FIPS 140-2 and Forcepoint Email Security

Forcepoint Email Security is an appliance-based security solution. 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. All components of Forcepoint email protection solutions reside on Forcepoint appliances, except the Email Security module of the Forcepoint Security Manager and the Email Log Server.

Forcepoint email protection solutions:

- Provide protection against malicious emails entering the network.
- Perform real-time content analysis to discover malware and spam.
- Ensure reliable and accurate delivery of email through domain and IP address-based message routing.
- Provide advanced detection of email attachment file types that may contain security threats.

Forcepoint Email Security protects against advanced email-based threats and data theft while on and off the corporate network. These email protection solutions use cryptography to protect the integrity of the sensitive data they collect while that data is being transmitted and stored. Forcepoint Email Security uses cryptographic libraries certified by National Institute of Standards and Technology (NIST) in the Federal Information Processing Standards (FIPS) Publication 140-2. NIST guidelines govern suggested strengths and implementations for cryptographic modules. The official publication describing this standard is FIPS PUB 140-2.

Forcepoint email protection solutions at versions 8.5.3 or later use the following cryptographic modules:

- Forcepoint C Cryptographic Module version 2.0.5, packaged in OpenSSL v1.0.2O
- Forcepoint Java Cryptographic Module version 3.0.1

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

All libraries are in place and were incorporated into the product with the release of version 8.5.3. See Forcepoint Email Security Release Notes version 8.5.3.

Security Requirements for Cryptographic Modules (FIPS 140-2)

The system is intended for commercial use. Because 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

  Most server communication is encrypted.

  - Appliance connection to Forcepoint Security Manager
  - Forcepoint Security Appliance Manager (FSAM) connections to Forcepoint Security Manager
  - Client browser and other connections to the appliance
  - Appliance connection to Email Log Server
  - Communication with the SQL database – Forcepoint Security Manager
  - Connections between appliances and other Forcepoint products
  - Appliance connection to Personal Email Manager and Forcepoint Secure Messaging end-user machines
  - Appliance connection to third-party products

    - Mail handling: SMTP TLS traffic and DKIM signing and verification
- Server Storage

  The server stores collected user and message activities.
    - Customer credentials
    - Configuration backups
    - Logs

FIPS 140-2 Certified Encryption Libraries

Forcepoint Email Security version 8.5.3 or later provides the option to use FIPS 140-2 certified cryptographic libraries for sensitive data flows. By default, FIPS 140-2 certified cryptographic libraries are enabled for all Email Security components, including internal communication and Java modules, and cannot be disabled.

For third-party services that communicate with Email appliances, FIPS-certified cryptography is disabled by default and must be enabled using the following command-line interface (CLI) command:

```
set openssl-fips --status enable
```

FIPS-certified cryptography for third-party communications can be disabled using the command `set openssl-fips --status disable`.

Cryptographic libraries that are FIPS 140-2 certified are used by Forcepoint Email Security components in the following deployments:

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

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

- Third-party SIEM providers
- SNMP protocol
- Filtering Service URL analysis

Forcepoint Email Security 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

FIPS 140-2 certified cryptographic libraries are enabled for most server communication by default and cannot be disabled. The exception is *Appliance connections to third-party products*, page 6, for which FIPS-certified cryptography must be enabled using the CLI.

Appliance connections to Forcepoint Security Manager

Forcepoint Email appliances communicate with the Forcepoint Security Manager to verify users, passwords, registered appliances, and license keys.

To establish a secure connection, Email appliances use 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 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.

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.

Appliance connections to Email Log Server

Forcepoint Email appliances communicate with the Email Log Server, which receives log records and processes them into the Log Database.

Communication with the SQL database – Forcepoint Security Manager

The Forcepoint Security Installer, which is used to install Forcepoint Security Manager and the Email Log Server, communicates with the SQL database and with Forcepoint Email appliances to verify login information and license keys.

Connections between appliances and other Forcepoint products

Forcepoint Email Security integrates with Forcepoint DLP to enable DLP policies that can detect the presence of sensitive data in an organization's email messages and execute appropriate actions to prevent data loss. Forcepoint Email appliances communicate with the Forcepoint DLP Manager to process DLP incidents.

The URL analysis options offered by Forcepoint Email Security are used to compare a URL embedded in an email message with a database of URLs categorized by Forcepoint as potentially dangerous or unwanted. The URL analysis services communicate with Forcepoint Web Security or the cloud-hosted Forcepoint URL Database to analyze URLs in messages.

The Forcepoint Email Security Hybrid Module is an optional feature, used for URL sandboxing and phishing education. When enabled Forcepoint Email appliances communicate with the Hybrid Module to pre-filter email messages and to collect log data on messages that are blocked by the Hybrid Module.

Appliance connection to Personal Email Manager and Forcepoint Secure Messaging end-user machines

Forcepoint Email appliances connect with the end-user modules Personal Email Manager and Forcepoint Secure Messaging to communicate query strings and message details. This communication occurs using the Forcepoint Java Cryptographic Module.

Appliance connections to third-party products

FIPS-certified cryptography is disabled by default for communication between Forcepoint Email appliances and third-party products, and must be enabled using the CLI.

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

- Third-party SIEM providers
- SNMP protocol
- Filtering Service URL analysis

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.

Logs

The Email Log Database stores logs of email messages, connections, administrator activities, end-user activities, and system events. Log files are encrypted using FIPS 140-2 certified cryptographic libraries.

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 compliant, this product configuration ensures that the server does not negotiate a non-FIPS approved algorithm.