

## Re: Security: VPN or RWW

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-04/msg02985.html>

---

- *From:* Joe <joe@xxxxxxxxxxxxxxxx>
  - *Date:* Tue, 22 Apr 2008 20:49:08 +0100
- 

SuperGumby [SBS MVP] wrote:

more to the point the default behaviour of \_most\_ VPN endpoints is to allow all traffic, action must be taken to limit available ports.

\_IF\_ VPN's defaulted to 'OK, you are connected, your admin must now specify what traffic is allowed' it would be better however I expect most DIYers would just open everything anyway.

There is also an inherent flaw in 'port limited VPN', most people would want 'Windows File Sharing' to work, there goes a big hole that many viri use for vector. Oh, and we want Outlook, so let's let RPC through the VPN, 'nother hole. The act of opening \_what we want\_ allows us to be attacked.

Well...yes. You can't have it open and closed at the same time. You either want to use something or you don't. And if you can use it, so can anyone who's remotely controlling your machine. If you really want to logon remotely as you do locally, then you cannot avoid opening access to a wide range of sensitive services.

There's no substitute for keeping machines used for business clean. And machines not used for business, for that matter, though that's much harder. Even if malware doesn't have a handy VPN to reach through, it can still log keystrokes, and phone them home.

Life could be easier with Vista. For all its current problems, it's possible to use it pretty well continuously without logging on as an admin, which I've never been able to do with XP. The trouble is, at the moment there's nothing that requires people to work unprivileged, and there are still writers of 'business' software who require their users to be able to write to system storage areas. Madness. Windows needs to acquire something of the \*nix ethos, where only really green beginners admit to logging on as an admin, and where a software vendor who demanded admin privileges for his users would be laughed out of the market. No matter \*how\* big he was.

The future? File sharing is for kids, it's a legacy of single-user, single-tasking applications on DOS, and has no place in business computing. Likewise peer-to-peer networking, there's no excuse for anyone needing to 'see' another workstation on the network.

Everything that users can write to outside their own private directories ought to be client-server by now. Put the read-only stuff on http for distribution. Build a PowerPoint engine into IIS, if it doesn't have one already.

## Re: Security: VPN or RWW

Anything that absolutely has to be worked on jointly goes onto a versioning database, so there's still no actual sharing.

We've already reached the point where official documents such as invoices are converted to and sent in a display/print format such as PDF, rather than in the somewhat dodgy Office format in which they were created. Though of course Adobe just couldn't resist building in extra 'features' which also turned out to be a bit dodgy...

Get rid of file sharing and the most vulnerable parts of Windows go, FTP goes, VPN has very few niche applications left. When all the network resources are concentrated in the server, either really or virtually, then nobody needs network browsing, nobody needs to have the same 'view' of the network locally and remotely. Whatever kind of encrypted remote link is used, connects from a single application at the remote end, not from the machine as a whole. VPN goes back to its original site-to-site roots, where only reasonably secure, audited networks are connected together.

Again, it's a matter of ethos. Simply drop SMB/CIFS, and people will just email files back and forth, though at least that doesn't open security holes in the network, and pretty much everyone checks email for malware. Drop the built-in VPN, and people will use even less secure third-party stuff. The way of working needs to move on.

Microsoft is certainly working in this direction, though painfully slowly.

.