Friday, July 29. 2011

550 Access Denied

The biggest problems with getting your Email to someone is getting through the receiving ends mail servers defences.

Sadly, long gone are the days of the early 90's where spam was really only something that was heard of in a supermarket, although it had been around for years, even on ARPANET, it was not of plague proportions like it reached in the mid-late 90's through to the problem it is today. Long gone also are the days where you can trust strangers to use your mail server, where it was common two decades ago for most mail servers to be open relays, but, as with anything that's available, it soon became abused, so to combat the problem of spammers abusing this privilege, MTA's like Sendmail soon released versions that no more by default permitted open relaying capabilities, like the 'ol saying... if you abuse it, you loose it!

Defence comes in many forms, most common is the well known method of DNSBL's (DNS based Real-time Block Lists), often also referred to as RBL's, PBL's, Blacklists, or even Blackhole Lists, these are DNS based lists of domain names and IP numbers of trouble makers, people who have given others grief in some form or another (spam, phishing, compromised, abuse, etc...), they become submitted to these lists by trusted persons, also through automated processes, including hidden addresses to trap spambots when they harvest websites looking for addresses to add to their spam-out lists.

Today there are more than 30 such public lists, each with their own listing criteria, however, there are only a handful of what are considered reputable lists that the vast majority of administrators use, not to mention many private lists (like the one we run), and in-house DNSBL's used amongst a group of ISP's, occasionally even sharing data between them. You can test a blacklist entry here

But DNSBL's are just one obstacle, before you get that far, you often go through several other checks like local access lists, hostname and DNS compliance testing, and so on, this is where greater than 90% of the rubbish is filtered out.

One of the best ways to help get your mail received is to ensure your DNS is properly configured. In your domains DNS zone file you should have an A record entry, and in your in-addr.arpa or ip6.arpa zone files for your IP allocations, a matching (rDNS) PTR record entry - for every machine, and in particular, for every server. RFC 1912, Section 2.1, para 1 and 2 clearly states "Every Internet-reachable host should have a name" and "Make sure your PTR and A records match" and "For every IP address, there should be a matching PTR record".

With IPv6 starting to get off the ground, it is going to be far more of an issue given that most people will end up with so many addresses. So it will be more important than ever to set correct DNS for your IPv6 and IPv4 addresses for any server that should be sending mail, be it a mail server, or a web server that might for example, run a forum or blog, and needs to send mail for confirmations, updates, password resets etc.

Another well used trick involves rejecting dynamic users, these are connections that have good forward and reverse DNS, but include things like a dotted or dashed version of their IP number, ppp, dial, xdsl, pool, cpe-, ip- , dyn, cable, and res, to name only some, in their hostname, this normally indicates a residential host, with likely no dedicated mail server or a genuine need to be directly sending mail. So in selecting a service, ensure your rDNS can be changed to a suitable name, if not, find a provider that does offer it, even if only by request to support. The recipients ISP's wont tolerate constant whitelist me please requests because you or your network provider can't get their act together, remember it's you/your host that are non compliant. So, in your naming conventions, don't use the IP number or parts of it in your DNS/rDNS entry for servers, but it is of course fine to do so for general PC's, laptops and mobiles that should have no reason to directly send Email to anyone, and make sure that your server hostname settings match, if they present a HELO/EHLO with rubbish, you can be sure you'll get blocked for that as well. Make life easy, give your servers a server-like name, eg: falcon.your.domain, and configure it and DNS for that name only, if you run a dedicated mail server, call it mail.your.domain, or some othername that resembles a servername, and ensure your DNS zone has that name listed in the MX record field.

If running a mail server, and you block a host because of policy, ie: access lists, milters, RBL's, etc, you must do this at the initial smtp connection, where your server can reject the message with a 55x error code so the sender knows they have been blocked, and why, the only time you are not required to do this, is if using an anti-spam set like spamassassin

and you silently drop high scored spam messages, low/medium scored should still be delivered, most anti spam mail server software has the ability to send a warning message and attach the original spammy message to it, I personally use a cutoff of around 15, that's high scored and silently discarded anything less and amavisd will warn the recipient and include the spam as an attachment, please do not ever use software that bounces spam or notifies the sender of the spam message, if you have accepted the message, you must either deliver it, or discard it, never bounce it (chances are the addresses will be forged anyway).

Speaking of forgeries, I also suggest you use SPF, you should not only publish your SPF record for your domain (and any domains you host), but enforce SPF checks on your mail servers too. There would be so much less phishing attacks, especially for financially related incidents, if only those organisations would use SPF.

When implementing SPF, I recommend testing thoroughly first by publishing a softfail condition, and once you're sure it works right, change your DNS SPF resource record (RR) to a hardfail, that's from ~all to -all. The modern way of using SPF in DNS is with the Type SPF, but, because there are a lot of lazy admins out there who have not updated their daemons or scripts, you should also publish your SPF data in the deprecated TXT method as well for the time being. In its simplest form, all you need is the IP address numbers of the servers you want to allow to send mail on your domains behalf, for instance this domain, ausics.net has the following SPF and TXT records:

v=spf1 ip4:27.33.160.23 ip4:62.113.243.167 ip6:2a00:f48:1029::1:a05d:e257 ip6:2001:470:67:524::0/64 -all"

This means only those addresses can send mail for any email address at ausics.net (based on envelope sender) (I do not recommend using name types or mx's, use IP address or ranges only, SPF is of course very powerful and can be extended to include other zones, and even use regex's, if you're new to this, stick to the basics only, don't over complicate things.) You must always remember, like everything DNS, you need to keep things up to date at all times, so if you change mail server IP's change your SPF too!

