA key pair generated	RSA pairwise consistency test for key pair generation	Soft error state	✓	-
DSA key pair generated	DSA pairwise consistency test for key pair generation	Soft error state	✓	-
ECDSA key pair generated	ECDSA pairwise consistency test for key pair generation	Soft error state	✓	-
A key is manually entered into the module	A manual key entry test	Soft error state	✓	✓
Module enters a bypass mode of operation	Bypass test using SHA-1	Critical error state (see 2.8.1)	✓	✓
Asymmetric key pair generated	Firmware Load Test using DSA signature verification	Soft error state	✓	✓

Table 12 Conditional self-tests

Notes:

Critical error state: all cryptographic operations and output of any data is inhibited. An error message is logged for the CO to review and requires action on the Crypto-Officer's part to clear the error state.

Soft error state: Logs an error message and disables all cryptographic operations and data output.

2.9 Design Assurance

Forcepoint LLC employ industry standard best practices in the design, development, production and maintenance of all of its products, including the FIPS 140-2 module.

This includes the use of an industry standard configuration management system that is operated in accordance with the requirements of FIPS 140-2, such that each configuration item that forms part of the module is stored with a label corresponding to the version of the module and that the module and all of its associated documentation can be regenerated from the configuration management system with reference to the relevant version number.

Design documentation for the module is maintained to provide clear and consistent information within the document hierarchy to enable transparent traceability between corresponding areas throughout the document hierarchy, for instance, between elements of this Cryptographic Module Security Policy (CMSP) and the design documentation.

Guidance appropriate to an operator’s role is provided with the module and provides all of the necessary assistance to enable the secure operation of the module by an operator, including the approved security functions of the module.

Delivery of the Cryptographic Module to customers from the vendor is via download of the firmware image from the Forcepoint website. See section 3.1.1. Once the Cryptographic Officer has received the cryptographic module, it is his/her responsibility to ensure its secure delivery to the users that he/she is responsible for.

2.10 Mitigation of Other Attacks

The module does not mitigate any other attacks.

3 Secure Operation

The module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in its approved mode of operation. The use of any interfaces and services not documented herein are prohibited and considered in violation of this Security Policy, and shall result in the non-compliant operation of the module.

3.1 Crypto-Officer Guidance

The Crypto-Officer is responsible for the proper initial setup of the Admin Console Management Tool software and the cryptographic module. Setup of the Admin Console software is done by installing the software on an appropriate Windows® workstation (refer to the *McAfee Firewall Enterprise version 8.3.2P03 and later Product Guide Revision B* for details regarding installation of management tools) on the same network as the module. When installing the Admin Console, a link to the documents page is added to the "Start" menu of the computer. To view the Sidewinder™ documents on the Forcepoint LLC web site, select
Start > Programs > McAfee > Firewall Enterprise > Online Manuals

Additional product manuals, configuration-specific application notes, and the KnowledgeBase are available at http://mysupport.mcafee.com.

3.1.1 Installation

The cryptographic module requires that the correct Forcepoint® Sidewinder™ version be installed on the appliance.

The Crypto-Officer must have a Forcepoint-provided grant number in order to download the required image. Grant numbers are sent to Forcepoint customers via email after the purchase of a Forcepoint product.

To download Forcepoint® Sidewinder™, the Crypto-Officer must:

1. In a web browser, navigate to www.mcafee.com/us/downloads/downloads.aspx and click **Download**.
2. Enter the grant number, and then navigate to the appropriate product and version.
3. Click **Patches**, and locate the link for the latest version (8.3.2P07).
4. Download the install USB image (.zip) file.
5. Write the image to a USB drive.

To install the firmware image onto the appliance, the Crypto-Officer must:

1. Insert the USB drive and start/restart the firewall.
2. Enter the boot menu, and then select the installation USB drive. The firewall boots from the installation media.
3. At the **McAfee Inc.** menu, accept the default, which is the **Operational System**.
4. At the **Welcome to McAfee Firewall Enterprise** menu, select the appropriate Sidewinder™ boot option.
5. When the installation complete message appears, remove the installation media from the firewall.

6. Press "**R**" to restart the firewall, and then press "**Enter**". The firewall restarts and displays standard restart information.

