Web Security On-prem

FIPS 140-2 with Forcepoint Web Security

Revision A

Contents

Introduction

- Provide protection against malware entering the network via Web channels, such as HTTP, HTTPS, and FTP.
- Perform real-time content analysis to discover malware and hidden threats.
- Can monitor traffic that uses any of more than 100 protocols.
- Provide highly-granular and flexible control of Internet access to enforce the precise requirements of an organization's Acceptable Use Policy (AUP)

Forcepoint Web protection solutions protect against advanced web-based threats and data theft while on and off the corporate network. These solutions include server software installed on corporate servers and software installed on client's computers.

These products use cryptographic modules to protect the integrity of the data they collect while that data is being transmitted and stored. National Institute of Standards and Technology (NIST) in the Federal Information Processing Standards (FIPS) Publication 140-2 defines security requirements for cryptographic modules. Forcepoint C Cryptographic Module and Forcepoint Java Cryptographic Module were certified by NIST under the Cryptographic Module Validation Program. The official publication describing this standard is FIPS PUB 140-2.

Forcepoint FIPS 140-2 certificates are available:

- Forcepoint C Cryptographic Module version 2.0.5 (Web protection solutions and Appliances)
- Forcepoint Java Cryptographic Module version 3.0.1 (Web Protection solutions)

All libraries will be in place and incorporated into the product after installation of a patch. See this article for information and instructions.

Additional details on the specific use of these modules are provided below.

Note

This document applies to the Forcepoint Web Security system after a manual FIPS hardening procedure has been performed. See the attachment in this article for details.

Security Requirements for Cryptographic Modules (FIPS 140-2)

The system is intended for commercial use. Since it uses encryption to perform security functions, it is subject to the guidelines set forth by NIST in the FIPS 140-2 publication for agencies that require compliance. The module validation process is called the Cryptographic Module Validation Program, and is outlined in the FIPS 140-2 publication. FIPS 140-2 is an all-encompassing encryption standard and specifies key management, communication mechanisms, and so forth.

The abstract from the FIPS 140-2 publication is provided here for convenience:

The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security in its computer and telecommunication systems. This publication provides a standard that will be used by Federal organizations when these organizations specify that cryptographic- based security systems are to be used to provide protection for sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/ electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

(http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

System Cryptographic Functions

The system employs two broad cryptographic functions:

- Server Communication
  All server communication is encrypted.
  - Client browser and other connections to the Forcepoint Appliance
  - Forcepoint Security Appliance Manager (FSAM) connections to Forcepoint Security Manager
  - Appliance connection to Forcepoint Security Manager
  - Communication with the SQL DB – Forcepoint Security Manager
- Server Storage
  The server stores collected user behavior.
  - Customer credentials
  - Configuration backups
  - Manager Storage (SQL database and forensics repository)

FIPS 140-2 Certified Encryption Libraries

Forcepoint Web protection solutions version 8.5.0 or later provide the option to use FIPS 140-2 certified cryptographic libraries for sensitive data flows. By default, FIPS 140-2 certified cryptographic libraries are on for all Web Security components except Content Gateway, where it must be enabled using the Content Gateway Manager. See Content Gateway Help for details.

Cryptographic libraries that are FIPS 140-2 certified are used by Forcepoint Web Security and Forcepoint URL Filtering components in the following deployments:

- Forcepoint Appliances
  - V Series (V5K, V10K, and V20K)
  - X Series (X10G)
- Software installations
- Virtual appliance installations

Components of the following do not use FIPS 140-2 cryptographic libraries:

- Hybrid module for Forcepoint Web Security
- Forcepoint Web Endpoint
- Remote Filter Module for Forcepoint URL Filtering
- Forcepoint Advanced Malware solutions
- Forcepoint CASB
- Forcepoint Mobile Security

See Configuration Requirements for Using FIPS-Certified Cryptography for additional information.

Forcepoint Appliances Encryption Use Cases

Forcepoint appliances (X Series, V Series, and virtual) are purpose-built machines for core components of Forcepoint products. Forcepoint appliances are security-hardened and optimized for performance, reliability, and ease of use.

