Configuring SMTP Routing

This chapter contains the following sections:

- SMTP Routes Overview, on page 1
- Routing Email for Local Domains, on page 2
- Managing SMTP Routes , on page 3

SMTP Routes Overview

This chapter explains the features that affect routing and delivery of email traveling through the Cisco Secure Email and Web Manager appliance, and use of the SMTP Routes page and **smtproutes** command.

SMTP Routes allow you to redirect all email for a particular domain to a different mail exchange (MX) host. For example, you could make a mapping from example.com to groupware.example.com . This mapping causes any email with @example.com in the Envelope Recipient address to go instead to groupware.example.com . The system performs an “MX” lookup on groupware.example.com , and then performs an “A” lookup on the host, just like a normal email delivery. This alternate MX host does not need to be listed in DNS MX records and it does not even need to be a member of the domain whose email is being redirected. The operating system allows up to ten thousand (10,000) SMTP Route mappings to be configured for your Cisco Content Security appliance. (See SMTP Routes Limits, on page 3.)

This feature also allows host “globbing.” If you specify a partial domain, such as example.com , then any domain ending in example.com matches the entry. For instance, fred@foo.example.com and wilma@bar.example.com both match the mapping.

If a host is not found in the SMTP Routes table, an MX lookup is performed using DNS. The result is not re-checked against the SMTP Routes table. If the DNS MX entry for foo.domain is bar.domain , any email sent to foo.domain is delivered to the host bar.domain . If you create a mapping for bar.domain to some other host, email addressed to foo.domain is not affected.

In other words, recursive entries are not followed. If there is an entry for a.domain to redirect to b.domain , and a subsequent entry to redirect email for b.domain to a.domain , a mail loop will *not* be created. In this case, email addressed to a.domain will be delivered to the MX host specified by b.domain , and conversely email addressed to b.domain will be delivered to the MX host specified by a.domain .

The SMTP Routes table is read from the top down for every email delivery. The most specific entry that matches a mapping wins. For example, if there are mappings for both host1.example.com and example.com in the SMTP Routes table, the entry for host1.example.com will be used because it is the more specific entry — even if it appears after the less specific example.com entry. Otherwise, the system performs a regular MX lookup on the domain of the Envelope Recipient.

SMTP Routes, Mail Delivery, and Message Splintering

Incoming: if one message has 10 recipients and they are all on the same Exchange server, AsyncOS will open one TCP connection and present exactly one message to the mail store, not 10 separate messages.

Outgoing: works similarly, but if one message is going to 10 recipients in 10 different domains, AsyncOS will open 10 connections to 10 MTAs and deliver them one email each.

Splintering: if one incoming message has 10 recipients and they are each in separate Incoming Policy groups (10 groups), the message will splinter even if all 10 recipients are on the same Exchange server. Thus, 10 separate emails will be delivered over a single TCP connection.

SMTP Routes and Outbound SMTP Authentication

If an Outbound SMTP Authentication profile has been created, you can apply it to an SMTP Route. This allows authentication for outgoing mail in cases where the Cisco Secure Email and Web Manager appliance sits behind a mail relay server that is at the edge of the network.

Routing Email for Local Domains

The Security Management appliance routes the following mail:

- ISQ released messages which ignore SMTP routing
- Alerts
- Configuration files that can be mailed to the specified destination
- Support request message that can be sent to the defined recipient as well

The last two types of messages use SMTP routes to be delivered to the destination.

The Email Security appliance routes mail to local domains to hosts specified using the **Management Appliance > Network > SMTP Routes** page (or the **smtproutes** command). This feature is similar to the sendmail **mailertable** feature. (The SMTP Routes page and **smtproutes** command are an expansion of the AsyncOS 2.0 Domain Redirect feature.)

Note If you have completed the System Setup Wizard in the GUI and committed the changes, you defined the first SMTP route entries on the appliance for each RAT entry you entered at that time.

Default SMTP Route

You can also define a default SMTP route with the special keyword ALL . If a domain does not match a previous mapping in the SMTP Routes list, it defaults to being redirected to the MX host specified by the ALL entry.

When you print the SMTP Routes entries, the default SMTP route is listed as ALL: . You cannot delete the default SMTP route; you may only clear any values entered for it.

Configure the default SMTP route using the **Management Appliance > Network > SMTP Routes** page or the **smtproutes** command.

