



Cisco Cloud/Hybrid Secure Email Overview

Published: July 28, 2017

Revised: March 22, 2021

Cisco Systems, Inc.

www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Cloud/Hybrid Secure Email Overview

© 2017 - 2021 Cisco Systems, Inc. All rights reserved.



CHAPTER 1**Understanding the Cisco Secure Email Service 1-1**

- Cisco Secure Email Cloud Service Overview 1-1
- Cisco Hybrid Secure Email Overview 1-4
- Managing Your Cisco Secure Email Service 1-7
- Service and Support 1-7

CHAPTER 2**Setting Up Your Cloud Environment 2-1**

- Accessing Your Email Cloud Gateways 2-1
 - Accessing the Web Interface and Command Line Interface 2-1
- Configuring Your Secure Email Cloud Gateways 2-1
 - Configuring Email Authentication 2-1
 - Configuring DKIM 2-2
 - Configuring SPF 2-2
 - Routing Outbound Email 2-2
 - Archiving Logs 2-2
- Configuring Your Servers 2-3
 - Using SMTP Call Ahead Validation 2-3

CHAPTER 3**Using the Cisco End-User Spam Quarantine 3-1**

- Understanding the Cisco End-User Spam Quarantine 3-1
 - Safelists and Blocklists 3-1
- Processing Messages in the Spam Quarantine 3-2
 - Releasing Messages from the Spam Quarantine to Your Inbox 3-2
 - Viewing Message Details 3-3
 - Taking Action on Multiple Messages at a Time 3-3
 - Accessing Safelists and Blocklists 3-3
 - Adding Entries to Safelists or Blocklists 3-4
 - Searching Messages in the Quarantine 3-4



Understanding the Cisco Secure Email Service

- [Cisco Secure Email Cloud Service Overview, page 1-1](#)
- [Cisco Hybrid Secure Email Overview, page 1-4](#)
- [Managing Your Cisco Secure Email Service, page 1-7](#)
- [Service and Support, page 1-7](#)

Cisco Secure Email Cloud Service Overview

Cisco Secure Email Cloud service provides an infrastructure that is maintained in resilient and geographically diverse Cisco data centers. The service provides email security based on an “in the cloud” or software as a service (SaaS) model. Your organization retains access to and visibility of the cloud-based infrastructure.

Throughout this guide, the term “email gateway” is used to mean a virtual email gateway.

Cisco Secure Email Cloud is an all-inclusive service. Software, hardware, and support are bundled together. The service includes the following features and functionality:

- **Consuming External Threat Feeds.** The External Threat Feeds (ETF) framework allows the email gateway to consume external threat information in STIX format communicated over TAXII protocol.
- **Sender Domain Reputation Filtering.** Sender Domain Reputation (SDR) filtering allows you to filter messages that come through the email gateway based on SDR that is determined by the Cisco SDR service.
- **New Data Loss Prevention (DLP) solution.** Cisco now provides an alternative DLP solution that allows seamless migration of all the existing DLP policies created in RSA DLP to the new DLP engine. After the upgrade, you can view or modify the migrated DLP policies in **Mail Policies > DLP Policy Manager** page in the web interface.



Note There is no support for RSA Enterprise Manager Integration in AsyncOS 11.0 and later. If you have DLP policies created in RSA Enterprise Manager, you must recreate those policies in your email gateway after the upgrade.

- **Anti-Spam** at the gateway, through the unique, multi-layer approach of IP Reputation Filters and IronPort Anti-Spam integration.
- **Anti-Virus** at the gateway with the Sophos and McAfee Anti-Virus scanning engines.

