

## Re: IAS / RRAS

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2005-01/0591.html>

---

**From:** Steven L Umbach (*n9rou\_at\_nospam-comcast.net*)

**Date:** 01/22/05

Date: Fri, 21 Jan 2005 19:50:28 -0600

Sorry for the delay, due to inclement weather and my cable company's level of customer service I was offline since Monday.

Yes you need a computer certificate on both the VPN and/or IAS server and the VPN client computer for l2tp. You can request one via Web Enrollment as you suggest for your VPN client but be sure to request the offline ipsec certificate. You will have to configure your CA to use that template first in the CA mmc console. Then be sure to select to store the certificate in the computer store. You will also need to verify that the CA's certificate is in the VPN client's trusted root store via certificates mmc snapin for computer. That can easily be exported to a .cer file and imported to other computers or also requested via Web Enrollment --- Steve

<http://support.microsoft.com/default.aspx?scid=kb:en-us:323342> -- this may help

"Jordan Samulaitis" <jordan@jvsDELETEnetworks.com> wrote in message news:uF11FXN\$EHA.2568@TK2MSFTNGP10.phx.gbl...

> *I am assuming I have certificate services installed on my workstation, ive  
> been using this one for a while..*

>

> *So you are basically saying*

>

> *Enable Routing and Remote access.*

> *Configure a VPN thru the wizard*

> *Configure the DHCP Relay Agent*

> *Install Certificate services*

> *goto <http://server/certsrv> on the workstation*

> *and click auto enroll?*

> *Configure the VPN connectoid and set it for l2tp connections?*

>

> *if that is the case I have done that and still was unsuccessful.*

>

> *Regards,*

> *Jordna*

>

> *"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message*

> news:%233aVvUG\$EHA.3368@TK2MSFTNGP10.phx.gbl...  
>> What do you mean it can not see the domain – through a VPN connection or  
>> otherwise??  
>>  
>> You do not have to use IAS. It is convenient if you have multiple rras  
>> servers in that you can configure Remote Access Policies on just the IAS  
>> server. So you may want to try to do without the IAS server until  
>> problems  
>> are resolved to rule it out as a problem.As far as certificates, you may  
>> first want to test with preshared key assuming you have an XP VPN client.  
>> When you install certificates, you need to install computer certificates  
> on  
>> both the VPN client and VPN server. If IAS will be used, then the IAS  
> server  
>> will need a computer certificate [or IAS/RAS certificate] or pre shared  
> key  
>> if used [recommended for testing ONLY]. Keep in mind that since L2TP uses  
>> ipsec that it will not work over a NAT connection unless you have the  
> NAT-T  
>> client installed on the VPN client. Also any firewalls have to allow L2TP  
>> traffic that uses different ports/protocols that pptp such as 1701 UDP,  
> 500  
>> UDP, and 4500 UDP [NAT-T]. Also protocol 50 for ESP needs to be allowed.  
> The  
>> link below also explains the new behavior for NAT-T in Windows XP Service  
>> Pack 2 which may need a registry mod to get it to work. --- Steve  
>>  
>> <http://support.microsoft.com/default.aspx?scid=kb;en-us:885407>  
>>  
>> "Jordan Samulaitis" <jordan@jvsDELETEnetworks.com> wrote in message  
>> news:%23ffXDIF\$EHA.2076@TK2MSFTNGP15.phx.gbl...  
>> > Hello everyone,  
>> >  
>> > I am currently testing VPN connectivity.  
>> >  
>> > This is my current test lab.  
>> >  
>> > – 1 Windows server 2003 standard edition with 1 network card  
>> > – Services – DNS/DHCP/IIS/RRAS/IAS all on the one server.  
>> > – 1 Windows XP workstation with 1 network card  
>> >  
>> > What I did first was setup RRAS and DHCP Relay agent. created a  
>> > VPNUser  
>> > account, and successfully logged on via PPTP. All fine and dandy.  
>> >  
>> > When it came down to try L2TP, I knew I had to install IAS and  
> certificate  
>> > services in order for the server to give out certificates and to have a  
>> > centralized logon, I authorized IAS into active directory and so on.  
> what  
>> > seems to happen is whenever I install IAS and start the service, when I

>> > *reboot my workstation it does not see the server nor the domain, even*  
> *when*  
>> > *I*  
>> > *try to ping the ip address it says timed out. Any reason for this? I*  
> *know*  
>> > *on the MS website in the VPN lab, they were using four servers, one for*  
>> > *IIS,*  
>> > *IAS, RRAS, DNS, DHCP.*  
>> >  
>> > *Is it because I have only one network card??? What could be my*  
> *problems?*  
>> > *Can I still setup L2TP connections without IAS ??*  
>> >  
>> > *Thanks in advance,*  
>> >  
>> > *Jordan*  
>> >  
>> >  
>>  
>>  
>  
>