

## Re: SBS VPN setup?

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-08/msg01912.html>

---

- *From:* "Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <[sbradcpa@xxxxxxxxxxx](mailto:sbradcpa@xxxxxxxxxxx)>
  - *Date:* Wed, 20 Aug 2008 07:19:26 -0700
- 

And I'm reviewing if I need to do client notifications at that point. :-)

Cliff Galiher wrote:

Eh, if you are properly monitoring your firewall (and why own one if you aren't) you can notice the change in traffic to indicate you've been exploited. MRTG, Nagios, etc...

–Cliff

"Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <[sbradcpa@xxxxxxxxxxx](mailto:sbradcpa@xxxxxxxxxxx)> wrote in message [news:%230vNbxoAJHA.4512@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%230vNbxoAJHA.4512@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

And if you have a hardware firewall you haven't flashed in years they just got in through a exploit.

:-)

Cliff Galiher wrote:

The 2-nic configuration is used when the SBS server will \*also\* act as your network's firewall. You purchase 2k3 PREMIUM and that comes with ISA to handle the firewall duties. One Nic is plugged straight into the internet modem (Cable, DSL, etc) and the other into a switch/hub to share the connection with other computers.

My problem is (and this is PERSONAL PREFERENCE HERE, others will disagree I'm sure) that if an exploit is found with ISA...say, for example a buffer overrun that allows code execution...they will be executing code ON YOUR DOMAIN CONTROLLER. Yes, in my opinion, that is very bad.

I prefer SBS 2k3 without ISA. Standard if you don't need SQL for a line-of-business app, premium if you do need SQL, but not use ISA either way. SBS plugs into a switch with the other computers and the switch is plugged into a firewall appliance with 2-nics. The firewall appliance could

Re: SBS VPN setup?

be anything, sonicwall, watchguard, or an MS ISA appliance would do. And the cable modem/DSL/whatever plugs into the other NIC of the firewall. That way all traffic passes through it.

To compare apples to apples, let us assume there is a network setup as I outlined above...and the firewall appliance is an ISA server, such as those available from Celestix. Now...the same exploit would still exist in ISA, so the hacker attacks ISA and is now running code on your firewall. But...the difference is....they've gained access ONLY to your firewall. Yes, it is still very bad, but also still much better than the hacker having the ability to nuke your Active Directory structure, or your exchange server, or the other components of SBS. The worst they will likely do is kill your internet access until you can get your firewall rebuilt and (hopefully) patched.

One could argue that once they have the firewall, they could attack the SBS server, but since SBS wouldn't have ISA, they'd have to find \*another\* exploit to attack it. So you've inherently added a layer of protection. The attacker would be \*REQUIRED\* to find two unrelated exploits to get past an ISA firewall and SBS. If ISA is \*on\* the SBS box (as it would be in a 2-nic configuration) then this is not the case. One exploit, at the perimeter, exposes your entire network.

It should be noted that SBS 2008 will \*NOT\* support 2-nics and will not come with ISA. So MS obviously feels that separating perimeter security from the domain controller is important enough to change the features of one of their major products (sbs.)

So, yes, I recommend 1 instead of 2. If the mobo comes with two, maybe they can be bonded to appear as one (more bandwidth) or one can be disabled...that isn't a big deal. I just don't recommend setting up SBS in the "2-nic configuration" that implies ISA and SBS running as a firewall. Running 1 NIC also means you \*need\* to consider what you'll use as a security defense at the edge, the internet connecting point. Most ISP's modems (cable or DSL) will operate with the third-party hardware out there, so you don't have to stress too much, but you should be considering a business class firewall at your edge.

-Cliff

"tlc\_13200@xxxxxxxxxxxxx"  
<tlc13200hotmailcom@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in message

Re: SBS VPN setup?

news:CFF931E3-B8EF-4E83-BFAB-308E29154617@xxxxxxxxxxxxxxxxxxxx

Cliff-

Are you advising me to only use a single NIC adapter and router/firewall instead of the usual 2 NIC's. Which the mobo might have... being that'll be a Xeon mobo?