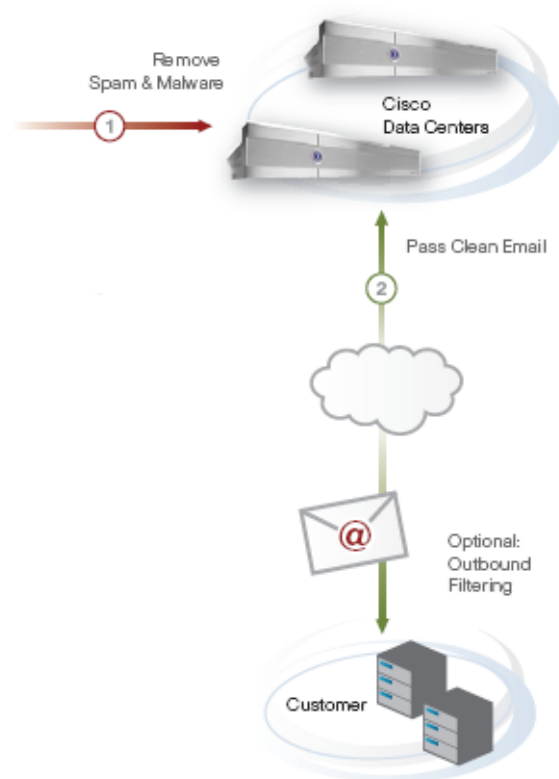
- **Graymail Detection and Safe Unsubscribing.** The email gateway allows you to:
 - Identify graymail using the integrated graymail engine and apply appropriate policy controls.
 - Provide a secure and easy mechanism for end users to unsubscribe from unwanted graymail using cloud-based Unsubscribe Service.
- **Outbreak Filters™.** Cisco's unique, preventive protection against new virus, scam, and phishing outbreaks that can quarantine dangerous messages until new updates are applied, reducing the window of vulnerability to new message threats.
- **Policy, Virus, and Outbreak Quarantines.** Provide a safe place to store suspect messages for evaluation by an administrator.
- **Spam Quarantine.** Provides end user access to quarantined spam and suspected spam.
- **Email Authentication.** The email gateway supports various forms of email authentication, including Sender Policy Framework (SPF), Sender ID Framework (SIDF), and DomainKeys Identified Mail (DKIM) verification of incoming mail, as well as DomainKeys and DKIM signing of outgoing mail.
- **File Reputation Filtering and File Analysis.** Advanced Malware Protection identifies emerging and targeted file-based threats in incoming and outgoing messages based on:
 - File reputation
 - File analysis (for certain files with unknown reputations)
 - Verdict updates
- **URL filtering.** URL filtering obtains the reputation and category of URLs in incoming and outgoing messages to allow several new functionalities.
- **S/MIME Security Services.** The email gateway now allows organizations to communicate securely using S/MIME without requiring that all end-users possess their own certificates. Organizations can handle message signing, encryption, verification, and decryption at the gateway level using certificates that identify the organization rather than the individual.
- **Email Encryption.** You can encrypt outgoing mail to address HIPAA, GLBA and similar regulatory mandates. To do this, you configure an encryption policy on the email gateway and use a hosted key service to encrypt the message.
- **Message Tracking.** The email gateway includes a message tracking feature that makes it easy to find the status of messages that the email gateway processes.
- **Mail Flow Monitoring.** Monitors the mail flow of all inbound and outbound messages that provides complete visibility into all email traffic for your enterprise.
- **Access Control.** For inbound senders, based upon the sender's IP address, IP address range, or domain.
- Extensive **message filtering** technology allows you to enforce corporate policy and act on specific messages as they enter or leave your corporate infrastructure. Filter rules identify messages based on message or attachment content, information about the network, message envelope, message headers, or message body. Filter actions allow messages to be dropped, bounced, archived, blind carbon copied, or altered, or to generate notifications.
- **Message Encryption via secure SMTP over Transport Layer Security.** Ensures messages traveling between your corporate infrastructure and other trusted hosts are encrypted.

Consolidated and robust reporting options analyze traffic data from geographically diverse infrastructure deployments to provide fully integrated security reporting. The email gateway third-generation reporting technology enables unprecedented insight into even the highest volume networks in the world. Detailed and accurate information is coalesced into clear and informative reports, suitable for all levels of an organization.

Message tracking gives your organization near real-time visibility into messages for tracking down message disposition. This feature can help resolve help desk calls quickly by determining the exact location of a message. Instead of having to search through log files, you can use the flexible tracking interface to locate messages.

Figure 1-1 illustrates the Cisco Secure Email Cloud deployment model.

Figure 1-1 Cisco Secure Email Cloud Security Deployment



Cisco Secure Email Cloud works as follows:

- The email gateway synchronizes configuration information between other email gateways that are referred to as the cluster configuration.
- The cloud-based cluster of email gateways accepts and processes inbound mail.
- The cloud-based Cisco Secure Email and Web Manager gathers the reporting and tracking data from the email cloud gateways. It functions as the central location for messages quarantined by policy or as spam from the email gateway cluster.
- Mail that is filtered based on policy is centrally quarantined.
- The system sends processed mail directly to your groupware server or Mail Transfer Agent (MTA), processes the outbound mail from the groupware server, and provides advanced content filtering and email encryption.

