FIPS Management

This chapter contains the following sections:

FIPS Management Overview

The Federal Information Processing Standard (FIPS) 140 is a publicly announced standard developed jointly by the United States and Canadian federal governments specifying requirements for cryptographic modules that are used by government agencies to protect sensitive but unclassified information. The Cisco Email Security appliance uses the Cisco SSL Cryptographic Toolkit to achieve FIPS 140-2 Level 1 compliance.

The Cisco SSL Cryptographic Toolkit is a a GGSG-approved cryptography suite that includes Cisco SSL, which is an enhanced version of OpenSSL's FIPS support, and the FIPS-compliant Cisco Common Cryptography Module. The Cisco Common Cryptography Module is a software library that Email Security appliance uses for FIPS-validated cryptographic algorithms for protocols such SSH.

Configuration Changes in FIPS Mode

The Email Security appliance uses Cisco SSL and FIPS-compliant certificates for communication when the appliance is in FIPS mode. See Switching the Appliance to FIPS Mode, on page 2 for more information.

To be FIPS Level 1 compliant, the Email Security appliance makes the following changes to your configuration:

- **SMTP receiving and delivery.** Incoming and outgoing SMTP conversations over TLS between a public listener on the Email Security appliance and a remote host use TLS version 1.0, 1.1, or 1.2 and FIPS cipher suites. You can modify the cipher suites using sslconfig when in FIPS mode. TLS v1 is the only version of TLS supported in FIPS mode.
- **Web interface.** HTTPS sessions to the Email Security appliance's web interface use TLS version 1.0, 1.1, or 1.2 and FIPS cipher suites. This also includes HTTPS sessions to the Spam Quarantine and other IP interfaces. You can modify the cipher suites using sslconfig when in FIPS mode.

- **Certificates.** FIPS mode restricts the kinds of certificates used by the appliances. Certificates must use one of the following signature algorithms: SHA-224, SHA-256, SHA-384, and SHA-512 and RSA keys of the size 1024, 1536, or 2048 bits. The appliance will not import certificates that do not use one of these algorithms. The appliance cannot be switched to FIPS mode if it has any non-compliant certificates in use. It will displays an error message instead. See Managing Certificates and Keys, on page 4for more information.
- **DKIM signing and verification.** RSA keys used for DKIM signatures and verification must be 1024, 1536, or 2048 bits in length. The appliance cannot be switched to FIPS mode if it has any non-compliant RSA keys in use. It will displays an error message instead. When verifying a DKIM signature, the appliance returns a permanent failure if the signature does not use a FIPS-compliant key. See Managing Keys for DKIM Signing and Verification, on page 5
- **LDAPS.** TLS transactions between the Email Security appliance and LDAP servers, including using an LDAP server for external authentication, use TLS version 1 and FIPS cipher suites. If the LDAP server uses MD5 hashes to store passwords, the SMTP authentication query will fail because MD5 is not FIPS-compliant.
- **Logs.** SSH2 is the only allowed protocol for pushing logs via SCP. For error messages related to FIPS management, read the FIPS Logs at the INFO level.
- **Centralized Management.** For clustered appliances, FIPS mode can only be turned on at the cluster level.
- **SSL Ciphers**. Only the following SSL ciphers are supported in FIPS mode: AES256-SHA:AES128-SHA:DES-CBC3-SHA.

Switching the Appliance to FIPS Mode

Use the fipsconfig CLI command to switch the appliance over to FIPS mode.

Note Only administrators can use this command. A reboot is required after switching the appliance from non-FIPS mode to FIPS mode.

Before You Begin

Make sure that the appliance do not have any objects that are not FIPS compliant, for example, a DKIM verification profile with a key size of 512 bits. To enable FIPS mode, you must modify all the non-FIPS-compliant objects to meet FIPS requirements. See Configuration Changes in FIPS Mode, on page 1. For instructions to check if your appliance contains non-FIPS-compliant objects, see Checking FIPS Mode Compliance, on page 4.

