How does the Exception Table on the ESA work?

Document ID: 118506

Contributed by Shiu Ng and Enrico Werner, Cisco TAC Engineers.

Oct 09, 2014

Contents

Introduction

This document describes how the Exception Table on the Email Security Appliance (ESA) works.

How does the Exception Table on the ESA work?

The Exception Table lists email addresses − full or partial − with two different types of behavior: Allow or Reject. In the Mail Flow Policies, the option "Use Sender Verification Exception Table" needs to be checked, otherwise the Exception Table entries will not be matched.

Allow Action

Allow listings in the Exception Table bypass Sender DNS Verification. If the envelope sender's domain or email address is listed in the Exception Table, the sender will be allowed to proceed with sending the mail to the ESA, whether the domain name of the envelope sender email address can be resolved or not. ***This is useful when sender DNS verification is enabled and the domain cannot be resolved*** (e.g. allow mail from internal or test domains, even if they would not otherwise be verified).

If Sender DNS Verification is enabled for the Mail Flow Policy in use, and an envelope sender's domain name cannot be resolved (it does not exist, cannot be resolved, or is malformed), the message will be rejected. Here is an example of an SMTP response:

```
SMTP code: 553
Message: #5.1.8 Domain of sender address <$EnvelopeSender> does not exist
```

If the email address or domain of the envelope sender is listed in the Exception Table with Allow behavior, then the sender can proceed with the remainder of the message (RCPT TO, DATA, etc, and normal processing of the message will take place: message filters, Anti−Spam scanning, etc.). This allows the message into the appliance despite the domain name of the sender not being verifiable. For example, the sender will be rejected under the following circumstances:

- the envelope sender is user@example.com
- the domain "example.com" does not exist
- user@example.com is not in the Exception Table allow list
- example.com are not in the Exception Table allow list
  mail from:user@example.com

This is the entry in the log for a rejected sender:

```
553 #5.1.8 Domain of sender address <user@example.com> does not exist
```

If an "allow" listing for @example.com is added, the sender is allowed and this entry will appear in the log:

```
mail from:<user@example.com>
250 sender <user@example.com> ok
```

Reject Action

A message will be rejected if the envelope sender matches a Reject listing in the Exception Table. By default, the SMTP response will be:

```
SMTP code: 553
Message: Envelope sender <$EnvelopeSender> rejected
```

If you have a listing such as user@example.com with "Reject" behavior, any mail sent where the envelope sender is "user@example.com" will be rejected:

```
mail from:<user@example.com>
553 Envelope sender <user@example.com> rejected
```

Updated: Oct 09, 2014 Document ID: 118506