- (Optional) Outbound mail can be sent to the Internet through the email gateway cluster.

Cisco Hybrid Secure Email Overview

Cisco Hybrid Secure Email is a unique service offering that combines a cloud-based email security deployment with an appliance-based email security deployment (on premises) to provide maximum choice and control for your organization. The cloud-based infrastructure is typically used for inbound email cleansing, while the on-premises appliances provide granular control—protecting sensitive information with data loss prevention (DLP) and encryption technologies.

Like the Cisco Secure Email Cloud service, the hybrid service is all-inclusive, with software, hardware, and support bundled together. The service includes the following features and functionality:

- **Consuming External Threat Feeds.** The External Threat Feeds (ETF) framework allows the email gateway to consume external threat information in STIX format communicated over TAXII protocol.
- **Sender Domain Reputation Filtering.** Sender Domain Reputation (SDR) filtering allows you to filter messages that come through the email gateway based on SDR that is determined by the Cisco SDR service.
- **New Data Loss Prevention (DLP) solution.** Cisco now provides an alternative DLP solution that allows seamless migration of all the existing DLP policies created in RSA DLP to the new DLP engine. After the upgrade, you can view or modify the migrated DLP policies in **Mail Policies > DLP Policy Manager** page in the web interface.



Note There is no support for RSA Enterprise Manager Integration in AsyncOS 11.0 and later. If you have DLP policies created in RSA Enterprise Manager, you must recreate those policies in your email gateway after the upgrade.

- **Anti-Spam** at the gateway, through the unique, multi-layer approach of IP Reputation Filters and IronPort Anti-Spam integration.
- **Anti-Virus** at the gateway with the Sophos and McAfee Anti-Virus scanning engines.
- **Graymail Detection and Safe Unsubscribing.** The email gateway allows you to:
 - Identify graymail using the integrated graymail engine and apply appropriate policy controls.
 - Provide a secure and easy mechanism for end users to unsubscribe from unwanted graymail using cloud-based Unsubscribe Service.
- **Outbreak Filters™.** Cisco's unique, preventive protection against new virus, scam, and phishing outbreaks that can quarantine dangerous messages until new updates are applied, reducing the window of vulnerability to new message threats.
- **Policy, Virus, and Outbreak Quarantines.** Provide a safe place to store suspect messages for evaluation by an administrator.
- **Spam Quarantine.** Provides end user access to quarantined spam and suspected spam.
- **Email Authentication.** The email gateway supports various forms of email authentication, including Sender Policy Framework (SPF), Sender ID Framework (SIDF), and DomainKeys Identified Mail (DKIM) verification of incoming mail, as well as DomainKeys and DKIM signing of outgoing mail.
- **File Reputation Filtering and File Analysis.** Advanced Malware Protection identifies emerging and targeted file-based threats in incoming and outgoing messages based on:

