

## Re: VPN Question

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/11752.html>

---

**From:**

**Date:** 10/16/02

Date: Tue, 15 Oct 2002 19:58:53 -0700

"Bernie M" <while\_up\_late@night> wrote:

>  
> *"Mesomorj" <newsgroup@only.please> wrote in message  
> news:ZvRq9.1693\$hV3.75878@newsb.telia.net...*  
>>  
>> *"Bernie M" <while\_up\_late@night> wrote:*  
>>  
>> > *Surfing the net from the office is completely different to surfing from  
>> home*  
>> > *while also having a VPN back to the office. Traffic to/from the  
> Internet*  
>> > *doesn't use the VPN tunnel to go out through the office firewall. How  
>> does*  
>> > *the office firewall protect a PC that's browsing the Internet via their  
>> ISP?*  
>>  
>> *You are confusing me.. but let's say that the remote users browse the  
>> internet through the VPN (that means they are using the companys  
>> gateway/firewall for outgoing/incomming traffic to internet.. and that is  
> the*  
>> *same rules as the local users). Perhaps this will be slow.. but that would  
>> be the same security level as sitting local right?*  
>>  
>> *If the remote users didn't surf through the company line then the question  
>> is:*  
>> *What if the company use a Linksys router for surfing the net (localy)..and  
>> the remote use their own Linksys also (to surf/VPN.. what is the  
> difference*  
>> *of security then?..they \*all\* have access to the LAN..*  
>>  
>> --  
>> *Johan Tuneld*  
>>  
>> *Your Guide To Filetransfer Fix for ICQ 2001/2002*  
>> *And a complete guide of Gateway / Firewall configuration for all ICQ  
> clients*

>> <http://www.tuneld.com>

>>

>>

>

>To provide the same level of security as if you were surfing from the  
>company LAN, yes, you would need to have the browser traffic go through the  
>VPN to the Internet via the company firewall and return back the other way  
>... performance would suffer. Typically this is not the way it works.

>

>If the remote user had their own router/firewall then, yes, security is  
>increased but how responsible is the remote user going to be? Do they  
>really know how to configure and then check that the router/firewall is  
>secure? Plus we're only talking about packet filtering firewalls here. Not  
>quite the same league as a full statefull application inspection firewall.  
>I realise it's horses for courses but the security of the office is only as  
>strong as the weakest link. I know what would give me the most doubt.

>

>As a network administrator I would be reluctant to provide VPN access to a  
>remote client unless they agree to abide by certain security policies.  
>After all, who must accept overall responsibility? How can an end user be  
>held responsible when they don't know what VPN stands for let alone how it  
>works?

>

>Lockdown the PC while the VPN is active ... better safe than sorry.

>

>BernieM

That is a good point. I would increase my security if I used a stateful packet inspection device at the remote location also? Maybe I should reconsider using the Linksys and go with a different firewall product for the remote locations.

It looks like I am going to go with a SnapGear for the main office location.

Thanks for everybody's insight and help.

Jeff

--

Jeff Grossman ([jeff@stikman.com](mailto:jeff@stikman.com))

- 
- **Next message:** : ["Re: net send"](#)
  - **Previous message:** [John Elsbury: "Re: Do I need a firewall?"](#)
  - **In reply to:** [Bernie M: "Re: VPN Question"](#)
  - **Next in thread:** [Mesomorf: "Re: VPN Question"](#)
  - **Messages sorted by:** [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)