Version 8.3.2P07 is now installed on the appliance. Then, to apply the 8.3.2E106 patch, the Crypto-Officer must load and install the patch:

Loading the patch on the command-line:

```
$> cf pack load pack=8.3.2E106 source=ftp
server=csftp.us.stonesoft.com directory=upload user=atl-
963845ro password=34bT4hF3AFJn
```

Installing the patch:

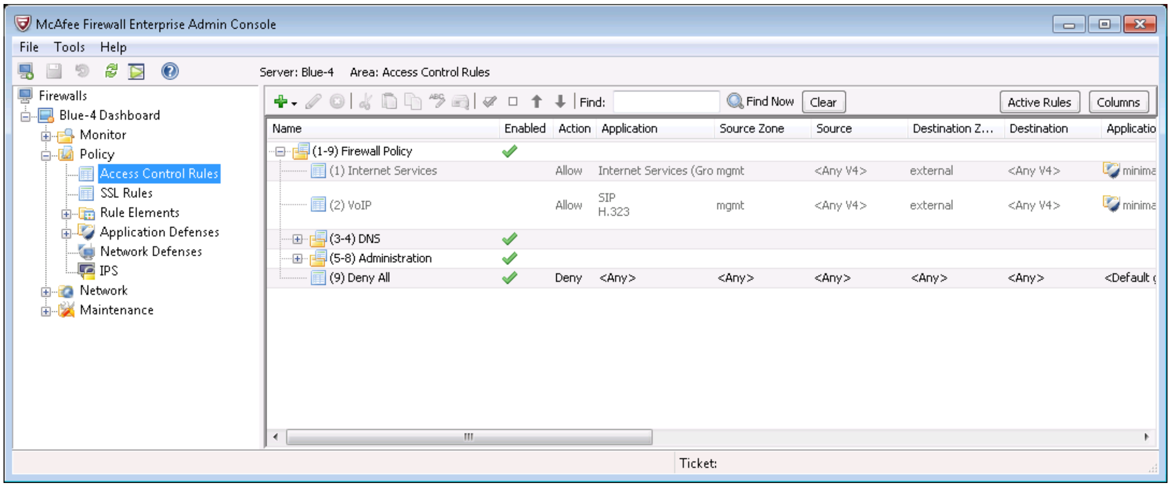
-- Install the epatch using '`cf pack install pack=8.3.2E106`' or install the epatch from the GUI **Software Management** screen.

3.1.2 Initialization

The Crypto-Officer is responsible for initialization and security-relevant configuration and management activities for the module. Initialization and configuration instructions for the module can also be found in the *McAfee Firewall Enterprise version 8.3.x Quick Start Guide Revision C*, *McAfee Firewall Enterprise version 8.3.2P03 and later Product Guide Revision B*, and this FIPS 140-2 Security Policy. The initial Administration account, including username and password for login authentication to the module, is created during the startup configuration using the Quick Start Wizard.

Before enforcing FIPS on the module, the CO must check that no non-approved service is running on the module.

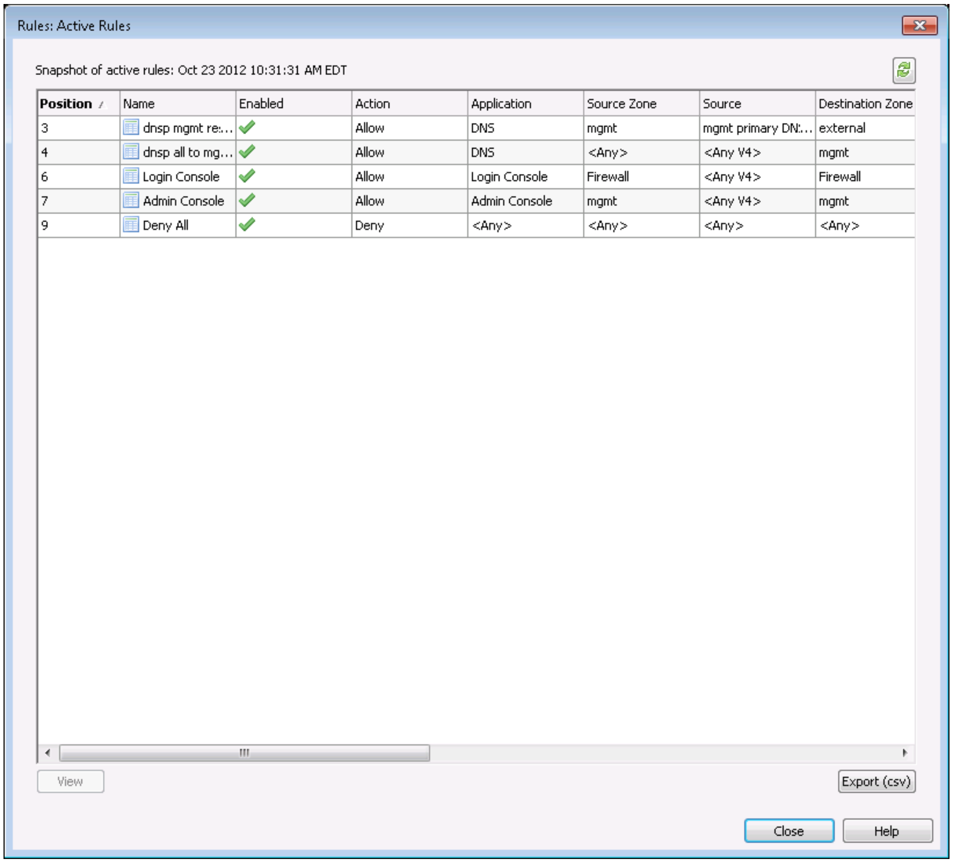
Services and proxies are automatically enabled when rules are created that reference those services/proxies. To view the services that are currently used in enabled rules, select "**Policy / Access Control Rules**". The Access Control Rules window appears as shown in Figure 4. From here, select the "**Active Rules**" button in the upper right corner of the window (see Figure 5). If the window lists any non-approved protocols, then those protocols must be disabled before the module is considered to be in its approved mode of operation.