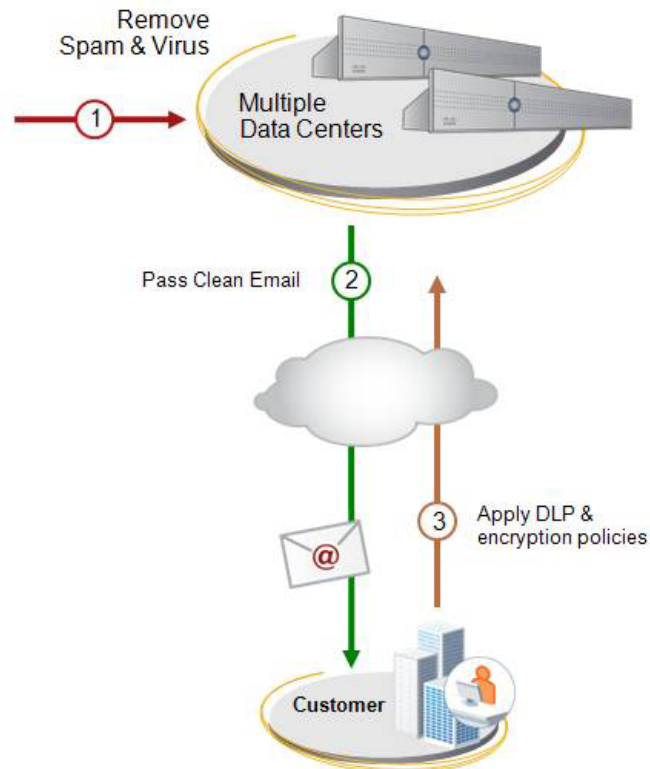
- File reputation
- File analysis (for certain files with unknown reputations)
- Verdict updates
- **URL filtering.** URL filtering obtains the reputation and category of URLs in incoming and outgoing messages to allow several new functionalities.
- **S/MIME Security Services.** The email gateway now allows organizations to communicate securely using S/MIME without requiring that all end-users possess their own certificates. Organizations can handle message signing, encryption, verification, and decryption at the gateway level using certificates that identify the organization rather than the individual.
- **Email Encryption.** You can encrypt outgoing mail to address HIPAA, GLBA and similar regulatory mandates. To do this, you configure an encryption policy on the email gateway and use a local key server or hosted key service to encrypt the message.
- **Email Security Manager.** A single, comprehensive dashboard to manage all email security services and applications on the email gateway. Email Security Manager can enforce email security based on user groups, allowing you to manage IronPort Reputation Filters, Outbreak Filters, Anti-Spam, Anti-Virus, and email content policies through distinct inbound and outbound policies.
- **Message Tracking.** The email gateway includes a message tracking feature that makes it easy to find the status of messages that the email gateway processes.
- **Mail Flow Monitoring.** Monitors mail flow of all inbound and outbound messages that provides complete visibility into all email traffic for your enterprise.
- **Access Control.** For inbound senders, based upon the sender's IP address, IP address range, or domain.
- **Extensive message filtering** technology allows you to enforce corporate policy and act on specific messages as they enter or leave your corporate infrastructure. Filter rules identify messages based on message or attachment content, information about the network, message envelope, message headers, or message body. Filter actions allow messages to be dropped, bounced, archived, blind carbon copied, or altered, or to generate notifications.
- **Message Encryption via secure SMTP over Transport Layer Security.** Ensures messages traveling between your corporate infrastructure and other trusted hosts are encrypted.

Consolidated and robust reporting options analyze traffic data from geographically diverse infrastructure deployments to provide fully integrated security reporting. The email gateway third-generation reporting technology enables unprecedented insight into even the highest volume networks in the world. Detailed and accurate information is coalesced into clear and informative reports, suitable for all levels of an organization.

Message tracking gives your organization near real-time visibility into messages for tracking down message disposition. This feature can help resolve help desk calls quickly by determining the exact location of a message. Instead of having to search through log files, you can use the flexible tracking interface to locate messages. Tracking spans both cloud-based and on-premises email gateways.

Figure 1-2 illustrates the Cisco Hybrid Secure Email deployment model.

Figure 1-2 Cisco Hybrid Secure Email Deployment



Cisco Hybrid Secure Email works as follows:

- The email gateway synchronizes configuration information between other Email gateways that are referred to as the cluster configuration
- The email cloud gateways accept and process inbound mail. The system sends processed mail to the on-premises email gateway, which carries out additional content filtering to filter messages by policy.
- The cloud-based Cisco Secure Email and Web Manager gathers the reporting and tracking data from the email cloud gateways as well as from the on-premises email gateway.
- The cloud-based Cisco Secure Email and Web Manager functions as the central quarantine for spam from the cloud-based email gateways.
- Mail that is filtered based on policy is quarantined on the Cisco Secure Email and Web Manager that filtered the messages.
- The on-premises email gateway delivers mail to your groupware server, processes the outbound mail from the groupware server, and provides advanced content filtering and email encryption.
- The on-premises email gateways send outbound mail to the Internet.

It is strongly recommended that you do not allow your cloud-based email gateways to relay bulk outbound messages, such as mass marketing mailers. Instead, you can limit relay traffic to transactional email. Capacity assurance does not include marketing communications or email generating programs or entities.

Managing Your Cisco Secure Email Service

You can manage and make changes to your cloud-based secure email service directly using the email gateway.

You can use the email gateway to do the following:

- View and track information about your cloud-based secure email service.
- Access reports.
- Access and modify the configuration of email cloud gateways.

Service and Support

**Note**

To get support for Cisco Secure Email Cloud Gateway, have your Contract Number ready when you call Cisco TAC.

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site for legacy IronPort: <http://www.cisco.com/web/services/acquisitions/ironport.html>

For non-critical issues, you can also access customer support from the email gateway. For instructions, see the User Guide or online help.