I've read using two is smarter, and you are now telling me that one is okay. Now, being a bit confused here on the subject, I had installed SBS 2k3 R2 for a client this past spring, using and installing 2 NIC's but finding that only is really being used at the 1Gbit speeds anyways. I know that security is an issue, and being that you have more input and a experience in the matter, will the 1 NIC do the job, and disable the second if it's on the mobo? I want it as secured as possible, and trouble free.

I've also notice, that a router/hub seems to work hand in hand depending on the ISP's modem, etc. So, just to clarifiy. 1 instead of 2??!?!?

"Cliff Galiher" wrote:

As I said, the consultant thing is just one of m pet peeves. And I tried to be careful and make sure you knew I wasn't targeting you specifically...but wanted you to understand why I give the answers I do. I'll post links to books before I take time to write a 30 step VPN deployment guide in here. It just isn't necessary when someone else has already done it in more detail than I ever could. So...really...don't take it personally.

Re: SBS VPN setup?

With that said, one minor thing I noticed in your latest post:

Please please PLEASE reconsider your server's 2-nic specs. This is really a configuration that is going out of favor (SBS 2k8 won't even support it) and using a domain controller as a gateway device is...in our modern security environment, unwise. It was probalby unwise even when 2k3 shipped...but Microsoft wasn't as security focused back then...but things are far more hostile on the net five years later. A good single nic server behind a good firewall appliance is, IMHO, highly recommended. You'll be happier in the long run and it is more upgradeable as well.

-Cliff

"tlc\_13200@xxxxxxxxxxxxx"

<tlc13200hotmailcom@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote

in message

[news:476DF91D-2D44-4E2F-89AC-DC5C5095ADEE@xxxxxxxxxxxxxxxxxxxxx](mailto:news:476DF91D-2D44-4E2F-89AC-DC5C5095ADEE@xxxxxxxxxxxxxxxxxxxxx)

> Wow guys, thanks!

>

> I got a bit frenzy when I first started this question last night

when > the

> search results popped up the troublesome issues of running

RWW/VPN's on

> SBS

> 2k3 with no bright light at the end of a tunnel.

Everything I read > during

> my

Re: SBS VPN setup?

> search points to trouble  
issues... only one link gave  
me some hope  
but > not  
> the right solution.  
>  
> And no, I am not asking  
for a FREE ride here, just to  
understand  
what I > am  
> getting myself into with  
all of this. I didn't want to  
sound cocky > about  
> asking for FREE help and  
charging the customer for  
the efforts... my  
> reasoning here was to find  
the proper research to  
determine a  
solution > for  
> him. Either paying  
someone else to help me do  
this, or buying the  
> materials  
> as you said "Cliff" to do  
learn it myself.  
>  
> To be honest, after serious  
consideration, being that I  
haven't  
bill > out  
> the  
> server yet, nor have I  
started the configuration for  
my client,  
(only > now  
> getting his cabling done—  
setting up a rack for the  
server, etc) I am  
> doing  
> my research now to  
determine which method  
and stage to take my  
client > to  
> the  
> next level.  
>  
> After serious  
consideration, as I said  
before... I will build out the  
> server, quote the customer

Re: SBS VPN setup?

the third-party solution at  
the moment  
until > I  
> learn and test the RWW  
solution before deploying it.  
Surely he will  
not  
> have  
> an issue at first with using  
GoToMPC for now, being  
that he and one  
> additional person will be  
only ones doing it for at  
least six  
months to > a  
> year.  
>  
> By then, I will have  
installed SBS 2k3 r2 onto a  
new testing server  
in > my  
> office, and run the test of  
setting up a RWW with  
either help or >  
research  
> materials.  
>  
> Joe's lengthy statement  
will have to be re-read  
again for me, there's  
> paragraphs and more  
paragraphs with explanation  
and analyzing the >  
solution.  
> I  
> thank you, Joe.  
>  
> But for now, I will do the  
Citrix solution and learn the  
efforts  
with > the  
> links you gave me above  
Cliff, and Steve. I just want  
my customer  
to > work  
> as  
> he needs too without too  
much down time. To  
configure and install  
RWW > is  
> new

Re: SBS VPN setup?

