

Re: Remote Desktop thru VPN and Network Security

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal_services/2005-01/0350.html

From: Robert Moir (robspamtrap+msnews_at_gmail.com)

Date: 01/17/05

Date: Mon, 17 Jan 2005 22:38:23 -0000

TJM wrote:

- > *I want my users to have access to there desktop computers from home.*
- > *For security reasons we currently allow our notebook users access*
- > *through VPN. The current policy is you have to use company equipment*
- > *that is part of our domain. Management now wants everyone to have*
- > *access to there computer from home. The issue with this is that it*
- > *allows users the ability to access corparate data from out of the*
- > *office. What I want to do is limit what they are allowed to do on the*
- > *network after connecting with VPN. I want them to only be able to use*
- > *Remote Desktop to access the network. We don't want them coping files*
- > *to there local systems.*
- > *Is there a way of doing this in the Windows VPN client? What happens*
- > *if the employees home computer has a virus of is not using a*
- > *firewall? What other security issues should I consider doing this.*

You have to understand that by allowing VPN access at all, you are giving up some measure of "security" in exchange for allowing people to work at home. Accepting this, we can go on to think about how to deal with the risks that arise.

I would consider having a separate network for the VPN clients to connect and authenticate to, separated from your main LAN by some kind of firewall/filter that will allow you some control over what passes through. At this choke point you can then restrict the dialled-in VPN users from passing any traffic to/from the local LAN except for your allowed exceptions (terminal services in this case).

This should also mitigate against viruses from an infected home machine attacking your internal corporate LAN, but will do nothing for the fact that your users might be infected with keylogging & password stealing trojans that report everything they type back to the person that infected them – sorry did you say we were dealing with confidential information here? Now you see what I meant when I said that doing this at all means you accept certain risks.

microsoft.public.windows.terminal_services: Re: Remote Desktop thru VPN and Network Security

Firewalling the VPN connections away from your main LAN also isolates what the users can do to a degree, and makes it difficult for them or malware on their machines to do things that you do not like, at least by mistake. But not impossible – if you told me that I couldn't copy documents direct from your server to my home machine, yet allowed me VPN/Terminal Services access via my desktop machine I could steal data from those documents just by opening them and copying and pasting, and you'd never know.

The question is how real is that demand for restricting data flow outside the corporation, and how far do you trust your user community? You might, for example, trust them not to harm your company intentionally, but do you trust them not to save their VPN password on the machine for convenience, inadvertently allowing their inquisitive and troublesome 12 year old kid access to your network (and please lets not pretend the average user's choice of password is much help here).

--
--

Rob Moir

Website - <http://www.robertmoir.co.uk>

Virtual PC 2004 FAQ - <http://www.robertmoir.co.uk/win/VirtualPC2004FAQ.html>

Kazaa - Software update services for your Viruses and Spyware.