

Re: More on Remote Desktop

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2004-10/2507.html

From: Dana Brash (dbrash_at_Phongsaly.com)

Date: 10/18/04

Date: Mon, 18 Oct 2004 21:00:41 +0800

learning learning learning....

cool stuff, that RDP, and a nice improvement over TS in Win2k

I still won't be opening up a port on my firewall for it, but I've already got VPN. ;-)

Thanks for the good info!

--

Dana Brash
MCSE, MCDBA, MCSA
dbrash@gmail.com

"Sooner Al" <SoonerAl@somewhere.net.invalid> wrote in message
news:uZsfthQtEHA.3320@TK2MSFTNGP15.phx.gbl...

>I believe his requirement, at least as I read it is to...

>

>>>> Our needs are to be able to remotely access the desktop to retrieve

>>>> files

>>>> and faxes through the internet.

>

> You can access both remote and local drives/print locally and
> remotely/etc, while in a Remote Desktop session, and subsequently
> cut-n-paste files between the local and remote PCs. The Remote Desktop
> connection simply needs to be configured for that in the Options -> Local
> Resources -> Local Devices configuration window when you open the
> connectoid...

>

> [http://support.microsoft.com/default.aspx?scid=kb;\[LN\];313292](http://support.microsoft.com/default.aspx?scid=kb;[LN];313292)

>

> Yes a VPN will work just fine. I was simply trying to help the original
> poster save a few \$\$\$\$ by using the existing functionality of the OS...and
> to keep it as simple as possible...:-)

>

> If you need to feel a bit safer you can always change the listening port
> on the XP Pro box to something other than the default TCP Port 3389. If
> you do change the listening port then make sure you...

>

> a) reboot the PC after making the registry change and
> b) make the change to the router port forwarding also.

>

> READ THESE TWO KB ARTICLES FIRST...

>

> <http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986>

microsoft.public.windowsxp.network_web: Re: More on Remote Desktop

> <http://support.microsoft.com/default.aspx?scid=kb;EN-US;322756>
>
> Change the Remote Desktop listening port and calling procedure...
>
> <http://support.microsoft.com/default.aspx?scid=kb;en-us;0306759>
> <http://support.microsoft.com/default.aspx?scid=kb;en-us;0304304>
>
> I always recommend that a "strong password" be used...AFAIK, the password
> exchange is encrypted also...You might reference Bill Sanderson's (MS-MVP)
> reply to a similar question...
>
> <http://groups.google.com/groups?hl=en&lr=&c2coff=1&threadm=OOCmqheZDHA.736%40TK2MSFTNGP09.phx.q>
>
> You also might consider changing the default client connection encryption
> level to "High" versus the default "Client compatible" and *ALWAYS* prompt
> for a password.... Note this is done on the XP Pro Remote Desktop host
> machine...
>
> http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/pree_rem_uvnl.asp
>
> --
> 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...
>
> "Dana Brash" <dbrash@Phongsaly.com> wrote in message
> news:emc3ZeMtEHA.220@TK2MSFTNGP15.phx.gbl...
>> Hi Al,
>>
>> I did not know that. That makes it a very different security story.
>> However, a port scan would reveal 3389 open and could invite a brute
>> force attack. Encryption is not authentication, and (particularly if he
>> doesn't use adequately complex passwords) there is still a chance that
>> someone could hack his system.
>>
>> Security aside, he's got the other requirement that he be able to "to
>> retrieve files and faxes". Perhaps I'm taking this too literally to mean
>> "download" and all he really want to do is be able to "view" them. If he
>> doesn't want to download, then Remote Desktop should be fine. If he does
>> want to download, or otherwise run locally on his laptop, then I don't
>> believe there is actually a way to do this using Remote Desktop, though
>> I'd love to know otherwise.
>>
>> Chances are good, though, that he's already got VPN capabilities on his
>> current hardware, so I'm not sure he'd have to get anything new. It just
>> seems like it's pretty commonly included these days. If not, he can get
>> a firewall to do it for \$100. Pretty small investment...
>>
>> I believe this one would meet his needs:
>> <http://www.linksys.com/products/product.asp?grid=33&scid=35&prid=537>
>>
>> Available at Amazon for \$99.99
>> http://www.amazon.com/exec/obidos/tq/detail/-/B00008WM9J/qid=1098071495/sr=8-1/ref=pd_csp_1/00
>>
>>
>> Thanks for the info.
>>
>> --