Another advantage of publishing SPF records is if sending to Live.com (Hotmail), or Gmail, under their scoring systems, you get a higher rating, meaning greater probability of inbox delivery.

Some people are anti-SPF claiming it messes up your mailing list posts, I've published SPF records for a great many years now, and have never seen any collateral damage like this, most modern list servers re-write the envelope sender address, so although a mailing list post might reflect From deletethis@ausics.net, the envelope sender which SPF uses, will be different, it will be from the domain of the sending list server, eg: cisco-nsp-bounces@puck.nether.net, so SPF receivers, would be testing if puck.nether.net is allowed to send for cisco-nsp-bounces@puck.nether.net, and not testing for deletethis@ausics.net. You can learn more about SPF at openspf.net.

The most popular used anti spam program, SpamAssassin, is used on a very large number of servers and proprietary hardware devices, it looks for keywords and styles and is based on a score system, so don't send Emails that are obviously spammy and it wont positive score you, SpamAssassin, like everything else, is not foolproof, nothing is, and anyone trying to convince you their solution is, is full of crap, but SpamAssassin works, and works really well. Some sites rely on outsourced services (or rules), meaning they pay a ridiculous amount of money for some re-badged server from one of the mobs selling these hardware devices and relying on their rules, their decisions, and don't custom configure the devices at all. I've seen and heard countless admins cursing those things, but, you got to expect that if you're prepared to let someone else decide what your network gets. Personally, I don't believe in those things, if I'm providing a mail service, that's for me and my colleagues to decide.

Note: SpamAssassin has an internal whitelist when it comes to URIBL's (which check links inside emails), some domains on that list should never be there, like mail.ru, and a few more, so I highly recommend adding into your local.cf the keyword option: clear_uridnsbl_skip_domain

If you run a mailing list, ensure it is configured to double opt in, and don't blindly add any addresses to it under any circumstances. Configure the list to suspend delivery of mail after a very small number of bounces - Mailman and Ecartis are able to do this, and, although its been many years since I looked at it, I think ezmlm also. Make sure only subscribed members can post to your lists, moderate new members for the first few messages if at all possible, spammers love to abuse mailing lists too. Having someone on a list that doesn't want to be, is the worst thing you can do, so make sure your list server works properly for those wishing to unsubscribe, and make sure it works by email as well as any web interface, nothing worse than having to use a web login to remove ones self from a mailing list. Failing to adhere to most of these things is another great way to be placed on a blocklist.

IP numbers are finite, yes, they get re-used, and it is possible the ranges allocated to you were previously used by low

life scum who spammed and the range was listed in one or more blacklists, you will have problems convincing blacklist maintainers removing that listing, ensure all PC's with access to your LAN are virus scanned and kept patched, this is especially so for Windows users. Research your service provider well, and if you're on ISDN/xDSL/Cable etc, perhaps explain to your ISP your dilemma and ask them to change your IP range, hopefully you do this when you first get your connection up and running before you migrate and go live on your new connection.

There are some whitelists around for SpamAssassin and hardware devices using nice-lists and reputation, there are some money grabbing bastards who operate some block/reputation lists, that when you are blocked via their lists, the reject message is telling you to go to some web site and pay to be whitelisted/get a good reputation - WTF? Seriously people, save your money - Trust can only be earned, not bought! I also work under the assumption of my network, my rules.

With relation to grey-listings, don't bother, many spam bots are cluey enough to retry these days, all it serves today is to delay legitimate Email, something that could cost you or your employer in many ways. I'm also not a real fan of DKIM, since it can, and does break with mailing lists (often you'll see it with gmail users), and when you have many domains on one server it gets trickier.

One thing I need to make clear to you if you're new to setting up your own mail servers, do not ever allow it to accept messages for non existent users or blindly relay for others, backscatter is the fastest way for your mail server to get blacklisted. Ensure you only relay for your local IP ranges, better still, use the message submission port (SMTP Auth) (port 587) and only accept inbound mail on smtp (port 25) that's destined to your own network from external addresses, and block outgoing port 25 on your router (with the exception of your mail servers IP of course) if at all possible.

In conclusion, if you follow the above rules, the chances of your mail getting through to the recipient, will be pretty good, you'll have less rubbish yourself to deal with, and overall, also be a better netizen

```
Posted by NoelB at 19:47
```

Nice article.
Anonymous on Jul 31 2011, 08:51

Hi to all, the contents present at this web page are
truly remarkable for people experience, well, keep up
the good work fellows.
Anonymous on Apr 25 2012, 16:41

I wanted to thank you for this excellent read!! I absolutely loved every bit of it.
I have got you saved as a favorite to look at new things you
post?
Anonymous on May 20 2012, 05:59

Great post, most of it is common sense for dudes that care, but good point about SPF that many admins don't think about, know, or understand, not that it's rocket science, but sad those who really need it, like banks, don't all use it.

BTW with IPv6, I was bitten by no reverse DNS recently, by google, they are rejecting IPv6 hosts now without a valid reverse DNS.
Anonymous on Jan 26 2014, 14:17

HA HA, I read your twitter comment, and this is post whirlpoolnetau says is spam? In the name of god, I would like to have what they are be smoking
Anonymous on Jan 26 2014, 22:40

I am aware it was nuked by moderator who calls itself "Thor", this jackass has long had it in for me, dating back to 2005/6, likely because of the ISP I worked for at the time, for a while Thor ran around stalking me, censoring my posts at any given chance, it is one reason I refuse to bother with whingepool, and wont be bothering with the fucked up place again.

I have seen countless other offsite referrals in identical cases, but it seems my blog post helping folks be better admins, is nothing more than "spam" , perhaps I should just fuck it all off then, given I have a reputation for not being some nice to spammers

Anonymous on Jan 27 2014, 22:21