

Re: SBS 2000 and wireless LAN

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-06/msg02680.html>

- *From:* "Rick Dilley" <rdilley@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 9 Jun 2005 09:49:02 -0400
-

Matt/Les,

Well big thank you to you both...I hope I speak for all the silent listeners in this NG.

As I review this thread, it seems to me to be the quintessential NG thread, problem identified, solution(s) offered, response by original questioner...

BRAVO SBS NG...

Rickd

"Les Connor [SBS Community Member – SBS MVP]" <les.connor@xxxxxxxxxxxx> wrote in message [news:OddKF\\$HbFHA.348@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OddKF$HbFHA.348@xxxxxxxxxxxxxxxxxxxxxxxx)

> Great piece, Matt :-).

>

> I'll add one bit, if I may.

>

> The AP devices aren't expensive. I've got a growing number of sites that use

> both of the topologies you've explained, simultaneously.

>

> The reasons for this are the growing number of a) mobile devices – including

> laptops – with wireless connections used by the biz; and b) outside the biz

> (by visitors, etc.)

>

> With the two access points, security on the external AP can be relaxed in

> favor of convenience, and maximized on the internal AP. Even with WPA

> secured internal AP, convenience for laptop users (where laptops are

> same_as_domain workgroup machines, username/passwords are sync'd, Outlook

is

> set up for HTTP/RPC, and off-line folders are in use) is not compromised

at

> all – they can move freely within and without the network.

>

> For not much more than a hundred bucks more, you can have your cake and eat

Re: SBS 2000 and wireless LAN

> it too :-).

>

> I won't mention that I really enjoy having this kind of connectivity when
I

> need to do on-site work ;-). Even with the SBS down, I have that AP on the
> outside so I can check in with y'all and get advice :-).

>

> --

> Les Connor [SBS Community Member – SBS MVP]

> -----

> SBS Rocks !

>

>

> "Matt Gibson" <mattg@xxxxxxxxxxxxxxxx> wrote in message
> news:ujTtwWHbFHA.3684@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

>> Sure thing Rick!

>>

>> Suprisingly enough, securing a wireless access point isn't really that
>> hard. (I'll define the word "secure" later on)

>>

>> There's two main topologies involved in doing this: Wireless users
>> outside, Wireless users inside.

>>

>> The first way (Wireless outside), involves making a back to back DMZ
>> in front of your SBS server. Basically, your networking will look like
>> this:

>>

>> Internet <=> Firewall <=> Access Point <=> SBS <=> Users

>>

>> (Note, this does assume that your SBS is dualhomed – 2 NICs)

>>

>> Wireless users will connect to the access point, and since they're
outside

>> of ISA (or RRAS), they don't really have any foothold into the internal
>> network. They can surf the web, and that's about it. (This setup is
also

>> great if you have visitors that need Wireless access). To access the
>> internal network, the wireless users will VPN in. This lets them be
part

>> of the domain, have access to the entire network, and also serves to
>> doubly encrypt the traffic going over the wireless connection (WPA
first,
>> then VPN second).

>>

>> Personally, this is my favorite way of setting up the network, because
if

>> the access point is "hacked", they do not gain a foothold on the
network.

>> NOTE: It is still possible to perform an ARP spoofing attack, and
>> redirect all network traffic over the wireless link.

>>

Re: SBS 2000 and wireless LAN

>> The second way is what most people normally do, just place a network
>> access point inside the network. While this is easier for the users
>> (since they don't have to VPN), it's also easier for the hackers. If
they
>> manage to gain access to your access point, they'll also gain full
access
>> to your network.
>>
>> Now, those are the two main topologies, but let's look at securing the
>> actual access point.
>>
>> SSID filtering:
>> Utterly Useless. The SSID is shown in plaintext quite often on even
a
>> quiet network, so anyone who's got a wireless scanner will pick up the
>> "hidden" SSID in seconds.
>>
>> MAC filtering:
>> Utterly Useless. Again, MAC address of connecting computers are
>> shown in plain text during normal communication. It's quite simple to
>> change the MAC address of your wireless card so you can "spoof" being a
>> legitimate computer.
>>
>> WEP encryption:
>> Mostly useless. Sadly enough, WEP encryption is easily broken on a
>> somewhat busy network. While it's better than nothing, it should not be
>> used to secure a network with any type of important data.
>>
>> WPA encryption:
>> So far, so good. The only known attack on a WPA encryption system is
>> brute force. So, if you're going to use WPA, make your key BIG, and
>> totally random.
>>
>> So, to recap...don't bother with anything else but WPA encryption.
>> Everything else makes your life a bit harder, and doesn't impact anyone
>> trying to get into your network at all.
>>
>> Let me know if I've skimmed over anything.
>>
>> Hope it helps!
>>
>> Matt Gibson – GSEC
>>
>>
>>
>>
>> "Rick Dille" <rdille@xxxxxxxxxxxxxxxx> wrote in message
>> news:edL6g7GbFHA.2664@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>> Hi Matt,
>>>
>>> And all along I thought I was doing a "good" thing.

Re: SBS 2000 and wireless LAN

◇ *From:* Rick Dilley

◆ **Re: SBS 2000 and wireless LAN**

◇ *From:* Matt Gibson

◆ **Re: SBS 2000 and wireless LAN**

◇ *From:* Rick Dilley

◆ **Re: SBS 2000 and wireless LAN**

◇ *From:* Matt Gibson

◆ **Re: SBS 2000 and wireless LAN**

◇ *From:* Les Connor [SBS Community Member – SBS MVP]

- Prev by Date: **Clarification on mx records**
- Next by Date: **Windows XP Automatic Log-off in SBS 2003 Domain**
- Previous by thread: **Re: SBS 2000 and wireless LAN**
- Next by thread: **POP 3 Connector**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**