microsoft.public.windowsxp.network_web: Re: More on Remote Desktop

```
>> Dana Brash
>> MCSE, MCDBA, MCSA
>>
>> dbrash@gmail.com
>>
>> "Sooner Al" <SoonerAl@somewhere.net.invalid> wrote in message
>> news:%23EualkItEHA.3556@TK2MSFTNGP10.phx.gbl...
>>> You realize the Remote Desktop data stream is encrypted the same as a
>>> PPTP VPN link...
>>>
>>> http://msdn.microsoft.com/library/default.asp?url=/library/en-us/termserv/termserv/remote des
>>>
>>> ...so opening one port for Remote Desktop, ie. TCP Port 3389, is not a
>>> big deal...IMHO...
>>>
>>> Unless of course the original poster wants to implement an L2TP/IPSec
>>> VPN server at home...or purchase additional/new hardware...
>>>
>>> --
>>> 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...
>>>
>>> "Dana Brash" <dbrash@Phongsaly.com> wrote in message
>>> news:ucrRsXhtEHA.3052@tk2msftngp13.phx.gbl...
>>>> Basic lowdown: You would use the Router's_public_IP :3389. On the
>>>> router you would create a 'service' (or however your particular piece
>>>> of hardware refers to port mapping) for port 3389 and point it to the
>>>> Static IP of the internal server. But again, I would strongly
>>>> recommend that you use VPN instead as opening this up is a huge
>>>> security hole. If you open port 3389 on your firewall to the world,
>>>> you will almost certainly get hacked. Please, please, please don't do
>>>> it. Secure your communications through a VPN Connection. You shouldn't
>>>> need any rules on your firewall to get between your clients and server
>>>> on your own LAN. You will need something in place to get into your LAN
>>>> from external.
>>>>
>>>> How it works:
>>>> Your DSL or Cable Modem or whatever your using gets a public IP
>>>> address, probably (99.9%) dynamically assigned. On the otherside, when
>>>> you dial up to earthlink, your laptop also gets a public IP. So the
>>>> first step in getting your laptop into that LAN server has got to be
>>>> making these two public IP's talk to each other. But as you're using a
>>>> home network, chances that your public IP is static are very, very
>>>> slim: so you don't know where to point your laptop to connect. You will
>>>> want to follow Al Jarvi's suggestion and go with something like
>>>> http://www.no-ip.com or I use http://www.changeip.com. These services
>>>> will let you map a DNS name to your dynamically assigned Public (Cable
>>>> or DSL) IP address. When you use these services, you no longer have to
>>>> know the IP because they keep a record and you just have to refer to
>>>> the URL. Mine is dana.blahblah.com (not really, but for example's
>>>> sake...) Even if you do decide to open 3389, you'll still want the
>>>> Dynamic IP DNS service so that you can find your network in the first
>>>> place.
>>>>
>>>> Your network must run a client-side service to update the Dynamic IP
>>>> DNS servers directly when your public IP address changes. There are
>>>> several ways to do it. The modem sometimes does it, the
```

