

Win XP SP2 and Cisco VPN Client

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-08/0064.html>

From: Jorge Zelaya (*mrjaz12_at_YAHOO.COM*)

Date: 08/13/04

Date: Fri, 13 Aug 2004 10:39:53 -0700
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

After installing Win XP SP2, the Cisco VPN Client no longer works unless you disable the Windows Firewall. After some trouble-shooting, the problem appears to be related to how Windows Firewall is handling the outbound Port Address Translation.

I'm running the Cisco Client with either TCP or UDP Encapsulation. Neither appears to work.

In this example, I am going to use Encapsulation on TCP port 80.

Here's a piece of the Windows Firewall log. I am attempting to make a connection to the VPN Concentrator on TCP port 80.

```
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tpack tcpwin icmptype  
icmptype info path
```

```
2004-08-13 09:52:05 OPEN UDP 192.168.1.100 ip.of.vpn.con 1304 62514 - - - - -
```

Notice that the protocol in the log appears as UDP.

However, the VPN Concentrator log show that the connection attempt is coming in on the correct port. TCP 80

A TCPDUMP packet capture reveals what's going on.

```
192.168.1.100.1304 > ip.of.vpn.con.80: S 16790492:16790492(0) win 65535
```

```
ip.of.vpn.con.80 > 192.168.1.100.1304: S 1649895458:1649895458(0) ack 16790493 win 65535
```

```
192.168.1.100.1304 > ip.of.vpn.con.80: S 16790492:16790492(0) win 65535
```

```
192.168.1.100.1304 > ip.of.vpn.con.80: R 16790493:16790493(0) win 65535
```

The TCP session is never established. The VPN client eventually times out and sends a Reset.

The Windows Firewall Log gives me the biggest clue as to why the session is never established. Could it be because the PAT is not created properly?

The protocol shows up as UDP instead of TCP. That could be the reason why that Syn-Ack packet the VPN

NT-Bugtraq: Win XP SP2 and Cisco VPN Client

Concentrator is sending is being ignored.

What software is at fault here? Is it the VPN Client or the Windows Firewall? Since it's Windows Firewall's job to create the PAT, it would be fair to point the finger at it.

There is one more thing that the Windows Firewall log points out. The destination port is 62514. What the???

This is what the Windows Firewall Log looks like when I make a successful Telnet (TCP Port 23) connection.

```
2004-08-13 10:25:08 OPEN TCP 192.168.1.100 192.168.2.200 1242 23 - - - - -
```

That looks normal to me. Any thoughts?

JAZ

Sr. Network Engineer

Do you Yahoo!?
Yahoo! Mail Address AutoComplete – You start. We finish.

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.