Procedure

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> setup
To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.
Are you sure you want to enable FIPS mode and reboot now ? [N]> y
Do you want to enable encryption of sensitive data in configuration file when FIPS mode is
 enabled? Changing the value will result in system reboot [N]> n
```

```
Enter the number of seconds to wait before forcibly closing connections.
[30]>
System rebooting.  Please wait while the queue is being closed...
Closing CLI connection.
Rebooting the system...
```

Encrypting Sensitive Data in FIPS Mode

Use the fipsconfig command to encrypt sensitive data such as passwords and keys, in your appliance. If you enable this option,

- The following critical security parameters in your appliance are encrypted and stored:
  - Certificate private keys
  - RADIUS passwords
  - LDAP bind passwords
  - Local users' password hashes
  - SNMP password
  - DK/DKIM signing keys
  - Outgoing SMTP authentication passwords
  - PostX encryption keys
  - PostX encryption proxy password
  - FTP Push log subscriptions' passwords
  - IPMI LAN password
  - Updater server URLs

Note All users, including the administrators, cannot view the sensitive information in the configuration files.

- Swap space in your appliance is encrypted to prevent any unauthorized access or forensic attacks, if the physical security of the appliance is compromised.

Procedure

```
mail.example.com> fipsconfig
FIPS mode is currently enabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> setup
To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.
Are you sure you want to disable FIPS mode and reboot now ? [N]> n
Do you want to enable encryption of sensitive data in configuration file when FIPS mode is
 enabled? Changing the value will result in system reboot [N]> y
Enter the number of seconds to wait before forcibly closing connections.
[30]>
System rebooting.  Please wait while the queue is being closed...
Closing CLI connection.
Rebooting the system...
```

Checking FIPS Mode Compliance

Use the fipsconfig command to check if your appliance contains any non-FIPS-compliant objects.

Procedure

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> fipscheck
All objects in the current configuration are FIPS compliant.
FIPS mode is currently disabled.
```

Managing Certificates and Keys

AsyncOS allows you to encrypt communications between the appliance and external machines by using a certificate and private key pair. You can upload an existing certificate and key pair, generate a self-signed certificate, or generate a Certificate Signing Request (CSR) to submit to a certificate authority to obtain a public certificate. The certificate authority will return a trusted public certificate signed by a private key that you can then upload onto the appliance.

When the appliance is in FIPS mode, you can continue to

The appliance's FIPS mode adds a number of restrictions to the certificates that the appliance uses in order for the appliance to be FIPS compliant. Certificates must use one of the following signature algorithms: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.

The appliance will not import certificates that do not use one of these algorithms. It also cannot be switched to FIPS mode if it has any non-compliant certificates in use on a listener. It will displays an error message instead.

A Non-FIPS status for a certificate will be displayed in both the CLI and the GUI when the appliance is in FIPS mode. When selecting a certificate to use for a feature, such as a listener or destination control, the appliance does not display non-compliant certificates as an option.

See Working with Certificatesfor more information on using certificates on your appliance.

You can use FIPS-compliant certificates with any of the following services:

- **SMTP receiving and delivery.** Use the **Network > Listeners** page (or the listenerconfig -> edit -> certificate CLI command) to assign the certificate to any listeners that require encryption using TLS. You may want to only enable TLS on listeners facing the Internet (that is, public listeners), or you may want to enable encryption for all listeners, including internal systems (that is, private listeners).
- **Destination controls.** Use the **Mail Policies > Destination Controls** page (or the destconfig CLI command) to assign the certificate as a global setting to for all outgoing TLS connections for email delivery.
- **Interfaces.** Use the **Network > IP Interfaces** page (or the interfaceconfig CLI command) to enable the certificate for HTTPS services on an interface, including the management interface.
- **LDAP.** Use the **System Administration > LDAP** page to assign the certificate for all LDAP traffic that requires TLS connections. The appliance can also use LDAP for external authentication of users.

Managing Keys for DKIM Signing and Verification

For an overview of how DomainKeys and DKIM work on the Email Security appliance, see Email Authentication.

Related Topics

- DKIM Signing, on page 5
- DKIM Verification, on page 5

DKIM Signing

When creating a DKIM signing key, you specify a key size. Email Security appliances in FIPS mode only support 1024, 1536, or 2048 bits key size. The larger key sizes is more secure; however, larger keys can have an impact on performance.

The appliance cannot be switched to FIPS mode if it has any non-compliant RSA keys in use. It will displays an error message instead.

FIPS-compliant signing keys are available for use in domain profiles and appear in the Signing Key list when creating or editing a domain profile using the Mail **Policies > Domain Profiles** page. Once you have associated a signing key with a domain profile, you can create DNS text record which contains your public key. You do this via the Generate link in the DNS Text Record column in the domain profile listing (or via domainkeysconfig -> profiles -> dnstxt in the CLI).

DKIM Verification

The appliance requires a message to use a FIPS-compliant key in order to verify a DKIM signature. If the signature does not use a FIPS-compliant key, the appliance returns a permanent failure.