microsoft.public.windowsxp.network_web: Re: More on Remote Desktop

```
>>>> router/firewall sometimes does it, or you can install a small client on
>>>> the OS that will do it. The key is, whichever machine holds the public
>>>> IP needs to be making the update (updating the public IP address
>>>> information with an internal IP address isn't going to help you). I
>>>> have mine setup so that my firewall makes the PPPoE connection to my
>>>> ADSL ISP. My firewall can be configured to update ChangeIP.com. So
>>>> when the PPPoE connection on the firewall gets a new public IP,
>>>> ChangeIP knows about it. If I was using ICS or RRAS on my server, I
>>>> would download and run the ChangeIP client on that server.
>>>>
>>>> So, when I want to connect to my internal server, here is how I do it.
>>>> I set up a VPN connection on my firewall, using L2TP and IPsec with a
>>>> pre-shared key. I configure my user there. I then create a VPN
>>>> connection on my laptop. My VPN connection is configured to first open
>>>> my dialup connection. It is then configured to connect to
>>>> dana.blahblah.com AS A URL, and pass it the right username, password,
>>>> and pre-sharedkey. It is also configured to use my LAN DNS servers for
>>>> DNS resolution (so I can reference my internal servers by name). The
>>>> firewall then authenticates and connects me, and gives me A LOCAL IP
>>>> ADDRESS ON MY LAN.
>>>>
>>>> Once I've created the VPN 'tunnel' to my LAN, and gotten my LAN IP
>>>> address, I can connect to resources just as if I'm sitting in my home
>>>> office. Once you have an internal IP, you don't have to worry about
>>>> ports anymore. Everything is dial-up slow now, but I can get there. I
>>>> think this solution will better meet your needs for getting to files
>>>> and faxes and what not anyway. Remote Desktop is not really going to be
>>>> your best option for transferring files (as in it won't do it).
>>>>
>>>> This is not simple stuff. It would be impossible for me to give you
>>>> all the information you need to get this up and running properly
>>>> without you doing other reading. A Google search for "VPN overview"
>>>> returns a bunch of great articles on the general nature of VPN. I
>>>> would suggest looking up the VPN configuration information from your
>>>> router/firewall vendor. If it doesn't perform this service, get a
>>>> Linksys or a Vigor or a Netgear or a DLink or a Cisco or a Netscreen or
>>>> a ...??? that does. Alternately, you can build up an RRAS box on
>>>> Win2k/2003 that can allow VPN, or ISA server will also perform this
>>>> function. Don't be tempted to use your server as the router, get a
>>>> machine (an older one should do) and dedicate it to the task.
>>>>
>>>> HTH,
>>>> =d=
>>>>
>>>> --
>>>> Dana Brash
>>>> MCSE, MCDBA, MCSA
>>>>
>>>> dbrash@gmail.com
>>>>
>>>> "mchjr01" <mchjr01@discussions.microsoft.com> wrote in message
>>>> news:D84E2E22-E96C-451F-AF67-728EC73745B4@microsoft.com...
>>>>> Dana,
>>>>>
>>>>> Thanks for your prompt reply.
>>>>>
>>>>> I have a home network with two laptops, a desktop and two printers.
>>>>> The
>>>>> laptops are wireless and the desktop is wired to a router - sharing
>>>>> the DSL
>>>>> connection as stand alone workstation to access the internet. The
>>>>> desktop is
```

microsoft.public.windowsxp.network_web: Re: More on Remote Desktop

>>>> being used as storage of huge files and as a fax server. So far, I
>>>> configured
>>>> the ip forwarding (desktop ip) on my router through TCP3389 and made
>>>> the
>>>> desktop ip static. On the laptops I made the IPs static as welll.
>>>>
>>>> Our needs are to be able to remotely access the desktop to retrieve
>>>> files
>>>> and faxes through the internet. From my laptop, I configured remote
>>>> desktop
>>>> to connect to as: ipdesktop:3389. When I am connected to my LAN I can
>>>> connect
>>>> with no problem, but when I try to connect via regular dial-up through
>>>> my
>>>> iISP (earthlink.net), I am getting the error messages that either the
>>>> desktop
>>>> is busy or I do not have the permissions to connect. Tell me, to
>>>> connect - do
>>>> I use the routersip:3389 or the desktopip:3389?
>>>>
>>>> Again thanks for your time and you are a valuable resources of
>>>> information -
>>>> keep up the good work.
>>>>
>>>> Mike
>>>>
>>>> "Dana Brash" wrote:
>>>>
>>>>> Hi Mike,
>>>>>
>>>>> A bit more information about your environment would be helpful. Are
>>>>> you in
>>>>> a domain or workgroup? What are you using for a firewall
>>>>> (brand/model)?
>>>>> How are you connected to the internet? Do you have a static public
>>>>> IP?
>>>>> etc...
>>>>>
>>>>> It does sound like you're getting blocked at the firewall, except for
>>>>> one
>>>>> thing. You said:
>>>>>
>>>>> >When I tried to connect via dial up outside of my LAN I am
>>>>> > getting an error message(...)
>>>>>
>>>>> What are you dialing in to? Do you mean that your laptop is making a
>>>>> Dialup
>>>>> connection to the internet, are you dialing in to your
>>>>> firewall/router, do
>>>>> you have RRAS configured internally to accept dial-in connections?
>>>>>
>>>>> If you are simply trying to get to the server via the public IP of
>>>>> the
>>>>> firewall, then you could open up port 3389 and have it point to your
>>>>> internal server, but this would open it up for everyone. Not a great
>>>>> idea.
>>>>> Depending on your firewall, you may be able to create a policy that
>>>>> would
>>>>> allow only your laptop through, particularly if you have a static IP
>>>>> to use.
>>>>> However, since you're a laptop, I assume you move around and stay in
>>>>> hotels

