SonicWall Email Encryption service data flow overview

Ensure the secure exchange of email containing sensitive customer data or confidential information.

This document addresses the data flow and security practices for safeguarding the Personally Identifiable Information (PII) and Personal Health Information (PHI) utilized by the SonicWall Email Encryption cloud service, available as an add-on subscription service for SonicWall Hosted and on-premises Email Security Solutions. The example outlined uses an email from a SonicWall user as an example of a sending client. It covers the encryption algorithms used by the cloud encryption service, the stored procedures that govern access control on the encrypted database, and explains how encryption keys are managed by the cloud encryption service. It also describes mitigating risks and quality assurance procedures that enforce these measures.

In the interest of brevity, a number of assumptions have been made concerning connection and delivery options. Please do not assume these are the only ways the cloud encryption service can handle data. The cloud encryption service has been maturing for over 14 years, and contains numerous configuration options to accommodate most any scenario.

Secure message flow between SonicWall Email Security and the cloud encryption service

SonicWall Email Encrytion Service is a cloud service hosted on the Amazon Web Services (AWS) cloud. In order to ensure complete security when operating in this environment, a Business Associate Agreement (BAA) is in place with Amazon.

During the entire lifecycle of a secure message, the message payload never resides on the system in unencrypted form. The diagram above illustrates how a SonicWall Email Security appliance and the cloud encryption service can interoperate.

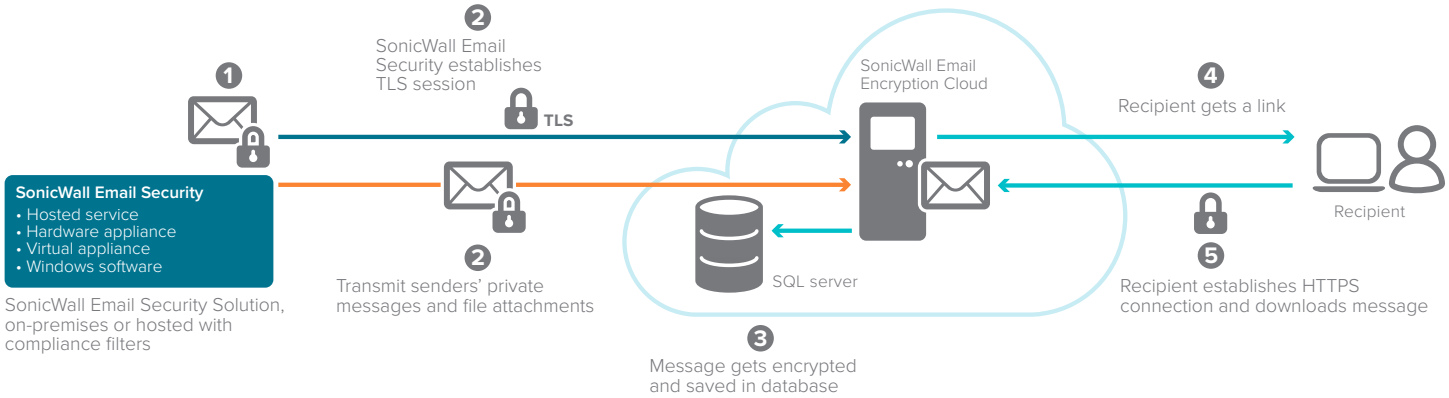

Figure 1. Message flow between SonicWall Email Security and the cloud encryption service

"During the entire lifecycle of a secure message, the message payload never resides on the system in unencrypted form."

The flow illustrated above incorporates the following encryption technologies:

1. The sender constructs and sends a message containing sensitive data such as PII or PHI. The SonicWall compliance filter will determine if the content of an individual message contains PII or PHI that must be encrypted. If so, SonicWall Email Security establishes a secure TLS session with the cloud encryption service.
2. Messages are transmitted from the SonicWall Email Security to the cloud encryption service using TLS encryption. The sender account is (optionally) dynamically created if it does not yet exist. The service calculates a digital fingerprint of this message upon arrival, which is later used for integrity comparison with the message that is transmitted to the recipient.
3. Messages are encrypted by the service using 256-bit AES and stored in the database in encrypted form.
4. A recipient account and inbox are dynamically created if they do not exist, and the recipient receives an email notification message with a link and guidance to log on to the cloud encryption portal (SSL 128-bit).
5. Using this log on information, the recipient not only accesses the message and all attachments via a secure server, but can, optionally, reply to the sender via the same secure interface. Message replies are composed in the cloud encryption service portal. While in transit, the messages are always stored on persistent storage in encrypted form.

Cloud Encryption service and FIPS 140-2 algorithms

The cryptography of the cloud encryption service is based on the Microsoft CryptoAPI and uses the FIPS 140-2 validated libraries provided by Microsoft as part of the Windows Server operating system. The encryption service is able to provide full FIPS 140-2 compliance services by utilizing the Microsoft CryptoAPI. For more information about Microsoft FIPS certificates, go to https://technet.microsoft.com/en-us/library/cc750357.aspx.

Data access control

The cloud encryption service employs industry-leading best practices for securing and controlling access to the database. While all data being sent and received from the encryption service is always protected through strong encrypted channels, the data resting in the database is protected

through a combination of strong encryption, field level access control and auditing enforced at the data layer. This combination of methods results in the data store being termed a "governed database."

A principle design feature of the database is that the application tier has no direct access to records and fields. This prevents rouge requests from accessing unauthorized data, or invalidating the integrity of the data store. Instead, the only way data (and the corresponding encryption keys) tracking and reporting can be accessed is by an authenticated user making a request to both the security and business logic layer. Each request is validated against the login permissions granted to the user making the request. These services are provided at the data level using a database approach known as Stored Procedures. Only after a request is validated will the data access action be allowed. This applies to both senders and recipients of messages.

Another benefit of this design is effective protection against SQL injection attacks and manipulation by hackers to access data not owned by them.

Encryption key management

The cloud email encryption service automatically handles encryption key management, removing this burden from end users. The system's application code automatically generates and stores a unique key for the encryption and decryption of each message, as well as for each megabyte of file attachment data. So, for example, a message containing a 5MB attachment will have 6 unique keys generated for protecting its data. Access to encryption keys is restricted by Data Access Control as described in the previous section, preventing unauthorized key access. Stored keys are automatically destroyed when their corresponding message has expired, which by default, is 30 days, but can be shorter if the customer wishes.

Best practice application design, coding and quality assurance

The cloud encryption service has a formal change control process to ensure that only verified software is ever placed into production. Product features and requests for defect repairs are reviewed by a Request Review Board comprised of senior product management, product development, quality assurance and support staff for inclusion into scheduled product releases. After approval, a cross-functional team ensures that engineering functional designs and quality assurance test cases can be traced back to formally documented requirements.

Product management, engineering, and quality assurance processes operate according to an established methodology. Prior to deployment, product release features, test case coverage and deployment instructions are documented and reviewed. Releases are first deployed by the operations team to a staging server for testing of both the software functionality and the deployment process itself. Ultimately the release to staging is published to production where it is then subjected to an internal acceptance test.

The cloud encryption service employs industry-leading best practices for securing and controlling access to the database. While all data being sent and received from the encryption service is always protected through strong encrypted channels, the data resting in the database is protected through a combination of strong encryption, field level access control and auditing enforced at the data layer. This combination of methods results in the data store being termed a "governed database."

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com