How do I configure the ESA to skip anti−spam and/or anti−virus scanning for my trusted senders?

Document ID: 117908

Contributed by Jackie Fleming and Enrico Werner, Cisco TAC Engineers.
Jul 10, 2014

Contents

Question:

How do I configure the ESA to skip anti−spam and/or anti−virus scanning for my trusted senders?

AsyncOS offers three main tools that you can use to skip anti−spam or anti−virus checking for your most trusted senders. Please note that the ESA does not advise skipping anti−virus checking at any time, even for your most trusted senders, because of the potential for inadvertent infection with viruses. The following is a discussion of the three ways you can skip anti−spam checking for some subset of your message flow.

The first tool available to you is the Host Access Table (HAT) Mail Flow Policies. Using Mail Flow Policies, you can identify senders by IP address (using either numeric IP addresses or PTR DNS names), by SenderBase score, or by a local DNS whitelist or blacklist. Once you have identified senders as trusted within a Sender Group in the HAT, you can then mark that sender group to skip anti−spam scanning.

For example, let's suppose that you wanted to identify a specific business partner, EXAMPLE.COM, that should not have anti−spam checking on their mail. You would have to find out SCU.COM's mail server IP addresses (or DNS pointer records). In this case, let's assume that EXAMPLE.COM has mail servers that will have IP addresses with DNS PTR records of "smtp1.mail.scu.com" through "smtp4.mail.scu.com." Remember in this case that we are looking at the PTR record (sometimes called reverse DNS) for the mail servers; this has nothing to do with the domain name that people at SCU.COM will use for outgoing mail.

You could create a new Sender Group (or use an existing sender group, such as WHITELIST) with Mail Policies>Overview>Add Sender Group. Let's create one called "NotSpammers". After you've submitted this page, you'll be returned to the Mail Policies>Overview screen, where you'll have the opportunity to add a new policy for this Sender Group. If you click on "Add Policy," you'll be given the opportunity to create a new policy. In this case, we want to only override the default policy in one area: Spam Detection. Give the policy a name and set the connection behavior to be "Accept," then scroll down to the Spam Detection section and set this policy to skip spam checking. Submit that new policy, and don't forget to "Commit Changes."

An alternative approach is to use Incoming Mail Policies to skip anti−spam scanning. The difference between the HAT and Incoming Mail Policies is that the HAT is entirely based on the IP information on the sender: the true IP address, the IP address as reflected in the DNS, the SenderBase score (which is based on the IP address) or a DNS whitelist or blacklist entry based on the IP address. Incoming Mail Policies are based on the message envelope information: who the message is to or who the message is from. This means that they are susceptible to being fooled by someone impersonating a message sender. However, if you want to simply skip all anti−spam checking for incoming mail coming from people who have email addresses that end in "@example.com," you could do that as well.

To create such a policy, go to Mail Policies>Incoming Mail Policies>Add Policy. This will let you add a policy that defines a set of senders (or recipients). Once you define the Incoming Mail Policy, it will appear in the overview screen (Mail Policies>Incoming Mail Policies). You can then click on the "Anti−Spam" column and edit the specific settings for anti−spam for this particular user.

The Anti−Spam settings for a particular policy have lots of options, but in this case, we simply want to skip anti−spam checking. Note here another difference between HAT−based policy and Incoming Mail Policies: the HAT can only let you skip or not skip anti−spam scanning, while Incoming Mail Policies have much greater control. For example, you could choose to quarantine spam from certain senders, and delete spam from other senders.

The third option for skipping anti−spam scanning is in Message Filters. (Note that Content Filters cannot be used for this because Content Filters occur after anti−spam scanning has already occurred). One of the actions in Message Filters is "skip−spamcheck." The message filter below will skip anti−spam checking for senders who have a particular IP address or who come from a particular domain name:

```
SkipSpamcheckFilter:
    if ( (remote-ip == '192.168.195.101') or
         (mail-from == '@example\\.com$')      )
    {
        skip-spamcheck();
    }
```

Updated: Jul 10, 2014 Document ID: 117908