Validating Recipients Using an SMTP Server

This chapter contains the following sections:

Overview of SMTP Call-Ahead Recipient Validation

The SMTP call-ahead recipient validation feature queries an external SMTP server before accepting incoming mail for a recipient. Use this feature to validate recipients when you cannot use LDAP Accept or the Recipient Access Table (RAT). For example, suppose you host mail for many mailboxes, each using a separate domain, and your LDAP infrastructure does not allow you to query the LDAP server to validate each recipient. In this case, the email gateway can query the SMTP server and validate the recipient before continuing the SMTP conversation.

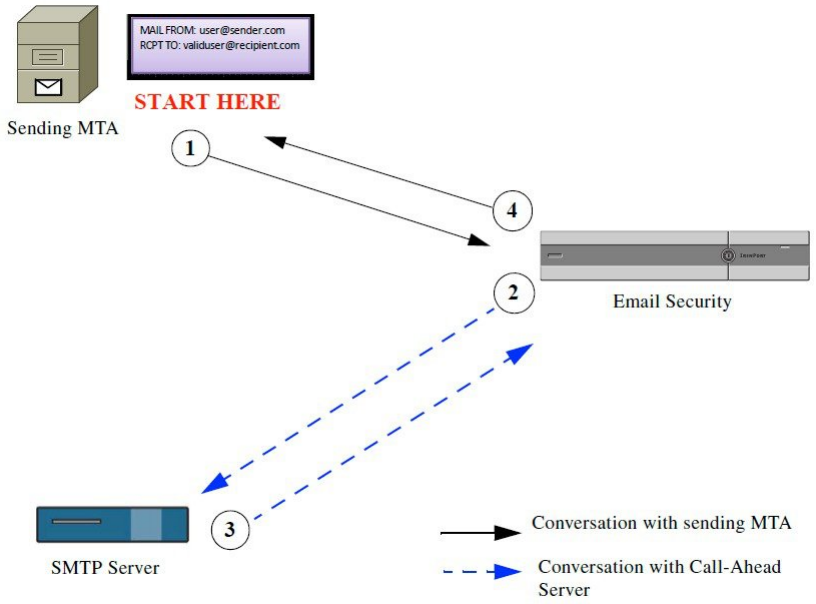
You can use SMTP call-ahead recipient validation in order to reduce processing on messages for invalid recipients. Typically, a message for an invalid recipient progresses through the work queue before it can be dropped. Instead, an invalid message can be dropped or bounced during the incoming/receiving part of the email pipeline without requiring additional processing.

SMTP Call-Ahead Recipient Validation Workflow

When you configure your email gateway for SMTP call-ahead recipient validation, the email gateway suspends the SMTP conversation with the sending MTA while it “calls ahead” to the SMTP server to verify the recipient. When the email gateway queries the SMTP server, it returns the SMTP server’s response to the Email Security appliance, and depending on the settings you have configured, you can accept the mail or drop the connection with a code and custom response.

The following figure shows the basic workflow of the SMTP call-head validation conversation.

Figure 1: SMTP Call Ahead Server Conversation Workflow



1. The sending MTA initiates an SMTP conversation.
2. The email gateway suspends the SMTP conversation while it sends a query to the SMTP server to verify the recipient, *validuser@recipient.com* .

Note If SMTP routes or LDAP routing queries are configured, these routes will be used to query the SMTP server.

3. The SMTP Server returns a query response to the email gateway.
4. The email 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 you configure 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.

Note If you have configured Directory Harvest Attack Prevention (DHAP) in the HAT, be aware that SMTP call-ahead server rejections are part of the number of rejections included in the maximum invalid recipients per hour that you specify. You may need to adjust this number to account for additional SMTP server rejections. For more information about DHAP, see the “Configuring the Gateway to Receive Email” chapter.

How to Validate Recipients Using an External SMTP Server

	Do This	More Info
Step 1	Determine how the email gateway connects to the SMTP server and interprets the server's responses.	Configuring the Call-Ahead Server Profile, on page 3
Step 2	Configure a public listener to use the SMTP server to validate recipients	Enabling a Listener to Validate Incoming Mail Via the SMTP Server, on page 6
Step 3	(Optional) Update your LDAP Routing query to determine the SMTP server to use when routing mail to a different host.	Configuring LDAP Routing Query Settings, on page 7
Step 4	(Optional) Configure the email gateway to bypass call-ahead validation for certain recipients	Bypassing SMTP Call-Ahead Validation for Certain Users or Groups, on page 8

Related Topics

- Configuring the Call-Ahead Server Profile, on page 3

Configuring the Call-Ahead Server Profile

When you configure the SMTP Call-Ahead Server Profile, you specify the settings that determine how the email gateway connects with the SMTP server and how it interprets the responses sent back from the SMTP server.

Procedure

Step 1 Click **Network** > **SMTP Call-Ahead**.

Step 2 Click **Add Profile**.

Step 3 Enter the settings for the profile. For more information, see *Table - SMTP Call-Ahead Server Profile Settings*.

