

Re: Possible to secure WEP?

Source: <http://newsgroups.derkeiler.com/Archive/Alt/alt.internet.wireless/2006-03/msg00577.html>

- *From:* Jeff Liebermann <jeffl@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 09 Mar 2006 09:33:40 -0800
-

Derek Broughton <news@xxxxxxxxxxxxxxxx> hath wroth:

hmmm. I think "termination=server" might have been sufficient for Mark's question, but this is all good for me :-)

It doesn't have to be a "server". It can be terminated in the router at the other end.

Now, you connect to a remote VPN server (termination). It gives you an additional IP address on its network as 192.168.25.53. Note that this IP cannot be in the same class C IP block as your own LAN.

ding,*ding*,*ding*! How come? That's not what the Talisman help said – it said "not in the DHCP range of your LAN". So my DHCP server is at 192.168.22.1 and gives out addresses in 192.168.22.100–150. I made the PPTP server address 192.168.22.10 and _it's_ assigning addresses in 192.168.22.20–30 range. I guess that's wrong.

Slow down. My explanation wasn't all that clear. Let's try again. Note the "111" and "1" in the 3rd octet below. This is how my office and home networks are setup. To keep it simple, my gateway router, DHCP server, and PPTP terminating server, are all built into the gateway router (WRT54Gv3 with DD-WRT v23).

Remote LAN Class C IP address block: 192.168.111.xxx
Remote LAN router IP address: 192.168.111.1
Remote LAN DHCP IP address pool: 192.168.111.100 -> 150
Remote LAN PPTP IP address pool: 192.168.111.90 -> 99

Local LAN Class C IP address block: 192.168.1.xxx
Local LAN router IP address: 192.168.1.1
Local LAN DHCP IP address pool: 192.168.1.100 -> 150
Local LAN PPTP IP address pool: 192.168.1.90 -> 97 (Optional)

Re: Possible to secure WEP?

WAN (internet) IP's are whatever the ISP delivers and can be anything.

I'm sitting on the Local LAN and the DHCP server gives me an IP address of perhaps 192.168.1.102. The Local LAN gateway is 192.168.1.1. When I run IPCONFIG, I get:

```
Ethernet adapter Local Area Connection:  
Connection-specific DNS Suffix . :  
IP Address. . . . . : 192.168.1.102  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1
```

I now use PPTP to connect (dial) my office WRT54Gv3. After wasting a few minutes trying to remember the password, I now get:

```
Ethernet adapter Local Area Connection:  
Connection-specific DNS Suffix . :  
IP Address. . . . . : 192.168.1.102  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1
```

```
PPP adapter Comix:  
Connection-specific DNS Suffix . :  
IP Address. . . . . : 192.168.111.93  
Subnet Mask . . . . . : 255.255.255.255  
Default Gateway . . . . . : 192.168.111.93
```

With this arrangement, I now have a 2nd IP address for the VPN. All my internet traffic now goes through the VPN tunnel. My Skype connection and GAIM connections immediately complain I'm logged in twice since they're now going through the tunnel at the office and then to the internet. I can surf the web, but it's kinda slow because I'm limited by the outgoing bandwidth of my office DSL connection. If I wanted, I could have unchecked the box buried in somewhere in the PPTP VPN client settings that said "use gateway on remote server". When I hit network neighborhood, I can see all the machines and print servers in my palatial office.

I don't know what the Talisman docs are mumbling about. The warning might be to NOT duplicate the IP address block at both ends. It can be done by carefully not duplicating any IP addresses on either end of the tunnel, but the chances of getting that right is about zero. Some VPN routers (Sonicwall) handle the duplicated class C IP address block problem gracefully. Others (Linksys BEFVP41) don't.

Where it screws up is if the Remote LAN is using the common 192.168.1.xxx and the DHCP server at some hot spot delivers 192.168.1.xxx. When you connect to this VPN, it could easily create an unuseable system with duplicated IP's. It's not too bad if the gateway points to the Remote LAN as all traffic to Local LAN devices, except the wireless router, ceases. That will work. But, if you have

Re: Possible to secure WEP?

Re: Possible to secure WEP?

to still access machines on the Local LAN, then there's a problem. That's why my office LAN is 192.168.111.xxx so that I can VPN from any common network (except 111). The most common complaint is if the Local LAN has a network printer, they complain that they can't print while connected to the VPN.

Even more complications:

1. Note the "optional" 192.168.1.90 -> 97 block at the local router. That's for a symmetrical system, where someone from the Remote LAN, might want to connect to the Local LAN via another tunnel. This is the common way I do router to router VPN's. You can open a tunnel from either direction.
2. Note that there are two IP address "pools". One is for DHCP. The other is for PPTP. They are different and cannot overlap. Users (and brain dead admins) should be warned to not assign fixed IP's in either range. This may have been what the Talisman docs were mumbling.
3. The function of broadcast based services such as DHCP and network browsing depends on how the VPN terminating router handles broadcasts. Many routers just block them as they're really not necessary and contribute substantial useless traffic through the tunnel. However, that means that network browsing will fail. So, you can always use:
Start -> Run -> \\netbios_name_of_windoze_server
or
Start -> Run -> \\ip_address_of_server
to open a remote server, share, or directory. Also works for remote printers.
4. IPSec VPN's are identical except they all multiple layers of authorization, authentication, anti-spoofing, encryption, and protocols. In other words, there are more options to confuse. However, once connected, they operate exactly the same as PPTP.
5. Netscreen routers are nice because it can do both PPTP and IPSec VPN's simultaneously. The remote users use PPTP because its simple. The router to router connections use IPSec, because it's more secure.

--

Jeff Liebermann jeffl@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
150 Felker St #D <http://www.LearnByDestroying.com>
Santa Cruz CA 95060 <http://802.11junk.com>
Skype: JeffLiebermann AE6KS 831-336-2558