

microsoft.public.security: Re: What is the trick to get Windows XP firewall to stay on (after a reboot)?

Re: What is the trick to get Windows XP firewall to stay on (after a reboot)?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-01/0512.html>

From: Alun Jones [MSFT] (alunj_at_online.microsoft.com)

Date: 01/12/05

Date: Wed, 12 Jan 2005 09:55:56 -0800

"Triffid" <triffid@nebula.net> wrote in message
news:hg2Fd.33132\$TN6.1040827@news20.bellglobal.com...

>

>

> *Alun Jones [MSFT] wrote:*

>> *The only way to tell for sure whether the firewall pays any attention to*

>> *the EPRT or PORT commands are to:*

>> *1. Check at the _server_ side to see what the command looked like when it*

>> *reached the server (that way, you can tell if NAPT is happening), to*

>> *compare with the command you sent.*

>

> *While I did not explicitly state that the EPRT and PORT commands reached*

> *the server exactly as typed, that is indeed what I observed.*

You have to state these things – while we've probably got a division working hard on one right now, I haven't yet been issued with a mind reading accessory. All I have to go on are what you tell me, and what I can reproduce myself.

> *In the case of a firewall external to the client, the firewall would*

> *listen on the port specified in the outgoing EPRT or PORT command – on*

> *behalf of the client – with no knowledge of the client's ability to accept*

> *a connection on the port he specified.*

>

> *Windows Firewall did not start a listen according to netstat –a and Port*

> *Explorer.*

You're thinking of a proxy, not a firewall. The two are not synonymous, even though they often serve similar functions.

A proxy accepts incoming connections, and acting on behalf of that incoming connection, creates a new connection onward. [Look up the less technological meanings of "proxy" in a dictionary, to see why it got that name.]

Re: What is the trick to get Windows XP firewall to stay on (after a reboot)?

microsoft.public.security: Re: What is the trick to get Windows XP firewall to stay on (after a reboot)?

A firewall, on the other hand, either stops or allows network traffic, based on its source and/or destination (and sometimes on its contents).

A NAT router (which may be a part of a firewall, or a separate entity) inspects and alters network traffic, forwarding most of them unchanged.

So, while a proxy would result in a new listening socket, a firewall does not. The firewall says "aha – I've been told to allow traffic through on port 12345", and it starts allowing traffic through on that port. It's a completely different layer of the network transport, and cannot be inspected or inferred through netstat –a.

>> *The firewall has no knowledge of the difference between a PORT command
>> that you specify by using literal and one that is specified by a client's
>> action (if it did, how would third-party FTP clients be supported?)
>
> So one would expect see a listen started in either case, but it is not
> according to the utilities I used.*

No, one would not expect to see a listen started in the case that you sent a "literal PORT" command, but you would see a listen started prior to an FTP client sending a PORT command that it (rather than you) has chosen to send. That would be the listening socket created by the FTP client, and whose address and port it uses in the PORT command.

> *The observed behavior suggests Windows Firewall is oblivious to the PORT
> command, rather it appears to be triggered by the client process' attempt
> to listen – perhaps contrary to your implied assertion that Windows
> Firewall resides "in front of" the TCP stack.*

The Windows Firewall analyses IP traffic for patterns that have been allowed or refused, and passes that IP traffic on to the next layer or does not pass, depending on whether the traffic is allowed or not.

Alun.

~~~~~

--

Software Design Engineer, Internet Information Server (FTP)  
This posting is provided "AS IS" with no warranties, and confers no rights.