> to me, and I want to do a  
good job by testing it out,  
reading and >  
making  
> sure  
> I don't make any mistakes.  
Not that I've had any serious  
issues in > the  
> past,  
> but it is a fear that I'd seen  
according to what people  
have posted. > I  
> will  
> be building a server with 2  
NIC cards- anyways, and a  
new router. > I've  
> read  
> people stating CISCO  
routers, maybe a solution...  
either way... I  
will > be  
> testing everything first,  
reading up and discovering  
if I'm doing it  
> right.  
> Being that my customer  
himself (President) and his  
Vice President  
will > be  
> the  
> only one's for at least six  
months doing the VPN in  
thing, figure >  
GoToMyPC  
> is  
> best until I learn and iron  
out the procedures of  
installing and >  
setting  
> up  
> things. I want him to be  
working smoothly for a  
while with that,  
and > then  
> switch over to his RWW  
onto the server.  
>  
> I guess that I was asking  
for it, wasn't I? But, I don't  
want you >  
"Cliff"

Re: SBS VPN setup?

> to  
> think I was taking  
advantage of you, or the  
likes of people who do. >  
Like  
> you  
> said here:  
>  
> "This is a valid concern  
for any consultant, which is  
why I  
presented > my  
> answers in the fashion I  
did. The problem always is,  
if you screw  
up, > it  
> isn't your network, it is  
somebody else's. It actually  
bothers me  
(and I  
> don't mean any offense to  
you, but it is how I feel)  
when a  
> consultant...who  
> is obviously getting  
paid....wants to dive into a  
new project and  
get > free  
> help. Don't get me wrong,  
EVERYBODY gets stuck,  
and and asking for  
help > is  
> not a bad thing. But when  
you AREN'T stuck then it is  
time to buy >  
proper  
> research materials."  
>  
> Not my intention here!!!  
NEVER IN A MILLION  
YEARS!  
>  
> I asked questions about  
finding if a solution exists.  
And doing my  
> research  
> online got me frustrated  
that there is some  
discouragement out  
there in  
> the

Re: SBS VPN setup?

> threads and white papers  
> on the net. I just want to  
> find a solution > that  
> would suit my customer  
> and pay whomever, that can  
> advise to set it  
> up > if  
> it  
> becomes above my head  
> or isn't clear to what I am  
> doing wrong. >

Hopefully,

> the  
> wizards on the RWW and  
> CEICW...

>  
> Therefore, I will copy  
> these threads which were  
> written here, and > save  
> them  
> to review again for later.  
So, hopefully no one here  
see's that I'm > trying

> to  
> take advantage of anyone,  
but simply to discover a  
solution and how  
to > go  
> about it. Until I test and  
deploy it on a server for  
myself... in the  
> meanwhile... my client  
with use the third-party  
solution... unless he  
> likes  
> it over the RWW?

>  
> Thanks!

>  
> "Cliff Galiher" wrote:

>  
>> Inline:

>>  
>> -Cliff

>>  
>>

"tlc\_13200@xxxxxxxxxxxxx"

<tlc13200hotmailcom@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

>> wrote

>> in message >>

[news:DACDFD9F-264B-4DDF-B348-88874ED641C9@xxxxxxxxxxxxxxxxxxxxx](mailto:news:DACDFD9F-264B-4DDF-B348-88874ED641C9@xxxxxxxxxxxxxxxxxxxxx)

Re: SBS VPN setup?

