

Re: Remote Desktop directly to another computer on the network

Re: Remote Desktop directly to another computer on the network

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.work_remotely/2006-03/msg00118.html

- *From:* "Sooner AI [MVP]" <SoonerAI@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 10 Mar 2006 16:14:23 -0600
-

I also forgot to mention SSL-Explorer. Its easy to setup, only uses one port through a firewall/router (TCP Port 443) and supports RDP natively (to multiple PCs) I might add. It also allows file transfers, tunneling, etc. Its actually quite good...

<http://3sp.com/showSslExplorer.do>

You can use any Java enabled browser AFAIK to connect to the server, etc...ie. basically clientless...

I would use it more but for the life of me I simply can not get a self signed certificate to install correctly so SSL-Explorer will use it...Bummer...:-(

--

AI Jarvi (MS-MVP Windows Networking)

Please post **ALL** questions and replies to the news group for the mutual benefit of all of us...

The MS-MVP Program - <http://mvp.support.microsoft.com>

This posting is provided "AS IS" with no warranties, and confers no rights...

"Sooner AI [MVP]" <SoonerAI@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:...

Another reason I like SSH (or VPN if it floats your boat as they say) is for simple secure file transfers. I generally use a free SFTP client called WinSCP for that to access my home SSH server. No need to even callup RDP just to transfer files. If you have the bucks WebDrive is nice because you can actually map a remote folder through the SSH tunnel. I do that, ie. use WebDrive, with a persistent SSH tunnel to my brothers SSH server. He has a static business class IP/account with his cable ISP. Its great for file transfers, ie. he puts a file in the common folder and I can grab it or vice versa...

The other positive, at least in my mind, with a SSH link is the use of

Re: Remote Desktop directly to another computer on the network

private/public key pairs (I use a 2048-bit RSA key pair) for authentication versus a password (strong or otherwise). The remote party must have the private key that matches the servers public key or the connection is not made period. The keys are further protected by a strong pass phrase. In my setup, and my brothers, password authentication is strictly prohibited and disabled. So the SSH link is encrypted from the get-go and the remote user can only logon to the SSH server with a valid private key and strong pass phrase. I like that...

Anyway, we all have our preferred methods and opinions. The discussion is good...

Later...

--

Al Jarvi (MS-MVP Windows Networking)

Please post *ALL* questions and replies to the news group for the mutual benefit of all of us...

The MS-MVP Program - <http://mvp.support.microsoft.com>

This posting is provided "AS IS" with no warranties, and confers no rights...

"auser" <auser@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:5166A126-6344-4F4C-98F2-5D50CA2A459B@xxxxxxxxxxxxxxxxxxxx>

i am not really disagreeing with you... each has its own advantages.. but when that 486 crashes... you'll think to yourself... maybe multiple ips aren't such a bad idea... lol

"Peter" wrote:

if you are using encryption in rdp 5.1 or higher, you will not be able to view the stream. You would be no more likely to crack the encryption than

you

would be to crack ssl encryption.. or ssh for that matter.

That is exactly my point.

VPN gives you only that advantage, that you do not have to

Re: Remote Desktop directly to another computer on the network

manage your
router forwarding ports, when you add more remote PCs.
And you do not have to remember which PC uses which
port.

But on the other hand, you have to maintain a VPN server, as
you have
pointed it out.
(I actually do it VPN way. My VPN server is running on old
486 Linux PC,
very low maintenance)