Sending/receiving email

Sunday, October 29, 2017 5:09 PM

Basics

CAN-SPAM act

https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

Email types

Commercial content – which advertises or promotes a commercial product or service, including content on a website operated for a commercial purpose;
Transactional or relationship content – which facilitates an already agreed-upon transaction or updates a customer about an ongoing transaction; and

If you have transactional emails only, then you don't need to worry about the CAN-SPAM act.

MX records

MX records in DNS are for *receiving* email, not for sending them.

Apparently an MX record isn't absolutely necessary (since it seemed to work for me), but it's not a bad idea to have one.

You can check to see what your MX records are set to using this page.

DKIM / SPF records

For sending emails, DKIM and SPF are used to verify that the sender is actually authorized to send for a particular domain.

An SPF record basically says "if you receive an email from bot.land, the sender's IP address needs to match whatever address was listed in the "include:" record below (amazonses.com)".

To set up DKIM:

- Go to SES in the AWS console
- Click your domain
- Click "View details"
- DKIM --> "Generate DKIM Settings"
- If you're using Route 53, you can click a button below that one that will automatically create the records in DNS.
  - You'll see them as CNAME records in Route 53.

To set up SPF records (reference):

- Just add this as a TXT record on your domain
  - "v=spf1 include:amazonses.com -all"
  - (I copied the quotation marks and everything)
  - Also note: Leaf says that if you want to update this to be able to send from other domains that you should edit the existing one rather than replace it with a new one ("you can add as many "include:" for the domains you want to include).

You can validate SPF records using something like mxtoolbox.

Note: once you've set up SPF, then you won't be able to send email from cPanel any longer.

Forwarding email

As of 10/29/2017, it doesn't look like Amazon handles email forwards automatically, so I did these steps:

- Set up the email address on my shared host (through cPanel)
    - Add a noreply@bot.land account
    - Go to "Forwarders" in cPanel and "add forwarder"
    - Forward email to "<personal address>+botlandnoreply@gmail.com", that way I can filter them there.
    - Test that I set it up correctly by emailing noreply@bot.land from my personal address. Note: this did seem to take way longer than it should have just for the email to arrive in my webmail through cPanel, and I don't think it ever forwarded the first email (but the second one worked).
- In AWS Route 53, I added an MX record
    - Name: blank (so that it's just bot.land)
    - Value: "10 bot.land."

Handling bounces properly

If you get a bounce, you need a blacklist set up to make sure that you don't contact that email address again. There are different kinds of bounces: hard bounces (message will never be able to be delivered), soft bounces (temporarily can't deliver, maybe you're sending too fast), spam complaints. Leaf doesn't recommend trying to write this stuff from scratch (although maybe it's not terrible; check this page). Bounces can be caused when an email address doesn't exist or if you try sending too many to the same mail server; it's just a broad term to mean that the mail server rejected your email address.

Leaf has never used something like this, but he's heard good things about it: sendy (paid).

Using an external service

If I'm going to use something like Zoho then I would need to point my MX records at Zoho. They should teach you how to set that up. BTW: Zoho has a free plan if I need to use it (scroll down on the pricing page).

Leaf's nightmare story

Leaf had a catch-all email so that "madeupaddress@hisdomain.com" would still get delivered to his address. He also had an SPF record that was a little more permissive; he used "+all" instead of "-all" so that emails could still be delivered even if they didn't match the SPF record, so maybe that painted a target on his back. It led to a backscatter attack that caused him to disable the catch-all email address.

He also linked this just for fun: https://en.wikipedia.org/wiki/Joe_job

Troubleshooting

If I have deliverability issues, I may need DKIM and SPF records. You can check everything using http://mxtoolbox.com/

Note: that site can check basically anything, but you first need to do a search for the dropdown to be enabled.