Server: Blue-4 Area: Access Control Rules

Name	Enabled	Action	Application	Source Zone	Source	Destination Z...	Destination	Applicatio
(1-9) Firewall Policy	✓							
(1) Internet Services		Allow	Internet Services (Gro	mgmt	<Any V4>	external	<Any V4>	minima
(2) VoIP		Allow	SIP H.323	mgmt	<Any V4>	external	<Any V4>	minima
(3-4) DNS	✓							
(5-8) Administration	✓							
(9) Deny All	✓	Deny	<Any>	<Any>	<Any>	<Any>	<Any>	<Default (

Figure 4 – Rules Window



Snapshot of active rules: Oct 23 2012 10:31:31 AM EDT

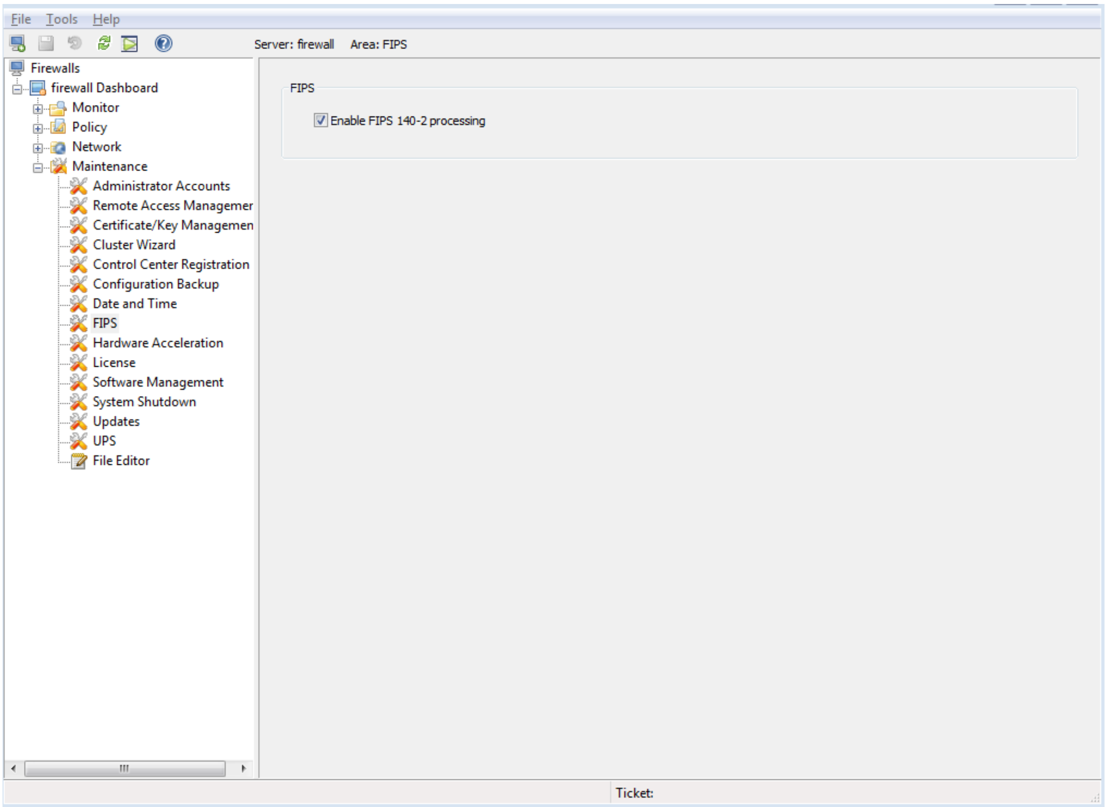
Position	Name	Enabled	Action	Application	Source Zone	Source	Destination Zone
3	dnsp mgmt re:...	✓	Allow	DNS	mgmt	mgmt primary DN:...	external
4	dnsp all to mg...	✓	Allow	DNS	<Any>	<Any V4>	mgmt
6	Login Console	✓	Allow	Login Console	Firewall	<Any V4>	Firewall
7	Admin Console	✓	Allow	Admin Console	mgmt	<Any V4>	mgmt
9	Deny All	✓	Deny	<Any>	<Any>	<Any>	<Any>

