Common Configuration Errors on the ESA

Document ID: 118465

Contributed by Liz Slocum and Enrico Werner, Cisco TAC Engineers.

Oct 13, 2014

Contents

Introduction

This document describes common configuration errors on Email Security Appliance (ESA).

What are the common configuration errors on the ESA?

Whether you are setting up a new evaluation or looking over an existing configuration, you can refer to this checklist of common configuration mistakes.

1. HAT

- Do not put positive SBRS scores like +5 or +7 into the WHITELIST. A range of 9.0−10.0 would be OK, but including lower scores will only make it more likely that spam will get through.
- Disable the UNKNOWNLIST, Envelope Sender DNS Verification and Connecting Host DNS Verification unless you really need and understand these.
- Instead of changing message size and other policy settings in each Mail Flow Policy, go to the Mail Flow Policies menu and choose the last option, "Default Policy Parameters".
- Limit maximum connections to three for most senders, and make this the default for new Mail Flow Policies.
- Check that SenderBase scores from −10.0 to −2.0 are included in the BLACKLIST. The documentation and setup wizards are overly conservative; we currently have no false positives in this range.

2. Policy

- Name policies after who gets them, not what they do. Name any content filters after what they do, and use abbreviations like Q_basic_attachments, D_spoofers, Strip_Multi−Media, where Q means quarantine and D means drop.
- Non−default policies should "Use Default Settings" for Anti−Spam, Anit−Virus, Content Filters and Outbreak Filters except where you really need special settings. Do not recreate those settings in each policy if it is not necessary.
- Untick "Drop infected attachments" or else you will pass on many blank emails where the virus has been stripped.
- Anti−Virus settings for outbound should notify the sender, not the recipient
- Outbreak Filters and Anti−Spam should be disabled on outbound

3. Incoming relays

If "Monitor > Overview" shows connections from your own servers and domains, you need to add them to the Incoming Relays setup. A very common mistake, when using the GUI, is to think that you have enabled the Incoming Relay feature when all you have done is add the entries to the table. In addition:

- Add a special HAT Sender Group for them, above WHITELIST, for reporting purposes. Choose no rate limiting or DHAP, but spam and virus detection are OK.
- Add a message filter to match your BLACKLIST policy action. For example:

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= −2.0
{ drop();}
```

In rare cases where you are re−injecting E−Mail (for example, re−processing inter−subscriber mail through the inbound mail policy), your filter will also need to exempt the reinjection interface. Normally this is not necessary.

4. DNS

Many customers force the ESA to query their internal DNS servers out of habit. In most installations, 100% of the DNS records we need are on the Internet, not in the internal DNS. It makes more sense to query the Internet root servers, reducing the forwarding load on the internal DNS.

5. Message and Content Filters

The most common error is to put matching conditions in Content Filters where they are not required. Most filters should list some actions, but the condition should be left blank. The filter will be *true* always, and will always run. You control which users/policies receive these actions by creating new Incoming or Outgoing mail policies as needed, and applying this filter to the policy. Here are incorrect and correct examples:

- It is almost always an error to use the rcpt−to condition in a message filter. The correct procedure is to

write an incoming content filter, and make it specific for a particular user by adding a recipient−based Incoming Mail Policy.

- It is almost always an error to have a content filter test for the presence of an attachment, then drop the attachment. The correct method is to always drop that attachment, without testing for its presence.

- It is almost always an error to use deliver(). Deliver means skip any remaining filters, then deliver. If you just want to deliver without skipping the rest of the filters, no explicit action is required (implied deliver).

7. Open Relay Prevention

Some services will check to see if your Message Transfer Agent (MTA) accepts addresses which potentially could result in open relay conditions. Since leaving your MTA as a functioning open relay is bad, these sites may add you to blacklists unless you reject these dangerous addresses in the SMTP conversation.

Add a special HAT Sender Group for them, above WHITELIST, for reporting purposes. Choose no rate limiting or DHAP, but allow spam and virus detection.

- Change to Strict Address Parsing (Loose is the default). This is necessary to prevent double @ signs in addresses.

- Reject (not strip) invalid characters. This is also necessary to prevent double @ signs in addresses.

- Reject (not accept) literals, and enter the following characters: *%!\\/?

Related Information

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

Updated: Oct 13, 2014 Document ID: 118465