Managing SMTP Routes

- Defining an SMTP Route, on page 3
- SMTP Routes Limits, on page 3
- Adding SMTP Routes, on page 3
- Exporting SMTP Routes, on page 4
- Importing SMTP Routes, on page 4
- SMTP Routes and DNS, on page 5

Defining an SMTP Route

The Email Security appliance routes mail to local domains to hosts specified using the **Management Appliance > Network > SMTP Routes** page (or the **smtproutes** command). This feature is similar to the sendmail mailer table feature. (The SMTP Routes page and **smtproutes** command are an expansion of the AsyncOS 2.0 Domain Redirect feature.):

Use the Management Appliance > Network > SMTP Routes page (or the **smtproutes** command) to construct routes. When you create a new route, you first specify the domain or partial domain for which you want to create a permanent route. You then specify destination hosts. Destination hosts can be entered as fully-qualified hostnames or as IP addresses. You can also specify a a special destination host of /dev/null to drop the messages that match the entry. (So, in effect, specifying /dev/null for the default route is will ensure that no mail received by the appliance is ever delivered.)

Multiple destination host entries can contain both fully-qualified hostnames and IP addresses. Separate multiple entries with commas.

If one or more of the hosts are not responding, messages will be delivered to one of the reachable hosts. If all the configured hosts are not responding, mail will be queued for that host (does not fail over to using MX records).

SMTP Routes Limits

You can define up to 10,000 routes. The final default route of ALL is counted as a route against this limit. Therefore, you can define up to 9,999 custom routes and one route that uses the special keyword ALL .

Adding SMTP Routes

Procedure

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > Network > SMTP Routes**.

Step 3 Click **Add Route**.

Step 4 Enter a receiving domain and destination host. You can add multiple destination hosts by clicking **Add Row** and entering the next destination host in the new row.

Step 5 You can specify a port number by adding ":<*port number*> " to the destination host: example.com:25

Step 6 Submit and commit your changes.

Exporting SMTP Routes

Similar to the Host Access Table (HAT) and the Recipient Access Table (RAT), you can also modify SMTP routes mappings by exporting and importing a file.

Procedure

Step 1 Click **Export SMTP Routes** on the SMTP Routes page.

Step 2 Enter a name for the file and click **Submit**.

Importing SMTP Routes

Similar to the Host Access Table (HAT) and the Recipient Access Table (RAT), you can also modify SMTP routes mappings by exporting and importing a file.

Procedure

Step 1 Click **Import SMTP Routes** on the SMTP Routes page.

Step 2 Select the file that contains the exported SMTP Routes.

Step 3 Click **Submit**. You are warned that importing will replace all existing SMTP Routes. All of the SMTP Routes in the text file are imported.

Step 4 Click **Import**.

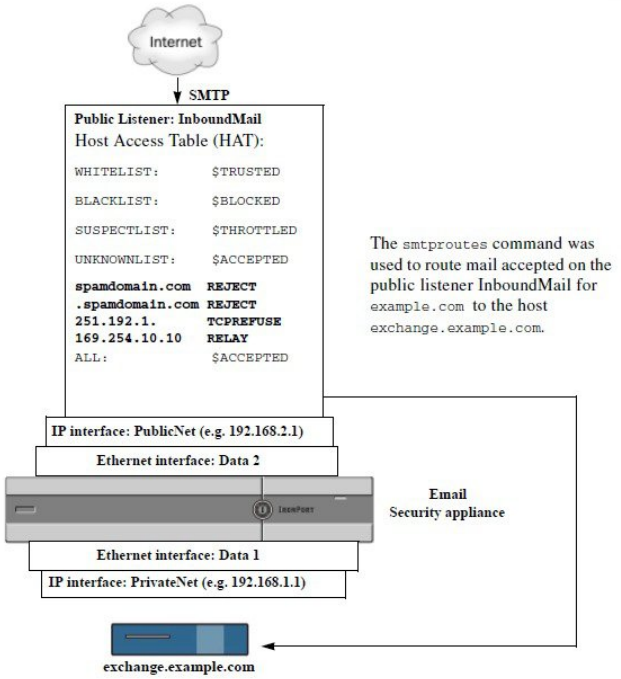
You can place “comments” in the file. Lines that begin with a ‘#’ character are considered comments and are ignored by AsyncOS. For example:

this is a comment, but the next line is not

ALL:

At this point, our Email Gateway configuration looks like this:

Figure 1: Email Gateway Configuration



SMTP Routes and DNS

Use the special keyword USEDNS to tell the appliance to do MX lookups to determine next hops for specific domains. This is useful when you need to route mail for subdomains to a specific host. For example, if mail to example.com is to be sent to the company's Exchange server, you might have something similar to the following SMTP route:

```
example.com exchange.example.com
```

However, for mail to various subdomains (foo.example.com), add an SMTP route that looks like this:

```
.example.com USEDNS
```