Step 4 Configure the advanced settings for the profile. For more information, see *Table - SMTP Call-Ahead Server Profile Advanced Settings*.

Step 5 Submit and commit your changes.

What to do next

- SMTP Call-Ahead Server Profile Settings, on page 4
- Call Ahead Server Responses, on page 6

SMTP Call-Ahead Server Profile Settings

When you configure the SMTP Call-Ahead Server Profile, you need to configure settings that determine how the email gateway connects with the SMTP server.

Table 1: SMTP Call-Ahead Server Profile Settings

Setting	Description
Profile Name	Name of the call-ahead server profile.
Call-Ahead Server Type	Choose from one of the following methods for connecting to the call-ahead server: • **Use Delivery Host**. Select this option to specify that the host for the delivery email address is used for the SMTP call-ahead query. For example, if the mail recipient address is *recipient@example.com* , the SMTP query is executed against the SMTP server associated with *example.com* . If you have configured SMTP routes or LDAP routing queries, these routes are used to determine the SMTP server to query. For details about configuring LDAP routing queries, see Configuring LDAP Routing Query Settings, on page 7. • **Static Call-Ahead Server**. Use this option to create a static list of call-ahead servers to query. You may want to use this option if you do not expect the names and locations of the call-ahead servers to change often. When you use this option, the email gateway queries the hosts in a round-robin fashion, starting with the first static call-ahead server listed. **Note** Note that when you choose the static call-ahead server type, no SMTP routes are applied to the query. Instead an MX lookup is performed, and then an A lookup is performed on the hosts to obtain the call-ahead IP addresses for the static servers.
Static Call-Ahead Servers	If you choose to use the static call-ahead server type, enter a list of host and port combinations in this field. List the server and port using the following syntax: ironport.com:25 Separate multiple entries with a comma.

The following table describes the SMTP Call-Ahead Server Profile advanced settings:

Table 2: SMTP Call-Ahead Server Profile Advanced Settings

Setting	Description
Interface	The interface used to initiate the SMTP conversation with the SMTP server. Choose to use the Management interface or Auto. When you select Auto, the email gateway attempts to automatically detect an interface to use. The Cisco IronPort interface attempts to connect to the SMTP server in the following ways: • If the call-ahead server is on the same subnet as one of the configured interfaces, then the connection is initiated by the matching interface. • Any configured SMTP routes are used to route the query. • Otherwise, the interface that is on the same subnet as the default gateway are used.
TLS Support for Recipient Validation	Select the **Enabled** radio button if you want to perform SMTP call-ahead recipient validation using TLS. **Note** The SMTP call-ahead recipient validation uses the same TLS version selected in the 'Other TLS Client Services' option in the 'SSL Configuration' page in your email gateway. **Note** If you select the 'TLS Support for Recipient Validation' option, make sure you add a valid client certificate in your email gateway to establish SMTP call-ahead recipient validation using TLS. **Note** TLS support for SMTP call-ahead recipient validation uses the DEFAULT SSL cipher list. The DEFAULT keyword is the OpenSSL DEFAULT cipher string, which is generally `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`.
MAIL FROM Address	The MAIL FROM: address to be used for the SMTP conversation with the SMTP server.
Validation Request Timeout	The number of seconds to wait for a result from the SMTP server. This timeout value is for a single recipient validation request which may involve contacting multiple call-ahead servers. See Call Ahead Server Responses, on page 6.
Validation Failure Action	The action to be taken when a recipient validation request fails (due to a timeout, server failure, network issue, or unknown response). You can configure how you want the email gateway to handle the different responses. See Call Ahead Server Responses, on page 6.
Temporary Failure Action	The action to be taken when a recipient validation request temporarily fails (and a 4xx response is returned from the remote SMTP server). This can occur when the mailbox is full, the mailbox is not available, or the service is not available). See Call Ahead Server Responses, on page 6.
Max. Recipients per Session	Maximum number of recipients to be validated in a single SMTP session. Specify between 1 - 25,000 sessions.

Setting	Description
Max. Connections per Server	Maximum number of connections to a single call-ahead SMTP server. Specify between 1-100 connections.
Cache	Size of the cache for SMTP responses. Specify between 100-1,000,000 entries
Cache TTL	Time-to-live value for entries in the cache. This field defaults to 900 seconds. Specify between 60 - 86400 seconds.

Call Ahead Server Responses

The SMTP server may return the following responses:

- **2xx**: When an SMTP code starting with 2 is received from the call-ahead server, the recipient is accepted. For example, a response of 250 allows the mailing action to continue.
- **4xx**: An SMTP code starting with a 4 means that a temporary failure has occurred in processing the SMTP request. A retry may later be processed successfully. For example, a response of 451 means the requested action was aborted or there was a local error in processing.
- **5xx**: An SMTP code starting with 5 means a permanent failure in processing the SMTP request occurred. For example, a response of 550 means the requested action was not taken or the mailbox was unavailable.
- **Timeout.** If no response is returned from the call-ahead server, you can configure how long to attempt to retry before a timeout occurs.
- **Connection error**. If a connection to the call-ahead server fails, you can configure whether to accept or reject a connection for the recipient address.
- **Custom Response**. You can configure to reject a connection with custom SMTP response (code and text) for validation failures and temporary failures.

