

## Re: RDP over SSL question

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal\\_services/2006-07/msg00149.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal_services/2006-07/msg00149.html)

---

- *From:* "Jeff Pitsch" <[jeff@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:jeff@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 7 Jul 2006 14:26:21 -0400
- 

Again, by doing this your exposing your internal network to the Internet. Are you sure your internal network is secure enough to stop people from hacking in? What happens (and it does happen) when someone hacks your server? Are you prepared to have your entire network at their disposal?

Jeff Pitsch  
Microsoft MVP – Terminal Server

Forums not enough?  
Get support from the experts at your business  
<http://jeffpitschconsulting.com>

"Maineiac" <[Maineiac@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Maineiac@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
<news:8134D11C-2083-4A70-96EA-9D17230A05F0@xxxxxxxxxxxxxxxxxxxx>

But everything I'm reading tells me communication is encrypted even though it is coming through the firewall on port 3389. For instance this article tells of the few things that do not get encrypted.  
<http://support.microsoft.com/default.aspx?scid=kb:en-us:275727&FR=1&PA=1&SD=HSCH>  
So after reading this article it sounds like as long as you are up on SP's and patches then the only data not encrypted is the Initial Connection and the Server Certificate. And it states in that article that those contain non-sensitive information.

Could you be mistaken or am I just not reading things properly?

Thank you and I appreciate your help.

"Cláudio Rodrigues" wrote:

Simply because this is not exactly RDP over SSL. The first paragraph of the article you pointed is clear:

"Windows 2003 Service Pack 1 included a new feature, RDP over SSL. This

Re: RDP over SSL question

feature will allow you to use TLS authentication and encryption with your RDP connections using SelfSSL to create the SSL certificate. It still uses RDP and TCP port 3389 so your firewall rules should not need to be modified."

"It still uses RDP and TCP port 3389"

This is for authentication purposes only (and for encrypting RDP). But the old RDP is still running on port TCP 3389.

If you need real RDP over HTTPS (so it can traverse firewalls, HTTPS proxies, etc) you need, as of today, something like the 2X LoadBalancer (<http://www.2x.com>). Or another product called RDP Tunnel or something like that.

--

Cláudio Rodrigues

Microsoft MVP

Windows Server – Terminal Services

"Maineiac" <Maineiac@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:3F74154C-2DC4-40B4-A78E-3EEC3922BBBE@xxxxxxxxxxxxxxxxxxxx>

I've found sites that explain how to do this and have gotten it working

internally as well. One site for example is here

<http://thelazyadmin.com/index.php?/archives/204-Configure-RDP-over-SSL-with-SelfSSL>

A couple questions though:

1. Why do I keep reading in the newsgroups here that it is not offered because it is my understanding this came out with 2003 SP1?
2. Now that I have it working internally on a test TS is it safe to open it on our firewall so employees can work from home? The TS is requiring SSL connections.

Re: RDP over SSL question