Setting Up Your Cloud Environment

- [Accessing Your Email Cloud Gateways, page 2-1](#)
- [Configuring Your Secure Email Cloud Gateways, page 2-1](#)
- [Configuring Your Servers, page 2-3](#)

Accessing Your Email Cloud Gateways

- [Accessing the Web Interface and Command Line Interface, page 2-1](#)

Accessing the Web Interface and Command Line Interface

You can access the web interface of all your email cloud gateways directly through the email gateway or using the URLs provided in your Welcome Letter.

You can use the details provided in your Welcome Letter to access all your email cloud gateways through the Command Line Interface (CLI).

Configuring Your Secure Email Cloud Gateways

- [Configuring Email Authentication, page 2-1](#)
- [Routing Outbound Email, page 2-2](#)
- [Archiving Logs, page 2-2](#)

Configuring Email Authentication

To authenticate email, you can use Sender Policy Framework (SPF) or DomainKeys Identified Mail (DKIM).

DKIM verifies the authenticity of email based on a signing key used by the sender. SPF verifies the authenticity of email based on DNS TXT records. SPF allows the owner of an Internet domain to use a special format of DNS records to designate which machines are authorized to send email for that domain.

Configuring DKIM

For instructions on configuring DKIM and defining content filter and message filter rules, see the following chapters in the *User Guide for AsyncOS for Cisco Secure Email Gateway*:

- Email Authentication
- Using Message Filters to Enforce Email Policies

Configuring SPF

Cisco provides a recommended SPF entry for your DNS TXT record, but does not manage the DNS of the customer owned domains, such as the Recipient Access Table of the email gateway. The format of the record is as follows:

```
x?urh3"/gzkuvu<' }k;0urh0>unique_name@0krj0z0eqo"/cnn
```

See [Service and Support, page 1-7](#).

After you have added the SPF record to the DNS, you can set up SPF verification and define content filter and message filter rules. See the following chapters in the *User Guide for AsyncOS for Cisco Secure Email Gateway*:

- Email Authentication
- Using Message Filters to Enforce Email Policies

Routing Outbound Email

For outbound mail through email cloud gateways, you must configure the email gateways to ensure that the cloud-based servers relay the mail on your behalf. See the following chapter in the *User Guide for AsyncOS for Cisco Secure Email Gateway*: Configuring Routing and Delivery Features.

Archiving Logs

Cisco does not store logs from your email cloud gateways. Historical logs are not archived and can be overwritten by log rotation. If you want to retain the logs, configure the log subscriptions on your email cloud gateways to use SCP Push (or SCP on Remote Server) as the log retrieval method. This method periodically pushes log files to an SCP server on a remote computer.

The method requires an SSH SCP server on a remote computer using the SSH1 or SSH2 protocol. The subscription requires a username, SSH key, and destination directory on the remote computer, and log files are transferred based on a rollover schedule that you set.

If your firewall blocks SSH access into your network, it is recommended that you explicitly allow the inbound SSH connections from the Cisco Cloud Email Security data centers.