Forcepoint Appliances server communication

Client browser and other connections to the Forcepoint Appliance

For configuration using HTTPS and SSH connections to the appliance and the Forcepoint Security Appliance Manager, the appliance uses FIPS 140-2 certified cryptographic libraries to establish a secure connection. The appliance uses the following algorithms:

Remote console access (SSH):

- AES128-CTR
- AES192-CTR
- AES256-CTR

Browser access (HTTPS):

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA
- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA

This communication occurs using the Forcepoint C Cryptographic Module.

Forcepoint Security Appliance Manager connections to Forcepoint Security Manager

The Forcepoint Security Appliance Manager (FSAM) communicates with the Forcepoint Security Manager to verify users, passwords, and registered appliances.

To establish a secure connection, the FSAM uses TLS with the best negotiated encryption algorithm from the following list:

- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA

This communication occurs using the Forcepoint C Cryptographic Module.

Forcepoint Appliances server storage

Appliance user account credentials

Default and custom account user names and passwords are encrypted using the SHA-512 hash algorithm from FIPS 140-2 certified cryptographic libraries.

Note

This does not include the password reset functionality. For more information, see this Knowledge Base article.

Configuration summaries

Files containing sensitive data that are generated as part of a back-up or configuration summary are encrypted using FIPS 140-2 certified cryptographic libraries.

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA
- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA

Note

By default, these files are stored locally and exported using FTP, TFTP, and Samba. We recommend using a secure transfer method for external storage and for sharing sensitive data outside the appliance.

Forcepoint Security Manager

Encryption is used for communication between the Forcepoint Security Manager server and the client machines used to access it.

On the server side, encryption is handled by the Forcepoint Java Cryptographic Module. On the client side, encryption is handled by the Web browser.

The different communication configurations allow the Forcepoint Security Manager to negotiate a variety of FIPS 140-2 approved algorithms and support different versions of Web browsers that might be running on the client machine. While it is expected that the users of the Forcepoint Security Manager configure their browser to be FIPS 140-2, this product configuration ensures that the server does not negotiate a non-FIPS approved algorithm.

Forcepoint Web Security Encryption Use Cases

Forcepoint Web Security Server Communication

Forcepoint Web Security server to server

Encryption of communication between Forcepoint Web Security services (for example, Policy Broker communicating with Policy Server) is accomplished using TLS with the best negotiated encryption algorithm from the following list:

- Policy Broker: TLSv1.2+ECDSA:AES256-SHA:DH-RSA-AES256-SHA:DHE-RSA- AES256-SHA
- Policy Server: TLSv1.2+ECDSA:AES256-SHA256

The Policy Broker cipher list is applied in inter-component communications such as Policy Broker with Policy Server and Policy Broker with Forcepoint Security Manager.

The Policy Server cipher list is applied in inter-component communications such as Policy Server with Filtering Service and Policy Server with Forcepoint Security Manager.

This communication occurs using the Forcepoint C Cryptographic Module and the Forcepoint Java Cryptographic Module.

Component to customer infrastructure communication

Forcepoint Web Security uses neither the Forcepoint C Cryptographic Module nor the Forcepoint Java Cryptographic Module for encrypting communication between Forcepoint components and the customer infrastructure.

Communication with customer components such as a network integration, a SIEM solution, a Directory Service, Remote Access Dial-in User Service (RADIUS), or ICAP does not use FIPS 140-2 certified cryptographic libraries. A customer-maintained VPN tunnel between Forcepoint

Web Security components and servers and customer infrastructure components should be considered.

By design, Decryption Port Mirroring (available when Content Gateway is deployed on an appliance) does not use FIPS 140-2 certified cryptographic libraries.

Forcepoint Web Security Server Storage

Forcepoint Web Security uses the Forcepoint Java Cryptographic Module for encrypting the data stored on the server.

The threat-related forensics data is stored on a disk and is encrypted in a forensics repository using AES-256 encryption. The corresponding threat data is stored in the SQL Server database.

A Forcepoint FIPS 140-2 certificate for Forcepoint Java Cryptographic Module version 3.0.1 is available.

The Policy Database, used to store configuration and policy data, is a PostgreSQL database. The Forcepoint deployment of PostgreSQL is not specifically configured to use FIPS certified libraries.

© 2024 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
Published 07 August 2024