

## Re: IPSEC

**Source:**

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.general/2005-02/0311.html>

---

**From:** Kerodo ([loopback\\_at\\_localhost.com](mailto:loopback_at_localhost.com))

**Date:** 01/28/05

Date: Thu, 27 Jan 2005 17:27:19 -0800

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?

--

Kerodo