Enabling a Listener to Validate Incoming Mail Via the SMTP Server

Once you create the SMTP Call-Ahead Server Profile, you need to enable it on a listener to allow the listener to validate incoming mail via the SMTP server. SMTP call-ahead functionality is only available on public listeners, as recipient validation is not necessary for private listeners.

Procedure

Step 1 Go to **Network** > **Listeners**.

Step 2 Click the name of the listener where you want to enable SMTP call-ahead functionality.

Step 3 In the **SMTP Call Ahead Profile** field, select the SMTP Call-Ahead profile you want to enable.

Step 4 Submit and commit your changes.

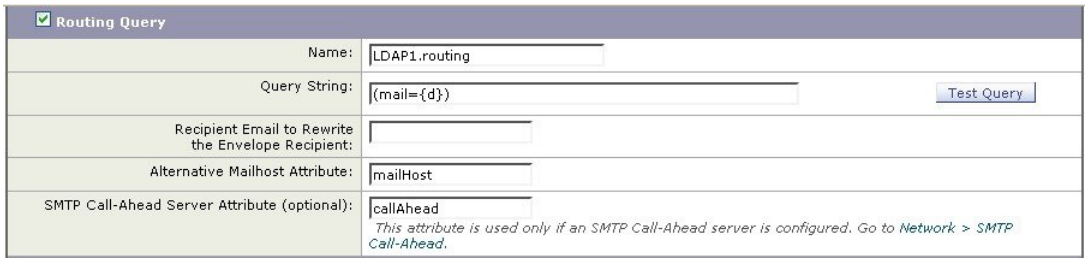
Configuring LDAP Routing Query Settings

If you use an LDAP routing query to route mail to a different mail host, AsyncOS uses the Alternate Mailhost Attribute to determine the SMTP server to query. However, there are cases where you may not want that to occur. For example, in the following schema, note that the mail host attribute (mailHost) has a different SMTP address than the servers listed in the call-ahead SMTP server attribute (callAhead):

```
dn: mail=cisco.com, ou=domains
mail: cisco.com
mailHost: smtp.mydomain.com
policy: ASAV
callAhead: smtp2.mydomain.com,smtp3.mydomain.com:9025
```

In this case, you can use the **SMTP Call-Ahead** field to create a routing query that directs the SMTP call-ahead query to the servers listed in the callAhead attribute. For example, you might create a routing query with the following attributes:

Figure 2: LDAP Routing Query Configured for SMTP Call-Ahead



In this query, the {d} represents the domain part of the recipient address, and the SMTP Call-Ahead Server Attribute returns the values for the call-ahead servers and the port that should be used for the query: smtp2.mydomain.com, smtp3.mydomain.com on port 9025.

Note This example shows just one way to configure a query that enables you to use the LDAP routing query to direct SMTP call-ahead queries to the correct SMTP servers. You are not required to use the query string or specific LDAP attributes described in this example.

SMTP Call-Ahead Query Routing

When routing an SMTP call-ahead query, AsyncOS checks for information in the following order:

1. Checks the domain name.
2. Checks for LDAP Routing queries.
3. Checks for SMTP Routes.
4. Performs a DNS Lookup (First an MX Lookup is performed, followed by an A lookup).

If there is no LDAP routing query or no SMTP Routes configured for the domain, the result of preceding state is passed to next stage. In any case where there is no SMTP Route present, a DNS lookup is performed.

When you use an LDAP Routing query for an SMTP call-ahead query and you also have SMTP routes configured, the routing behavior depends upon the values returned by the routing query.

- If the LDAP routing query returns a single hostname without a port, the SMTP call-ahead query applies SMTP routes. If the SMTP routes only lists the destination host as the hostname, a DNS lookup is performed to obtain the IP address of the SMTP server.
- If the LDAP routing query returns a single hostname with a port, the SMTP route is used, but the port returned by the LDAP query is used over any ports specified in SMTP routes. If the SMTP routes only lists the destination host as the hostname, a DNS lookup is performed to obtain the IP address of the SMTP server.
- If the LDAP routing query returns multiple hosts with or without ports, SMTP routes are applied, but the ports returned by the LDAP routing query are used over those present in SMTP routes. If the SMTP routes only lists the destination host as the hostname, a DNS lookup is performed to obtain the IP address of the SMTP server.

Bypassing SMTP Call-Ahead Validation for Certain Users or Groups

You may want to enable SMTP call-ahead validation on a listener but skip the SMTP call-ahead validation for certain users or groups of users.

You may want to skip SMTP call-ahead validation for recipients for whom mail should not be delayed during SMTP call-ahead queries. For example, you could add a RAT entry for a customer service alias that you know is valid and will likely need immediate attention.

To configure bypassing SMTP call-ahead validation via the GUI, select **Bypass SMTP Call-Ahead** when you add or edit the RAT entry