microsoft.public.windowsxp.network_web: Re: More on Remote Desktop

```
>>>>> and get on wireless at the airport and Starbucks and what not, and
>>>>> that
>>>>> you're pretty much not going to have a static IP for your laptop.
>>>>>
>>>>> If you are trying to dial in to an RRAS server, you need to make sure
>>>>> that
>>>>> your user account has dial-in permission enabled. Are you in a
>>>>> Domain? Do
>>>>> this in Active Directory Users and Computers on your user properties.
>>>>> It
>>>>> doesn't sound like you're actually dialing in to an RRAS server, so I
>>>>> won't
>>>>> pursue this idea at this point....
>>>>>
>>>>> So, I would suggest creating a VPN tunnel into your LAN from outside.
>>>>> Then
>>>>> your laptop will make a connection to the internet, and once
>>>>> connected to
>>>>> the internet can open a tunnel through your firewall. Your firewall
>>>>> can
>>>>> then authenticate you, encrypt your packets and let you in to the LAN
>>>>> 'just
>>>>> like' you're sitting on the LAN itself (albeit much, much slower).
>>>>> Many
>>>>> home products these days offer VPN capabilities, as do RRAS, and ISA
>>>>> server
>>>>> as well.
>>>>>
>>>>> HTH
>>>>> =d=
>>>>>
>>>>>
>>>>> --
>>>>> Dana Brash
>>>>> MCSE, MCDBA, MCSA
>>>>>
>>>>> dbrash@gmail.com
>>>>>
>>>>> "mchjr01" <mchjr01@discussions.microsoft.com> wrote in message
>>>>> news:C6FC5687-8050-4D70-B6A5-81F4F3FBD4D2@microsoft.com...
>>>>> > Sorry on bugging you on this remote desktop issue but I really need
>>>>> > to
>>>>> > remotely access my desktop where I store my huge files and use it
>>>>> > as a fax
>>>>> > server.
>>>>> >
>>>>> > This is what I have done so far:
>>>>> >
>>>>> > On the desktop that I would like to access remotely, I changed the
>>>>> > IP to
>>>>> > static. On the router I enabled the virtual server and added the
>>>>> > desktop
>>>>> > static IP to forward through TCP3389.
>>>>> >
>>>>> > When I initiated remote access from my laptop I type: desktop
>>>>> > ip:3389. I
>>>>> > tried it while I am connected on the same LAN network where the
>>>>> > desktop -
>>>>> > I
>>>>> > got through. When I tried to connect via dial up outside of my LAN
>>>>> > I am
>>>>> > getting an error message of either the remote PC is busy or do not
```

microsoft.public.windowsxp.network_web: Re: More on Remote Desktop

```
>>>>> > have
>>>>> > permissions to connect.
>>>>> >
>>>>> > My suspicion is I am being blocked by the router's firewall. Is
>>>>> > there a
>>>>> > way
>>>>> > I can make my laptop's IP static and add the same IP on my router
>>>>> > as
>>>>> > trusted?
>>>>> > Do I assign the static IP just like the way I did it on the
>>>>> > desltop.
>>>>> >
>>>>> > I have SP2 update installed on my XP-Pro.
>>>>> >
>>>>> > Please advice and again many thanks to you.
>>>>> >
>>>>> >
>>>>> > Mike
>>>>>
>>>>>
>>>>>
>>>>
>>>>
>>>
>>>
>>
>>
>
```