ESA Block Blank From: Addresses Configuration Example

Document ID: 117814

Contributed by Tomki Camp and Enrico Werner, Cisco TAC Engineers.
Jun 16, 2014

Contents

Introduction

This document describes how configure block blank ***From:*** addresses in AsyncOS for the Cisco Email Security Appliance (ESA).

Background Information

A blank ***From:*** address can be interpreted in several ways. Email messages have both envelope addresses and addresses in the message headers. The envelope addresses are created during the Simple Mail Transfer Protocol (SMTP) conversation when a message is received. SMTP requires an envelope−from address that is non−null; therefore it is not possible to receive a message with a blank envelope−from address. The envelope−from address <> is a special case that is specifically used by mailers in order to send bounce messages. This is a signal to the receiving mailer that a bounce cannot be sent to that address; it is used to prevent mail loops.

The message headers, which include the ***From:*** header, are all considered part of the message content and are not required to match the envelope addresses. This is used to good effect by list email. An example is where long recipient lists are not included in the content ***From:*** header, but a list return address is often given instead. This is also used in spam and viruses in order to mislead recipients about the sender of the message.

Some messages have been observed to have no ***From:*** lines or blank ***From:*** lines. Although it might seem desirable to drop messages with blank ***From:*** lines as probable spam, remember that it might offer little in the way of an improved spam capture rate, but might increase false positives. A large percentage of application−generated mail, newsletters, and bounces might have blank ***From:*** addresses and most spam seems to have a false ***From:*** field.

Configure

Here is a message filter that drops messages that either have no ***From:*** in the message header or a blank ***From:*** header. The filter evaluates to true if there is no ***From:*** header at all, or if the header has a null value.

Use the filters command on the CLI in order to install message filters.

```
block_null_from_headers: if (NOT header("From")) {
drop();
}
```

Here is a filter that drops messages with a ***From:*** <> content header:

```
block_null_bounce_headers: if (header("From") == "^$") {
drop();
}
```

Verify

Use this section in order to confirm that your configuration works properly.

Connect to the ESA using Telnet on port 25 and send two test messages − one message without a ***From:*** header and another message with an empty ***From:*** header.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- ***Technical Support & Documentation − Cisco Systems***

Updated: Jun 16, 2014 Document ID: 117814