

# Re: VPN versus Terminal Server for remote workers

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-11/msg03638.html>

---

- *From:* "SuperGumby [SBS MVP]" <[not@xxxxxxxxxxxx](mailto:not@xxxxxxxxxxxx)>
  - *Date:* Mon, 26 Nov 2007 00:28:08 +1100
- 

The mechanism of 'split tunneling', ie. not using the VPN as default gateway, breaks your security whether implemented in software or hardware.

The logic behind it is that if split tunneling is implemented an infected PC establishes a connection to your network and the malware calls home without going through your firewall, 'Hey, the machine I'm on just linked to their corporate network, FUN TIME'. An attacker then connects to the malware, again without traversing and therefore being stopped by your firewall, and has full access to the corporate network through the remote system.

Split tunneling is BAD. All VPN clients should force the default gateway as the VPN server. Like everyone else I commonly break this rule.

It's funny really. The less high up in the corporate ladder the easier it is to explain to the user 'I'm sorry, but when you are connected to HQ we do not want you being able to go direct to the internet, it's a security thing.', and the more likely they will accept it. As you move up the ladder you are more likely to hit a user 'stuff you, my time is important!!! and if I don't split the tunnel my internet is slow.'. Of course, the higher up the ladder the more important that security principles are followed and the more damaging the consequences should they not be.

Get it in writing:

By default and intention 'split tunneling' of VPN connections is not allowed. I have been asked to allow users to use split tunnelling and therefore am not responsible if an attack comes through this vector. The purpose and consequences of these actions have been explained to Joe Bloggs on this day dd/mm/yyyy who below acknowledges this by signature.

"Larry Struckmeyer" <[lstruckmeyer@mis-wizards.com](mailto:lstruckmeyer@mis-wizards.com)> wrote in message [news:uAXZvZwLIHA.820@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uAXZvZwLIHA.820@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Claus:

That looks good. I've never understood why some of the others, un named here, do not allow one to use both the tunnel and the default gw at the "same" time. I will message "un named here", (whose initials are WG) to

Re: VPN versus Terminal Server for remote workers

see if they have revised this since I last visited this issue.

Strangely, with hw to hw, it is not a problem. But with sw to hw, using their mobile client, you get one or the other, in my admittedly limited experience.

Thanks for your help.

--

Larry

"Claus" <cjobs@xxxxxxxxxxxx> wrote in message  
[news:OAgJ7UwLIHA.2024@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OAgJ7UwLIHA.2024@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

3060 supports about 100 simultaneous connections. Only traffic to the subnet goes through the VPN. The rest goes out to your default GW.

--

Claus

"Larry Struckmeyer" <lstruckmeyer(at)mis-wizards(dot)com> wrote in message [news:e1hgiLwLIHA.4684@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:e1hgiLwLIHA.4684@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

What about the simultaneous use of the tunnel and the default gateway?

--

Larry

"Claus" <cjobs@xxxxxxxxxxxx> wrote in message  
[news:OyTSsDwLIHA.1212@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OyTSsDwLIHA.1212@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Larry,

We are using SonicWall 3060 at several locations. They have something called GlobalVPN client. It works very well. Once the software is installed, you can email the key file to the user to give them access. They import the file and select "enable". It is very easy for the user.

--

Claus

"Larry Struckmeyer"  
<lstruckmeyer(at)mis-wizards(dot)com>  
wrote in  
message  
[news:OkYaV\\$tLIHA.2432@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OkYaV$tLIHA.2432@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Re: VPN versus Terminal Server for remote workers

Hi Kevin:

Hoping you can help here.  
With the "solid" hardware  
that supports VPN  
that I have used, you have to  
have either a corresponding  
piece of  
that same flavor hw at both  
ends, or a mobile user  
software client  
from that mfg, say  
Watchguard or NetGear.

If all the remote users are in  
one, or even two places, the  
hardware  
to hardware route seems  
perfect. But if there are 15  
single users at  
15 distinct locations, this  
has proved impractical for  
our folks. The  
mobile software that I have  
used and tried is a pita to  
configure and  
maintain, and when it is  
active you can only use the  
tunnel, not your  
browser independently.

Please tell me there is a  
better way and that I have  
missed it.

--

Larry

"Kevin Weilbacher"

<kw@xxxxxxxxxxxxxxxxxxxx>

wrote in message

[news:E8F65A78-3F6D-453A-8AA3-D7F10D5B8ADF@xxxxxxxxxxxxxxxx](mailto:news:E8F65A78-3F6D-453A-8AA3-D7F10D5B8ADF@xxxxxxxxxxxxxxxx)

for 10-15  
users, if you  
wanted to  
go VPN,  
then I  
would say  
look for a

Re: VPN versus Terminal Server for remote workers

solid  
hardware  
box that  
supports  
VPN.

as far as  
using Term  
Server, the  
question  
really is:  
does the app  
that they  
will be  
using work  
in a term  
server  
environment?

the  
advantage  
of Term  
Server is  
that the  
remote  
users are  
connecting  
to a  
separate  
server, and  
not directly  
to the SBS  
server.

--

Kevin  
Weilbacher  
[SBS MVP]  
"The days  
pass by so  
quickly  
now, the  
nights are  
seldom  
long"  
\*

"Orlando  
Bob"  
<OrlandoBob@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in  
message

Re: VPN versus Terminal Server for remote workers

[news:3907BC27-BE28-40E7-8E54-91C1061AA639@xxxxxxxxxxx](mailto:news:3907BC27-BE28-40E7-8E54-91C1061AA639@xxxxxxxxxxx)

What  
are  
the  
pros  
and  
cons  
of  
using  
VPN  
versus  
Terminal  
Server  
to  
support  
10-15  
remote  
workers?  
The  
primary  
application  
is  
a  
.NET  
Windows  
Forms  
application  
that  
seems  
to  
run  
fairly  
well  
over  
a  
VPN  
connection.  
I  
am  
inclined  
to  
use  
VPN  
unless  
there  
are  
compelling  
reasons  
to  
set

Re: VPN versus Terminal Server for remote workers

up  
a  
Terminal  
Server.