>>> Hi Steve B-  
>>>  
>>> I was just thinking  
about using a software like:  
"GoToMyPC" by >>>  
Citrix,  
>>> and  
>>> the suggestion you  
made sounds interesting  
too... I will surely  
have >>> to  
>>> check  
>>> it out.  
>>>  
>>> Even though the  
suggestion from Apirl and  
Cliff are quite  
helpful to >>> an  
>>> extent... my concern is  
the learning curve of setting  
up a  
VPN/RWW >>> and  
>>> not  
>>> knowing how it will  
turn out.  
>> This is a valid concern  
for any consultant, which is  
why I  
presented >> my  
>> answers in the fashion I  
did. The problem always is,  
if you screw  
up, >> it  
>> isn't your network, it is  
somebody else's. It actually  
bothers me  
(and >> I  
>> don't mean any offense  
to you, but it is how I feel)  
when a  
>> consultant...who  
>> is obviously getting  
paid...wants to dive into a  
new project and >> get  
>> free  
>> help. Don't get me  
wrong, EVERYBODY gets  
stuck, and and asking  
for >> help  
>> is  
>> not a bad thing. But

Re: SBS VPN setup?

when you AREN'T stuck  
then it is time to buy >>  
proper  
>> research materials.  
Maybe it is a book, or  
maybe it is an education  
>> class,  
>> or maybe it is partnering  
with another expert in your  
area and  
sharing  
>> the  
>> work (and the profits) to  
ensure client satisfaction.  
But the  
idea of  
>> charging a client while  
asking for free walkthroughs  
is concerning  
to >> me.  
>> Maybe that's not what  
you are doing...I am  
generalizing here...but I  
>> wanted  
>> to be clear why I answer  
the way I do.  
>>  
>> > Being that I'd read so  
many issues and threads  
>> > on the internet with  
clients having issues of  
setting one up.  
Either >> > a  
>> > port  
>> > not forwarding, or  
another issue as server not  
beening seen on the  
>> > connections.  
>> Yep, and that is usually  
because users dive in. I can't  
stress how  
>> important a test setup is.  
I first got SBS 2k3 in the  
action pack >> in  
>> 2004  
>> (four years ago) so...I  
know you say you haven't  
renewed yet, but >> unless  
>> you  
>> let it expire a LONG  
time ago, you should still

Re: SBS VPN setup?

have SBS 2k3 >> floating  
>> around.  
>>  
>> > My concern is down  
time and problems.  
Although I'd spoken to the  
>> > representative at Citrix  
about their product, it seems  
more >> >  
appealing  
>> > for  
>> > me  
>> > to have my client go  
this route for now, and  
maybe another >> >  
solution  
>> > later,  
>> > or  
>> > simply figuring out the  
RWW as trial and error  
without affecting  
him >> > to  
>> > continue to work!  
(hopefully I can set up a  
RWW/VPN on the  
server >> > and  
>> > not  
>> > affect him to still use  
"GoToMyPC" while doing  
it)?  
>> That is a choice you  
have to make. GoToMyPC  
is another component >>  
that  
>> must  
>> be properly set up,  
secured, and administered. I  
personally see no  
>> benefit  
>> and a few drawbacks.  
But you would get support  
from Citrix, so  
maybe >> it  
>> becomes a wash for you.  
>>  
>> > So, I have two more  
questions.  
>> > Do you really think it  
is easier to set up a RWW in  
SBS 2003 R2 >> > (2008)  
>> > Standard as you claim?

