

8Signs PC Firewall Problem

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-04/0557.html>

From: mrsimpleton (mrsimpleton_at_angelfire.com)

Date: 04/14/04

Date: 13 Apr 2004 20:38:07 -0700

First let me say that 8Signs PC Firewall is AWESOME!!!
Just one little thing about it bugs the heck out of me.

First a little understanding of my network setup...

PC2

PC3 <---> Switch <---> PC1 <---> Cable Modem

PC4

All PCs are Pentium III 500s or faster with at least 128 Megs Of
Memory or more.

Chipsets are either Intel or Via.

Network Adapters: PC1 WAN Linksys LNE100TX v4, LAN Compaq Netelligent
10/100TX

PC2 LAN Realtek RTL8139A

PC3 LAN Linksys LNE100TX v2

PC4 LAN Realtek RTL8139A

WAN Realtek RTL8139A (NOT CONNECTED)

All Network Adapters are running 100 Mbs FullDuplex

My hardware is pretty generic. I don't have any dell's or compaq's or
E-Machines, or any weird computers.

All PCs are running Windows 2000 Professional SP4.

PC1 is using Internet Connection Sharing to share the internet
connection.

PC1 is also running 8Signs PC Firewall V2.2a

PC1 also has a Proxy Server Running, Proxy+ 3.0.

All downloads are done using Internet Explorer 6.0 SP1 with the latest
critical update, Q832894.

The Problem...

If I try to download anything from PC2, PC3 or PC4, via Http or Ftp,
it starts to do it for a second but then it just slows down to a crawl
and hangs and does a little more and hangs and then some more and
hangs and flip flops between 20KBytes/s and 80KB/s. That's about as
clear as I can put the problem.

Variations...

comp.security.firewalls: 8Signs PC Firewall Problem

If I download the something from PC1, Blazingly Stupidly Fast as always, 350KB/s.

If I turn 8 Signs PC Firewall Off, Blazingly Stupidly Fast.

If I set PC2, 3 or 4 to go through the Proxy Server, Blazingly Stupidly Fast.

If I have the firewall ON but tell it to allow all traffic, it's a setting and not me making a rule to allow all traffic, Blazing Stupidly Fast.

If I have the firewall ON but make a rule to ALLOW ALL TRAFFIC, Slows down to a crawl.

So when ever the firewall is running and is set to filter the packets, I have the problem.

I was running Conesal PC Firewall before on PC1, never had a problem.

Things I have tried...

As listed above PC4 has 2 Realtek Network Cards in it. So I put 8Signs PC Firewall on that computer and set that computer to share the internet connection. SAME PROBLEM. So it's not my hardware. 2 different machines with differnet network card manufactures have the same problem.

Now I have played with my HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters settings. Such as TCP Window Size, MTU, MTU Discovery, MTU Black Hole Detect and many others. I got a whole list of them from a german website. I've been having fun and I don't speak german but had google translate the website for me.

<http://translate.google.com/translate?u=http%3A%2F%2Fwww.synapse.de%2Fregcheck%2Fger%2Fregistry%2Fwin->

And I've been to the microsoft website and many many others.

My point being, no matter how I set things, I can't improve the performance of the clients when downloading off of the internet. I can only retard their performance and make them worse. I get maximum performance if I just return all my registry settings to there normal defaul settings, which I have done and just leave them alone.

I have also ran Performance from Administrative Tools in Windows 2000 on PC1 and set it to show me all errors in either IP, TCP or UDP. I tried to download something again from a website. Well I still had the same problem, BUT, no errors were popuping up, everything was still at zero. (Alot of help that was.)

I should say (IMPORTANT) that I can go to the www.nasa.gov website and watch the nasa channel online no problem. I can also go to any website no problem. I can play shockwave games no problem AND I can download small 1 meg or less programs no problem.

CONCLUSIONS...

The problem seems to come into play when my network speed exceeds 200KB/s. It is almost as if, the computer isn't fast enough to filter the packets in realtime. I thought of that. I checked the Windows 2000 Task Manager which monitors CPU usage on PC1. No matter what I did, as long as I left PC1 alone and just surfed the net from PC2, 3 or 4, the CPU usage never went above 12%. I've got power to spare. It's not a computer speed problem.

There is a problem with transferring the packets at 200KB/s or greater from the WAN Adapter, through the packet filter, and out the LAN adapter. But it's not because the computer isn't fast enough or because there's a compatibility problem with the 2 network adapters since I ran 8Signs on PC4 and had the same problem.

I was wondering if it's a buffer problem, as in the buffer on the LAN adapter is being overrun and needs to be enlarged. I know a great deal about computers but when we get into things like the guts of the operating system I begin to deal with things that I have no idea what they are. So I don't even know if such a buffer even exists or where to find it. For all I know it goes from the WAN Buffer to the 8Signs Buffer to the LAN Buffer and it's the 8Signs buffer that needs to be enlarged.

I was also wondering if there's a way to put a waitstate into the flow of packets thru PC1. The computer is trying to flow the packets on thru as quickly as possible and maybe that's the problem, if things were a bit slower, maybe I wouldn't have the problem. I realize this would slow down my overall KB/s but since I average 350 KB/s, I think I can afford to lose a few. I have played with my MTUs and TCP Window Size to accomplish this but realized this is the wrong way to go about it.

So any ideas, anyone has, would be GREATLY appreciated. I am also open to the idea of using a DIFFERENT firewall, as long as I can make rules for 2 different network adapters, and can make rules by either IP address, Port Number or Protocol and I would prefer it, if it didn't do application filtering, I would be welcome to any alternative firewall suggestions anyone has.

I have tried Kerio, I like it a lot, I couldn't get it to allow anything through so I scrapped it and went to 8signs. Hey, if somebody would want to tell me how to get Kerio to work, that would be fine too.

Just point me in a direction, give me a clue, that's all I ask.

mrsimpleton

PS. Don't email me since Angelfire is going out of business and I haven't got a new email address yet. Thank You.