

Re: RDP Printing by station

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal_services/2006-12/msg00598.html

- *From:* "flippergonzo" <flippergonzo@xxxxxxxx>
 - *Date:* 14 Dec 2006 16:09:46 -0800
-

Hey TP;

thank you VERY much for your reply. This makes more sense to me now, and I think I understand my options a little better.

You are definitely correct, all types of printing would have to be disallowed. The good thing though is that any stations that are flagged as non-printing stations can not print for ANY users.

The other good thing is that each user connects to an app/database that is specific to their environment. For instance, we might have an app server hosting 5 instances of the same app with each pointing to a different database. This way a user connecting from a static IP address to an RDP session will be connecting to their own database and app. This way the IP address of 192.168.1.100 (very common) would in theory be unique to that environment. Machine name might work even better because we can also control that and it's less likely to be non-unique in the case of home users behind a dsl router.

This is ok for disconnected sessions because we would make sure that the app checks to see that it's allowed to print at print time rather than at startup. This way if we disconnect and reconnect at another station, we're still ok.

One other solution that I was thinking about is messing around with multiple NIC's on the terminal server. This way we can say if the app/database (separate server) sees the connection coming from NIC1 on the term server then it's allowed to print and if it's NIC2, then it's not. I'd then just have to ensure that the client stations that are not allowed to print all connect to NIC2 and this i can handle easy enough via DNS. The only thing I'd question there is if you connect to a term server on it's #1 NIC that all subsequent traffic for that session is limited to NIC # 1. If not then this solution would not work or we'd have to look at multiple term servers...which is an option.

I hope this all makes sense...

Re: RDP Printing by station

Thanks again for your response, you've been incredibly helpful.

On Dec 14, 1:12 pm, "TP" <tperson.knowsp...@xxxxxxxxxxxxxxxxxxx> wrote:

1.) My thought behind static ips was that you could use multiple TS listeners on the same ip. For example, port 3389 would have print redirection enabled, whereas port 3390 would have print redirection disabled. Using IPSec, we could define which ip addresses were permitted to connect to each listener. In that way, we could control which stations were allowed to print, and which were not—without any modifications to your software.

I am not sure this is a possible solution anymore, because you said that there would be printing to not only redirected printers but network printers as well. Redirected printers would not appear [when connecting from a disallowed machine], but the network printers would still be there. You could still disable printing in your application if they were connected via the "printing disabled" listener.

Also, what if there are several machines behind a NAT and some allow printing whereas some do not? In this case all machines would have the same public ip so IPSec would treat them the same.

The other concern I have is if you need printing to be disabled on a particular station for one user, but for another user they should be able to print from the same station. In this case the above ipsec solution would not work.

You can obtain the client name and ip address using WTSQuerySessionInformation. Keep in mind that the ip address is the client's *local* ip address, which may not be the real ip address if they are behind a NAT device. For example, on a TS server with 100 users connected from various different offices, there may be several of them that have ip address 192.168.1.100.

You need to account for session disconnects/reconnects. In this case, the user could originally connect from an ip that is permitted, disconnect their session, and reconnect from an ip that is not permitted. If your software only checks permissions at startup, it would still think they can print. This is easily solvable as well by changing timeout settings, handling the disconnect/reconnect events, etc.

2.) Virtual channels run within each TS session. The traffic is encrypted along with the other TS traffic. Basically they are a way that you can use for a program on the local PC to send/receive data to/from a program running in the user's

Re: RDP Printing by station

session on the server. For example, in your case you may create a VC named Jefchn1. Your client software would use this channel to send the local MAC address to your server software.

Terminal Services Virtual Channels

<http://msdn2.microsoft.com/en-gb/library/aa383509.aspx>

Scriptable Virtual Channels (easier than above)

<http://msdn2.microsoft.com/en-gb/library/aa383253.aspx>

-TP

flippergonzo wrote:

Hey TP;

yes, that assumption is correct, my apologies for not being clearer about that. Some stations can print, others can not. Additionally, some users can print and others can not. Basically, the most restrictive of the combo 'wins' and the user can either print or not print. IP addresses will more often than not be dynamic addresses.

1) It's "possible" that we could force all non-printing computers to use a static address. That and/or the clientname could be used in much the same way as I'd thought about for the MAC address. Is it possible to obtain either the client name or ip address (ip address would work better, but I'll have to go over the ramifications of both) from within the session through an API call?

2) I'll have to do some research into the Virtual Channel option. You kind lost me there... I'm guessing here, but are you referring to something similar to a VPN tunnel where if a TS client session authenticates to a 3rd party software then this virtual session is created and you can print through it?

Using option 1 and writing the requirement for a static IP and/or clientname for printing machines as part of the contract when a client buys the software sounds easier!

Re: RDP Printing by station

Cheers, Jef