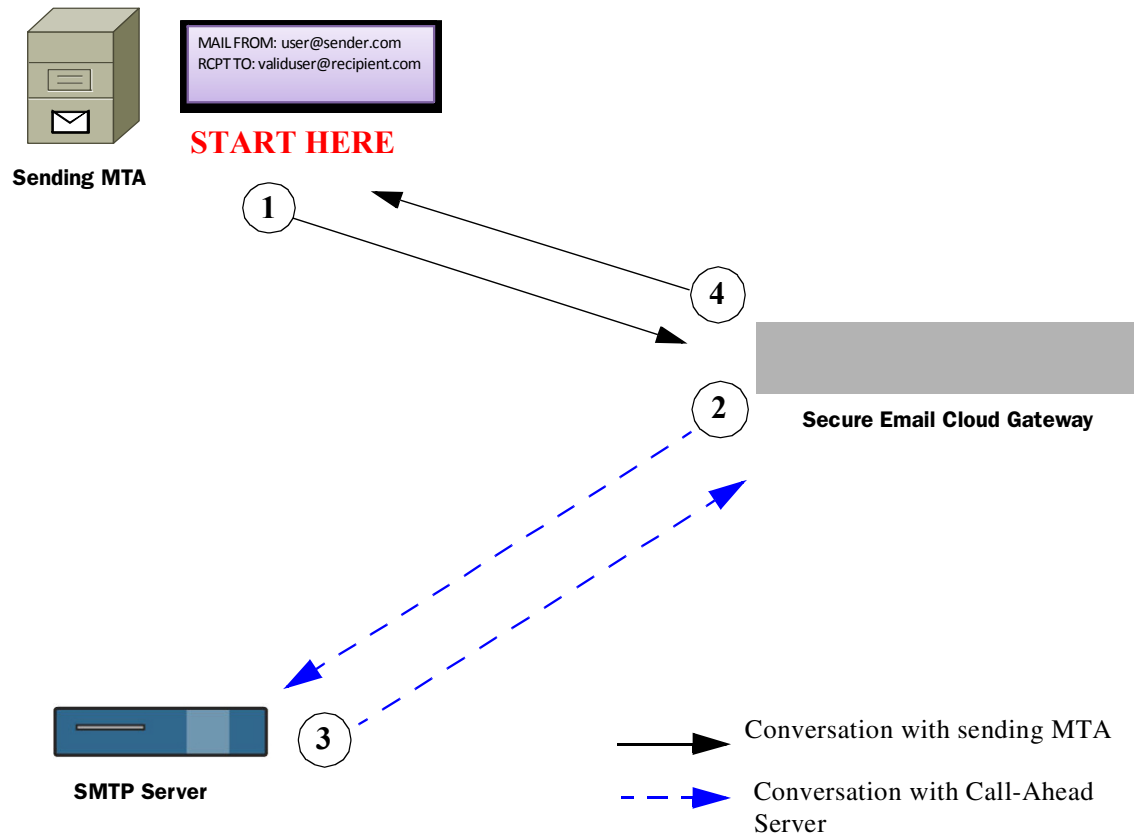
See *User Guide for AsyncOS for Cisco Secure Email Gateway*.

Configuring Your Servers

Using SMTP Call Ahead Validation

Cisco Secure Email Cloud uses SMTP call ahead validation for recipient validation, a seamless and elegant way to validate recipients while minimizing administrator overhead. This approach has minimal or no impact to firewall settings already in place with an existing solution.

Figure 2-1 SMTP Call Ahead Server Conversation Workflow



SMTP call ahead works as follows:

- Step 1** The sending email system (MTA) opens a connection with the email cloud gateway. As part of the initial SMTP protocol conversation, the sender email system passes along the RCPT TO information.
- Step 2** The secure email cloud infrastructure keeps the incoming connection open and initiates a call to the SMTP server. As part of this communication, the email cloud gateway passes the RCPT TO information to your SMTP server (for example, Microsoft Exchange).
- Step 3** Depending on whether the user in RCPT TO: is valid or invalid, the SMTP server sends a 200-series status or a 500-series status, respectively.

For SMTP call ahead to work properly, on your MTA or groupware server ensure that sender verification features (for example, SPF checks, TLS checks, and DHAP schemes) that might block connections from cloud-based servers have been disabled for the specified IP addresses.

- Step 4** The email cloud gateway resumes the SMTP conversation and sends a response to the sending MTA, allowing the conversation to continue or dropping the connection based on the SMTP server response (and settings configured in the SMTP Call-Ahead profile).

Due to the order of processes in the email pipeline, if the message for a given recipient is rejected by the RAT, then the SMTP call-ahead recipient validation will not occur. For example, if you specified in the RAT that only mail for *example.com* is accepted, then mail for *recipient@domain2.com* is rejected before SMTP call-ahead recipient validation can occur.

For more details about how SMTP call-ahead validation occurs, see *User Guide for AsyncOS for Cisco Secure Email Gateway*.



Using the Cisco End-User Spam Quarantine



Note

Use this chapter only if you have enabled the End-User Spam Quarantine.

- [Understanding the Cisco End-User Spam Quarantine, page 3-1](#)
- [Processing Messages in the Spam Quarantine, page 3-2](#)

Understanding the Cisco End-User Spam Quarantine

Spam includes but is not limited to:

- Advertising mail, pyramid schemes, chain letters, and propaganda
- Unwanted questionable subject matter, or abusive or threatening mail
- Mail that contains a false or misleading header, subject line, sender, return address, or routing or transmission path
- Mail that uses a third-party domain name without permission

The Spam Quarantine minimizes the impact of spam by implementing appropriate policies and technology. Mail messages that have been identified as spam are quarantined. If the messages are not spam, you can remove them from the quarantine and add the sender to a safelist. Or if the messages are truly spam, take no action. Quarantined mail is not calculated into your mailbox capacity limit and is automatically deleted after a certain number of days.