## Re: SBS VPN setup?

>> I would contend it is as easy to setup RWW initially, but maybe not >> 'easier.' There are things to consider at your perimeter and >> decisions >> to >> be made about how tightly you want to lock down RWW. But it \*is\* >> easier >> to >> administer after the fact. Adding new machines, etc...because it is >> all >> integrated with the SBS wizards. >> >> > And using RWW/VPN that is included on SBS, can more than one user >> > access >> > the >> > server at the same time, or not? >> RWW does not connect to the server. It just uses the server to >> connect >> to a >> PC (or multiple PC's) so you could achieve the same net effect. >> Multiple >> users can use RWW at the same time, yes. Native VPN is just another >> network >> connection, so yes again, multiple connections are allowed...but I >> wouldn't >> recommend letting users log onto the server. Shared file access, >> sure. >> But >> if you need users to log onto a machine, whether VPN, RWW, or >>

Re: SBS VPN setup?

GoToMyPC,

>> that

>> machine should \*NOT\*  
be the SBS server. EVER!!!

In that

scenario, >> you

>> should be planning a  
separate TS server

deployment or another

method >> to

>> get

>> employees access to  
local applications.

>>

>> >

>> > I appreciate your  
efforts in answering my  
question regarding this.

>> In your other post, you  
also asked for a book  
recommendation (I  
didn't

>> want

>> to reply twice...just  
seems messy and further  
splinters the  
thread.) >> So,

>> here you go.

>>

>>

[http://www.amazon.com/gp/reader/0735622809/ref=sib\\_dp\\_pt#reader-link](http://www.amazon.com/gp/reader/0735622809/ref=sib_dp_pt#reader-link)

>>

>> Written by Charlie

Russel (a regular here as  
well) and in the  
advanced

>> chapter is a section on  
setting up L2TP/IPSec

VPNs. It gets you

the >> idea

>> of

>> where you'll be going,  
but since it is primarily an  
SBS book, not

a >> VPN

>> book, it may not give  
you the level of detail you  
want if you run

into

>> trouble. For that, I

recommend:

Re: SBS VPN setup?

>>

>>

<http://www.amazon.com/Deploying-Networks-Microsoft-Technical-Referen>

>>

>> Between the two. one to help you see how a VPN fits into your SBS >> design, >> and the other to dig into the inner workings of VPN's in a Microsoft >> environment, you should have all of the resources at your disposal >> to >> make >> an insightful and accurate decision for your client.

>>

>>

>>>

>>> Thanks!

>>>

>>> Dave-

>>>

>>> "SteveB" wrote:

>>>

>>>> As especially April has indicated you should really look at the >>>> wonderful >>>> functionality built in to SBS 2003 (& SBS 2008) which is RWW.

It is

>>>> really

>>>> quite easy to setup and most of the time there is no need for

VPN >>>> at

>>>> all.

>>>> RWW is also quite secure and if you need additional security on top >>>> of

>>>> the

>>>> normal there is a product (AuthAnvil) from Dana Epp, a MS >>>> security

>>>> MVP.

Re: SBS VPN setup?

>>>>

>>>>

"tlc\_13200@xxxxxxxxxxxxx"

>>>>

<tlc13200hotmailcom@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

>>>> wrote

>>>> in message >>>>

[news:43F3E927-1507-41D1-8F80-BECC83046AE3@xxxxxxxxxxxxxxxxxxxxx](mailto:news:43F3E927-1507-41D1-8F80-BECC83046AE3@xxxxxxxxxxxxxxxxxxxxx)

>>>> > Also a question

Cliff/April (Anyone) –

>>>> >

>>>> > The article which I  
found discovered claims that  
it will help >>>> > setup

>>>> > a

>>>> > server

>>>> > as a router, is this  
truly necessary if behind a  
router

already? >>>> > I

>>>> > know

>>>> > it

>>>> > might sound like a  
stupid question, but being I  
have never

done >>>> > this

>>>> > before,

>>>> > I intend to see by  
building a small server test  
to determine

if >>>> > this

>>>> > works

>>>> > efficiently or not?

Like to know if this is a  
good security >>>> >  
measure

>>>> > to

>>>> > work

>>>> > with?

>>>> >

>>>> > Thanks,

>>>> >

>>>> > Dave –