NetTestFirewallIssues

DCC

The DCC maintainers have been in touch, noting that several sites seem to have set up SpamAssassin and DCC, but have not modified their firewalls to allow DCC traffic through! This is wasting their bandwidth, and we'd appreciate if users could check their configuration.

To check it, run 'cdcc info':

cdcc info

The output should contain lines like this:

dcc1.dcc-servers.net,- RTT+0 ms anon
dcc2.dcc-servers.net,- RTT+0 ms anon
...

There should be *at least one*, preferably more than half a dozen, of the public DCC servers listed. If this is not the case, a likely cause is an interfering firewall (see below).

Also note that DCC requires that you open your firewall for DCC reply packets on UDP port 6277. Here's sample firewall rules required:

allow udp local gt 1023 to remote 6277

allow udp remote 6277 to local gt 1023

IPTables Setup:

Assuming you allow all outbound packets out of your machine, you only need to add an INPUT rule to your /etc/sysconfig/iptables file. Add the following line in your INPUT chain, above any REJECT rules:

-A <chain-name> -p udp -m udp --sport 6277 -j ACCEPT

Also, if you're running a large site, processing upwards of tens of thousands of messages a day, the DCC maintainers have requested that you consider setting up your own DCC server as described in dccd(8), and arrange to peer with the rest of the public servers.

Razor

The Razor2 system requires outbound access to servers on tcp port 2703 in general (the servers are, at the moment, on the class C 66.151.150.0/24, but allowing only access to those machines would be too restrictive).

It also requires outbound access to those servers on tcp port 7.

It does not require that the razor servers connect to any open ports on your machine. All the connections are typical TCP client connections (ie: from a local port >1023) to port 7 or port 2703 on the razor server.

It does not use UDP or ICMP, with the exception of performing DNS lookups for server discovery.

If you are still using razor1, upgrade, as Spamassassin does not support this now. Razor1 made outbound connections to servers on tcp port 2702.

Pyzor

Pyzor uses both udp and tcp port 24441. It looks as though the client communicates with the server via udp but the server answers back with a tcp connection.