

Re: [SLE] SMTP authentication

Source: <http://linux.derkeiler.com/Mailing-Lists/SuSE/2006-05/msg00098.html>

- *From:* "Hylton Conacher (ZR1HPC)" <hylton@xxxxxxxxxxxxx>
 - *Date:* Mon, 01 May 2006 18:08:04 +0200
-

Sandy Drobic wrote:

Hylton Conacher (ZR1HPC) wrote:

I admit this is going a bit overboard with the authentication but it could happen nevertheless.

Sandy, the above paragraphs were pivotal to my understanding. Free beer/fruit juice on the house for Sandy.

So eventhough my local SMTP server dials up to the internet with a certain username and password, that same username and password would not be used as authentication between my local SMTP server and the ISP's one, should it be used as a relay?

Your smtp server should not dial up to the internet. How the network is configured and in what way it connects to the internet is a task that the Operating System is should take care of, be that a permanent conenction, a semi-permanent connection via DSL/Cable or a dial-up connection that is opened by cron or on request by a dial-up daemon.

OK, it was used figurativly, but I see that I am going to need to get another box here to act as the dialup server+firewall+IPS.

Network planning mode ON :)

Postfix merely tries to send a mail off. This might require an internet connection when the mail is destined for an external server. Now it is your task to decide how the system should react:

– either defer all outgoing mails until you connect to the internet, then flush out all the mails in the queue. That would be appropriate for a dial-up connection. Postfix should not accept mails directly from the internet in that case. That should be done by the ISP that is hosting your mail domain. Your local server would use an external program like fetchmail to poll the mailservier of your ISP, download the mails and feed them to Postfix.

Re: [SLE] SMTP authentication

This is the method I would use.

– or you have a permanent connection to the internet. Then Postfix can send mails as soon as they are coming in from the clients. If you do not have a static ip address (your ip address doesn't change even if you shut down and reconnect to the internet) you should configure Postfix to send outgoing mails via the mailserver of your provider. The reason is that many mailservers, especially those of the big companies and ISPs are configured to reject mails coming from a non-static ip address. They have made the experience that the overwhelming majority of mails coming from dynamic ip addresses are spam.

Carlos said earlier that the SMTP server might not accept from a dynamic IP and I wondered if sending to the ISP mailserver would prevent bounved mails.

The easiest way to test it is to set up several mail accounts in your mailclient and configure each account to send with the same user/pass to your ISP mailserver.

Sorry, I didn't see that I was able to specify the name and password the new SMTP server I had added. :()

I've added a new entry for smtp.gmail.com and used my gmail username to authenticate. It didn't request a password so I assume that will come up when I send the message.

Are you talking about Postfix or your Mailclient?

My Mozilla mailclient.

Are these methods also used if the sender is a SMTP server or are different criteria used? ie see above just below OR.

Which restrictions are used mostly depends on what kind of recipient address the email has. I'll give you a Postfix example:

Your server has the following configuration:

```
mydestination = example.org
mynetworks = 192.168.1.0/24
smtpd_recipient_restrictions =
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_unauth_destination,
```

Re: [SLE] SMTP authentication

permit

Now, a client in your internal network with the ip 192.168.1.15 connects to your server and wishes to send an email to user@xxxxxxxxxxxxxxxxxxxxx
Postfix examines the restrictions and evaluates one restriction check after another if a check is returning a value of either "OK, PERMIT" or "REJECT".

The first check in smtpd_recipient_restriction is "permit_mynetworks". It checks, if the connecting client is in the same network as has been defined in mynetworks. In this case, the client is indeed within the network 192.168.1.0/24, so the check returns "OK" and the mail is accepted. No other checks need to be evaluated.

Next, a client with the ip address 80.242.23.16 connects from the internet to your server and wants to send an email to unknown@xxxxxxxxxxxxxxxxxxxxx

Postfix first checks again "permit_mynetworks". This time the check comes up empty because the client ip is NOT in mynetworks.

I thought it would have rejected after the mynetworks check as it did not match. It doesn't matter if it meets anything else, mynetworks says the client must be in a certain IP range, finished

The check permit_mynetworks" returns "OK" if the client ip address is in mynetworks. If not, the check simply returns a "DUNNO" which means Postfix should continue and evaluate the next check. The test does NOT say "All clients must be in mynetworks, otherwise the mail is rejected". That would mean that you can't accept mail from clients that you do not know.

The correct interpretation of this check is: "If you are a member of my network I can trust you and accept any mail you want me to send to the world.
If you do not belong to my network, I can't trust you implicitly. Though you might ask "permit_sasl_authenticated" if your credentials are sufficient to trust you.

So Postfix tries the next check: permit_sasl_authenticated.
Well, the client did not authenticate, so this check also returns an empty result. The next check, "reject_unauth_destination" evaluates if the recipient address is in a domain that Postfix is responsible for, otherwise it returns "REJECT" as result.
In this case, the domain somewhere-else.org is not in

Re: [SLE] SMTP authentication

mydestination, so the check returns "REJECT" and the mail is rejected.

What kind of restriction checks are configured for a mailserver is completely up to you and your requirements.

I fully understand your example although I cannot see in the example why the "reject_unauth_destination" variable needed to be checked.

The check "reject_unauth_destination" is one of the most important checks when you configure Postfix. This check rejects all mails that Postfix can not deliver locally and would have to send out to the internet!

"unauth_destination" in this case are all recipient addresses that Postfix itself is not responsible for. All other recipient addresses are rejected. The log then says "Relay access denied".

In other words, this test separates the trusted clients that either belong to mynetworks or have authenticated and thus are allowed to relay mails through this server, or the untrusted clients that may only send mails that this server feels responsible for.

There is a bit of confusion creeping in here when you say that the SMTP is not responsible for. An SMTP server is responsible only for sending email. If my SMTP server is the only SMTP relay server between the host and destination, that "reject_unauth_destination" is a little cruel as then the message will be rejected. Would it be rejected to the SMTP server that sent it to me and that SMTP server would have to find, via DNS, an alternate route to the destination?

All tests after that check only apply to external (or internal) untrusted clients.

It is also the reason why that check should come immediately after the checks for the trusted clients in the order of restrictions.

Frequently you encounter badly configured servers that trust clients when they claim "I have your ip address" or "I belong to your domain". The spam zombies try to find these servers and often try to impersonate such trusted clients. That is the reason why you should only trust clients that have proven their identity in a way you can trust. The ip address is practically impossible to fake during the course of such a smtp communication. You can trust that the ip address of the client is actually the ip address the client is really using.

OK, I'll try and remember though Whew, the brain is spinning. I'm going to need a new brain when I actually start setting this Postfix server up :)

Thankfully I trust no-one, with very few exceptions.

--

Check the headers for your unsubscription address

Re: [SLE] SMTP authentication

Re: [SLE] SMTP authentication

For additional commands send e-mail to suse-linux-e-help@xxxxxxxx

Also check the archives at <http://lists.suse.com>

Please read the FAQs: suse-linux-e-faq@xxxxxxxx