Figure 5 – Active Rules Window

The process for enabling FIPS mode is:

1. Under “**Policy/Application Defenses/ Defenses/HTTPS**”, disable all non-approved versions of SSL, leaving only TLS 1.0 operational.
2. Under “**Maintenance / Certificate Management**”, ensure that the certificates only use approved cryptographic algorithms.
3. Select “**Maintenance / FIPS**”. The FIPS check box appears in the right pane (shown in Figure 6).

4. Select “**Enable FIPS 140-2 processing**”.
5. Save the configuration change.
6. Select “**Maintenance / System Shutdown**” to reboot the firewall to the Operational kernel to activate the change.



Server: firewall Area: FIPS

FIPS

☑ Enable FIPS 140-2 processing

Figure 6 – Configuring For FIPS

Whether the module has been upgraded to a validated firmware version from an earlier firmware, or shipped with a validated firmware version already present, it is required to delete and recreate all required cryptographic keys and CSPs necessary for the module's secure operation. The keys and CSPs existing on the module were generated outside of the module’s approved mode of operation, and they must now be re-created for use in the approved mode. To ensure the module’s secure operation, the CO shall replace the following keys and CSPs:

- Firewall Authentication private key
- Local CA private key

Instructions for the replacement of CSPs are contained in the Forcepoint® Sidewinder™ FIPS 140-2 Configuration Guide.

The module is now operating in the approved mode of operation.

3.1.3 Management

When configured according to the Crypto-Officer guidance in this Security Policy, the module only runs in the approved mode of operation. While in the approved mode, only approved and allowed algorithms may be used; the use of non-approved algorithms is prohibited. The Crypto-Officer is able to monitor and configure the module via the web interface (GUI over TLS), SSH, serial port, or direct-connected keyboard/monitor. Detailed instructions to monitor and troubleshoot the systems are provided in the *McAfee Firewall Enterprise 8.3.2P03 and later Product Guide Revision B*. The CO must monitor that only approved algorithms as listed in Table 3 are being used for TLS, DTLS, and SSH sessions.

If any irregular activity is noticed or the module is consistently reporting errors, then Forcepoint Customer Support should be contacted.

3.1.4 Monitoring Status

The Crypto-Officer must monitor the module's status regularly for an approved mode of operation and active bypass mode.

The "show status" service to determine the current mode of operation involves examining the Admin Console's FIPS mode checkbox, shown in Figure 6. This can also be done via the following CLI command:

```
cf fips query
```

When correctly configured, the module will display the following message:

```
fips set enabled=yes
```

The "show status" service as it pertains to bypass is shown in the GUI under **VPN Definitions** and the module column. For the CLI, the Crypto-Officer may enter "**cf ipsec policydump**" to display the active VPNs, while "**cf ipsec q type=bypass**" will display get a listing of the existing bypass rules.

If any irregular activity is noticed or the module is consistently reporting errors, then Forcepoint Customer Support should be contacted.

3.1.5 Zeroization

It is the Crypto Officer's responsibility to zeroize the module's keys when necessary. In order to zeroize the module of all keys and CSPs, it is necessary to first rebuild the module's image, essentially wiping out all data from the module. Once a factory reset has been performed, default keys and CSPs must be set up as part of the renewal process. These keys must be recreated as per the instructions found in section 3.1.2. Failure to recreate these keys will result in a non-compliant module.

For more information about resetting the module to a factory default, please consult the documentation that shipped with the module.

3.2 User Guidance

When using key establishment protocols (RSA and DH) in the approved mode, the User is responsible for selecting a key size that provides the appropriate level of key strength for the key being transported.

3.3 Non-Approved Mode of Operation

When initialized and configured according to the Crypto-Officer guidance in this Security Policy, the module does not support a non-approved mode of operation.