DynablockIssues

I'm an ISP, and mails from our dialups are hitting RCVD_IN_DYNABLOCK.

RCVD_IN_DYNABLOCK refers to the Dynablock list, which lists IP addresses that should not be sending mail directly to another server, without passing through a "smarthost" outgoing relay. SpamAssassin gives this a small positive score.

If you're running SpamAssassin as an ISP, your dialup pools may be listed in Dynablock. In this case, your host is the "smarthost" – but it's also where SpamAssassin is running. So even if your customers are doing the "right thing", relaying via your host, they'll get hit – because as far as SpamAssassin can tell, a mail from a Dynablock-listed IP address is being sent to the scanner, without passing through a "smarthost" on the way. It doesn't know that they're *your* dialup pools.

The way around this is to get SpamAssassin to "trust" the dialup IP pool's addresses, so that they're exempted from the Dynablock test. e.g., if your dialup pools use the IP range 10.222.111.0-255, add this line:

trusted_networks 10.222.111/24

in /etc/mail/spamassassin/local.cf .

To specify multiple trusted networks, add multiple "trusted_networks" lines.

Mails from our users submitted to our MSA or "smarthost" are hitting RCVD_IN_DYNABLOCK.

In SpamAssassin 3.2.0 or later you can use the **msa_networks** option to list your MSAs. The syntax is identical to the trusted_networks option. Any mail submitted to a machine listed in msa_networks will be trusted (provided that all relays above/after the MSA relay are also trusted).

In versions of SpamAssassin older than 3.2.0 you will either need to use one of the other options listed on this page or, if using 3.1, apply a patch to add msa_networks to your install of SpamAssassin.

I'm an ISP, and mails from our customers, using POP-before-SMTP for authentication, are hitting RCVD_IN_DYNABLOCK.

Just like your "smarthost" has to be told who your POP-before-SMTP users are, SpamAssassin (if running on that same "smarthost" machine) has to be to too. There's a custom plugin for just that:

http://wiki.apache.org/spamassassin/POPAuthPlugin

I'm an ISP, and mails from our customers, using authenticated connections from another ISP, are hitting RCVD_IN_DYNABLOCK.

This problem (involving SMTP Auth connections from dynamic addresses) is similar to other "false positives" such as SPF_FAIL RCVD_IN_SORBS_DUL and various other RBL problems.

Note: The problem described was fixed in version 3.0.2. However, some MTAs such Postfix don't support RFC 3848 and will therefore still exhibit the described problem since SpamAssassin won't be able to automatically trust authenticated users if the MTA doesn't leave a supported authentication token in the relay's Received header.

Update (2006-07-14): Postfix 2.3 includes support for adding its own style of authentication info to its received headers by setting *smtpd_sasl_authenticated_header = yes*, which is disabled by default, in your Postfix config. **SpamAssassin 3.1.4** and later includes support for this Postfix auth info.

this patch]: This will not fix TLS-authenticated sessions. See [http://dev.riseup.net/privacy/postfix/ which munges the Received headers. DarylC.W.O'Shea: This should work to avoid the Dynablock problem in this specific situation but isn't recommended since it destroys the audit trail provided by the Received headers.

Update (2008-06-20): Postfix 2.5+ includes native support RFC 3848 setting *smtpd_sasl_authenticated_header* is not needed but optional.

This is another Dynablock-related issue. If:

- 1. your customer opens an authenticated SMTP connection to your "smarthost" from a Dynablock-listed dialup pool,
- 2. and you're running SpamAssassin on that "smarthost" machine,
- 3. and the message is to be delivered to a local recipient on that machine,

then their message will still be hit by RCVD_IN_DYNABLOCK, because it's an SMTP connection from a DYNABLOCK-listed host, directly to your mail server. SpamAssassin doesn't know that it was an *authenticated* connection.

As a **workaround only** for MTAs that either don't supply any auth tokens or don't supply auth tokens supported by SpamAssassin (if they're not already supported the devs don't know about them – let us know), you could add a custom local rule that matches the Received header format that your mailserver adds for successfully-authenticated connections. For example, if your mail server adds this line for an authenticated client:

```
  Received: from 192.168.2.125 (CPE0004e24b9419-CM000a7365d82c.cpe.net.cable.rogers.com
      [63.139.187.25]) (authenticated (0 bits)) by services04.student.cs.uwaterloo.ca
      (8.11.7/8.11.7) with ESMTP id hA41X1B23955 for <recipient@example.org>; Mon,
      3 Nov 2003 20:33:03 -0500 (EST)
```

Then you could define a rule like this:

```
  header LOCAL_AUTH_RCVD    Received =~ /\(authenticated \(\d+ bits\)\) by services04\.student\.cs\.uwaterloo\.
ca /
```

Note the use of your server's hostname, so that spammers cannot fake the data without knowledge of your server's header format and so on.

I'm not an ISP, but I do have a mail server on an RFC1918 address (10.*.*.*, 172.16.*.* or 192.168.*.*) and incoming mails are hitting RCVD_IN_DYNABLOCK.

SA 2.6x has a trust path bug where it will wind up over trusting if one of these IPs is in the path. It winds up trusting the ISP relay server and decides it's part of your network, and thus thinks the dialup user dropped off directly to your MX.

You can fix it by forcing SA to only trust one host as shown below (replace "192.168.1.1" with your mail server address):

```
  trusted_networks        192.168.1.1/32
```