Note

Find out from your administrator how many days the quarantine holds on to mail before it is deleted.

No special hardware, software, or security authorization is required to access the Spam Quarantine. You receive Spam Quarantine notifications on a regular basis listing messages identified as spam.

Safelists and Blocklists

You can create safelists and blocklists to better control which mail messages are treated as spam. Safelists enable you to ensure that certain users or domains are never treated as spam, while blocklists ensure that certain users or domains are always treated as spam.

**Note**

Find out from your administrator the maximum number of entries you can add to your safelist and blocklist.

See [Accessing Safelists and Blocklists](#), page 3-3.

Processing Messages in the Spam Quarantine

Spam quarantine notifications provide details of messages so you can determine whether the messages are truly spam. You can process messages directly from a spam quarantine notification, or you can access the Spam Quarantine by clicking the links found in the body of the notification.

If the message is spam, do nothing. The message is kept in quarantine for a certain number of days (check with your administrator) and then deleted.

- [Releasing Messages from the Spam Quarantine to Your Inbox](#), page 3-2
- [Viewing Message Details](#), page 3-3
- [Viewing Message Details](#), page 3-3
- [Taking Action on Multiple Messages at a Time](#), page 3-3
- [Accessing Safelists and Blocklists](#), page 3-3
- [Searching Messages in the Quarantine](#), page 3-4

Releasing Messages from the Spam Quarantine to Your Inbox

If the message is not spam, then release the message from the quarantine to your inbox. You can also add the sender to your safelist to prevent future messages from the sender from being quarantined.

Procedure

Step 1 In the Spam Quarantine notification, click **Not Spam** next to the message you want to release.

Step 2 In the confirmation message that appears, click **Add Sender to Safelist**.

If you release the message and do not add the sender to the safelist, future messages from the sender may be quarantined.

Viewing Message Details

If you require details other than the message sender and the subject to determine whether a message is spam, you can view the entire message before taking action on it.

Procedure

Step 1 In the Spam Quarantine notification, click the message's Subject link to display the Message Details page.



Note If you already took action on the message, the Message Not Found page appears.

Step 2 From the drop-down list, choose the action you want to take. Options are: “Release,” “Release and Add to Safelist,” and “Delete.”

If you take no action, the message is deleted from the quarantine in a certain number of days (check with your administrator).

Step 3 Click **Submit**.

Step 4 In the confirmation message, confirm your intended action.

Taking Action on Multiple Messages at a Time

Procedure

Step 1 In the Spam Quarantine notification, click one of the links to access the Spam Quarantine.

Step 2 Select the check box next to each message on which you want to take action.

Step 3 From the drop-down list, select the action you want to take, and click **Submit**.

If you take no action, the messages is deleted from the quarantine in a certain number of days (check with your administrator).

Step 4 In the confirmation message, confirm your intended action.

Accessing Safelists and Blocklists

Entries can be added to safelists and blocklists using the following formats:

- wugtBfqockp0eqo
- ugtxgt0fqockp0eqo
- fqockp0eqo

You cannot add a sender or domain to both safelists and blocklists at the same time. However, if you add a domain to a safelist, and the email address for a user of that domain to the blocklist (or vice versa), the email gateway applies both rules. For example, if you add `gzcornng0eqo` to the safelist, and add `igqtigBgzcornng0eqo` to the blocklist, the email gateway delivers all mail from "gzcornng0eqo" without scanning for spam, but will treat mail from `igqtigBgzcornng0eqo` as spam.

You cannot allow or block a range of subdomains using the following syntax: `0fqockp0eqo0`. However, you can explicitly block a specific domain using the following syntax: `ugtugt0fqockp0eqo0`.

Adding Entries to Safelists or Blocklists

Procedure

- Step 1** In the Spam Quarantine notification, click one of the links to access the Spam Quarantine.
 - Step 2** From the **Options** drop-down list, choose **Safelist** or **Blocklist**.
 - Step 3** Enter the email address or domain, and click **Add to List**.
-



Note

Unlike safelist entries, you can add blocklist entries only from the Options menu in the End-User Spam Quarantine.

Searching Messages in the Quarantine

Procedure

- Step 1** In the Spam Quarantine notification, click one of the links to access the Spam Quarantine.
 - Step 2** In the **Search Messages** field, enter the term for which you are searching, and click **Search**.
-