Upload Problem Post-Mortem

Posted At : November 16, 2009 2:07 PM | Posted By : Mark Kruger
Related Categories: Hosting and Networking

We had a ticklish issue arise with a customers recently. We host an application for them that allows them to upload files. As they began to use the application more heavily they noticed that file uploads above a certain size were failing. The size was fairly modest. Uploads sized between 1 and 4 megs were simply timing out. We eventually came up with a solution, but not before some head scratching. Here is the play-by-play.

To be more specific, the problem was that larger files posted from *inside* the customer network would fail. We tested uploads from various computers not associated with the customer network and all of them were successful. We took a stab at changing various server settings. First we looked at CF settings. We adjusted time out values. We adjusted the "post" and "Throttle" settings. When none of these bore fruit we moved to the web server settings (ISS) and started adjusting CGI timeouts and the like - all to no avail. Why change the server settings first? Because even if there is a low probability of success it causes relatively slight impact to make such changes.

This led us to our firewall. We surmised that some setting on our firewall was terminating the connection - perhaps due to something odd in the packet header or whatever. The firewall in this case was a dedicated FreeBSD firewall (Mon0wall - pfsense). So we adjusted scrub settings and tried the different connection state management settings (including ones for high latency). Again, none of these were successful.

The Plot Thickens

It so happens we own 2 public subnets and we have more than one kind of firewall running. So as a test we set up a sample upload script on a server coming through one of the other firewalls (a Cisco PIX) and one of the other subnets. This test was *successful*. Ahah! ...we thought. It must be something about PFSense that doesn't like packets from this one network. We took a spare PIX off the shelf and swapped out the firewall fully expecting that this would solve our problem. Alas, it did not. It seems that the customer network simply doesn't like *one of our subnets* regardless of which firewall product we were using. We were down to routing - and that meant packet sniffing and analyzing (which also means keep sharp objects away from the Muse).

Epiphany

Before going down that arduous road a slight tickle developed in the back of my brain. In the old days when everyone and their brother was installing proxy servers in enterprise networks we used to have problems with dynamic content. One of the things we used to do is force traffic to use SSL connections. Proxy servers tend to ignore SSL traffic. Now we had been assured that no such device was in use on the customer network, but perhaps the customer firewall or traffic shaping router was forcibly closing these connections. SSL has the advantage of obscuring the actual contents of packets (barring some sort of man in the middle attack) so something tasked with introspecting them can't really see what's going on. Maybe switching to SSL would do the trick.

We quickly set up an SSL test through that same subnet and sure enough, the file uploaded successfully. We added a cert to our customers site - problem solved.

Lesson Learned

If you suspect some sort of filtering technology of interfering with legitimate traffic, try SSL first. It could save you from swapping out firewalls and reconfiguring servers. I'm sure it's not a panacea - but it *is* an easy 45 minute fix as apposed to staying up till 3:00 am to change hardware.