

Re: IPSEC

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-01/0602.html>

From: Kerodo (loopback_at_localhost.com)

Date: 01/29/05

Date: Fri, 28 Jan 2005 16:13:30 -0800

In article <ep37GzWBFHA.4008@tk2msftngp13.phx.gbl>, bogus@microsoft.com says...

> *More specific filter actions will win....*

>

> *Best practice is to use the Windows Firewall to provide that statefulness
> and use IPsec filters/IPsec transport to augment that and optionally provide
> per-packet authentication/encryption.*

>

>

> *"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message
> news:O5\$nuuQBFHA.3472@TK2MSFTNGP14.phx.gbl...*

>> *Ok. Well that is fine. Ipsec is a good way to learn how to setup basic
>> firewall rules. It would not block traffic into your network with a source
>> port of 80 TCP because you need to allow the return traffic back into your
>> computer [via a mirrored filter entry] when you initiate an internet
>> connection to a website. Since ipsec is not stateful it will allow any
>> traffic in with a source port of 80 TCP. The block all IP rule would not
>> stop that traffic because an ipsec specific rule will override and ipsec
>> general rule such as block all IP [don't ask me the specific way in which
>> that is calculated as I don't know]. Anyhow your computer is in no grave
>> danger but ipsec filters act like old packet filter firewalls before
>> stateful packet inspection came along. --- Steve*

>>

>>

>> *"Kerodo" <loopback@localhost.com> wrote in message
>> news:MPG.1c6334d1a52d583c989684@news.west.cox.net...*

>>> *In article <aeOdnZ5mBY-6DmTcRVn-sw@comcast.com>, n9rou@n0-spam-for-me-
>>> comcast.net says...*

>>>> *There is no way to do general logging with ipsec in Windows 2000. W2003
>>>> does*

>>>> *offer some logging such as for dropped packets. You would need to use a
>>>> software firewall such as Sygate to have some logging. Sygate is free
>>>> for*

>>>> *personal user, is a stateful firewall [unlike ipsec], and has
>>>> extensive*

>>>> *logging capabilities. Ipsec is not meant to be a first line internet
>>>> firewall. One weakness of a packet filtering firewall is that due to the
>>>> rules it is possible for a user to scan your internal network by*

> >>> *manipulating the source port of the scan. For instance you may be*
> >>> *allowing*
> >>> *all traffic from port 80 to your computer from the internet. I could use*
> >>> *a*
> >>> *program such as Supercan 4 to scan your network by using port 80 as the*
> >>> *source port for my scan. A stateful firewall would not allow that. I*
> >>> *think*
> >>> *ipsec is great for what it is good at, particularly on the lan, but I*
> >>> *would*
> >>> *not use it as a permanent primary internet firewall. --- Steve*
> >>
> >> *Thanks Steven, that's helpful. I'm very familiar with all the firewalls*
> >> *out there today. I'm playing with ipsec mostly out of curiosity, to see*
> >> *if I could find something to use as a packet filter that's ultra lite on*
> >> *resources, mostly just for fun. Sounds like I'd be better off with*
> >> *something like CHX-I, which also has stateful inspection.*
> >>
> >> *If my ipsec rules only allow outbound traffic on remote port 80 (source:*
> >> *my address, destination: any address), then wouldn't ipsec block any*
> >> *incoming traffic from remote 80 if I also have a block all incoming rule*
> >> *in place? Or does ipsec not care about the direction of the traffic?*
> >>
>

Thanks to both Steve's... I think I'm safer with stateful inspection.
At first I was misunderstanding things I think. I didn't realize that
allowing traffic out on 80 would also allow it back in if I want things
to work right. Thanks for the clarification and help.. :)

--
Kerodo