

Re: VPN versus Terminal Server for remote workers

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-11/msg03681.html>

- *From:* "SuperGumby [SBS MVP]" <not@xxxxxxxxxxx>
 - *Date:* Mon, 26 Nov 2007 11:46:44 +1100
-

I think my confusion was in 'mobile software client'. In AU what you guys call a 'cell phone' we call a 'mobile', with possibly added confusion due to 'HUH? of course both (hard and soft) can do this.(most times, or possibly optional from the admin)'. I wasn't sure if we were talking about Windows VPN client, Windows Mobile VPN client, or a 3rd party VPN client.

HEY!!! If you guys call it a 'cell' why isn't it Windows Cell 6?

"Larry Struckmeyer" <[lstruckmeyer\(at\)mis-wizards\(dot\)com](mailto:lstruckmeyer(at)mis-wizards(dot)com)> wrote in message news:uTZBTZ7LIHA.4272@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi Super:

Well, I have been trying to say that in my, admittedly limited experience, the mobile software client that I have used blocks any access to the internet. It is tunnel to the appliance or nothing. If you want access to the inet, you have to break the connection to the appliance VPN, and disable the mobile client.

The same mfg's appliance to appliance VPN is both at the same time. There may be a way to configure the appliance to be VPN only, and the software to be/do both, but I admit that I have not looked very hard. This is the first time I have had a reason to question it.

Sort of like taking for granted that the bus will go from stop A to stop B to stop C, without considering that it might be quicker and easier to walk or bicycle from A to C. Very crude, but you get the drift. When one is presented with a fig, we tend to see it as a fig. But really, unless tested, how do we know it is a fig?

—

Larry

"SuperGumby [SBS MVP]" <not@xxxxxxxxxxx> wrote in message news:e3HMIS7LIHA.4808@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Re: VPN versus Terminal Server for remote workers

Larry, I do not understand what you mean by this statement:

However, this does not really help me understand why the hardware will allow it while the software mobile client will not.

Both hard and soft VPN mechanisms allow split tunneling and though it may not be a standard option in some VPN client software (I think the Cisco client's ability can be hidden or disabled by admin) and IME is common for 'commodity routers' to default to split tunneling, the option is _normally_ there.

"Larry Struckmeyer" <lstruckmeyer(at)mis-wizards(dot)com> wrote in message news:%23SoQvA7LIHA.4308@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

I have always explained it thusly:

If one gets in a small boat and ventures out into a busy waterway, all kinds of bad things can happen. Storms, currents, waterfalls, bigger boats, hi jackers, pirates, and so on.

If one wants to cross the river and gets into a secure tunnel, not much bad will happen.

What I failed to consider is the consequences of allowing some of each at the same time, as explained by SG.

However, this does not really help me understand why the hardware will allow it while the software mobile client will not.

--
Larry

"Claus" <cjobs@xxxxxxxxxxxxxx> wrote in message news:eYCnay2LIHA.4308@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

SG,

I never thought about it from that angle. I see the likelihood of this happening as very slim but you are right, in theory that would be possible.

Re: VPN versus Terminal Server for remote workers

--

Claus

"SuperGumby [SBS MVP]"

<not@xxxxxxxxxxxx> wrote in message

news:eQGrGc2LIHA.5400@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

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

Re: VPN versus Terminal Server for remote workers

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(at)mis-wizards(dot)com>
wrote in
message
news:uAXZvZwLIHA.820@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Claus:

That looks good. I've never understood why some of the

Re: VPN versus Terminal Server for remote workers

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 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@xxxxxxxxxxxxxx>

wrote in
message

news:OAgJ7UwLIHA.2024@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Re: VPN versus Terminal Server for remote workers

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:elhgiLwLIHA.4684@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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

--
Larry

"Claus"

Re: VPN versus Terminal Server for remote workers

<cjobs@xxxxxxxxxxxxxx>

wrote

in

message

news:OyTSsDwLIHA.1212@xxxxxxxxxxxxxxxxxxxxxxxx

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".

Re: VPN versus Terminal Server for remote workers

It
is
very
easy
for
the
user.

--

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

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

Re: VPN versus Terminal Server for remote workers

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

Re: VPN versus Terminal Server for remote workers

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

Re: VPN versus Terminal Server for remote workers

"Kevin
Weilbacher"
<kw@xxxxxxxxxxxxxxxxxxxx>
wrote
in
message
news:E8F65A78-3F6D-453A-8AA

for
10-15
users,
if
you
wanted
to
go
VPN,
then
I
would
say
look
for
a
solid
hardware
box
that
supports
VPN.

as
far
as
using
Term
Server,
the
question
really
is:
does
the
app
that
they
will
be
using

Re: VPN versus Terminal Server for remote workers

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"

Re: VPN versus Terminal Server for remote workers

<OrlandoBob@xxxxxxxxxxxx>
wrote
in
message
news:3907BC27-BE28-40E

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

Re: VPN versus Terminal Server for remote workers

compelling
reasons
to
set
up
a
Terminal
Server.